وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح–ورقلة–

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر في الحقوق

تخصص : قانون جنائي و علوم جنائية

مذكرة بعنوان:

جرائم تقنية المعلومات في ظل الاتفاقية العربية 2010

وفي التشريع الجزائري

إعداد الطلبة:

حمبلي عمار

عثماني دليلة

إشراف الأستاذ:

أ.د خويلدي السعيد

أعضاء لجنة المناقشة:

لقب واسم الاستاذ	الرتبة العلمية	الجامعة	الصفة
د/ عبايدي دلال	أستاذة محاضرة "أ"	جامعة ورقلة	رئيسا
أ.د/ خويلدي السعيد	أستاذ التعليم العالي	جامعة ورقلة	مشرفا و مقررا
أ/ بن عمر ياسين	أستاذ محاضر "ب"	جامعة ورقلة	مناقشا

السنة الجامعية : 2022/2021

بسم الله الرحمن الرحيم

قال الله تعالى:

﴿يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات﴾

سورة المجادلة / الأية: 11.

شكر وعرفان

قال رسول الله عليه أفضل الصلاة وأزكى السلام: "من صنع إليكم معروفا فكافئوه فإن لم تجدو ما تكافئوه فادعوا له حتى تروا أنكم قد كافأتموه" صدق رسول الله عليه الصلاة والسلام.

لا يسعنا في هذا المقام إلا أن نتوجه بالشكر أولاً وقبل كل شيء إلى المولى عز وجل على توفيقه لنا في إتمام هذا العمل المتواضع.

كما يسرنا أن نتقدم بوافر الشكر والتقدير إلى الأستاذ الدكتور المشرف " خويلدي السعيد" الذي تفضل علينا بتوجيهاته ونصائحه القيمة التي أنارنا بها في سبيل إنجاز هذا العمل.

كما لا يفوتنا أن نخلص بالشكر إلى أعضاء لجنة المناقشة على ما سوف يقدمونه من توجيهات وتوصيات يكون لها الأثر في تصويب هذه المذكرة.

كما نتوجه بالتحية والشكر إلى كافة أساتذة كلية الحقوق والعلوم السياسية لجامعة قاصدي مرباح بورقلة، وكل طاقمها الإداري، إلى جميع زملائنا في الدراسة وكل من قدم لنا يد المساعدة من قريب أو بعيد إلى كل هؤلاء شكراً.

إهداء

اهدي ثمرة هذا العمل إلى:

والدي رحمه الله... طيب الله ثراه.

أمي الغالية رحمة الله عليها... طيب الله ثراها.

زوجتي وأبنائي الأفاضل... أدامهم الله ذخراً لي.

إخوتي... رعاهم الله دوماً.

رفقاء دربي وزملائي بكلية الحقوق ورقلة وفقهم الله دوماً.

إهــداء

أحمد الله عزوجل أن وفقني لإتمام هذا البحث بغير حول

مني ولا قوة، فلله الحمد والمنة

إلى روح والدي الطاهرة، تغمده الله برحمته الواسعة

وأسكنه فسيح جناته، وجعل قبره روضة من رياض الجنة..

إلى رمز الكفاح والتضحية...أمي الكريمة حفظها الله وأرضاها عني في الدنيا والآخرة.

إلى زوجي العزيز حفظه الله ورعاه. إلى فلذة كبدي أبنائي أنار الله دربهم

إلى إخوتي فتح الله لهم أبواب الخير

إلى كل مكافح يسعى جاهدا لتثبيت دعائم العدالة

إلى كل مخلص يسعى لتبني آلية جديدة لمكافحة الجريمة المستحدثة

إلى كل طلاب العلم أينما وجدو أهدي عملي هذا♡

المقدمة

المقدمة:

لا غرو في أن الواقع المعاش يعرف تسارعاً غير مسبوق في أنظمة ومسار التطور العلمي والتكنولوجي، ما أدى إلى ثورة تكنولوجية ومعلوماتية وإعلامية في مختلف مجالات الحياة الخاصة والعامة في ظل ما أصبح يختزل في مسمى البيئة الرقمية أو بيئة المعلوماتية.

وبقدر ما أصبحت تمثله هذه البيئة الجديدة من ضرورة حتمية للنشاط الانساني الفردي وشبكة العلاقات الاجتماعية الخاصة بين الأفراد أو بينهم وبين مؤسسات الدولة تحت طائلة الحكومة الالكترونية وما يمكن أن تسفر عنه هذه الأخيرة من تقديم وتوصيل الخدمات ذات الطابع الشخصي أو المعرفي أو الإداري في أسرع وقت وأقل تكلفة وأيسر الطرق، وبدقة عالية إلا أن ذلك رافقه انحراف في التعامل مع معطيات الأنظمة المعلوماتية على مختلف أنواعها، فأصبحت مجالاً مفتوحاً لتنامي التهديدات والانتهاكات الناتجة عن استغلال الوسائط المعلوماتية في مجالات الحياة المختلفة على نحو ما يضر بالمصالح الخاصة للأفراد. كانتهاك سرية الحياة الخاصة، أو سرقة الحسابات الالكترونية، أوحتى المصالح العامة لمؤسسات الدولة كتزوير البيانات والمعطيات المعلوماتية أو أعمال التجسس والتحويل.

وإذا كان تطور جرائم تقنية المعلومات مرتبط بالتطور التاريخي لتقنية المعلومات، منذ بدايتها الأولى المتعلقة بالحوسبة، وتقنية الاتصال، وتقاربهما واندماجهما وتطورهما فإنه يجب على القانون الجنائي مواكبة هذه التطورات التكنولوجية التي تتيح الفرصة الملائمة والواسعة لإساءة استخدام إمكانيات الفضاء المعلوماتي، وأن يعمل على ردع الأفعال الإجرامية.

والاتفاقية العربية تهدف إلى رفع هذا التحدي ومواجهة ظاهرة الإجرام المعلوماتي حيث تعتبر من الاتفاقيات العربية الحديثة في مجال مكافحة جرائم تقنية المعلومات، وكانت الجزائر من بين الدول الموقعة والمصادقة عليها ومن ثم أصبحت هذه الاتفاقية تحتل مكانة سامية بعد الدستور في التشريع الداخلي.

وعليه جاءت هذه الاتفاقية كإضافة للمنظومة التشريعية الخاصة بمكافحة جرائم المعلومات حيث نصت على أحكام موضوعية وإجرائية وأحكام متعلقة بقواعد التعاون القانوني والقضائي الدولي الغرض منها مكافحة جرائم تقنية المعلومات مكافحة فعالة.

إن الدراسة المقارنة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات بينها وبين ما ذهب إليه المشرع الجزائري، كل ذلك لعله يساهم في الاستفادة من تبادل المعرفة و الوقوف عند مواطن الضعف والقوة في كل منها بهدف الاستفادة أو العمل على تعديلها أو سد الفراغ الموجود فيها.

أهمية الدراسة:

تكمن أهمية الدراسة في هذا الموضوع فيما يلي:

- ✓ الدور الذي تؤديه تقنية المعلومات في مختلف نواحي الحياة.
- ✓ البحث في هذا الميدان لابد أن يكون مستمرا حتى نواكب تطور تقنية المعلومات وما ينجر عنها من جرائم.
- ✓ عدم كفاية النصوص التقليدية في مكافحة مثل هذه الجرائم.
- ✓ توفر مثل هذه البحوث للباحثين في مجال القانون الجنائي جانب من المعرفة بأحدث ما تم إصداره من مواثيق إقليمية وعربية وصكوك، وتشريعات ونظم الدول العربية بشأن جرائم تقنية المعلومات.

إشكالية البحث: ما مدى مسايرة المشرع الجزائري في إيجاد قوانين تتماشى مع المبادئ التي جاءت بها الاتفاقية العربية 2010.

أهداف الدراسة:

- ✓ تسليط الضوء على ظاهرة الإجرام التقني باعتباره ظاهرة مستحدثة.
- ✓ بيان ومعرفة الأحكام الموضوعية التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

- ✓ التعرف على آليات التعاون الدولي التي تضمنتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ومدى فاعليتها للتصدي والحد من أخطار جرائم تقنية المعلومات.

أسباب اختيار الموضوع:

- ✓ الرغبة في خوض غمار موضوع يجمع بين ما هو تقني، وما هو قانوني.
- ✓ الانتشار الواسع لجرائم تقنية المعلومات وضرورة التصدي لها خاصة بعد ما أصبحت تقنية المعلومات محركة لجميع نواحي الحياة وشتى المجالات خاصة بعد انطلاق مشروع الحكومة الالكترونية في الجزائر، وعملية رقمنة سجلات الحالة المدنية وتسجيلات التلاميذ في المدارس والثانويات والجامعات مما يستوجب توفير الحماية الجزائية لهذه الأنظمة الخاصة بهذه العمليات، إضافة إلى الانطلاق في نظام التوقيع الالكتروني وعمليات التجارة الالكترونية.

منهج الدراسة:

لقد اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي وذلك ما يستوفيه البحث في النصوص القانونية وذلك لوصف وتحليل الجرائم التي تتضمنها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وما ذهب اليه المشرع الجزائري.

التقسيم المنهجي للدراسة:

ولتحقيق أهداف هذا البحث تمت دراسة الموضوع وفق خطة مقسمة إلى فصلين:

الفصل الأول: الإطار المفاهيمي لجرائم تقنية المعلومات في الاتفاقية والعربية 2010

ومقسم إلى مبحثين:

المبحث الأول: مفهوم تقنية المعلومات

المبحث الثاني: مفهوم الاتفاقية العربية وخصائصها وسمات الجريمة المعلوماتية

الفصل الثاني: التطور القانوني لجرائم تقنية المعلومات في الاتفاقية العربية 2010 والتشريع الجزائري

وهم مقسم إلى مبحثين:

المبحث الأول: صور جرائم تقنية المعلومات في الاتفاقية العربية 2010 والتشريع الداخلي

المبحث الثاني: الجرائم المستجدة في الاتفاقية العربية ومسايرتها مع التشريع الجزائري

الفصل الأول: الإطار المفاهيمي لجرائم تقنية المعلومات في الاتفاقية العربية 2010.

تمهيد

يعد البحث المستمر في موضوع جرائم تقنية المعلومات، ذو أهمية بالغة في الوقت الراهن نظراً للتطور المستمر والدائم لتقنية المعلومات وعدم كفاية النصوص التقليدية في مكافحة هذا النوع من الجرائم، الأمر الذي استدعى إلى استحداث ما تم إصداره من مواثيق إقليمية، عربية، وصكوك، وتشريعات، ونظم الدول العربية المتعلقة بجرائم تقنية المعلومات، ومن بينها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010. لذلك سنخصص دراسة هذا الفصل من خلال مبحثين، نتناول فيهما؛ مفهوم تقنية المعلومات ومكوناتها والتعريف بها وبوسائلها التقنية (المبحث الأول)، ثم التعريف بالاتفاقية العربية وخصائص وسمات الجريمة المعلوماتية (المبحث الثاني).

المبحث الأول: مفهوم تقنية المعلومات

المطلب الأول: تعريف تقنية المعلومات

أدى الاندماج بين فرع تقنية الحوسبة، وفرع تقنية الاتصال إلى ظهور فرع جديد تقني اصطلح عليه: تقنية المعلومات وهذا المصطلح مركب من كلمتين وهما لفظ: تقنية، ولفظ: المعلومات،

الفرع الأول: المقصود بالتقنية

الفرع الثاني: المقصود بالمعلومات

الفرع الثالث: تعريف تقنية المعلومات

الفرع الأول: المقصود بالتقنية

لتحديد المقصود بمصطلح التقنية، فإن الأمر يقتضي التطرق إلى تعريف التقنية لغة أولاً واصطلاحا ثانياً.

أولاً تعريف التقنية لغةً: كلمة تقنية هي تعريب لكلمة « technology » أو تكنولوجيا الإنجليزية والتي تقابلها في الفرنسية « technologie »، وهو من أصل الكلمة الإغريقية القديمة « technologas » اللمركبة من شقين الأول منه هو « techno » ويعني أو يشير إلى الصنعة أو الفن أو المهارة1. ونتاج البحوث، والذي يستخدم لتوفير كل ما هو ضروري لمعيشة الناس. والتقنية استخدمت في العصر الحديث بعد ظهور الثورة الصناعية للدلالة على مصطلح عام يشير إلى استخدام التقنية استخداماً أمثل في مختلف مجالات العلم والمعرفة من خلال معرفتها وتطبيقها وتطويعها لخدمة الإنسان ورفاهيته2. مكا تعنى أيضا التطبيق العملي للاكتشافات والاختراعات المختلفة التي جاءت نتيجة للبحث العلمي، فهي عبارة عن تحويل النظريات والقوانين العامة العلمية إلى أساليب وتطبيقات خاصة في مختلف أوجه النشاط الاقتصادي والاجتماعي، فهي إذن تحويل خلاصة البحوث المبتكرة العلمية إلى ابتكارات علمية في ميادين الحياة المختلفة3.

كما تعني التطبيق العملي للاكتشافات والاختراعات المختلفة4.

ثانيا تعريف التقنية اصطلاحا: تشير كلمة تقنية كمصطلح إلى العلم التطبيقي ووسائله الفنية الذي يهتم بتطبيق النظريات ونتائج البحوث والذي يستخدم لتوفير كل ما هو ضروري لمعيشة الناس5

ويتضح من خلال التعاريف السابقة أن التقنية هي التطبيق العملي للعلم والنظريات بهدف الحصول على نتائج تساعد على تسهيل وتطوير الحياة من كل النواحي لتوفير الوقت والجهد.

---

[1] عبد الغفور عبد الفتاح قاري، معجم المصطلحات، المكتبة والمعلومات إنجليزي – عربي، مكتبة الملك الوطنية، الرياض، 2000، صفحة 279.

[2] محمود علم الدين، تكنولوجيا المعلومات وصناعة اتصال جماهيري، العربي للنشر والتوزيع، 3 ط، 1990، صفحة 203.

[3] محمود علم الدين، تكنولوجيا المعلومات وصناعة الإتصال الجماهيري، العربي للنشر والتوزيع، 1990، صفحة 16-17.

[4] المرجع نفسه، صفحة 205.

[5] فيصل هاشم شمس الدين، تقنية المعلومات (ووسائل الإتصال، التةظيف، الثقافة)، الطبعة الأولى، شمس للنشر والتوزيع، القاهرة، 2008، صفحة 12.

الفرع الثاني: معنى المعلومات

أولاً تعريف المعلومات لغةً: المعلومات جمع والمفرد معلومة والمعلومة مشتقة من مادة علم ودلالتها فيها تدور بوجه عام حول المعرفة التي يمكن نقلها واكتسابها[1]، والمعلومات أخبار وتحقيقات أو كل ما يؤدي إلى كشف الحقائق وإيضاح الأمور واتخاذ القرار.

وتعرف المعلومات بصفة عامة على أنها مجموعة الرموز والحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال أو للتأويل والتفسير والمعالجة سواء بواسطة الأفراد، أو الأنظمة الإلكترونية بحيث يمكن جمعها وتجزئتها أو تغييرها وهي تتميز بالمرونة مما يتيح نقلها بوسائل وأشكال مختلفة[2].

الفرع الثالث: تعريف تقنية المعلومات

هناك من يعرف تقنية المعلومات على أنها الحصول على المعلومات الصوتية والمصورة والرقمية والتي في نص مدون، وتجهيزها واختزالها، وبثها وذلك باستخدام توليفة من المعدات الميكرو إلكترونية الحاسبة والاتصالية عن بعد، في حين يرى آخر بأنها البحث عن أفضل الوسائل لتسهيل الحصول على المعلومات وتبادلها وجعلها متاحة لطالبها بسرعة وفعالية[3]، وبناءاً عليه فإن تقنية المعلومات لها جوانب ثلاث يمكن التمييز بينها، الجانب الأول هو تقنية تسجيل البيانات، والجانب الثاني هو تقنية تحليل البيانات، ثم الجانب الثالث وهو تقنية توصيل البيانات وفي تطور هذه الجوانب الثلاث مرت هذه العملية بأربعة مراحل هي: مرحلة الوسائل وهي مرحلة تعكس التطور التقني الإنساني العام، المرحلة الثانية وهي مرحلة الوسائل الميكانيكية ثم مرحلة الوسائل الإلكتروميكانيكية، فالمرحلة الرابعة هي مرحلة الوسائل الإلكترونية [4].

---

[1] هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، القاهرة، 1995، صفحة 41.
[2] نقلاً عن طارق الدسوقي، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، صفحة 38.
[3] محمود علم الدين، المرجع السابق، صفحة 38.
[4] محمود علم الدين، المرجع السابق، صفحة 39.

المطلب الثاني: مفهوم جرائم تقنية المعلومات

تعد جرائم تقنية المعلومات جرائم مستحدثة في المجال الجنائي مقارنة بالجرائم التقليدية الأخرى، وأسوة بالجرائم المستحدثة حاول الفقه إيجاد مصطلح موحد لمفهومها حيث كانت هناك عدة اتجاهات في تعريفها، كما أن هذه الجرائم لها طبيعة خاصة ومجموعة من الخصائص والسمات تميزها عن غيرها من الجرائم التقليدية وهو ما سوف نتطرق إله من خلال الفروع التالية:

الفرع الأول: تعريف جرائم تقنية المعلومات

تعد ظاهرة جرائم تقنية المعلومات من الظواهر المستحدثة في المجال الجنائي مقارنة بالجرائم التقليدية حيث يقتضي التعريف بها معرفة جذورها التاريخية التي مرت بها عبر تطورها، وكذلك تحديد المصطلحات الدالة عليها كظاهرة إجرامية مستحدثة من أجل الوصول لتعريف مقبول لتوصيف هذه الظاهرة. وهو ما سنتطرق له في هذا الفرع من خلال: التطور التاريخي لجرائم تقنية المعلومات (أولاً)، المصطلحات المستخدمة للدلالة على ظاهرة جرائم تقنية المعلومات (ثانياً)، المقصود بجرائم تقنية المعلومات (ثالثاً).

أولا/ التطور التاريخي لجرائم تقنية المعلومات:

ارتبط تطور جرائم تقنية المعلومات بالتطور التاريخي لتقنية المعلومات، منذ بدايتها الأولى المتعلقة بتقنية الحوسبة وتقنية الاتصال وحتي تقاربهما واندماجهما وتطورهما. البداية الأولى لظاهرة جرائم تقنية المعلومات كانت في نهاية الخمسينيات من القرن العشرين، هذا ما أشارت إليه الدراسات البحثية الأكاديمية، لكن ضمن ما أصطلح عليه إساءة استخدام الحاسوب، المؤسس على البعد الأخلاقي، وفي عقد الستينات تناولت وسائل الاعلام أنشطة إساءة استخدام الحاسوب بشكل واسع، حتي وصفت هذه المرحلة بمرحلة طرح البيانات الأولى لإجرام تقنية المعلومات، كما وصفت سنوات السبعينات من القرن العشرين بأنها حملت بذور ملامح ظاهرة جرائم تقنية المعلومات، أما عقدي الثمانيات والتسعينات من نفس القرن، فقد حملا تحديداً لمفهوم وماهية هذه الجرائم، حيث تبلور فيها مفهوم ظاهرة جرائم تقنية المعلومات، واتسعت دائرة الشعور بأهمية المعلومات وعظم وحجم المخاطر

الناجمة عن الاعتداء عليها، والضرورة الملحة لحماية المعلومات عن طريق توفير أدوات قانونية فاعلة لوسائل معالجتها ونقلها.1

وعليه يمكن القول أن جرائم تقنية المعلومات مرت أثناء تطورها بعدة مراحل يمكن إيجازها على النحو الآتي:

1-مرحلة الدلالة الأخلاقية لظاهرة جرائم تقنية المعلومات:

تبدأ هذه المرحلة من أواخر خمسينات القرن الماضي إلى سبعينيات من نفس القرن، حيث أن في أربعينات القرن العشرين لم يتم استخدام الحواسيب على صعيد الحياة العامة، بل اقتصر استخدامها على كل من المؤسسات العسكرية والمؤسسات الكبرى على نطاق ضيق. أما خمسينات القرن العشرين، وتحديدا في نهاية هذه العشرية سنة 1958 تم توثيق أول جريمة ارتكبت بواسطة الحاسوب في الولايات المتحدة الأمريكية حسب ما اشارت إليه الدراسات البحثية الأكاديمية2.

وتعد ستينات القرن الماضي فترة ظهور أول معالجة لظاهرة جرائم تقنية المعلومات، كالمقالات والمواد الصحفية التي تناقش التلاعبات بالبيانات المخزنة والاستخدام غير المشروع للبيانات المخزنة ونظم الحاسوب وتدمير تلك الأنظمة، مما اطلق على هذه الفترة وصف مرحلة طرح البيانات الأولية لأجرام تقنية المعلومات3 وبدأ بروز مفهوم ما اصطلح عليه "اساءة استخدام الكمبيوتر" وثار التساؤل حينها إن كانت تلك الأفعال مجرد سلوكيات غير أخلاقية أم هي جرائم بالمعني القانوني؛ لكن بقيت نظرة التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني4.

---

[1] نائل عبد الرحمان صالح، (واقع جرائم الحاسب في التشريع الأردني،) مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة، من 1-3مايو ،2000الإمارات العربية المتحدة، ص .190-191

[2] علي حسن الطوالبة، مرجع سابق، ص96.

[3] نظر: نائل عبد الرحمان صالح، مرجع سابق، ص.190و علي حسن الطوالبة، مرجع سابق، ص93.

[4] نظر: علي جابر الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، ص8.

2- مرحلة الدلالة القانونية لظاهرة جرائم تقنية المعلومات:

هذه المرحلة تشمل سنوات السبعينات من القرن الماضي، وهي تمثل مرحلة الانطلاقة الحقيقية للدراسة والبحوث المتخصصة في مجال الحاسوب، وتتميز هذه المرحلة بأهم ميزة هي انحسار الدلالة الأخلاقية التي كانت تؤسس عليها ظاهرة جرائم تقنية المعلومات، وتبلور الدلالة القانونية للظاهرة، إضافة إلى بروز الدراسات المتخصصة الرسمية الأكاديمية لهذه الظاهرة، والاهتمام الفقهي بها. ونتيجةً للاندماج بين الحوسبة والاتصال ظهرت الانشطة التي تستهدف المعطيات عن بعد، كاختراق شبكات الحاسوب والتوصل غير المصرح به مع أنظمة الاتصال البعدي[1]. تم تحديد أولي لمحل الاعتداء في جرائم تقنية المعلومات وموضوعها معطيات الحاسوب بدلالتها الواسعة، وشهدت هذه الفترة من السبعينات دراسات مسحية وأبحاث علمية رسمية، منها: دراسة معهد ستانفورد العلمي للأبحاث المتواجد في أمريكا سنة، 1971 حيث رصد 1600حالة إساءة استخدام الحاسوب، وللتحضير لمناقشة مشروع قانون الجريمة الاقتصادية، قدم المعهد سابق الذكر استبيان في عام 1979 وجهه إلى 72 مدعي عام فكانت النتائج بأن أربعون منهم أفادوا بوصول224 جريمة متصلة بالحاسوب إلى علمهم، كما تم تحريك 190 من تلك الجرائم على مرتكبيها، و176 جريمة قضت المحكمة فيها بإدانة. كما أن معهد الإجرام وقانون العقوبات الاقتصادي المتواجد في ألمانيا، في دراسة له تضمنت وصفا مفصلا لـ 31 جريمة ارتكبت بواسطة تقنية المعلومات[2].

3-مرحلة تبلور مفهوم ظاهرة جرائم تقنية المعلومات ونشأة أنواع أخري منها:

إذا كانت سنوات السبعينات من القرن الماضي قد حملت بذور ملامح ظاهرة جرائم تقنية المعلومات فإن السنوات التالية لها قد جلبت تحديداً لمفهوم وماهية هذه الجرائم، ومنه قد تبلور خلالها مفهوم ظاهرة جرائم تقنية المعلومات، وتوسع الشعور بعظم وأهمية المعلومات وحجم المخاطر المترتبة عن الاعتداء عليها مما يستوجب حمايتها من خلال توفير أدوات قانونية فاعلة لوسائل معالجتها ونقلها[3]. حيث شهدت سنوات الثمانينات، تبلور ركائز السياسة التشريعية في مجال جرائم تقنية

[1] علي حسن الطوالبة، مرجع سابق، ص 95.

[2] المرجع نفسه، ص96.

[3] انظر: نائل عبد الرحمان صالح، مرجع سابق، 190.

المعلومات، وكذلك سن قوانين لحماية استخدام الحاسوب وتجريم بعض الأفعال1. كما شهدت التسعينيات القرن العشرين بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات، تنامياً هائلاً في حقل جرائم تقنية المعلومات وتغيراً في نطاقها ومفهومها، فظهرت أنماط جديدة، منها الأنشطة التي تقوم على فكرة تعطيل الأنظمة التقنية ومنعها من القيام بعملها المعتاد، وشهدت نفس الفترة ظهور انشطة ما اطلق عليه (بجرائم المحتوى الضار)، وهي جرائم تنطوي على إثارة الفتن والأحقاد أو المساس بكرامة واعتبار الأشخاص، أو المستهدفة للترويج لمواد أو أفعال غير مشروعة أو غير قانونية، ونشطت أيضا جرائم نشر الفيروسات عبر مواقع الإنترنت2. ومع تزايد حجم ونطاق جرائم تقنية المعلومات، سيما مع ظهور شبكة الإنترنت والطريق السريع للمعلومات، برزت الدعوة إلى ضرورة تظافر الجهود لحماية البيانات على الخط عن طريق وضع قواعد عامة، تسترشد بها الدول في تشريعاتها الداخلية3. كما يجب على القانون الجنائي أن يتماشى مع التطورات التكنولوجية التي تتيح فرصاً واسعةً لإساءة استخدام الفضاء المعلوماتي، من خلال مواكبة التطورات والعمل على ردع الأفعال الإجرامية4.

الفرع الثاني: المصطلحات المستخدمة للدلالة على ظاهرة جرائم المعلومات

تباينت المصطلحات التي أطلقت للدلالة على ظاهرة جرائم تقنية المعلومات، وذلك راجع إلى انعكاس واقع كل مرحلة من المراحل التي مرت بها تقنية المعلومات في تطورها على المصطلح المستخدم، فمنذ بداية ظهور الفرع التقني المتعلق بالحوسبة، مروراً بظهور الفرع التقني الأخر فرع الاتصال حتى لحظة تقارب هذين الفرعين التقنيين واندماجهما وتطورهما إلى يومنا هذا، لم يتم التدليل على هذه الظاهرة بمصطلح موحد. وأمام هذا الواقع التقني، برزت مصطلحات مختلفة دالة على السلوكيات الإجرامية المتعلقة بالتقنية، فبعض تلك المصطلحات دلت على الأفعال المتعلقة بالحوسبة، وبعضها حاول أن يشمل بدلالته قطبي التقنية، ومنها من شملت دلالته عموم التقنية باعتبار ما

[1] لي حسن الطوالبة، مرجع سابق، ص.95-96

[2] أ نظر: يونس عرب(،صور الجرائم الإلكترونية واتجاهات تبويبها،) ورشة عمل- تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات ، 2-4ابريل ،2006مسقط- سلطنة عمان، و علي جابر الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، ص9-10.

[3] انظر: محمد أمين الشوابكة، جرائم الحاسوب والإنترنت،(الجريمة المعلوماتية،) ط ،1دار الثقافة للنشر والتوزيع ، عمان، الأردن، ،2009ص 8

[4] أنظر: هلالى عبد اللاه أحمد، مرجع سابق، ص97.

تحقق من اندماج وتألف بين مجالاتها، ومع الاستخدام الواسع للإنترنت في الحياة المدنية، برزت اصطلاحات حاولت التقارب مع هذه البيئة المدمجة لوسائط تقنية ولوسائل المعالجة وتبادل المعلومات1.

وعليه يمكن تقسيم تلك الاصطلاحات التي قيلت للدلالة على الجرائم التقنية إلى طائفتين هما: طائفة الاصطلاحات ذات الطابع الأخلاقي أو الإعلامي، وطائفة الاصطلاحات ذات المحتوى الجنائي القانوني2.

أولا: طائفة الجرائم ذات الطابع الأخلاقي أو الإعلامي

تضم هذه الطائفة كل من مصطلح إساءة استخدام الحاسوب وجرائم أصحاب الياقات البيضاء والجرائم الاقتصادية المرتبطة بالحاسوب.

1. مصطلح إساءة استخدام الحاسوب Computer abuse

أطلق على ظاهرة الجرائم التقنية في بداية نشأتها مصطلح إساءة استخدام الحاسوب وشاع هذا المصطلح خلال تلك الفترة، على أساس أخلاقي ثم استعمل في التشريعات3 بعد ذلك، وهو أقدم المصطلحات تقريبا لكن هذا المصطلح لا يفرق بين السلوك الإجرامي والسلوك غير الأخلاقي، وبالتالي لا يدل دلالة واضحة ومحددة على ظاهرة الجرائم التقنية كونه يشمل مفهوم جرائم تقنية المعلومات والأفعال الغير أخلاقية التي لا تعد أفعال إجرامية.

2. الجرائم الاقتصادية المرتبطة بالحاسوب

أطلق هذا المصطلح على الجرائم التي تستهدف معلومات قطاعات الأعمال أو التي تستهدف أمن المعلومات من حيث السرية وسلامة المحتوى وتوفير المعلومات، وبالتالي يخرج من

[1] المعيني سرحان حسن، (التحقيق في جرائم تقنية المعلومات)، مجلة الفكر الشرطي – القيادة العامة لشرطة الشارقة– الإمارات، المجلد 20، العدد 79، أكتوبر 2011، ص24.

[2] المعيني سرحان حسن، المرجع نفسه، ص24.

– [3] علي حسن الطوالبة، مرجع سابق، ص42

نطاقها من جرائم التعدي غير المشروع على البيانات الشخصية أو الحقوق المعنوية على المصنفات الرقمية، وكذلك يخرج من نطاقها جرائم المحتوى غير المشروع أو الضار، كما أن هذا المصطلح شاع في العديد من الدراسات السابقة وهو يعود حالياً إلى واجهة التقارير الإعلامية، ومنه لا يعتبر هذا المصطلح شاملاً لكافة أنواع جرائم تقنية المعلومات.

3. جرائم أصحاب الياقات البيضاء

هذا الاصطلاح يغلب عليه الطابع الإعلامي أكثر من الأكاديمي، وظهر حديثاً بفضل عالم الاجتماع سذرلاند SUTHERLAND الذي أطلقه على الجرائم التي ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة، حيث استفاد مرتكبو هذه الجرائم من انتشار شبكة الإنترنت في القيام بأعمالهم وتطويرها وتوسيع رقعتها الجغرافية بعد ما كانت محلية أصبحت عالمية، وأهم الجرائم المرتكب من قبل هذه الطائفة، الرشوة والتلاعب بالشيكات والاختلاس والسرقة وتزوير العلامات التجارية للشركات العالمية ووضعها على منتجات علمية غير مشهورة وحتى على منتجات محلية، ومن ثمة هذا المصطلح لا يكون دقيقاً في التعبير عن ظاهرة الجرائم التقنية[1].

ثانيا: طائفة الاصطلاحات ذات المحتوى الجنائي القانوني.

تضم هذه الطائفة مجموعة من الاصطلاحات الدالة على ظاهرة الجرائم التقنية من هذه المصطلحات نذكر، مصطلح احتيال الحاسوب ومصطلح جرائم المعلوماتية ومصطلح الجرائم الإلكترونية ومصطلح جرائم الحاسوب والجرائم المرتبطة بالحاسوب ومصطلح جرائم الإنترنت ومصطلح جرائم الفضاء المعلوماتي ومصطلح جرائم التقنية العالية ومصطلح جرائم نظم المعلومات ومصطلح جرائم تقنية المعلومات.

1- مصطلح احتيال الحاسوب أو غش الحاسوب:

[1] المعيني سرحان حسن، التحقيق في جرائم تقنية المعلومات، مرجع سابق، ص25.

استخدم مصطلح احتيال الحاسوب للدلالة على عموم ظاهرة جرائم تقنية المعلومات، غير أن غش الحاسوب أو احتيال الحاسوب أو نصب الحاسوب هي أفعال للجريمة التقنية وصورة من صور ظاهرة جرائم تقنية المعلومات، ومنه لا يمكن للجزء أن يعبر عن الكل فهذه الأفعال ليست قادرة على التعبير عن الظاهرة برمتها1، فثمة اصطلاحات أكثر دقة للتعبير عن الكل2.

2- مصطلح جرائم المعلوماتية:

هذا المصطلح مركب إضافي بين كلمة جرائم وكلمة معلوماتية، ومصطلح المعلوماتية استعمل أول مرة من قبل مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفيتي سابقاً MIKHAILOV.I.A كإسم لعلم المعلومات العلمية، ثم ذاع استخدامه بشكل واسع، وقد صاغت الأكاديمية الفرنسية تعريفا له في جلستها المنعقدة في 6 أبريل 1967 على أنه علم التعامل العقلاني –على الأخص بواسطة آلات أوتوماتكية–مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماداً للاتصالات في ميدان التقنية والاقتصاد والاجتماع3.

ومنه فإن مصطلح جرائم المعلوماتية يدل على الجرائم الواقعة على البيانات المعالجة آلياً واستخدم في وصف ظاهرة الجرائم التقنية المستحدثة، غير أن هذا المصطلح غير مناسب باعتبار أن المعلوماتية أصبحت الآن فرعاً مستقلاً بين فروع المعرفة العلمية وعلومها، متعلق بإنشاء وإدارة قواعد البيانات4.

3-مصطلح الجرائم الإلكترونية:

مصطلح الجرائم الإلكترونية Electronic crime، يشمل كلمة الإلكترونية التي تدل في مجال المعلومات على كل وسيلة تستخدم لإدخال البيانات الإلكترونية أو قراءتها أو مشاهدتها أو سماعها، وبالرغم من عدم تأييد بعض المؤلفين لإطلاق مصطلح الجرائم الإلكترونية على الجرائم

[1] علي حسن الطوالبة، مرجع سابق، ص43.

[2] المعيني سرحان حسن، مرجع سابق، ص25

[3] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، د ط، دار الجامعة الجديدة للنشر، الاسكندرية، ص43.

[4] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت،)رسالة مقدمة استكمالا لمتطلبات الحصول درجة الماجستير في العلوم الشرطية(، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2004، ص29.

التقنية المستحدثة1، وكذلك بعض التشريعات العربية أطلقته على قوانينها المتعلقة بمكافحة جرائم تقنية المعلومات2. إلا أن هذا المصطلح يربط الجريمة بالإلكترونيات التي تشمل مختلف الأجهزة الإلكترونية مما يجعل المجال واسعاً يتجاوز وسائل تقنية المعلومات إلى غيرها من الوسائل ذات الطابع الإلكتروني من جهة، ومن جهة أخرى فإن هذا المصطلح Electronic crime يكتب غالبا E-crime حيث أن حرف E يستخدم قبل الكلمات لتحويلها من مجال مدلولها التقليدي إلى المجال ذي الطابع الإلكتروني المرتبط بوسائل تقنية المعلومات، مثل البريد الإلكتروني E-mail والتجارة الإلكترونية E-commerce والحكومة الإلكترونية وغيرها، ومنه فإن هذا المصطلح واسع الدلالة3.

4-مصطلح جرائم الكمبيوتر والجرائم المرتبطة بالحاسوب

يعبر بمصطلح جرائم الحاسوب للدلالة على الأفعال التي يكون الحاسوب نفسه هدفاً للجريمة فيها، أما مصطلح الجرائم المرتبطة بالحاسوب، يعبر به عن الجرائم التي يكون جهاز الحاسوب وسيلة لارتكاب الجريمة، حيث واكب هاذين المصطلحين ظاهرة الجرائم التقنية المستحدثة منذ بدايتها ولم يكن التمييز بينهما متيسراً في تلك الفترة، إلا في ظل تطور الظاهرة ومحاولة الفقهاء تحديد أنماط جرائم الحاسوب، وكان هذان المصطلحين أكثر دقة للدلالة على الظاهرة4 خلال تلك الفترة، حتي ظهور الإنترنت، فانتشر اصطلاح (Cyber crime) الذي أعتبر بأنه مصطلح شامل لجرائم الحاسوب والشبكات، وشاع استخدامه في النطاق الأوروبي عموماً كما انتشر خارجه، ولم يعد ثمة تمييز كبير بين جرائم الحاسوب أو الإنترنت لما بينهما من وحدة ودمج في بيئة معالجة وتبادل المعطيات5.

---

[1] عادل عزام سقف الحيط في مؤلفه جرائم الذم والقدح والتحقير المرتكب عبر الوسائط الإلكترونية، مبرر ذلك بأن هذا المصطلح يشمل الحاسوب وأنظمته، والشبكات الداخلية للأجهزة والإنترنت ومختلف الوسائط الإلكترونية، و كل وسيلة تستخدم الإدخال البيانات الإلكترونية أو قراءتها أو مشاهدتها أو سماعها، كما يشمل في دراسته المصطلحين: الجرائم السيبرالية والجرائم الافتراضية، أنظر: عادل عزام سقف الحيط ،جرائم الذم والقدح والتحقير المرتكب عبر الوسائط الإلكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان الأردن، ص 37.

[2] القانون القطري، القانون رقم)14(لسنة 2014 يسمى قانون مكافحة الجرائم الإلكترونية، وكذلك القانون الأردني رقم)27(لسنة 2015 المسمى قانون الجرائم الإلكترونية، قانون دولة فلسطين رقم)16(لسنة 2017 تحت اسم الجرائم الإلكترونية.

[3] محمد بن نصير محمد السرحاني، مرجع سابق ص29.

[4] علي حسن الطوالبة، مرجع سابق، ص45.

[5] المعيني سرحان حسن، مرجع سابق، ص26.

الفرع الثالث: المقصود بجرائم تقنية المعلومات

تعتبر جرائم تقنية المعلومات من الجرائم المستحدثة فقد أحاط تحديد المقصود بها العديد من الغموض، كما اختلف الفقه الجنائي حول تحديد المقصود بجرائم تقنية المعلومات وكانت هناك اتجاهات مختلفة في تعريفها، منقسمة بين من يعتنق المعنى التقني في تعريفه لجرائم تقنية المعلومات وآخر يقول بالمعنى الموضوعي.

1. تعاريف ذات المعنى التقني:

من الناحية التقنية تعرف جرائم تقنية المعلومات بأنها (نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة، أو غير مباشرة كوسيلة، أو هدف لتنفيذ الفعل الإجرامي المقصود)[1].

كما عرفها كل من R. Totty وA. Hardcastle بعبارات يغلب عليها الطابع التقني بأنها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام حاسب: وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسب فيها إيجابياً أكثر منه سلبياً[2].

وما يلاحظ على التعاريف السابقة أنها تعتمد على وسيلة تقنية المعلومات في تعريف جرائم تقنية المعلومات.

1. تعاريف ذات المعنى الموضوعي:

يرى مؤيدو الاتجاه الموضوعي في تعريف جرائم تقنية المعلومات بأنها تلك التي تقع على الحاسب أو داخله، ومن أمثلة تعاريف هذا الاتجاه ما جاء به مجموعة من الخبراء حول جريمة تقنية المعلومات بأنها نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب والتي تحول عن طريقه[3].

---

[1] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والإنترنيت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 01 إلى 03 مايو صفحة 1036.

[2] هشام محمد فريد رستم، المرجع السابق، صفحة 406.

[3] هشام محمد فريد رستم، المرجع السابف، صفحة 407.

وبعد عرض الاتجاهين السابقين، يتضح أنه لا يمكن الأخذ بأحدهما دون الآخر لتحديد المقصود بجرائم المعلومات.

المبحث الثاني: مفهوم الاتفاقية العربية 2010 وخصائص وسمات الجريمة المعلوماتية

المطلب الأول: التعريف بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010

الفرع الاول : التعريف بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

تعتبر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من الاتفاقيات العربية الحديثة في مجال مكافحة جرائم تقنية المعلومات على مستوى الدول العربية، وهي عبارة عن اتفاق دولي إقليمي معقود بين هذه الدول في نطاق جامعة الدول العربية بصورة خطية وقد حررت هذه الاتفاقية بمدينة القاهرة في جمهورية مصر العربية في 15 محرم 1432هـ، الموافق 21 ديسمبر 2010مـ من أصل واحد، باللغة العربية، أودعت بالأمانة العامة لجامعة الدول العربية، وتحديًدا لدى الأمانة الفنية لمجلس وزراء العدل العرب، ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب، على أن تسلم كذلك نسخة مطابقة للأصل لكل دولة من الدول الأطراف وإثباتًا لذلك، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب، بتوقيع هذه الاتفاقية نيابة عن دولهم، وهذه الدول هي:

المملكة الأردنية الهاشمية، دولة الإمارات العربية المتحدة، مملكة البحرين، الجمهورية التونسية، الجمهورية الجزائرية الديمقراطية الشعبية، المملكة العربية السعودية، جمهورية السودان، الجمهورية العربية السورية، جمهورية العراق، سلطنة عمان، دولة فلسطين، دولة قطر، دولة الكويت، الجمهورية العربية الليبية الشعبية الاشتراكية العظمي (سابقا)، جمهورية مصر العربية، المملكة المغربية، الجمهورية الإسلامية الموريتانية، الجمهورية اليمنية.

أولا/ الشكل العام للاتفاقية: تتكون الاتفاقية من ديباجة وثلاثة وأربعين (43) مادة موزعة على خمسة (5) فصول:

1. دباجة:

تظهر الدباجة رغبة الدول العربية الموقعة في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها؛ واقتناعها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات؛ وأخذا بالمبادئ الدينية والأخلاقية السامية ولاسيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزامها بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، قد اتفقت على ما ورد في الاتفاقية من فصول.

2. فصول ومواد الاتفاقية.

الفصل الأول: أحكام عامة من المادة الأولى (1) إلى المادة الرابعة (4)صون السيادة[1].

الفصل الثاني: التجريم ويضم المواد من المادة الخامسة (5) إلى المادة الواحدة والعشرين (21)[2].

الفصل الثالث: الأحكام الإجرائية من المادة الثانية والعشرين (22) إلى المادة التاسعة والعشرون (29)[3].

---

[1] المادة (1) الهدف من لاتفاقية، المادة (2) المصطلحات، المادة (3) نطاق تطبيق الاتفاقية، المادة (4) صون السيادة.

[2] تتضمن هذه المواد جرائم مرتبة حسب ترتيب مواد هذا الفصل من المادة)5(إلى المادة)21(وهي: جريمة الدخول غير المشروع جريمة الاعتراض غير المشروع، الاعتداء على سلامة البيانات، جريمة إساءة استخدام وسائل تقنية المعلومات، جريمة التزوير، جريمة الاحتيال، جريمة الإباحية، الجرائم الأخرى المرتبطة بالإباحية، جريمة الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع الإلكترونية، الشروع والاشتراك في ارتكاب الجرائم. المسؤولية الجنائية للأشخاص الطبيعية والمعنوية، تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات.

[3] وهذه الاحكام الإجرائية تتمثل في نطاق تطبيق الأحكام الإجرائية، التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، أمر تسليم المعلومات، تفتيش المعلومات المخزنة، ضبط المعلومات المخزنة، الجمع الفوري لمعلومات تتبع المستخدمين، اعتراض معلومات المحتوى.

الفصل الرابع: التعاون القانوني القضائي من المادة الثلاثين (30) إلى المادة الثالثة والأربعين (43)1.

الفصل الخامس: أحكام ختامية.

الفرع الثاني: المصطلحات الواردة في الاتفاقية العربية لسنة 2010.

تناولت الاتفاقية العربية مصطلحات تقنية قد يصعب فهمها، لذلك سنتناول في هذا الفرع المصطلحات المستخدمة للدلالة على الجانب التقني.

أولاً: المصطلحات المستخدمة للدلالة على الجانب التقني.

1. **تقنية المعلومات Le système informatique:** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبط بها سلكياً أو لاسلكياً في نظام أو شبكة2.
2. **مزود الخدمة Le fournisseur de service:** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.
3. **البيانات Les données:** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها.
4. **البرنامج المعلوماتي Le programme informatique:** مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.

---

[1] وتتمثل في: الاختصاص القضائي، تسليم المجرمين، المساعدة المتبادلة، المعلومات العرضية المتلقاة، الإجراءات المتعلقة بطلب التعاون والمساعدة المتبادلة، رفض المساعدة، السرية وحدود الاستخدام، التحفظ العاجل على المعلومات المخزنة في انظمة المعلومات، الكشف العاجل للمعلومات تتبع المستخدمين المحفوظة، التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة : الوصول إلى معلومات تقنية المعلومات عبر الحدود، التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى، جهاز متخصص.

[2] عرف قانون مكافحة جرائم تقنية المعلومات لسلطنة عمان في الفصل الأول المادة1/ب(تقنية المعلومات ب" الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات المعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة"، راجع: المرسوم السلطاني رقم2011/12 الجريدة الرسمية العدد 929.

5. **النظام المعلوماتي Le logiciel informatique:** مجموعة برامج وأدوات معدة لإدارة ومعالجة البيانات والمعلومات.
6. **الشبكة المعلوماتية Le réseau informatique:** وهو عملية ربط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.
7. **الموقع Le site:** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.
8. **الالتقاط La réception:** مشاهدة البيانات أو المعلومات أو الحصول عليها.
9. **معلومات المشترك Les informations de l'utilisateur:** أية معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمات، هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه ومعلومات الدفع المتوفرة بناءاً علي اتفاق أو ترتيب الخدمة، أية معلومات أخرى عن موقع تركيب معدات الاتصال بناءاً على اتفاق الخدمة.

2. أهداف الاتفاقية العربية 2010

تهدف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أساساً إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات بهدف الحفاظ على أمن وسلامة مجتمعاتها وأفرادها حسب ما جاءت به المادة الأولى من هذه الاتفاقية، كما جاءت نصوص هذه الاتفاقية لتخاطب الدول الأطراف فيها وتلزمهم لاتخاذ كافة الإجراءات التشريعية والتنظيمية المناسبة لوضع الأحكام التي وردت فيها موضع التنفيذ سواء كانت هذه الأحكام موضوعية أو أحكام إجرائية، أو تلك المتعلقة بالتعاون الدولي وذلك وفقاً لتشريعاتها وأنظمتها الداخلية، وأما بخصوص الأحكام الموضوعية التي وردت في الاتفاقية العربية فقد نصت المادة الخامسة منها على ضرورة إلتزام كل دولة طرف بتجريم الأفعال الواردة في الفصل الثاني منها المعنون بـ"التجريم" حيث تضمن هذا الفصل جملة من النصوص على شكل مواد من المادة السادسة إلى الثامنة عشر وهذه المواد تتضمن أفعال مجرمة تشكل جرائم تقنية المعلومات وهي، فعل الدخول غير المشروع، الاعتراض غير المشروع، الاعتداء على سلامة البيانات، إساءة استخدام وسائل تقنية المعلومات، التزوير والاحتيال، الاستخدام

غير المشروع لأدوات الدفع الإلكتروني، جرائم الإباحية والجرائم الأخرى المتعلقة بها، الاعتداء على حرمة الحياة الخاصة، إضافة إلى جرائم ترتكب بواسطة تقنية المعلومات تتمثل في جرائم الإرهاب، الجرائم المتعلقة بالجريمة المنظمة، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة.

المطلب الثاني: خصائص وسمات الجريمة المعلوماتية

كثيراً ما يقع الخلط وعدم التمييز بين خصائص الجريمة المعلوماتية وصعوبات مكافحتها، على الرغم من وجود حدود فاصلة بين الموضوعين، فخصائص الجريمة المعلوماتية يراد بها ما تنفرد به من مميزات، والتي لا يمكن فصلها بالضرورة عنها مقارنة بباقي الجرائم العادية الأخرى، في حين أن صعوبات مكافحة الجريمة المعلوماتية تشكل مجموعة من التحديات التي لا تتعلق بالجريمة المعلوماتية لوحدها، بل تشترك فيها كذلك مع بعض الجرائم الأخرى العابرة للحدود أو الجرائم المنظمة، وهي ليست لصيقة بالجريمة المعلوماتية بالقدر الذي لا يمكن فصلها عنها.

وعليه فإن مسألة صعوبة الاثبات، أو التحقيق في الجرائم المعلوماتية ليست سمات ملازمة للجريمة المعلوماتية، بقدر ما هي إشكاليات أو تحديات مرتبطة بالجريمة المعلوماتية، وسوف يأتي الحديث عنها لاحقا.

الفرع الأول: خصائص الجريمة المعلوماتية

أولا: وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات

يشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي، وذلك من أجل معالجتها الكترونياً، بما يمكن المستخدم من إمكانية تصحيحها أو محوها أو تخزينها واسترجاعها، أو طباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية[1].

وعلى الرغم من ارتكاب جرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي (الادخال، المعالجة، الاخراج)، فإن لكل مرحلة من

[1] عادل يوسف عبد النبي الشكري، (الجريمة المعلوماتية وأزمة الشرعية الجزائرية)، مجلة الكوفى مركزة دراسات الكوفى، العدد 7، 2008، ص 115.

هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر الى طبيعتها ارتكابها إلاّ في وقت محدد، ففي مرحلة الادخال المعلوماتي يمكن ادخال معلومات غير صحيحة، أو عدم ادخال وثائق أساسية، وفي مرحلة المعالجة الآلية للبيانات، فإنه يمكن إجراء أي تعديلات تحقق الهدف الاجرامي عن طريق التلاعب في برامج الحاسب الآلي، أما في مرحلة المخرجات فقد يقع التلاعب في النتائج التي يخرجها الحاسوب بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة1.

من المفيد الاشارة إلى أن بعض التشريعات وسعت تعريف المعدات المستخدمة في مجال المعالجة الآلية إلى تلك التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، ومن الشائع وصف بيانات الحاسوب مثلا كتمثيل للحقائق والمعلومات التي يمكن قراءتها ومعالجتها، أو تخزينها بواسطة الحاسوب، توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب، والبعض الآخر لم يحدد موقفه، لكن من المرجح في الممارسة العملية أن تتضمن تلك البيانات والمعلومات على وسائط التخزين المادية (مثل الأقراص الصلبة، وبطاقات الفلاش للتخزين)، وكذا البيانات والمعلومات المخزنة في نظام بث المعلومات سواء السلكية أو البصرية، أو تردد الراديو2.

ثانيا: الصبغة العالمية للجريمة المعلوماتية

تتصف الجريمة المعلوماتية بكونها جريمة ذات بعد عالمي أو دولي، لكن لا ينبغي أن يفهم من ذلك أنها جريمة دولية، ذلك أن هذه الأخيرة محددة على سبيل الحصر ومعرفة وفق نظام روما الأساسي في: جرائم الحرب، جرائم العدوان، جريمة الابادة البشرية، الجرائم ضد الانسانية، ما يجعل بالضرورة التفرقة بين النوعين تستدعي التدقيق، فالجريمة المعلوماتية تصنف في مجال القانون الجنائي الدولي، بخلاف الجريمة الدولية التي تصنف في مجال القانون الدولي الجنائي3.

---

[1] محمد ياسر أبو الفتوح، "خصائص وتصنيفات الجريمة المعلوماتية"، مقال منشور على الموقع الالكتروني
Almohakmoonalarab.ahlamontada.com/109-topic

[2] ذياب موسى البداينة، "الجرائم الالكترونية (المفهوم والأسباب)"، ورقة علمية مقدمة الى الملتقى العلمي الموسوم ب: الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية، عمان الأردن، .2014.

[3] محمد الصالح روان، الجريمة الدولية في القانون الدولي الجنائي، رسالة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2009/2008، ص 70.

والحديث عن صفة العالمية للجريمة المعلوماتية ارتبط بالتقنيات الحديثة، وما صاحبها من تطور في مجال الاتصال بحيث ألغيت الحدود الجغرافية بين الدول، فتخطت بذلك الجريمة المعلوماتية حدود الدولة التي ترتكب فيها لتتعدى آثارها إلى عدة بلدان على مستوى العالم، فالتقنيات المتصلة عالمياً قد جعلت من هذه الجريمة عابرة للحدود، وعليه فالطبيعة العالمية تمكن الجاني من ارتكاب الجريمة في دولة ما، وتؤثر على المجني عليه في دولة أخرى[1]، بل أنه من الممكن أن يكون هناك ضرر محتمل في بلد ثالث، وعليه تعد جرائم المعلومات شكلاً جديد من الجرائم العابرة للحدود الوطنية أو الاقليمية، أو القارية، وقد خلفت هاته الخاصية الكثير من الاشكالات القانونية في مسألة الاختصاص القضائي والتحديات التي تقترن به[2].

ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية" على غرار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

[1] مشتاق طالب وهيب، "مفهوم الجريمة المعلوماتية ودور الحاسب بارتكابها"، مجلة العلوم القانونية والسياسية، جامعة ديالي، (العراق)، المجلد الثاني، العدد 1، 2014، ص 345.

[2] راجع على التوالي: محمد علي سالم، حسون عبيد هجيج، "الجريمة المعلوماتية"، مجلة جامعة بابل للعلوم الانسانية جامعة بابل(العراق)، المجلد 14 العدد 3، 2008، ص 92.

ثالثاً: الجريمة المعلوماتية أقل عنفاً وجهداً في التنفيذ

لا تتطلب جرائم المعلومات عنفاً لتنفيذها، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة عنف وايذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع والكسر وغير ذلك.

وعلى هذا الأساس تتميز جرائم المعلومات بأنها من الجرائم الهادئة، أو الناعمة، حيث لا تحتاج الى العنف، وكل ما تحتاج إليه هو عامل الخبرة، والذكاء، والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني في ارتكاب الأفعال غير المشروعة، فهي من الجرائم النظيفة التي تستخدم الأرقام والبيانات وليس لها أثر خارجي مادي[1].

الفرع الثاني: السمات الخاصة بالمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز، المجرم المعلوماتي عن غيره من المجرمين، وقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parker واحداً من أهم الباحثين الذين اهتموا بالجريمة المعلوماتية بصفة عامة، وبالمجرم المعلوماتي بصفة خاصة. إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه[2].

فالمجرم المعلوماتي من ناحية، ينتمي في ألكثير من الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم والمعرفة، وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي[3].

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز لها الأستاذ PARKER بكلمة S.K.R.A.M وهي تعني

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013، ص 16.

[2] Parker (Done B) Figding computer crime A neur Framework for protecting information 1998/P 114

[3] Sutherland (Eduin H) « White collar criminality » Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968.

المهارة .Skill؛

المعرفة Knowledge؛

الوسيلة Resource؛

السلطة Authority؛

وأخيراً الباعث Motives.1

تعد المهارة: المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة: فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته. كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي. فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

أما الوسيلة: فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها.

أما السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي

[1] حاجب هيام، الجريمة المعلوماتية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2005-2006، صفحة 9.

على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها. وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات، وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

وأخيرا يأتي الباعث وهو الحافز لارتكاب الجريمة، كالرغبة في تحقيق الربح المادي بطريق غير مشروع، وبناءاً على ما تقدم يمكن أن نقسم مجرمي المعلومانية Cyber criminals إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هذه الطوائف فيما يأتي :

- تضم الطائفة الأولى : Pranksters الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).
- أما الطائفة الثانية Hackers فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.
- وتتضمن الطائفة الثالثة Malicious Hakers هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية وموزعيها.
- أما الطائفة الرابعة Personnel problem solvers فهم الطائفة الأكثر شيوعاً بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.
- وتتضمن الطائفة الخامسة Career Criminals مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أوعلى الأقل

يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

- أما الطائفة السادسة Extreme Advocates فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحياناً إلى النشاط الإجرامي، ويتركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه، وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي. تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفاً جذاباً لهذه الجماعات.
- وأخيرا تأتي الطائفة السابعة The Criminially Negligent والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه –في مجال الحاسبات الآلية وفي أغلب الأحيان– نتائج خطيرة قد تصل إلى حد إزهاق الروح.

الفرع الثالث: دوافع الجريمة المعلوماتية

يقول الدكتور ADAM GRAYCAR مدير المعهد الأسترالي لعلم الإجرام، بأن الجريمة تحتاج إلى أربعة عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

- أولا: دافع معين لارتكاب العمل؛
- ثانيا: الهدف ضحية محاسبة؛
- ثالثا: الفرصة المواتية؛
- رابعا: غياب عيون الأمن1.

إذا فالدافع والقصد يشكل أحد الركائز في جميع الجرائم. وبالنسبة لجرائم الحاسب الآلي والإنترنت فهي لا تختلف في وضعها العام عن أسباب أي جريمة أخرى تقليدية. فثمة دوافع عديدة تحرك العينات لارتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم، ويمكن تلخيص هذه الدوافع فيما يلي:

أولا: الدوافع الشخصية

أ/الدوافع المادية:

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل، وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية. ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب الذي يتيح تعزيز هذا الدافع بما تحققه من ثراء فاحش، والدليل على ذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000 فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي أي ما يعادل أكثر من 8 مرات2.

[1] نائلة محمد فريد قورة، جرائم الحاسب الآلي اللإقتصادية، دراسة نظرية وتطبيقية، منشورات الحاتي الحقثوقية، صفحة 63.

[2] Rose Philipe, la criminalité informatiqueque seis-je, 1ère edition, PU 1988, Page 490.

ومنذ بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال الإنترنت هو تحقيق الكسب المالي، ففي دراسة الفقيه Parker الصادرة في إحدى المجلات المتخصصة بخصوص موضوع الأمن المعلوماتي تبين أن: 34% من جرائم الغش المعلوماتي من أجل اختلاس الأموال، 23% من أجل سرقة المعلومات، 19% من أجل الإتلاف، 15% من أجل سرقة وقت الحاسوب لأغراض شخصية1.

ب/ الدوافع الذهنية أو النمطية:

الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنيت غالبا هي صورة البطل والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبوا هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، فيحاولون إيجاد الوسيلة إلى تحطيمها، أو التفوق عليها.

ثانيا :الدوافع الخارجية

أ/ دافع الانتقام وإلحاق الضرر برب العمل

قد يكون الانتقام مؤثرا في ارتكاب تلك الجرائم، ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات و ديون المنشأة2.

ولقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة، مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل.

[1] G. Delmare, sécurité informatique, ressources informatique, N°1.
Comment se protéger contre le cirme informatique, temps réels, 1984, Page 264.

وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة لديها[1].

ب/ الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية

يميل مرتكبوا هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجادها والتفوق عليها. ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم المعلوماتية الذين يمضون وقتاً طويلاً أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات لإظهار تفوقهم على الوسائل التقنية.

إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها من قبل المنظمات الإجرامية (مجموعات الجريمة المنظمة) لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة. هذا وإن كان الفعل الواحد قد يعكس دوافع متعددة وخاصة، فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات دوافعه سياسية وإيديولوجية في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، وقد تتداخل وتشترك هذه الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينهما[2].

[1] حاجب هيام، المرجع السابق، صفحة 14.
[2] حاجب هيام، المرجع السابق، نفس الصفحة.

الفصل الثاني:

التطور القانوني لجرائم تقنية المعلومات في ظل الاتفاقية العربية 2010 والتشريع الجزائري

تمهيد :

إن التطور الفكر الإجرامي لا بد أن يقابله تفعيل الفكر القانوني، بحيث أن ظهور الانترنت وما أسفرت عنه من ظهور ظاهرة الإجرام ألمعلوماتي يستدعي بالضرورة وجود مواجهة جنائية جديدة وفعالة كونه إجرام يقع على انتهاك المواقع المعلوماتية وسرقة بياناتها مما يستدعي أن يكون هناك تطور موازي ومواكب في الإطار القانوني خاصة في ظل واقع المعلوماتية الذي يتسم بالحركية والتحول الدائمين وظهور الحاجة الى الحماية الجنائية للنظم المعلوماتية والبيانات التي تتداول عبرها وإن مراجعة المراحل التطورية التي مرت بها معالجة ظاهرة الجرائم المعلوماتية منذ نشأتها تبين أنها في تطور دائم ومستمر وفي كل مرة تظهر بشكل جديد مسايرة بذلك التقنيات ، والتطبيقات الجديدة[1].

هذا بشكل عام أما إذا تحدثنا عن مواكبة العالم العربي لهذا التطور في مجال تقنية المعلومات، فالأمر يختلف حيث أنه لا يزال رغم البحوث والدراسات والمؤتمرات ينظر إلى الجريمة على أنها جزء من التشريع التقليدي وهو سبب مباشر لتأخر تشريعاتنا الجزائية عن مثيلاتها في القانون الجزائي الأجنبي.

إذ ليس هناك في العالم العربي ما يستحق الوقوف عنده كثيرا، فإنه للأسف لا توجد أي دولة عربية قد قامت بتقديم قوانين جديدةNew Lawsخاصة بها أو حتى تحديث قوانينها الخاصة وتستوعب تلك المستجدات الإجرامية، فالدول العربية لازالت بعيدة عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي[2] فما يوجد في البلدان العربية هو عملية تطويع للقوانين السابقة ومحاولة إدخال هذه الجرائم الإلكترونية تحت بعض نصوصها، متناسية طبيعة هذه الجرائم وما تخلفه من خسائر مادية والغموض الذي يكتشف لحظة ارتكاب الجريمة الإلكترونية[3].

وفي الجزائر لم يظهر أول نص قانوني في مجال جرائم المعلوماتية (جرائم المساس بأنظمة المعالجة الآلية للمعطيات) إلا سنة 1988في فرنسة حيث أنه إلى غاية هذا التاريخ لم يكن يتمتع أي من الدولتين (الجزائر و فرنسا) بتشريع عقابي في هذا المجال[4].

---

[1]الطيبي البركة، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتورة الطور الثالث تخصص قانون جنائي، الحماية الجنائية لنظام المعالجة الآلية للمعطيات –دراسة مقارنة– السنة 2021/2020 ص 63

[2]جعفر جاسم الطائي، جرائم تكنلوجيا المعلومات رؤية جديدة للجريمة، دار البداية الإصدار الثاني 2016ص232

[3]نفس المرجع، ص 232

4نسيم دردور ، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن ، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي ،جامعة منتوري (قسنطينة) سنة 2013/2012،ص 10

وأول نص تشريعي جزائري في مجال الإجرام المعلوماتي لم يظهر في قانون العقوبات إلا في 26جويلية2001بموجب قانون رقم01-09، المواد 144 و144مكرر1 و144 مكرر2 و146من قانون العقوبات الجزائري والمتعلق بجريمة القذف والسب والإهانة إزاء رئيس الجمهورية أو في ما يخص دين الإسلام الرسول وباقي الأنبياء أو ما هو معلوم من الدين) ومن خصوصيات المادة144مكرر في قانون العقوبات الجزائري حيث أدرج فيها للأول مرة مصطلح"...وسيلة إلكترونية أو معلوماتية التي تسمح بتجريم الأفعال السالفة الذكر.[1]

ويبدو أن المشرع الجزائري سارع إلى محتوى هذا التطور التكنولوجي بالتشريع الجنائي وإحاطته بالجريمة الإلكترونية بإصدار قانوني أدرج فيه تصورا مواكبا لمراحل هذه الجرائم وتشكيلاتها واهدافها من خلال القانون رقم04-15 المؤرخ في10نوفمبر 2004 كما أن المشرع الجزائري خطا خطوات عامة وسريعة في هذا المجال وذلك بالأخذ بتجريم صور الاعتداء على شبكة الانترنت والمساس بالبيانات المعالجة آليا.

ولقد نص قانون العقوبات الجزائري في القسم السابع مكرر من الفصل الثالث منه، على مجموعة الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والتي تشكل ما يعرف بالجريمة المعلوماتية، بالإضافة إلى ذلك جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010 بمجموعة أخرى من الأفعال والتي تشكل صورا جديدة من جرائم تقنية المعلومات. وذلك سواء تعلق الأمر بالمساس بتقنية المعلومات أو بارتكاب جرائم تقليدية باستعمال الوسائل التكنولوجية الحديثة والمتمثلة في تقنية المعلومات ومنه سنقوم بعرض مختلف هذه الصور الإجرامية متصورين أنه يمكن تقسيم هذا الفصل إلى مبحثين نعتقد أولها صور جرائم تقنية المعلومات في ظل الاتفاقية العربة والتشريع الجزائري (مبحث أول) والجرائم المستجدة في الاتفاقية العربية ومدى مسايرة التشريع الجزائري لها (مبحث ثاني).

[1]زيبحة زيدان محامي معتمد لدى ا لمحكمة العليا وجلس الدولة-الجريمة المعلوماتية في التشريع الجزائري والدولي. دار الهدى عين مليلة – الجزائر، ص45.

المبحث الأول: صور جرائم تقنية المعلومات في ظل الاتفاقية والتشريع الجزائري

إن مفهوم جرائم تقنية المعلومات من المفاهيم الحديثة التي رافقت تطور تقنية المعلومات وهي جرائم عابرة للحدود ونظرا وخطورتها على أمن الدولة العربية ورغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات، فوافق مجلس وزراء الداخلية والعدل العرب في اجتماعها المنعقد في مقر الأمانة العامة لجامعة الدول العربية بالقاهرة على ما يسمى بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات وصادقت الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي رقم14-252 المؤرخ في 08سبتمبر 2014.

حيث ألزمت المادة الخامسة من الاتفاقية كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها وذلك وفقا لتشريعات أنظمتها الداخلية.[1]

المطلب الأول: صور جرائم تقنية المعلومات في الاتفاقية العربية

ولذ كر هذه الصور لابد من تحليل ما تضمنه الفصل الثاني منها نصوص في شكل مواد تتضمن مجموعة من الأفعال التي تعبر عن جرائم تقنية المعلومات من أجل بيان الحلول التي انتقاها لها المشرع العربي لمكافحة تلك الجرائم.

الفرع الاول: الجرائم التي تستهدف تقنية المعلومات.

نصت الاتفاقية محل البحث عن الجرائم التي تستهدف تقنية المعلومات في المواد من 6إلى11منها، وسوف نتحدث عنها فيما يلي.

أولا: جريمة الدخول غير المشروع.

نصت المادة (6)من الاتفاقية العربية لسنة2010 على جريمتين

-جريمة الدخول أو الاتصال غير المشروع.

-وجريمة البقاء والاستمرار في الإيصال مع كل أو جزء من تقنية المعلومات.

1:جريمة الدخول أو الاتصا ل غير المشروع

يعرف الدخول أو الاتصال غير مشروع بأنه "الولوج والاتصال بكل أو جزء من النظام أو شبكة تقنية المعلومات دون رضا المسؤول عن النظام " أو هو الولوج والوصول إلى المعلومات والمعطيات المخزنة داخل تقنية المعلومات للاطلاع عليها أو لمجرد التسلية أو إشباع الشعور بالنجاح في اختراق الحاسب الآلي[2].

---

[1] أحمد حمي، زهيرة كيسي-صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة2014 المركز الجامعي لتامنغست، الجزائر-تاريخ الإسلام 2017/09/21-تاريخ القبول 2018/07/24، العدد 1، ص797

[2] أحمد حمي، زهيرة كيسي، المرجع السابق، ص781

ولم تكن التشريعات على مستوى العالم العربي تعرف هذه الجريمة، ولم تكن هناك أي نصوص تشريعية تتعلق بالجرائم الإلكترونية أو الدخول غير المشروع، فكانت تطبق عليه النصوص التقليدية في قانون العقوبات، ولقد اختلفت في تسمية هذه الجريمة والتي أسماها المشرع المصري بالدخول غير المشروع، ووفاقه على هذه التسمية المشرع الكويتي والمشرع السعودي ، وهناك تشريعات أطلقت عليها الدخول دون تصريح كالمشرع الأردني والقانون الإنجليزي، وأطلق عليها المشرع الأمريكي الدخول غير المصرح به وهناك تشريعات أطلقت عليها جريمة الدخول إلى النظام المعلوماتي بطريق الغش المشرع الفرنسي كما أطلق عليها المشرع العماني الدخول بدون وجه حق [1].

ففعل الدخول إلى كل أو جزء من تقنية المعلومات قد يكون منطقيا كما يمكن أن يكون ماديا ويتحقق هذا الأخير بإدخال وحدة ما داخل تقنية المعلومات بطريقة غير مشروعة أو ربط أي وحدة ما بوسائل اتصال مادية كالأسلاك مثلا، والدخول المنطقي–الافتراضي–يكون مثلا باستعمال كلمة المرور أو الرقم السري الذي يسمح بالدخول إلى تقنية المعلومات كل ذلك بانتحال صفة شخص له حق الدخول[2]

وهذا الدخول يتحقق عند تحقق الاتصال بتقنية المعلومات بحيث يكون الكل أو الجزء الذي تم الاتصال به مفتوحا بعدما كان مغلقا، وجريمة الدخول أو الاتصال إلى تقنية المعلومات جريمة قصديه، تقوم بقصد الجنائي العام، تترتب الجريمة إذا علم الجاني بدخولها أو باتصال غير مشروع بنظام تقنية المعلومات خاصة بالغير دون وجه حق.

2: جريمة البقاء أو الاستمرار في الاتصال:

ويقصد به التواجد داخل النظام المعلوماتي ضد إرادة وعلم من له الحق في السيطرة على هذا النظام. وهذه الجريمة منصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة1/6 ويتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة البقاء أو الاستمرار في الاتصال صورة البقاء في كل أو جزء من تقنية المعلومات أو الاستمرار في الاتصال، ويتسع ليشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد للتهرب من دفع إتاوة[3].

ولقد نصت الاتفاقية العربية على الصورة المشددة لجريمة الدخول أو البقاء في الفقرة(2)من المادة السادسة بنصها، «تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال"

---

[1] أشرف محمد نجيب السعيد الرديني، جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، مجلة روح القوانين – العدد الخامس والتسعون–إصدار جويلية 2021 جامعة المنصورة ص370

[2] أحمد حمي، زهيرة كيسي، المرجع السابق، ص 781

[3] أحمد حمي، أ.زهيرة كيسي المرجع السابق، ص782

أ–محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير البيانات المحفوظة والأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر والمستخدمين والمستفيدين.

ثانيا: جريمة الاعتراض غير المشروع:

وحدتها المادة السابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنها" الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بينات تقنية المعلومات"

ثالثا: الاعتداء على سلامة البيانات.

جريمة الاعتداء على سلامة البيانات نصت عليها المادة الثامنة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتقابلها المادة الرابعة4من اتفاقية بودابست لسنة2001 حول الإجرام المعلوماتي.

ويتحقق الركن المادي في هذه الجريمة بفعل الاعتداء على سلامة البيانات ويتخذ صورتين:

الصورة الأولى: أن يتم محو البينات والمعلومات كلية وتدميرها إلكترونيا.

الصورة الثانية: أن يتم تشويه البينات والمعلومات أو البرامج عن طريق إعاقة أو تعديل أو حجب بينات تقنية المعلومات قصدا أو بدون وجه حق وهي جريمة قصديه[1].

رابعا: جريمة إساءة استخدام وسائل تقنية المعلومات.

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة التاسعة على الأفعال المادية المكونة لهذه الجريمة وتتحقق متى ارتكبت الأفعال الآتية"

1: إنتاج أو بيع أو شراء أو استراد أو توزيع أو توفير:

ا–أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب–كلمة سر نظام معلومات أو شفيرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2–حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة[2].

خامسا: جريمة التزوير.

[1] أحمد حمي، زهير كيسي، المرجع السابق ص 783

[2]أنظر المادة 6. من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

يعرف التزوير بأنه تغيير الحقيقة في محرر بالطرق التي حددها القانون تغييرا من شأنه أن يرتب ضررا للتغيير، وبنية استعمال هذا المحرر فيما أعدا له[1].

ومفهوم التزوير في مجال جرائم تقنية المعلومات «هو تغيير الحقيقة في البيانات باستخدام وسائل تقنية المعلومات تغييرا من شأنه أن يرتب ضررا وبنية استعمالها كبيانات صحيحة"[2].

وحتى تقوم هذه الجريمة لابد من توفر الركن المادي والذي يتكون من العناصر الآتية:

1-العنصر الأول: تغيير الحقيقة

تغيير الحقيقة في جرائم تقنية المعلومات يتخذ شكلين:

ا-الشكل الأول منهما يتم بالتلاعب في المعلومات المخزنة في تقنية المعلومات.

ب-والشكل الأخر يتمثل في إدخال معلومات غير صحيحة ينتج عنها مستند غير صحيح.[3]

2-العنصر الثاني: أن يقع التزوير في محرر أو مستند معلوماتي

حسب نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فإن التزوير يقع في بينات بغرض تغيير حقيقتها.

3-العنصر الثالث: أن يقع تغيير الحقيقة بإحدى طرق التزوير

في هذا المجال فإن طرق التزوير لتغيير الحقيقة يكون بواسطة تقنية المعلومات بحسب نص المادة العاشرة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

4-عنصر الضرر: انقسم الفقه حول مفهوم الضرر في مجال التزوير الذي يتم بواسطة تقنية المعلومات بين فريق يضيق من فكرة الضرر وهذا الفريق الذي استند على أراء الفقيه" جارو «يرى هذا الفريق عدم قيام الضرر في تزوير المعلوماتي إلا إذا انصب التزوير على وثيقة قانونية لها بعد قانوني، بينما يرى الفريق الأخر أنه كلما كانت له خسارة بالضرر قائم فربط هذا الفريق بين فكرة الضرر في التزوير المعلوماتي والخسارة الناتجة عن التزوير ولا يهم أن تكون الوثيقة معدة الإثبات أم لا[4].

سادسا: جريمة الاحتيال

---

[1]معتوق عبد الطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن(مذكرة ماجستير) كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر-باتنة ص45.

[2]أنضر المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية

[3]نفس المرجع ص46

[4]معتوق عبد الطيف نفس المرجع،ص46

لا يوجد تعريف محدد لجريمة الاحتيال المعلوماتي وقد حاولت منظمة التعاون الاقتصادي والتنمية تعريف الاحتيال بأنه كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به،يتعلق بالمعالجة الآلية للبينات ونقلها[1].

وهذه الجريمة منصوص عليها في المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات "التسبب بإلحاق ضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير، عن طريق:

1- إ دخال أو تعديل أو محو أو حجب المعلومات والبيانات.

2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3-تعطيل الأجهزة والبرامج والمواقع الإلكترونية"

إن الاتفاقية العربية لم تعرف الاحتيال في مجال تقنية المعلومات واكتفت ببيان الأفعال المشكلة للسلوك الإجرامي الذي أشرنا إليه سابقا.

وهذه الأفعال تتسبب إ لحاق ضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير.

وتجدر الإشارة هنا إلا أن جريمة الاحتيال المعلوماتي جريمة عمدية صورة الركن المعنوي فيها هو القصد الجنائي العام والقصد الجنائي الخاص والمتمثل في نية التملك[2].

الفرع الثاني: الجرائم التي تقع بواسطة تقنية المعلومات.

تعتبر الجرائم التي تقع باستخدام تقنية المعلومات جرائم تقليدية منصوص عليها في أغلب قوانين العقوبات وتشكل هذه الجرائم إذا ما ارتكبت بواسطة تقنية المعلومات، جرائم تقنية المعلومات ومن ثم تصبح تقنية المعلومات عنصرا من عناصر التجريم وهذه الجرائم حسب الاتفاقية العربية محل البحث هي:

أولا: الجريمة الإباحية:

حسبما ورد في الاتفاقية العربية لمكافحة جرائم تقنية، فإن الركن المادي لهذه الجريمة هي: إنتاج أو عرض أو توزيع أو توفير أو نشر أو بيع أو استراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

كما أن العقوبة تشدد إذا تعلقت بإباحية الأطفال القصر.

[1] أحمد حمي، زهير كيسي المرجع السابق، ص784

[2] أحمد حمي، زهيرة كيسي نفس المرجع، ص 785

كما أن الفقرة 3من المادة12من الاتفاقية أشارت إلى جريمة الاستغلال الجنسي للأطفال والقصر عبر وسائل تقنية المعلومات حيث تقع الجريمة بوجود طفل أو قاصر لم يتعدى سن الرشد حتى يكون محل عرض مرئي أو مسموع يتضمن عرضا للأعضاء الجنسية للطفل أو يقوم بارتكاب سلوك جنسي.

وتتضمن الأفعال المجرمة حيازة مواد إباحية للأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

أما الجرائم الأخرى المرتبط بالإباحية لم تعرفها المادة 13من الاتفاقية والمتمثلة في المغامرة حيث وردت بهذا اللفظ في نسخة الجريدة الرسمية العدد 57 وكلمة مغامرة وردت في النسخ الأخرى بلفظ المقامرة. والمقامرة مجرمة في جميع الدول العربية سواء بالطريقة التقليدية أو باستخدام وسائل تقنية المعلومات.

اما الاستغلال الجنسي الذي ورد في نص المادة 13 من الاتفاقية فيكون غالبا من نتائج الاتجار بالبشر من النساء والأطفال بغرض الإكراه علي ممارسة الدعارة[1].علما أن المشرع الجزائري جرم فعل الوسيط في ممارسة الدعارة والإباحية وذلك في المواد 343 إلى 345 من قانون العقوبات والسماح للغير تعاطي الدعارة[2].

ثانيا: جريمة الاعتداء على حرمة الحياة الخاصة.

جريمة الاعتداء على حرمة الحياة الخاصة منصوص عليها في المادة 14من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث أن غالبية الدساتير تكفل حق الشخص في حماية حياته الخاصة.

إلا أن هذا قد الحق ينتهك عندما يتم نشر معلومات أو صور تتصل بحرمة الحياة الخاصة للأفراد حيث أتاحت شبكات تقنية المعلومات إمكانية الوصول إلى البيانات الشخصية والمعلومات الخاصة السرية للأفراد أو عائلتهم.

وقد عاقب المشرع الجزائري على الاعتداء على الحياة الخاصة في المادة 303 مكرر [3]من قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من50.000دجإلى300.000دج وذلك إذا قام بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه كما أن المادة303مكرر 1 تعاقب بنفس عقوبة المادة303مكرر كل من احتفظ أوسمح بأن توضع في متناول الجمهور أوالغير أو استخدم بأي وسيلة كانت التسجيلات أو الصور الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

---

[1]أنظر أحمد حمي زهيرة كيسي، ص786 بالتصرف

2أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص الجزء الأول ،الطبعة السابعة عشر، دار هومة، الجزائر، 2014 ص127

[3]القانون06-23 المؤرخ في 20 ديسمبر 2006،ج رقم 84،ص23

وتتخذ جريمة الاعتداء على حرمة الحيات الخاصة في مجال تقنية المعلومات أشكالا متعددة من أبرزها:

1-جمع وتخزين بينات شخصية صحيحة بدون ترخيص:

وتتحقق هذه الصورة بالجمع والتخزين لبيانات شخصية تخص أشخاص ويتم هذا الجمع أو التخزين بصورة غير قانونية مع أشخاص أو جهات ليس لهم الحق في القيام بهذا الجمع أو التخزين لهذه البيانات ويتحقق الركن المادي لهذه الجريمة بتحقق الجمع أو التخزين البينات الشخصية لأشخاص وبشكل غير مشروع أما الركن المعنوي يتحقق بعلم الجاني بأنه يقوم بجمع أو تخزين هذه البيانات الشخصية بشكل غير مشروع واتجاه إرادته إلى ذلك[1]

2-الإفشاء غير المشروع للبينات الشخصية:

يعتبر إفشاء البيانات الشخصية السرية سواء تم عن طريق الخطأ او لغير الهدف الذي جمعت له اعتداء يمس الحياة الخاصة للإنسان ومن أمثلة ذلك المعلومات المتحصل عليها من عملية الإحصاء السكاني لا يجوز استعمالها لغير هذا الهدف ولو كان مشروعا مثل استعمالها في الأغراض الضريبة لكونها لم تستعمل في الإطار المحدد الذي جمعت من أجله المعلومات[2].

3-استخدام بينات شخصية غير صحيحة:

وهذه الصورة تستخدم فيها بينات الأفراد على وجه غير صحيح على نحو غير مشروع. ويكون في الغالب التلاعب بالبينات من أشخاص عاملين لدى شركات التأمين مقابل الحصول على ربح مادي .ومن أمثلة هذه الحالة ما قام به موظفون في شركة تأمين في الولايات المتحدة الامريكية"trw comptant credit" هذه الشركة مختصة في تزويد البنوك والشركات الكبرى بمعلومات عن المركز الائتماني للأفراد ووضعيتهم المالية مقابل اشتراك يدفعه العملاء، وكانت الشركة تحتفظ بمعلومات في أجهزة الكمبيوتر لديها عن أكثر من 50 مليون شخص ، فقام موظفون لدى هذه الشركة بتعديل المعلومات التي تظهر مركزا سيئا للشخص والتلاعب بها بمقابل مالي مما يتيح لصاحب المعلومات أن يظهر في وضعية مالية مريحة، مما تسبب في تورط البنوك والشركات الكبرى في التعامل مع قرابة (100) شخص من الأفراد سيئ الوضع المالي [3] .

ثالثا: الجرائم المتعلقة بالإرهاب والمرتكب بواسطة تقنية المعلومات.

1أسامة بن غانم عبيد، حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والأنترنت، المجلة العربية للدراسات الأمنية والتدريب المجلد 32 العدد 46 ص71

[2]معتوق عبد اللطيف، مرجع سابق ص 71

[3]أنظر معتوق عبد اللطيف، مرجع سابق، ص 71

نصت الاتفاقية العربية لمكافحة الإرهاب بتاريخ 22 أفريل 1998 في مادتها الأولى على تعريف ظاهرة الإرهاب، حيث اعتبرتها:" كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى لقاء الرعب بين الناس أو توزيعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر[1].

ويتمثل السلوك الإجرامي في الإرهاب المعلوماتي حسب نص المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في:

1- نشر افكار ومبادئ جماعة إرهابية والدعوة لها.

2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات الإرهابية.

4- نشر النعرات والفتن الاعتداء على الأديان والمعتقدات.

كل هذه الأفعال المجرمة تتم بواسطة تقنية المعلومات.

رابعا: الجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات:

إن الجريمة المنظمة المرتكبة بواسطة تقنية المعلومات تشمل الجرائم الآتية:

1 جريمة غسيل الأموال[2]: ويقصد بغسيل الأموال أو تبيض الأموال وهي العبارة التي استعملها المشرع الجزائري في قانون العقوبات ب "إخفاء المصدر الإجرامي للممتلكات والأموال، لاسيما ما يسمى ب المال القذر وتمر عملية التبييض تقنيا بثلاث مراحل، توظيف المال، التمويه والإدماج.[3]إن تقنية المعلومات وفرت لمجرمي غسيل الأموال كل الوسائل السريعة التي تعين على تحويل الأموال وسرية التعامل وعدم ترك الأثر وذلك بفضل توفر البنوك التي تتبنى مبدأ سرية الحسابات البنكية.

ولقيام هذه الجريمة لابد من تحقيق الركن المفترض والمتمثل في وجود جريمة سابقة، أي أن تكون الأموال محل الغسيل" عائدات إجرامية"

كما يجب تحقق السلوك الإجرامي وهو القيام بتحويل أو نقل الأموال غير المشروعة، أي جراء عمليات مصرفية لتحويل الأموال وتكون عبر وسائل تقنية المعلومات كتحويل من حساب إلى حساب آخر عن طريق

---

[1] احمد حمي، زهيرة كيسي، المرجع السابق، ص 787 -788

[2] انظر المادة 1/19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الجريدة الرسمية العدد 75 بتاريخ 2014/09/28

[3]. أحسن بوسقيعة، مرجع سابق، ص449

شبكة الأنترنت، أو إخفاء المصدر الحقيقي للأموال عن طريق التمويه أو القيام بحيازة هذه الأموال مع العلم أنها عائدات إجرامية وذلك لإضفاء الصفة المشروعة على تلك الأموال.

وتجدر الإشارة إلى أن هذه الجريمة عمدية تتطلب توفر القصد الجنائي العام (العلم والإرادة) والقصد الجنائي الخاص وهو نية إخفاء المصدر غير المشروع لهذه الأموال، أو تمويه المصدر غير المشروع لتلك الممتلكات.[1]

2-جريمة الترويج للمخدرات والمؤثرات العقلية أو الاتجار بهما: إن جريمة الاتجار بالمخدرات والمؤثرات العقلية مجرمة في أغلب التشريعات الوطنية والدولية، ومن بين الاتفاقيات الدولية؛ الاتفاقية الموحدة المتعلقة بالمخدرات لسنة 1961 والمتممة باتفاقية المؤثرات العقلية بفينّا سنة 1988، و في الجزائر صدر القانون 18/04 المؤرخ في 2004/12/25 المتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الاستعمال و الاتجار غير المشروعين بهما.

وتتحقق جريمة الاتجار بالمخدرات باستخدام وسائل تقنية المعلومات خاصة عبر الانترنيت عن طرق إنشاء موقع أو نشر معلومات على شبكة الانترنت للترويج للمخدرات والمؤثرات العقلية أو تسهيل التعامل فيها.

من أمثلة إمكانية ترويج المخدرات عبر شبكات تقنية المعلومات، قيام المنظمات الكولومبية لتجارة المخدرات بإتباع الممارسات التي تقوم بها الشركات العادية لتنويع الأسواق والمنتجات، واستغلت بذلك أسواقا جديدة في كل من دولة الاتحاد السوفياتي ودول أوروبا الشيوعية سابقا.[2]

3-جريمة الاتجار بالأشخاص:

وهي الجريمة التي نصت عليها الاتفاقية في المادة 3/16 منها.ونص عليها المشرع الجزائري في المادة 303 مكرر4 من القانون 01/09 المتمم والمعدل ل ق ع، حيث جاء فيها:"يعد الاتجار بالأشخاص تجنيد أو نقل أو تنقيل أو إيواء أو استقبال شخص أو أكثر بواسطة التهديد بالقوة أو باستعمالها أو غير ذلك من أشكال الإكراه".

4-جريمة الاتجار بالأعضاء البشرية:

[1] المرجع نفسه،ص450

[2] أحمد حمي زهيرة كيسي، المرجع السابق،ص789

وردت هذه الجريمة في المادة 4/16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وكذلك نص عليها المشرع الجزائري في المواد 303 مكرر 16 إلى 303 مكرر 29.[1]

وأفعال الاتجار بالأعضاء تشكل ثلاث جرائم منصوص عليها في ق ع وهي:

ا-جريمة انتزاع عضو أو نسيج أو خلايا من جسم شخص بمقابل أو منفعة(المادة303مكرر16).

ب-جريمة الحصول على عضو من جسم دون موافقة صاحبه(المادة 303مكرر17).

ج-جريمة عدم التبليغ عن جريمة الاتجار بالأعضاء البشرية (المادة 303مكرر25).

خامسا: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة.

ورد النص على هذا النوع من الجرائم في المادة 17 من الاتفاقية العربية حيث جاء فيها "انتهاك حق المؤلف كما هو معروف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد أو غير الاستعمال الشخصي".

إن التطور السريع الذي شهدته تقنية المعلومات جعلت من انتهاك حق المؤلف والحقوق المجاورة مشكلة تطرح بقوة حيث مكنت شبكة الانترنيت لمرتكبي هذه الجرائم من القيام بعملية القرصنة وانتهاك حق المؤلف والحقوق المجاورة.

وفي الجزائر فإن المشرع ذكر الأفعال التي تشكل جريمة التقليد، وذلك في المادة 151 من الأمر 03-05[2] المتعلق بحماية حقوق المؤلف و الحقوق المجاورة على أنه:"يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

1-الكشف غير المشروع للمصنف أو المساس بصلامة مصنف أو أداء لفنان مؤد أو عازف.

2-استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.

3-استيراد أو تصدير نسخ مقلدة من مصنف أو أداء.

4-بيع نسخ مقلدة لمصنف أو أداء.

5-تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء.

كما نصت المادة 152 من الأمر 03-05 أنه:" يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف هذا الأداء عن طريق التمثيل أو الأداء العلني أو البث الإذاعي أو السمعي

---

[1] أضيفت المواد بالقانون رقم 01/09 المؤرخ في 25فبراير2009 الجريدة الرسمية عدد ص6

[2] ج. الأمر 03-05الصادر بتاريخ2003/07/19 المتعلق بحق المؤلف و الحقوق المجاورة المعدل و المتمم للأمر 73-14، ر عدد44 بتاريخ 2002/07/23

البصري أو التوزيع بواسطة الكابل أو أية وسيلة نقل أخرى لإشارات تحمل أصواتا أو صورا أو بأي منظومة معالجة معلوماتية" و عاقبت المادة 153 من نفس الأمر على جنحة التقليد بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة 500.000 إلى1.000.000 دج.

سادسا: الاستخدام غير المشروع لأدوات الدفع الإلكترونية

هذه الجريمة كانت نتيجة لعملية التجارة بوسائل تقنية المعلومات وهو ما يعرف بالتجارة الالكترونية ومن وسائل الدفع الالكتروني نجد البطاقات الذكية: فهي تحتوي على شريحة بها معالج دقيق ومزود بنظام أمان لحمايتها ويمكنها اختزان ملايين من النقود(الدولارات) فهي تجمع جميع العمليات من سحب النقود والوفاء والائتمان.[1]

وتعد الجرائم التي تقع على هذا النوع من وسائل الدفع حسب المادة 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فإن السلوك الإجرامي يتمثل في:

1-كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكتروني بأي وسيلة كانت.

2-كل من استولى على بيانات أي أداة من أدوات الدفع واستعمالها أو قدمها للغير أو سهل للغير الحصول عليها.

3-كل من استخدم الشبكات المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4-كل من قبل أداة من أدوات الدفع مزورة مع العلم بذلك.

هذا كان عن صور جرائم تقنية المعلومات في الاتفاقية العربية(مطلب أول) وسوف ننتقل إلى صور جرائم تقنية المعلومات في التشريع الجزائري (مطلب ثاني)

المطلب الثاني: صور جرائم تقنية المعلومات في التشريع الجزائري.

رغبة من المشرع الجزائري في حماية مصالح معينة، فقد استحدث نصوص جديدة ضمن القسم السابع مكرر من القانون 15/04المؤرخ في2004/11/10 المتمم والمعدل لقانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات".

يحتوي هذا القسم السابع على المواد من 394 مكرر إلى 394 مكرر7، يجرم فيها بعض الاعتداءات التي تمس سير النظام والمتمثلة في الدخول والبقاء غير المشروع في كل أو جزء من نظام المعالجة الآلية

[1] معتوق عبد اللطيف، مرجع سابق ص75

للمعطيات، ويشدد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل النظام. وتعتبر هي الجريمة الأساسية والتي من خلالها يمكن ارتكاب الجرائم الأخرى المنصوص عليها في هذا القسم[1].

وتتخذ الجريمة المعلوماتية إحدى الصور التالية:

جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات (فرع أول)، وجريمة الاعتداء العمدي على المعطيات (فرع ثاني).

الفرع الأول: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

لهذه الجريمة صورتان، الصورة البسيطة (أولا)، والصورة المشددة (ثانيا).

أولا: الصورة البسيطة للجريمة

تتمثل في مجرد الدخول أو البقاء غير المشروع وتتكون من ركنين مادي ومعنوي.

1- الركن المادي:

ويتحقق الركن المادي بإحدى الصور التالية:

أولها، اختراق الأجهزة الرئيسية بطريقة الغش إلى نظام المعالجة الآلية للمعطيات وثانيها، البقاء أو المكوث بطريقة الغش في نظام المعالجة الآلية أو جزء منه، فالمادة 394 مكرر تشير لوجود صورة بسيطة للدخول إلى نظام أو البقاء فيه وأخرى شدد فيها المشرع العقوبة إذ نصت المادة 394 مكرر من قانون العقوبات انه" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير للمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخزين نظام استعمال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين ،والغرامة من500000 إلى 150000دج[2]ومن خلال استقراء نص المادة 394 مكرر نجد أنها نصت على ظرفين تشدد فيهما عقوبة الدخول أو البقاء داخل النظام ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام على تأدية وظيفته ويكفي لتوفير هذا الظرف المشدد أن يكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم القدرة على تأدية وظيفته .[3]

ويقصد بفعل الدخول هنا وهو الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات ذلك الدخول المعنوي أو الإلكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي ولا يعد فعل الدخول

---

[1] غنية باطلي، الجريمة الإلكترونية دراسة مقارنة، طبعة ،2015، منشورات الدار الجزائرية الجزائر 2015ص134

[2] عزيزة رابحي الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتورة في القانون كلية الحقوق والعلوم السياسية، جامعة أبو بكر بالقايد تلمسان الجزائر 2018، ص 162

[3] المرجع نفسه، ص162

بحد ذاته غير مشروع وإنما يتخذ وصفه الإجرامي انطلاق من كونه قد تم دون وجه حق أو دون ترخيص مايستشف من المادة 394 مكرر من قانون العقوبات الجزائري[1].

وما بلا حظ من خلا هذه المادة أن المشرع الجزائري اعتبر جريمة الدخول غير المرخص بيه جريمة شكلية التي لا يشترط القيام الركن المادي فيها تحقيق النتيجة الإجرامية أي انه مجرد الدخول إلى نظام المعالجة الآلية للمعطيات بأكمله أو جزء منه فقط، بشرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو خطأ[2].

نعتقد أن المشرع الجزائري قد أصاب كثيرا عندما جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش لأنه يكون هذا بمثابة تدبير تحفظي وقائي يساهم بشكل كبير في التصدي لظاهرة الإجرام المعلوماتي من خلا غلق الباب أمام المجرمين من التهرب من المسؤولية الجنائية عن فعل الاعتداء.

2- الركن المعنوي

تعتبر جريمة الدخول غير المشروع جريمة عمديه حيث يتخذ فيها الركن المعنوي صورة القصد الجنائي؛ أي توافر القصد الجنائي العام دون القصد الجنائي الخاص حيث لا تتطلب المادة 394 مكرر من قانون العقوبات الجزائري نية خاصة لدى الجاني حتى تقوم هذه الجريمة، ولابد من توافر عنصري العلم والإرادة[3].

ثانيا: جريمة الدخول غير المشرع في صورتها المشددة

فالملاحظ أن المشرع الجزائري شدد في العقوبة وجعلها مضاعفة بنص المادة 394 مكرر ق.ع إذا ترتب عن الدخول أو البقاء في النظام المعلوماتي حذف أو تغير لمعطيات المنظومة إذ نص في الفقرة2 من المادة المشار إليها على ما يلي: (تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة).

ويتضح من هنا أن الحرص على حماية نظام المعلوماتية لم يتوقف عند تجريم الدخول إليه أو البقاء فيه بل في مواجهة ما هو أخطر منها وهو ما يترتب عنها من نتائج ومنها:

1. حذف البينات أو المعطيات أو تغييرها.
2. تخريب نظام اشتغال المنظومة.

إن حصول عملية التحريف والتغيير أو التخريب في المنظومة تعد أبرز صور الجريمة لكونها تجسد الركن المادي للجريمة وتعطي انطباعا على بلوغ المجرم مبتغاه ويتجسد الركن المادي هنا بإحداث تغير في

---

[1] ونوغي نبيل. زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة، الجزائر المجلد الرابع – العدد الثالث – السنة سبتمبر2019، ص 133

[2] نفس المرجع، ص133

[3] غنية باطلي، المرجع السابق، ص166

البيانات وذلك بمحوها كليا أو جزئيا أو تشويهها بحيث تصبح غير صالحة للاستعمال في ذات الوقت يتحقق الركن المعنوي لهذه الجريمة بتوافر العلم بأن تتجه إرادة الجاني لتحقيق نتيجة تصرفه ومن ثم فإن جريمة الإتلاف والتخريب جريمة عمدية وهي لا تقتصر على تغير البينات بل قد تصل إلى تخريب نظام اشتغال المنظومة كلية كما تصورها نص المادة 394 مكرر ق.ع وبصدد ذلك ضاعف المشرع العقوبة.[1]

الفرع الثاني: جريمة الاعتداء العمدي على المعطيات وسير النظام.

أولا: جريمة الاعتداء العمدي على المعطيات.

نصت المادة 394 مكرر 1 من قانون 15/04 سالف الذكر " يعاقب بالحبس من 6 أشهر إلى3سنوات وبغرامة من 500.000دج إلى2.000.000دج،كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها." إن هذا الاعتداء يكون على مستوى محتوى المعالجة وليس على المستوى الوظيفي للمعطيات ويتضح هنا أن القانون الجنائي يحمي المعطيات نفسها. ويتجسد النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات في إحدى الصور الثلاثة وهي: الإدخال L'introductifonوالمحو (الإزالة) l'effacement أو التعديلModificationولا يشترط اجتماعهما، بل يكفي إحدى هذه الأفعال حتى يقوم الركن المادي مع عدم وجود التصريح بذلك وهذا ما يدل عنه مصطلح بطريق الغش.[2]

أما عن الركن المعنوي في جريمة الاعتداء العمدي على معطيات النظام جريمة عمديه لابد من توافر القصد الجنائي لدى مرتكبها. ويتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة.[3]

ثانيا: جريمة الاعتداء العمدي على نظام المعالجة.

تعتبر المنظومة المعلوماتية هدفا دائما للقراصنة نظرا لما تحتويه من معطيات هامة تتعلق بالأشخاص المعنوية أو الطبيعية، قصد استعمالها لأغراض متعددة عادة ما تكون بقصد تحقيق عوائد مالية أو الابتزاز أو التهديد.[4]

---

[1] زيبحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطبعة والنشر عين مليلة، الجزائر سنة الطبع 2011

[2] غنية باطلي المرجع السابق، ص173

[3] غنية باطلي، المرجع السابق، ص177

[4] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات قانون الإجراءات الجزائية، قوانين خاصة

والمشرع الجزائري لم ينص على هذه الجريمة وذلك للتشابه الكبير بينها وبين جريمة الاعتداء العمدي على المعطيات واستبعدها كجريمة قائمة بذاتها وجريمة الاعتداء العمدي على المعطيات بالإدخال أو الإزالة أو التعديل بالضرورة تؤدي إلى تعطيل النظام عن أداء وظيفته[1].

والركن المادي في فعل توقيف النظام عن أداء نشاطه ودوره المعتاد أي إعاقة أو تشويه عمل النظام المبرمج للمعطيات. ولا يشترط في فعل التعطيل كل عناصر النظام جملة بل يكفي أن يؤثر على أحد العناصر فقط وتتمثل صور الاعتداء على النظام فيما يلي:

1. **التوقيف أو الإعاقة أو التعطيل:Entrave**

ويقصد به تقييد حركة الحاسب الآلي على نحو يصيب نظامه بالشلل المؤقت وقد تكون الإعاقة مادية كأعمال العنف على أجهزة الحاسب الآلي المادية وشبكاته عن طريق تخريبها بالكسر أو التحطيم أو منع المستخدم من الاستفادة من خدمات النظام ، أو معنويا كالبرامج والمعطيات وذلك بإتباع التقنيات التالية: إدخال برنامج فيروسي والفيروس هو رمز معلوماتي Code informatique، يتم إدخاله عشوائيا إلى الجهاز ويمكن أن يتسبب في إرباك وظيفته، أو باستخدام قنابل منطقية أو بتعديل كلمة السر وهذا الإرباك يؤدي إلى تغير في حالة عمل النظام. [2]

2. **الإفساد و التعييب:Fausser** وتقنيات الإفساد والتعييب متعددة منها استخدام القنبلة المعلوماتية التي يمكن من خلالها إدخال معلومات تتكاثر داخل النظام وتجعله غير صالح للاستعمال.

وجريمة الاعتداء العمدي على سير عمل النظام جريمة عمديه يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة.

هذا بالإضافة إلى ذلك، هناك جريمة التعامل غير المشروع في معطيات صالحة لارتكاب جريمة، فهناك مجموعة من الأفعال الخطيرة التي نصت عليها المادة 394 مكرر 02 الفقرة الأولى من قانون العقوبات الجزائري وهذه الأفعال تشمل مختلف أشكال التعامل الواقعة على المعطيات، والتي قد تؤدي إلى استعمال واستخدام هذه المعطيات في جريمة أخرى.

بالإضافة إلى ذلك يوجد التعامل غير المشروع في معطيات محصلة من الجرائم، والتي نصت عليها الفقرة الثانية من المادة 394 مكرر02 من قانون العقوبات الجزائري على: «يعاقب.... كل من يقوم عمدا وعن طريق الغش ما يلي:

---

[1] غنية باطلي، المرجع السابق، ص179

[2] أنظر، غنية باطلي الجريمة الإلكترونية، ص179 ،180

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" فالجريمة تتحقق بواحدة من الأفعال المذكورة ولا يشترط اجتماع كل هذه الأفعال ويكفي توافر القصد العام لقيام هذه الجريمة دون القصد الخاص.[1]

المبحث الثاني: الجرائم المستجدة في الاتفاقية العربية ومسايرة التشريع الجزائري لها:

إن مفهوم جرائم تقنية المعلومات من المفاهيم الحديثة التي رافقت تطور تقنية المعلومات، بيد أن هذه التقنية وإن كان من الصعب حصر جميع إيجابياتها، أدت بدورها إلى ظهور العديد من الجرائم الإلكترونية العابرة للحدود التي لا يمكن لأي دولة القضاء عليها منفردة أو على الأقل الحد من انتشارها إلا بتعزيز جهود التعاون الدولي والإقليمي في المجال الأمني والقضائي والتقني .ورغبة من الدول العربية في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات وافق مجلس وزراء الداخلية والعدل العرب في اجتماعهما المنعقد في مقر الأمانة العامة لجامعة الدول العربية بالقاهرة على ما يسمى "الاتفاقية العربية لمكافحة جرائم تقنية

[1] أنظر غنية باطلي المرجع السابق، ص، ص 90،91.

المعلومات"(وقع على الاتفاقية بتاريخ 2010/12/21م بالقاهرة، وصادقت عليها الجزائر بموجب المرسوم الرئاسي رقم252/14 المؤرخ في 8 سبتمبر 2014م[1]

وأمام الصعوبات الكبيرة التي واجهت الدول في مكافحة الجريمة المعلوماتية عبر قوانينها الداخلية وفي مواجهة أصعب خاصية لها كونها جريمة متعدية للحدود، وجدت الدول نفسها مضطرة للانخراط في الحقل الدولي من إعلانات وعهود واتفاقيات دولية من أجل مكافحة الجريمة السيبريانية والجزائر بدورها انتهجت سياسة الانفتاح وصادقت على مجموعة من الاتفاقيات التي تخص هذا المجال، ولذلك يجدر بنا أن نتساءل ما الجديد الذي جاءت بيه الاتفاقية العربية (مطلب أول) وما مدى مسايرة التشريع الوطني للاتفاقية العربية (مطلب ثاني).

إن الاتفاقية العربية لمكافحة جرائم تقنية لمعلومات جاءت لتضيف آليات جديدة لمكافحة جرائم تقنية المعلومات خارج إقليم الدولة الواحدة، بما يشكل تعاونا بين الدول العربية في إطار جامعة الدول العربية.

ويقصد بالتعاون القضائي الدولي" مجمل الإجراءات التي تتخذها السلطات القضائية داخل الدولة بصدد جريمة محددة أو مجرمين محددين(متهمين أو محكوم عليهم) والمنصوص عليها في الاتفاقيات الدولية التي تكون الدولة طرفا فيها بمقتضى التشريعات الوطنية النافذة".

أكدت الاتفاقية العربية، في جريمة الدخول غير مشروع بتشديد العقوبة في حالة ما إذا ترتب عن فعل الدخول غير المشروع أو البقاء إضافة إلى فعل تعديل أو نسخ أو تدمير البيانات ووسائل تقنية المعلومات، الحصول على معلومات حكومية سرية وهذا جديد على المشرع الجزائري.[2]

جاءت أيضا بتجريم أفعال الاعتداء على نظام تقنية المعلومات عن طريق تجريم التزوير والاحتيال باستخدام تقنية المعلومات.

أما المشرع الجزائري فقد جرم الاحتيال المعلوماتي من خلال سنه للقانون رقم 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات[3] مما بين مدى الصعوبة التي واجهت المشرع في تطبيق نص جريمة النصب والاحتيال التقليدية على الاحتيال المعلوماتي، وتفاديا للإخلال بالمبادئ العامة للقانون الجنائي.

---

[1] الجريدة الرسمية للجمهورية الجزائرية، العدد 57،المؤرخة في28 سبتمبر 2014م

[2] أنظر، أحمد حمي، زهيرة كيسي، ص791

[3] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66/فالمشرع الجزائري لم يتطرق لأشكال من النص المادة156 المضمن لجرائم المساس بالأنظمة المعالجة الآلية للمعطيات، ج.ر عدد71ص8

ولكن المشرع الجزائري لم يتطرق لأشكال من النصب والاحتيال المعلوماتي بتصور وقوعها كالحصول على خدمة أو منفعة عبر شبكة الانترنت واستعمل فيها الجاني طرقا احتيالية للحصول عليها، فالملاحظ أن نص المادة 372 من قانون العقوبات الجزائري لا يمكن تطبيقه عن هذا الفعل مما يتيح استيعاب الاحتيال المعلوماتي الذي يقع للحصول على منفعة أو خدمة عبر شبكة الانترنت.

جرمت الاتفاقية العربية أفعال الاعتداء على نظام تقنية المعلومات عن طريق تجريم التزوير. فالركن المادي لجريمة التزوير التقليدية يتمثل في تغيير الحقيقة في المحرر بإحدى الطرق التي نص عليها المشرع إضرارا بالغير، أما في جريمة التزوير المعلوماتي فإن تغيير الحقيقة يتخذ صورتين تتمثل في إدخال معلومات غير صحيحة ينتج عنها مستند غير صحيح.[1]

ولقد اشترط المشرع في جريمة التزوير التقليدية أن يقع فعل تغير الحقيقة على محرر من المحررات العمومية أو الرسمية أو المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الإدارية والشهادات، كما اشترط المحرر أن يكون في شكل "كتابة" أوعبارات خطية، في حين أنه في جريمة التزوير المعلوماتي فإن المستند المعلوماتي هو الدعامة المادية التي تم تحويل المعطيات المعالجة عليها، فيكون إما قرص مضغوط أو شريط. أما بالنسبة للمشرع الجزائري فقد أدرج النصوص الخاصة بالتزوير في المحررات في المواد من 214 إلى 229 من قانون العقوبات التي تشترط المحرر لتطبيق جريمة التزوير، وعليه فإنه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير فالجديد.[2]

فالجديد الذي جاءت به الاتفاقية وجرمته هو التزوير المعلوماتي.

جاءت الاتفاقية بتجريم الاباحية بنص خاص مع تشديد العقوبة في حالة إباحية الأطفال والقصر، حيث تمثل جريمة الإباحية والجرائم المرتبطة بها خطرا بالغا على فئة الأطفال، حيث تشمل هذه الجرائم تحريض القصر وإغوائهم على أنشطة جنسية غير مشروعة عبر الوسائل الإلكترونية.

أما بالنسبة للمشرع الجزائري لم بنص على جرائم الإباحية الالكترونية، رغم انتشارها الواسع باستعمال تقنية المعلومات وخاصة تأثيرها البالغ على فئة القصر الذين تستهدفهم هذه الجرائم بشكل خاص وهذا رغم استحداث كل من مصالح الشرطة والدرك الوطني فرقا خاصة للتحقيق في الجريمة الالكترونية ضد الأطفال،

[1] معتوق عبد الطيف الإطار القانوني لمكافحة جرائم المعلوماتية في المشرع الجزائري والتشريع المقارن، المرجع السابق 2012،2011، ص49

[2] المرجع نفسه، ص47

بحيث تعمل هذه الفرق على تقفي العناوين الالكترونية للمواقع الإلكترونية عبر الأنترنت، والتي تحرض القصر على الدعارة انطلاق من شكاوى المواطنين.[1]

كما أن الفقرة 3 من المادة12 من الاتفاقية أشارت إلى جريمة الاستغلال الجنسي للأطفال والقصر عبر وسائل تقنية المعلومات حيث تقع الجريمة في وجود طفل أو قاصر من يتعدى سن الرشد حتى يكون محل عرض مرئي أو مسموع يتضمن عرضا للأعضاء الجنسية للطفل أو يقوم بارتكاب سلوك جنسي.

وتتضمن الأفعال المجرمة حيازة مواد إباحية للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

أما الجرائم الأخرى والمرتبطة بالإباحية لم تعرفها المادة 13 من الاتفاقية والمتمثلة في المغامرة حيث وردت بهذا اللفظ في نسخة الجريدة الرسمية العدد 57 وكلمة مغامرة وردت في النسخ الاخرى بلفظ المقامرة.[2]

والمقامرة مجرمة في جميع الدول العربية سواء بالطريقة التقليدية أو باستخدام وسائل تقنية المعلومات.

جاءت الاتفاقية بجديد تجريم جميع صور الجرائم المتعلقة بالإرهاب وتلك الجرائم المتعلقة بالجريمة المنظمة في حالة ارتكابها باستخدام تقنية المعلومات.

يمكننا القول إنه رغم تضمن قانون العقوبات للأفعال الموصوفة بالإرهاب، إضافة إلى قوانين أخرى كالقانون رقم:01-50 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما والقانون رقم :09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3] إلا أنها لم تتضمن النص صراحة على تجريم الإرهاب الإلكتروني.[4]

المطلب الثاني: مدى تماشي التشريع الجزائري مع الاتفاقية العربية.

لقد تعاظمت المصالح المرتبطة بمعطيات النظام في وقتنا الحاضر، إلى حد أصبح معه تدخل المشرع الجنائي أمر لا بد منه لحمايتها لتشتمل حماية، كل المعطيات مع تشديد الحماية منها على طوائف معينة تحظى بأهمية استثنائية، وتطال مختلف صور المعالجة ومواضيعها، وذلك بالنظر للخسائر الكبيرة التي باتت تهدد مصالح الأشخاص والدول من جراء هذه الجرائم.[5]

1يزيد بوحليط، المرجع السابق، ص282

2أحمد حمي زهيرة كيسي، المرجع السابق ص786

3في هذا الصدد، خوّل المشرع الجزائري بموجب المادة (04) من قانون رقم:09-04 لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من جرائم الإعلام و الاتصال المنصوص عليها بموجب المادة (13) من القانون نفسه، حق الرقابة الالكترونية على الأفعال ذات الصلة بجرائم الإرهاب و التخريب أو الجرائم الماسة بأمن الدولة، أو الاعتداء على منظومة معلوماتية بما يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، وما يلاحظ تضمن هذا النص على الرقابة الإلكترونية و لكن كفعل وقائي من هذه الجرائم و لم ينص صراحة على جرائم الإرهاب الإلكتروني بصفة مستقلة رغم تعدد أشكاله.

4يزيد بوحليط، المرجع السابق، ص ص 212-213

5الطيبي المرجع السابق، ص49

الأمر الذي أدى بالمشرع الجزائري إلى التدخل بوضع حماية جنائية موضوعية لهاته المعطيات من خلال عدة نصوص، بداية باستحداث القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المعدل بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 والقانون16-02 المؤرخ في19 يونيو سنة 2016، بمقتضى المواد من 394 مكرر إلى 394مكرر8 جرم من خلالها الاعتداءات الواردة على نظام المعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله من الجزاء.

وبالرغم من تداركه في هذا القانون(15-04) للفراغ القانوني في مجال الإجرام المعلوماتي، بتجريمه لكافة الاعتداءات التي تمس بنظم المعالجة الآلية للمعطيات من خلال هاته النصوص القانونية الخاصة، إلا أنه أغفل تجريم الاعتداءات الواردة على منتوجات الإعلام الآلي فلم يقم باستحداث نص خاص بالتزوير المعلوماتي ولم يتبنى الاتجاه الحديث الذي أخذت به التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

* كما قام بسن قانون09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها.

كما أصدر قانون رقم 18-07المؤرخ في 10 يونيو2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي يحوي مجموعة من الإجراءات التي تهدف المعطيات ذات الطابع الشخصي للشخص الطبيعي وتضمن عدم المساس بحياته الحاصلة، وكذا إنشائه للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي التي تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون.

كما اتجه المشرع إلى تجريم بعض أشكال الجرائم الالكترونية بموجب بعض القوانين الخاصة كقانون البريد والمواصلات السلكية ولا سلكية وقانون التأمينات الاجتماعية الذي نص على الجرائم المتعلقة بإساءة استخدام بطاقة الضمان الاجتماعي. إضافة إلى النص على الجرائم الخاصة بالتوقيع والتصديق الالكترونيين بموجب القانون رقم:15-04 المؤرخ في 2015/02/01يتعلق بالتوقيع والتصديق الإلكترونيين.

غير أن المشرع لم يساير بعض الجرائم الواردة في الاتفاقية العربية مثل جريمة التزوير المعلوماتي، جرائم إفساد النظام المعلوماتي، جريمة الترويج والاتجار بالمخدرات الرقمية، وعليه يجب على المشرع تدارك الفراغ التشريعي من خلال تعديل النصوص التقليدية أو مسايرة الاتفاقية العربية.

لم يجرم المشرع الجزائري كافة أشكال الإرهاب الإلكتروني، الذي أصبح لا يستغنى عن استعمال تقنية المعلومات حيث اقتصر المشرع على جريمة الإشادة بالأفعال الإرهابية التي تتم بأية وسيلة كانت.[1]

كما أضفى المشرع الحماية الجزائية على برامج الحاسوب وقواعد البيانات بموجب الأمر رقم 03-05 يتعلق بحقوق المؤلف والحقوق المجاورة بهدف حمايتها من جرائم التقليد.

لم يشترط المشرع لقيام الجريمة الالكترونية خضوع النظام المعلوماتي للحماية الفنية،حيث يهدف المشرع من وراء ذلك إلى إضفاء الجزائية على كافة أنظمة المعالجة الآلية للمعطيات بغض النظر عن تمتعها بالحماية الفنية أم لا.

لم يجرم المشرع الجزائري جريمة إفساد سير نظم المعالجة الآلية لمعطيات واكتفى بنصوص المواد (394 مكرر إلى 394 مكرر2) والمتمثلة في فعل اعتراض والتقاط المراسلات، التي تتم داخل النظام المعلوماتي أو بين مجموعة من الأنظمة، في حين جرمته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المادة (7)، لم يجرم المشرع الجزائري سرقة وقت الآلية للمعطيات، ربما اعتقد منه بأن الحماية الجنائية للمعطيات، هي حماية غير مباشرة للنظام المعلوماتي بموجب المادة(394 مكرر).[2]

وأخيرا برغم النقائص المسجلة يمكن القول أن المشرع الجزائري لا زال في مرحلة بناء لمنظومة جزائية فعالة ومتكاملة في مجال مكافحة الجرائم الالكترونية يسير في خطى ثابتة برغم التحديات الموضوعية الإجرائية التي يفرضها التعامل مع هذه البيئة الافتراضية حيث أن المشرع الجزائري يصادق على الاتفاقيات ولكنه يتأخر في تنفيذها.

[1] أنظر يزيد بوحليط، ص538

[2] يزيد بوحليط، مرجع نفسه، ص 539-540ا

الخاتمة

الخاتمة:

بعد الانتهاء من الدراسة والبحث في جرائم تقنية المعلومات وفقا لما ورد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، توصلنا إلى أنها حاولت التفريق لمختلف صور جرائم تقنية المعلومات حتى التي غفل عنها المشرع الجزائري، حيث حرصت على:

-تجريم الأفعال المرتكبة ضد أمن المعلومات من حيث سرية وسلامة تأخر البيانات والنظم، وتحديدا الدخول والاعتراض غير المشروعين، والاعتداء على سلامة البيانات وإساءة استخدام وسائل تقنية المعلومات.

-التطرق إلى طائفة من الجرائم التي ترتكب بواسطة تقنية المعلومات من خلال تجريم المحتوى غير المشروع المتمثل في الأفعال الإباحية، حيث نصت على تشديد العقوبة على كل ما يتعلق بإباحة الأطفال والقصر والجرائم الأخرى المرتبطة بالإباحية وهي المقامرة والاستغلال الجنسي، إضافة إلى تحريم الاعتداء على حرمة الحياة الخاصة.

-تحريم استخدام تقنية المعلومات في ارتكاب جرائم الإرهاب الجرائم المتعلقة بالجريمة المنظمة خاصة جرائم غسيل الأموال، جرائم الإتجار الأعضاء غير المشروع كالتجارة في المخدرات والمؤثرات العقلية، والتجارة بالأشخاص والأعضاء البشرية، وأخيرا التجارة غير المشروع بالأسلحة.

-النص على الجوانب الإجرائية ونطاق تطبيقها وآليات التعاون القضائي الدوليين في سبيل مكافحة جرائم تقنية المعلومات.

وبعد هذا التحليل الاتفاقية: يمكن الخروج بالنتائج التالية:

أولا: بخصوص الشكل العام للاتفاقية من حيث تبويبها وتقسيمها وأسماء الجرائم والمواد التي وردت فيها وهو ما سلكه المشرع الجزائري وذلك في القانون09 -04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحته.

ثانيا: حرصت الاتفاقية على بيان معاني المصطلحات الواردة من خلال شرحها وهو ما يخدم الشرعية الجزائية والتفسير الضيق للنص الجنائي.

ثالثا: بالنسبة للتجريم:

يتفق المشرع الجزائري في القانون 04-15 مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في تحريم صور جرائم تقنية المعلومات الآتية:

جريمة الدخول والبقاء غير المشروعين، جريمة الاعتداء على سلامة البيانات، جرائم إساءة استخدام وسائل تقنية المعلومات، إلى جرائم اعتداء على حرمة الحياة الخاصة وجرائم الإرهاب والمرتكبة بواسطة تقنية المعلومات.

رابعا: بخصوص الجوانب الإجرائية والتعاون الدولي، وأهم الأحكام التي حرصت الاتفاقية على بيانها هي:

1. التحفظ العاجل على البيانات المخزنة في تقنية المعلومات.
2. التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين.
3. أمر تسليم المعلومات.
4. التحفظ العاجل على البيانات المخزنة.
5. اعتراض معلومات المحتوى.

وهذا ما سار عليه المشرع الجزائري حيث نص أي القانون 04-05 تقريبا على نفس الإجراءات التي تضمنتها الاتفاقية.

وعليه يمكن الخروج بالتوصيات التالية:

1. ضرورة تكفل المشرع بسبق قوانين تحمي أدوات الدفع الالكتروني من الاستعمال غير المشروع كما ورد في نص المادة الثامنة عشر 18 من الاتفاقية العربية.
2. ضرورة الإسراع في سن قانون خاص يجمع بين الجوانب الموضوعية والجوانب الإجرائية لمكافحة جرائم تقنية المعلومات.
3. إمداد وتدريب قضاة متخصصين في الفصل في جرائم تقنية المعلومات.
4. ضرورة تخصيص مادة مستقلة تحرم نشر كل ما يتعلق بالاعتداء على الأديان بواسطة تقنية المعلومات مع تحديد صور الاعتداءات بشكل صريح.

قائمة المراجع والمصادر

Les Références

قائمة المراجع والمصادر: Les Références :

الاتفاقيات الإقليمية :

1. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

كتب القانون :

1 – القانون القطري، القانون رقم 14 لسنة 2014 يسمى قانون مكافحة الجرائم الإلكترونية، القانون الأردني رقم 27 لسنة 2015 المسمى قانون الجرائم الإلكترونية، قانون دولة فلسطين رقم)16 لسنة 2017 تحت اسم الجرائم الإلكترونية.

المراجع:

1. باطلي غنية، الجريمة الإلكترونية دراسة مقارنة، طبعة ،2015، منشورات الدار الجزائرية الجزائر 2015.
2. جعفر جاسم الطائي، جرائم تكنلوجيا المعلومات رؤية جديدة للجريمة، دار البداية الإصدار الثاني 2016.
3. حاجب هيام، الجريمة المعلوماتية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2005–2006.
4. زيبحة زيدان محامي معتمد لدى ا لمحكمة العليا وجلس الدولة–الجريمة المعلوماتية في التشريع الجزائري والدولي. دار الهدى عين مليلة –الجزائر.
5. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات قانون الإجراءات الجزائية، قوانين خاصة.
6. طارق الدسوقي، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

7. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكب عبر الوسائط الإلكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان الأردن.
8. عبد الغفور عبد الفتاح قاري، معجم المصطلحات، المكتبة والمعلومات إنجليزي – عربي، مكتبة الملك الوطنية، الرياض، 2000.
9. علي جابر الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع.
10. علي حسن الطوالبة، الجرائم الإلكترونية، الطبعة الأولى، جامعة العلوم التطبيقية، مملكة البحرين، 2008.
11. فيصل هاشم شمس الدين، تقنية المعلومات (ووسائل الاتصال، التوظيف، الثقافة)، الطبعة الأولى، شمس للنشر والتوزيع، القاهرة، 2008.
12. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والإنترنيت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 01 إلى 03 مايو .
13. محمود علم الدين، تكنولوجيا المعلومات وصناعة اتصال جماهيري، العربي للنشر والتوزيع، 3 ط، 1990.
14. نائل عبد الرحمان صالح، واقع جرائم الحاسب في التشريع الأردني، مؤتمر القانون والكمبيوتر والإنترنت، كليةالشريعة والقانون جامعة الإمارات العربية المتحدة، من الفاتح إلى 3 مايو2000.
15. نائلة محمد فريد قورة، جرائم الحاسب الآلي اللإقتصادية، دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية.
16. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، القاهرة، 1995.
17. هلالى عبد الإله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2006.

المجلات و المقالات:

1. محمد الصالح روان، الجريمة الدولية في القانون الدولي الجنائي، رسالة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2009/2008.

2. محمد أمين الشوابكة، جرائم الحاسوب والإنترنت،(الجريمة المعلوماتية،) ط 1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

3. محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة مقدمة استكمالا لمتطلبات الحصول درجة الماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2004.

4. أشرف محمد نجيب السعيد الرديني، جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، مجلة روح القوانين – العدد الخامس والتسعون–إصدار جويلية 2021 جامعة المنصورة.

5. ذياب موسى البدية، الجرائم الالكترونية (المفهوم والأسباب)، ورقة علمية مقدمة الى الملتقى العلمي الموسوم بـ: "الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية "، كلية العلوم الاستراتيجية، عمان الأردن،2014.

6. على التوالي، محمد علي سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الانسانية جامعة بابل، العراق، المجلد 14 العدد 3، 2008.

7. صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013.

8. الطيبي البركة، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة دكتورة الطور الثالث تخصص قانون جنائي، الحماية الجنائية لنظام المعالجة الآلية للمعطيات –دراسة مقارنة–السنة 2021/2020 .

9. عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائرية، مجلة الكوفى مركزة دراسات الكوفى، العدد 7، 2008.

10.مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسب بارتكابها، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، المجلد الثاني، العدد 1، 2014.

11. معتوق عبد الطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن(مذكرة ماجستير) كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر– باتنة

12. المعيني سرحان حسن، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، الإمارات، المجلد 20، العدد 79، أكتوبر 2011.

13. أحمد حمي، زهيرة كيسي–صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة2014المركز الجامعي لتامنغست، الجزائر–تاريخ الإسلام 2017/09/21–تاريخ القبول 2018/07/24، العدد 1.

14. ، صور الجرائم الإلكترونية واتجاهات تبويبها، ورشة عمل– تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات ، 2–4 أبريل2006مسقط، سلطنة عمان.

15. نسيم دردور ، جرائم المعلوماتية على ضوء القانون الجزائري و المقارن ، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي ،جامعة منتوري (قسنطينة) سنة 2013/2012.

16. عزيزة رابحي الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتورة في القانون كلية الحقوق والعلوم السياسية، جامعة أبو بكر بالقايد تلمسان الجزائر2018.

الموقع الالكتروني :

1– محمد ياسر أبو الفتوح، خصائص وتصنيفات الجريمة المعلوماتية، مقال منشور على الموقع الالكتروني: Almohakmoonalarab.ahlamontada.com/109–topic

قائمة المراجع باللغات الأجنبية

1. Parker (Done B) Figding computer crime A neur Framework for protecting information 1998/P 114

2. Sutherland (Eduin H) « White collar criminality » Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968.
3. Rose Philipe, la criminalité informatiqueque seis-je, 1ère edition, PU 1988, Page 490.
4. G. Delmare, sécurité informatique, ressources informatique, N°1. Comment se protéger contre le crime informatique, temps réels, 1984, Page 264.

فهرس المحتويات

فهرس المحتويات

شكر وعرفان 2

إهداء 3

إهــداء.....4

المقدمة:.....2

أهمية الدراسة: 3

أهداف الدراسة: 3

أسباب اختيار الموضوع: 4

منهج الدراسة:.....4

التقسيم المنهجي للدراسة:.....4

تمهيد 6

الفرع الأول: المقصود بالتقنية 7

الفرع الثاني: معنى المعلومات.....8

الفرع الثالث: تعريف تقنية المعلومات 8

المطلب الثاني: مفهوم جرائم تقنية المعلومات 9

الفرع الأول: تعريف جرائم تقنية المعلومات 9

الفرع الثاني: المصطلحات المستخدمة للدلالة على ظاهرة جرائم المعلومات.....12

الفرع الثالث: المقصود بجرائم تقنية المعلومات.....17

المبحث الثاني: مفهوم الاتفاقية العربية 2010 وخصائص وسمات الجريمة المعلوماتية.....19

المطلب الأول: التعريف بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 19

الفرع الاول : التعريف بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 19

الفرع الثاني: المصطلحات الواردة في الاتفاقية العربية لسنة 2010. 21

المطلب الثاني: خصائص وسمات الجريمة المعلوماتية 23

الفرع الأول: خصائص الجريمة المعلوماتية.....23

الفرع الثاني: السمات الخاصة بالمجرم المعلوماتي.....26
الفرع الثالث: دوافع الجريمة المعلوماتية.....30
تمهيد :.....34
المبحث الأول: صور جرائم تقنية المعلومات في ظل الاتفاقية والتشريع الجزائري.....36
المطلب الأول: صور جرائم تقنية المعلومات في الاتفاقية العربية 36
الفرع الاول: الجرائم التي تستهدف تقنية المعلومات. 36
الفرع الثاني: الجرائم التي تقع بواسطة تقنية المعلومات. 40
خامسا: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة.....45
سادسا:الاستخدام غير المشروع لأدوات الدفع الإلكترونية.....46
المطلب الثاني: صور جرائم تقنية المعلومات في التشريع الجزائري.....46
الفرع الأول: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.....47
الفرع الثاني: جريمة الاعتداء العمدي على المعطيات وسير النظام.....49
المبحث الثاني: الجرائم المستجدة في الاتفاقية العربية ومسايرة التشريع الجزائري لها: 51
المطلب الثاني: مدى تماشي التشريع الجزائري مع الاتفاقية العربية.....54
الخاتمة.....أ
قائمة المراجع والمصادر: 60
فهرس المحتويات 66
الملخص :.....68

الملخص :

نعيش اليوم عصراً جديداً من التقدم العلمي والتقني في مجال تكنولوجيا المعلومات والإتصالات، نتج عنه إحداث ثورة تنموية بشرية على جميع المستويات والأصعدة المحلية والعالمية، وأصبحت عملية تبادل المعلومات والمعارف تتم بسهولة ويسر ، وعلى جانب آخر فقد خلق هذا التطور التكنولوجي العديد من المخاطر والأضرار لا سيما وضعف الرقابة عليها مما أدى إلى ظهور نوع جديد من الجرائم المتطورة والتي تختلف عن سابقاتها من حيث طريقة وأسلوب ارتكابها وشكل وصفات المجرم وطباعه سميت بجرائم تقنية المعلومات وأصبحت تمثل تهديداً مباشر وواضحا للأمن والإستقرار المحلي والعالمي. وإزاء ذلك سعت العديد من الدول إلى تطوير نظمها التشريعية بما يتوافق مع ظاهرة الإجرام التقني الحديثة.

الكلمات المفتاحية: المعلوماتية؛ جرائم؛ الاتفاقية؛ المعالجة الآلية ؛ التشريع الوطني.

Résumé

Nous vivons de nos jours une nouvelle ère marquée par un progrès scientifique et technique dans les domaines des technologies d'information et de télécommunication, duquel il en résulte une révolution de développement humaines, sur différents niveaux sur le plan local autant qu'international. L'échange d'information et de connaissances est désormais une fortement accessible, par ailleurs, ces développements technologiques ont contribué à la création de nouvelles menaces et risques, notamment avec l'impossibilité de leur contrôle de façon permanente, ainsi, nous constatons de nouvelles pratiques criminelles de pointe très différente de leurs précédentes de part leur manière d'orchestration, et les caractéristiques du criminel. Des pratiques nommées conventionnellement « crimes de techniques d'information », lesquelles menacent directement de plus en plus la sécurité et la stabilité locales au même titre qu'internationale. Et face à cette situation, de nombreux états œuvrent inlassablement dans le but de mettre ces littératures et texte juridique au même diapason avec la criminalité technologique moderne.

Mot clé: informatique ; cimes ;convention; traitement automatise ; la législation nationale

Abstract :

We are now living in a new era marked by scientific and technical progress in the fields of information and telecommunication technologies, which resulted in a revolution of human development on different levels locally as well as internationally. The exchange of information and knowledge is now highly accessible, moreover, these technological developments have contributed to the creation of new threats and risks, in particular with the impossibility of their permanent control, thus, we are seeing new advanced criminal practices very different from their previous ones in their way of orchestrating, and the characteristics of the criminal. Practices conventionally called "information technology crimes", which increasingly and directly threaten local and international security and stability. Faced with this situation, many states are working tirelessly to bring these laws and legal texts in line with modern technological crime.

keywords: informatics ; cimes ;convention; automated pracessing ; national législation