صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014

Types of information technology crimes according to Arab convention 2014

طالب الدكتوراه/ أحمد حمي *
المركز الجامعي لتامنغست، الجزائر
hemmi1972@gmail.com
الأستاذة/ زهيرة كيسي
المركز الجامعي لتامنغست، الجزائر
zahkis@gmail.com

تاريخ الاستلام: 2017/09/21 تاريخ القبول للنشر: 2018/07/24

❖❖❖❖❖❖❖

ملخص:

لقد 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 الجرائم تقنية المعلومات. وذلك سواء تعلق الأمر بالمساس بتقنية المعلومات في حد ذاتها أو بارتكاب جرائم تقليدية باستعمال الوسائل التكنولوجية الحديثة والمتمثلة في تقنية المعلومات.

من خلال هذا العمل سنقوم بعرض مختلف هذه الصور الإجرامية مع الوقوف عند كل جريمة.

الكلمات المفتاحية: تقنية المعلومات؛ المعلوماتية؛ جرائم؛ الاتفاقية؛ المعالجة الآلية.

Abstract:

The Algerian criminal code in section 7 bis, chapter 3, enlists a set of acts compromising the automatic processing of information also called the cybercrime. Besides, the Arab Treaty on Combating Cybercrime 2010 brought out another array of offences involving information technology, both compromising the information technology itself, and committing traditional crimes using modern technological means namely IT.

In the present paper different forms of offences shall be brought to light and considered, each, in greater details.

Key words: *information technology; Informatics; crimes; convention, automated treatment.*

* المؤلف المراسل.

مقدّمة:

تعد "تقنية المعلومات" من السمات المميزة لهذا العصر ، ويقصد بها كل وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لاسلكيا في نظام أو شبكة"[1].

إن مفهوم جرائم تقنية المعلومات من المفاهيم الحديثة التي رافقت تطور تقنية المعلومات، وهي جرائم عابرة للحدود، حيث إنها أصبحت تهدد أمن ومصالح الدول العربية وسلامة مجتمعاتها، ورغبة منها- 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 يسمي" الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"[2]. وصادقت الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي رقم 14-252 المؤرّخ في 8 سبتمبر سنة 2014.

حيث ألزمت المادة الخامسة من الاتفاقية كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها وذلك وفقا لتشريعاتها وأنظمتها الداخلية ومنه نطرح الاشكال الآتي:

ما هي صور جرائم تقنية المعلومات التي نصت عليها الاتفاقية العربية لسنة2014؟

ترجع أهمية البحث في جرائم تقنية المعلومات إلى الدور المهم الذي تلعبه تقنية المعلومات في الوقت الراهن نظرا للتطوّر المستمر والدائم لتكنولوجيا المعلومات، ولخطورتها ومدى انتشارها ومن ثم يلزم تعاون دولي لمكافحتها وبيان الدور الذي تلعبه الاتفاقيات الدولية في مكافحتها والحدّ منها ومنع انتشارها.

وتهدف هذه الدراسة إلى عرض ودراسة صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، وذلك من خلال تحليل ما تضمنه الفصل الثاني منها من نصوص في شكل مواد تتضمن مجموعة من الأفعال التي تعبر عن جرائم تقنية المعلومات من أجل بيان الحلول التي استقاها لها المشرع العربي لمكافحة تلك الجرائم.

وتكمن صعوبات الدراسة في قلة البحوث والدراسات التي تناولت موضوع صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة2010، مما نتج عنه انعدام المراجع القانونية المتخصصة في هذا الشأن، لذلك سنكتفي بعرض وتحليل نصوص الاتفاقية ومقارنتها بنصوص قانونية أخرى، بالاعتماد على المنهج التحليلي الوصفي المقارن المناسب لدراسة وتحليل النصوص القانونية، وذلك من خلال مبحثين:

المبحث الأول: الإطار المفاهيمي للاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

المبحث الثاني: الجرائم المنصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

المبحث الأول

الإطار المفاهيمي للاتفاقية العربية لمكافحة جرائم تقنية المعلومات

نتطرق في هذا المبحث إلى كل من تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتحديد أهدافها (المطلب الأول) ثم سنتناول الأحكام العامة للاتفاقية (المطلب الثاني).

المطلب الأول: تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وأهدافها

نتناول في هذا المطلب تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (الفرع الأول)، ثم أهدافها (الفرع الثاني).

الفرع الأول: تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

عرفت اتفاقية فينّا لقانون المعاهدات الاتفاقية بأنها عبارة عن "اتفاق دولي يعقد بين الدول في صيغة مكتوبة والذي ينظمه القانون الدولي، سواء تضمنته وثيقة واحدة أو وثيقتان متصلتان أو أكثر ومهما كانت تسميته الخاصة"[3]. وباعتبار (تحذف هذه الكلمة) والمعاهدات الدولية نوعان:

- **معاهدات عقدية:**

وهي التي تعقد بين شخصين أو أكثر من أشخاص القانون الدولي العام، الغرض منها تنظيم العلاقات بين الدول على حسب الطرق التي تراها مناسبة.

- **ومعاهدات شارعة:**

وهي تلك التي تضع تشريعا يكون ملزما لأكثر من شخص من أشخاص القانون الدولي وتسمى أيضا المعاهدات الجماعية، ولهذه الأخيرة أربعة أنواع:

- **المعاهدات القارية:**

هي التي تضم مجموعة من الدول في قارة واحدة كالاتحاد الإفريقي مثلا.

- **المعاهدات الخاصة:**

تلك التي تضم مجموعة من الدول تتمتع بمواصفات معينة، مثال الدول المصدرة للنفط (أوبيك).

- **المعاهدات الجماعية:**

وهي التي تضم جميع الدول أو غالبيتها مثل ميثاق الأمم المتحدة.

- **المعاهدات الدولية الإقليمية:**

وهي التي تضم مجموعة من الدول تقع في قارة أو أكثر مثل ميثاق جامعة الدول العربية وكذلك المعاهدات والاتفاقات المعقودة في نطاقها، ومن المعاهدات المعقودة في نطاق جامعة الدول العربية الاتفاقية العربي لمكافحة جرائم تقنية المعلومات[4].

مما سبق يمكن تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنها الاتفاق الدولي الإقليمي المعقود بين الدول العربية في نطاق جامعة الدول العربية بصورة خطية في أكثر من وثيقة والذي وافق عليه مجلس وزراء الداخلية والعدل العرب في اجتماعهما المنعقد في مقر الأمانة العامة لجامعة

الدول العربية بتاريخ 2010/12/21 م بالقاهرة وتسميته "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات".

وتتكون الاتفاقية من ديباجة و ثلاثة وأربعين (43) مادة موزعة على خمسة (5) فصول كما يأتي:

الفصل الأول: أحكام عامة من المادة الأولى إلى المادة الرابعة.

الفصل الثاني: التجريم من المادة الخامسة إلى المادة 21.

الفصل الثالث: الأحكام الإجرائية من المادة 22 إلى المادة 29

الفصل الرابع: التعاون القانوني القضائي من المادة 30 إلى 43.

الفرع الثاني: أهداف الاتفاقية

حددت الهدف من الاتفاقية كل من ديباجتها والمادة الأولى منها، حيث جاء في الفقرة الأولي والثانية من الديباجة، أن الدول العربية الموقعة على الاتفاقية "رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها.

واقتناعا منا بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات" فإن الاتفاقية تهدف إلى:

- تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات،

- درء أخطار جرائم تقنية المعلومات حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[5].

المطلب الثاني: الأحكام العامة للاتفاقية

سنتكلم في هذا المطلب عن مجالات تطبيق الاتفاقية (فرع أول)، والمصطلحات المستعملة فيها (فرع ثاني).

الفرع الأول: مجالات تطبيق الاتفاقية وصون سيادة الدول

لقد نصّت الاتفاقية على المجال الذي تطبق فيه، وذلك مع ما يتفق مع مبدأ سيادة الدول وعدم التدخل في الشؤون الداخلية.

أولاً- مجالات تطبيق الاتفاقية:

حددت الاتفاقية العربية لمكافحة تقنية المعلومات مجال تطبيقها في المادة الثالثة(3) منها حيث نصّت على أنها تنطبق على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية:

- إذا ارتكبت في أكثر من دولة.

- إذا ارتكبت في دولة وتم الاعداد أو التخطيط لها أو توجيهها أو الاشراف عليها في دولة أو دول أخرى.

- إذا ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطتها في أكثر من دولة.

- إذا ارتكبت في دولة وكانت لها أثار شديدة في دولة أو دول أخرى.

ثانياً- صون السيادة الدولية:

نصت الاتفاقية في المادة الرابعة (4) على:

أ- تلتزم كل دولة طرف وفقا لنظامها الأساسي أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

ب- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفرع الثاني: المصطلحات المستعملة[6].

إن إيراد تعاريف المصطلحات لأغراض هذه الاتفاقية، يبدد اللبس ويساعد على الفهم الصحيح لجرائم تقنية المعلومات، فيقصد بالمصطلحات الآتية في هذه الاتفاقية التعريف المبيّن لكل منها:

1- تقنية المعلومات:

أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبط بها سلكيا أو لاسلكيا في نظام أو شبكة[7].

2- مزود الخدمة:

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:

ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها...

4- البرنامج المعلوماتي:

مجموعة من التعليمات والأوامر قابلة لتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.

5- النظام المعلوماتي:

مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

6- الشبكة المعلوماتية:

ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

7- الموقع:

إمكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

8- الالتقاط:

مشاهدة البيانات أو المعلومات أو الحصول عليها.

9- المعلومات المشترك:

أية معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:

أ) نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمات.

ب)هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه ومعلومات الدفع المتوفرة بنا علي اتفاق أو ترتيب الخدمة.

ج) أية معلومات أخرى عن موقع تركيب معدات الاتصال بنا على اتفاق الخدمة.

المبحث الثاني

الجرائم المنصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

في هذا المبحث سوف نقسم الجرائم المنصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى قسمين، القسم الأول يحتوى على الجرائم التي تستهدف نظام ووسائل تقنية المعلومات (المطلب الأول)، أما القسم الثاني فهو للجرائم التي ترتكب باستعمال تقنية المعلومات (المطلب الثاني).

المطلب الأول: الجرائم التي تستهدف تقنية المعلومات

نصّت الاتفاقية محل البحث عن الجرائم التي تستهدف تقنية المعلومات في المواد 06 إلى 11 منها، والتي سوف نتطرق إليها من خلال الفروع الآتية:

الفرع الأول: جريمة الدخول غير المشروع

نصت المادة السادسة (6) من الاتفاقية العربية لسنة2010 على جريمتين، جريمة الدخول أو الاتصال غير المشروع وجريمة البقاء او الاستمرار في الاتصال مع كل أو جزء من تقنية المعلومات.

أولاً- جريمة الدخول أو الاتصال غير مشروع:

يعرف الدخول أو الاتصال غير مشروع بأنه: "الولوج والاتصال بكل أو جزء من نظام 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[8].

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[9].

والدخول يتحقق وينتهي عند تحقق الاتصال بتقنية المعلومات بحيث يكون الكل او الجزء الذي تم الاتصال به مفتوحا بعدما كان مغلقا، والاتصال يكون عن بعد بوسائل اتصال لاسلكية بين الوحدة التي تعد أداة الجريمة وبين تقنية المعلومات.

وتجدر الإشارة في هذا الصدد إلى أن جريمة الدخول أو الاتصال إلى تقنية المعلومات جريمة قصديه، تقوم بالقصد الجنائي العام، أي بتوافر العلم والإرادة، حيث يكفي أن يعام الجاني أنه يدخل أو يقوم بالاتصال غير مشروع بنظام تقنية معلومات خاصة بالغير دون أن يكون له الحق في ذلك[10].

ثانياً- جريمة البقاء او الاستمرار في الاتصال:

ويقصد به التواجد داخل النظام المعلوماتي ضد إرادة وعلم من له الحق في السيطرة على هذا النظام[11]. وهذه الجريمة منصوص عليها في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 1/6 ويتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة البقاء او 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[12].

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:

أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

ب) الحصول على معلومات حكومية سرية[13].

الفرع الثاني: جريمة الاعتراض غير مشروع

هذه الجريمة منصوص عليها في المادة الثامنة من قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها[14].

كما نصت عليها المادة الثالثة من اتفاقية بودابست لسنة 2001 حول الاجرام المعلوماتي وحددتها 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 بيانات تقنية المعلومات"

وهذه الجريمة يمكن استخلاصها من استقراء المادة 394 مكرر 2 من قانون العقوبات الجزائري، حيث يمكن استخلاص منها فعل إعاقة أو اعتراض طريق نظام المعلومات أو المعطيات المرسلة عن طريق نظام المعلوماتية بغرض قرصنتها والاتجار فيها[15].

الفرع الثالث: الاعتداء على سلامة البيانات

جريمة الاعتداء على سلامة البيانات نصت عليها المادة الثامنة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتقابلها المادة الرابعة (4) من اتفاقية بودابست لسنة 2001 حول الاجرام المعلوماتي.

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

الصورة الأولى: أن يتم محو البيانات والمعلومات كليا وتدميرها إلكترونيا.

الصورة الثانية: أن يتم تشويه البيانات والمعلومات أو البرامج عن طريق إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق[16] وهي جريمة قصدية.

الفرع الرابع: جريمة إساءة استخدام وسائل تقنية المعلومات

جريمة إساءة استخدام وسائل تقنية المعلومات معاقب عليها في قانون جرائم تقنية المعلومات لدولة عمان، حيث أن المادة 11منه تنص على أن "يعاقب بالسجن ...كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو بيع وشراء أو استيراد أو توزيع أو عرض أو إتاحة برامج أو أدوات أو أجهزة مصممة أو مكيفة لأغراض ارتكاب جرائم تقنية المعلومات أو كلمات سر أو رموز تستخدم لدخول نظام معلوماتي0، أو حاز أدوات أو برامج مما ذكر، وذلك بقصد استخدامها في ارتكاب جرائم تقنية المعلومات"[17].

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد نصت على الافعال المادية المكونة لهذه الجريمة حيث نصت المادة التاسعة أن جريمة إساءة استخدام وسائل تقنية المعلومات تتحقق متى ما ارتكبت الأفعال الآتية: "

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

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

ب) كلمة سر نظام معلومات أو شيفرة 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.

الفرع الخامس: جريمة التزوير

يعرف التزوير بأنه تغير الحقيقة في محرر بالطرق التي حددها القانون تغيرا من شأنه أن يرتب ضررا للغير، وبنية استعمال هذا المحرر فيما أعد له[18].

ومفهوم التزوير في مجال جرائم تقنية المعلومات، هو "تغير الحقيقة في البيانات باستخدام وسائل تقنية المعلومات تغيرا من شأنه ان يرتب ضررا وبنية استعمالها كبيانات صحيحة"[19].

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

العنصر الأول: تغير الحقيقة

تغير الحقيقة في جرائم تقنية المعلومات يتخذ شكلين:

- الشكل الأول منهما يتم بالتلاعب في المعلومات المخزنة في تقنية المعلومات.
- والشكل الاخر يتمثل في إدخال معلومات غير صحيحة ينتج عنها مستند غير صحيح[20].

العنصر الثاني: أن يقع التزوير في محرر أو مستند معلوماتي

حسب نص الاتفاقية العربية لمكافحة تقنية المعلومات فإن التزوير يقع في البيانات بغرض تغير حقيقتها.

العنصر الثالث: أن يقع تغيير الحقيقة بإحدى طرق التزوير

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

- 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 علي أراء الفقيه "جارو" يرى هذا الفريق عدم قيام الضرر في التزوير المعلوماتي إلا إذا انصبّ التزوير على وثيقة قانونية لها بعد قانوني، بينما يرى الفريق الأخر أنه كلما كانت هناك خسارة فالضرر قائم، فربط هذا الفريق بين فكرة الضرر في التزوير المعلوماتي والخسارة الناتجة عن التزوير ولا يهم أن تكون الوثيقة معدة للإثبات أم لا[21].

الفرع السادس: جريمة الاحتيال

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 للبيانات ونقلها[22].

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

1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

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

3- تعطيل الأجهزة والبرامج والمواقع الالكترونية".

تعرف جريمة الاحتيالl'escroquerie بأنها الاستيلاء على مال مملوك للغير بخداعه وحمله على تسليم ذلك المال[23]. أو بأنها: "استعمال الجاني وسيلة من وسائل التدليس المحدد على سبيل الحصر وحمل المجني عليه بذلك على تسليم الجاني مالا مملوكا للغير".

إن السلوك الإجرامي المشكل للركن المادي في جريمة الاحتيال المعلوماتي يتمثل في المعلومات والوسائل الاحتيالية التي يلجأ إليها الجاني والتي تتمثل في التلاعب في معطيات ومعلومات تقنية المعلومات المخزنة، وقد أوردت التوصية رقم 89/R9 للمجلس الاوربي تعريفا للاحتيال المعلوماتي أقرته الأمم المتحدة وبينت من خلاله السلوك الاجرامي للاحتيال المعلوماتي وجاء فيه بأنه الادخال أو المحو أو التعديل أو كبت البيانات أو برامج الحاسوب او التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية لشخص

أخر بقصد الحصول على منفعة اقتصادية غير مشروعة له[24]. والاتفاقية العربية لم تعرف الاحتيال في مجال تقنية المعلومات واكتفت ببيان الأفعال المشكلة للسلوك الإجرامي والمتمثلة في:

1- إدخال أو تعديل أو محو أو حجب للمعلومات و البيانات .

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

3- تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

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

- أما النتيجة الإجرامية: هي التسليم؛ بالرغم من أن فكرة تسليم المال تثير إشكالية التسليم المادي للمال، إلا أن نظرية التسليم المعادل التي أرستها محكمة النقض الفرنسية حلت الإشكال القائم، حيث نجد أن تطبيق هذه النظرية في حالة التحويل بواسطة تقنية المعلومات للأموال أمر مقبول ويعتبر هذا التحويل تسليما للمال[25] .

وتجدر الإشارة هنا إلى أن جريمة الاحتيال المعلوماتي جريمة عمدية صورة، الركن المعنوي فيها هو القصد الجنائي العام والقصد الجنائي الخاص والمتمثل في نية التملك[26].

المطلب 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:

الفرع الأول: جريمة الإباحية

لقد وفرت شبكة تقنية المعلومات أكثر الوسائل فاعلية وجاذبية لصناعة ونشر الإباحية، حيث جعلت الإباحية بشتى وسائلها من أفلام وصور وفيديوهات و حوارات سواء كانت مباشرة أو مسجلة في متناول الجميع وتحاول المواقع الإباحية بهدف الربح المادي أن تسهل عملية الدخول إلي مواقعها وتحميل الأفلام الإباحية منها[27]. وهذه الجريمة اتخذت أشكالا متعددة نتيجة لمسايرتها لتقنية المعلومات، كإنشاء المواقع الإباحية. كما توجد شبكات ومنظمات إجرامية تقوم بنقل حفلات وعروض إباحية مباشرة أو مسجلة للترويج للإباحية وتكون موجهة في الغالب إلي شريحة الشباب ومقابل عمولات مالية، مما جعل هذه الصورة من الإباحية تتطور وتتحول إلي إباحية إلكترونية عبر وسائل تقنية المعلومات[28].

وحسب ما ورد في الاتفاقية العربية لمكافحة تقنية المعلومات، فإن الافعال المشكلة للركن المادي لهذه الجريمة هي:

إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

كما أن العقوبة تشدد إذا تعلقت بإباحية الاطفال القصر.

كما ان الفقرة 3 من المادة 12 من الاتفاقية أشارت إلي جريمة الاستغلال الجنسي للأطفال والقصّر عبر وسائل تقنية المعلومات حيث تقع الجريمة وجود طفل أو قاصر لم يتعد سن الرشد حتى يكون محل عرض مرئي أو مسموع بتضمن عرضا للأعضاء الجنسية للطفل أو يقوم بارتكاب سلوك جنسي.

وتتضمن الافعال المجرمة حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء 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 الأخرى[29] بلفظ المقامرة. والمقامرة مجرمة في جميع الدول العربية سواء بالطريقة التقليدية أو باستخدام وسائل تقنية المعلومات. حيث أن جريمة المقامرة تتم عبر شبكة الانترنيت بتنظيم ألعاب القمار عبر تملك وإدارة مشروع للمقامرة على الإنترنت مثال ذلك: ما يعرف الآن ببطاقات الاشتراك في برنامج البنتاغون، وهو عبارة عن برنامج اشتراك مالي يصبح فيه الفرد رابحا إذا تمكن من إحضار عدد من المشتركين ويزداد ربحه كلما احضر مشتركين جدد. وهو برنامج تسهل فيه مشاريع إدارة القمار على الإنترنت أو تشجيع مشاريع المقامرة عبر الإنترنت، واغلب مواقع القمار موجودة في حوض الكاريبي وجزر انتيجوا وجمهورية الدومينيكان، هذا حسب ما كشفت عنه شرطة F. B. I في امريكا . بعد متابعة لمواقع الانترنت التي تقوم بالمقامرة[30].

أما الاستغلال الجنسي الذي ورد في نص المادة 13 من الاتفاقية فيكون غالبا من نتائج الاتجار بالبشر من النساء والاطفال بغرض الاكراه على ممارسة الدعارة. علما أن المشرع الجزائري جرم فعل الوسيط في ممارسة الدعارة والإباحية وذلك في المواد 343 إلي 345 من قانون العقوبات والسماح للغير تعاطي الدعارة [31] ولم يحدد ما إذا كانت عبر وسائل المعلوماتية أو شبكة الأنترنت.

الفرع الثاني: جريمة الاعتداء على حرمة الحياة الخاصة.

جريمة الاعتداء على حرمة الحياة الخاصة منصوص عليها في المادة 14 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث أن غالبية الدساتير تكفل حق الشخص في حماية حياته الخاصة. إلا ان هذا الحق قد ينتهك عندما يتم نشر معلومات أو صور تتصل بحرمة الحياة الخاصة للأفراد حيث أتاحت شبكات تقنية المعلومات إمكانية الوصول إلي البيانات الشخصية و المعلومات الخاصة السرية للأفراد أو لعائلاتهم.

وقد عاقب المشرع الجزائري على الاعتداء على الحياة الخاصة في المادة 303 مكرر[32] من قانون العقوبات "يعاقب بالحبس من ستة اشهر إلي ثلاثة سنوات وبغرامة من 50.000 دج إلي 300.000 دج وذلك اذا قام بالتقاط أو تسجيل أو نقل مكلمات أو احاديث خاصة أو سرية أو نقل صورة لشخص في مكان خاص بغير اذن صاحبها او رضاه. كما ان المادة 303 مكرر1 تعاقب بنفس عقوبة المادة 303 مكرر كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغر أو استخدم بأي وسيلة كانت

التسجيلات أو الصور الوثائق المتحصل عليها بواسطة أحد الافعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

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

- جمع وتخزين بيانات شخصية صحيحة بدون ترخيص:

وتحقق هذه الصورة بالجمع والتخزين لبيانات شخصية تخص أشخاصا 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 للبيانات 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[33].

- الإفشاء غير المشروع للبيانات الشخصية:

يعد إفشاء البيانات الشخصية السرية سواء تم عن طريق الخطأ أو لغير الهدف الذي جمعت له اعتداء يمس الحياة الخاصة للإنسان ،[34] ومن أمثلة ذلك، المعلومات المتحصل عليها من عملية الإحصاء السكاني لا يجوز استعمالها لغير هذا الهدف ولو كان مشروعا مثل استعمالها في الأغراض الضريبية نظرا لاستعمالها في غير الإطار المحدد الذي جمعت من أجله المعلومات[35].

- استخدام بيانات شخصية غير صحيحة:

وهي الصورة التي يتم فيها استخدام بيانات الأفراد على وجه غير صحيح على نحو غير مشروع، ويكون في الغالب التلاعب بالبيانات 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 الأمريكية "trw company credit " هذه الشركة متخصصة 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 مائة (100) شخص من الأفراد سيئي الوضع المالي[36].

الفرع الثالث: الجرائم المتعلقة بالإرهاب والمرتكب بواسطة تقنية المعلومات.

عرفت المادة الأولى من اتفاقية جنيف لسنة 1937 الظاهرة الإرهابية بأنها: "الأعمال الإجرامية الموجهة ضد الدولة، وتهدف إلى إحداث حالة من الرعب في أفكار أشخاص معينين أو مجموعة من الناس أو لدى العامة.

ونصت 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 أياً كانت بواعثه أو أغراضه، يقع

تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر[37].

إن جرائم الإرهاب المرتكب بواسطة تقنية المعلومات يتميز عن غيره من أنواع الارهاب بالطريقة المستحدثة في استخدام وسائل تقنية المعلومات.

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

1- نشر أفكار ومبادئ جماعة إرهابية والدعوة لها.

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

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

4- نشر النعرات والفتن ولاعتداء على الاديان والمعتقدات.

كل هذه الافعال المجرمة تتم بواسطة تقنية المعلومات.

- الجرائم المتعلقة بالجريمة المنظمة والمرتكبة بواسطة تقنية المعلومات:

إن الجريمة المنظمة المرتكبة بواسطة تقنية المعلومات تشمل الجرائم الآتية:

أ- **جريمة غسيل الأموال**[38]:

ويقصد بغسيل الأموال أو تبييض الأموال وهي العبارة التي استعملها المشرع الجزائري في قانون العقوبات ب"إخفاء المصدر الإجرامي للممتلكات والأموال، لاسيما ما يسمى بـ المال القذر وتمر عملية التبييض تقنيا بثلاث مراحل، توظيف المال، التمويه والإدماج[39]. 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 لا بد من تحقق 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 إجراء عمليات مصرفية لتحويل الأموال وتكون عبر وسائل تقنية المعلومات كتحويل من حساب إلى أخر عن طريق شبكة الانترنيت، 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 اخفاء المصدر غير المشروع لهذه الأموال، أو تمويه المصدر غير المشروع لتلك الممتلكات[40].

ب- جريمة الترويج للمخدرات والمؤثرات العقلية أو الاتجار بهما.

إنّ جريمة الاتجار بالمخدرات والمؤثرات العقلية مجرمة في أغلب التشريعات الوطنية والدولية، ومن بين الاتفاقيات الدولية؛ الاتفاقية الموحدة المتعلقة بالمخدرات لسنة1961 والمتممة باتفاقية المؤثرات العقلية لسنة 1971 واتفاقية الامم المتحدة المتعلقة بمكافحة الاتجار غير مشروع بالمخدرات والمؤثرات العقلية بفينّا سنة 1988، وفي الجزائر صدر القانون 18/04 المؤرخ في 2004/12/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بهما.

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

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

ج- 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".

د- جريمة الاتجار بالأعضاء البشرية:

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 مكرر29[41].

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

- جريمة انتزاع عضو أو نسيج أو خلايا من جسم شخص بمقابل أو منفعة (المادة 303مكرر16).
- جريمة الحصول على عضو من جسم دون موافقة صاحبه(المادة 303مكرر17).
- جريمة عدم التبليغ عن جريمة الاتجار بالأعضاء البشرية (المادة 303مكرر25).

الفرع الرابع: جرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة

ورد النص على هذا النوع من الجرائم في المادة17 من الاتفاقية العربية محال البحث حيث جاء فيها "انتهاك حق المؤلف كما هو معرف 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 ولغير الاستعمال الشخصي".

إنّ 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.

وقد نصت أغلب التشريعات المقارنة على هذه الجرائم ضمن أحكام القوانين الخاصة بالملكية الفكرية كفرنسا المادة L335 -2 من قانون حماية الملكية الفكرية التي نصت على جنحة التقليد؛ كتقليد مصنف أدبي مكتوب أو موسيقي أو رسم وغيرها من الاعمال الفنية ذكرتهم المادة . كما جرمت المادة L335 -3 إعادة إنتاج أو توزيع وبأي طريقة كانت مصنف محمي بموجب قانون الملكية الفكرية كما نصت المادة L112 -1على حماية البرامج المعلوماتية وأقر حماية تمتد لمدة 15 سنة من تأريخ اختراعها حسب نص المادة L123 -5[42].

وفي الجزائر فإن المشرع ذكر الأفعال التي تشكل جريمة التقليد، وذلك في المادة 151 من الأمر 03-05 [43] المتعلق بحماية حقوق المؤلف والحقوق المجاورة على أنه: "يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف .
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة .
- استيراد أو تصدير نسخ مقلدة من مصنف أو اداء.
- بيع نسخ مقلدة لمصنف أو اداء.
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو اداء.

كما نصت المادة 152 من الامر 03-05 أنه: "يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الاداء عن طريق التمثيل أو الاداء العلني أو البث الاذاعي السمعي أو السمعي البصري أو التوزيع بواسطة الكابل أو بأية وسيلة نقل اخري لإشارات تحمل اصوتا أو صورا أو باي منظومة معالجة معلوماتية" وعاقبة المادة 153 من نفس الأمر على جنحة التقليد بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 إلى 1.000.000 دج.

الفرع الخامس: الاستخدام غير المشروع لأدوات الدفع الإلكترونية

هذه الجريمة كانت نتيجة لعملية ارتباط التجارة بوسائل تقنية المعلومات وهو ما يعرف بالتجارة الإلكترونية، حيث ازدادت جرائم الاستخدام غير المشروع لأدوات الدفع الإلكترونية.

ومن وسائل الدفع الإلكترونية 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[44].

وتعدد الجرائم التي تقع على هذا النوع من وسائل الدفع[45] فحسب المادة 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فإن السلوك الاجرامي يتمثل في:

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

- كل من استولى على بيانات أي اداة من ادوات الدفع واستعملها أو قدمها للغير أو سهل للغير الحصول عليها.

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

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

الخاتمة:

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

حيث تضمنت هذه الاتفاقية جرائم تستهدف وسائل تقنية المعلومات وأخرى جرائم تقليدية ترتكب بواسطة تقنية المعلومات.

وبعد دراسة وتحليل مواد هذه الاتفاقية يمكن الخروج بالنتائج التالية:

- حرصت الاتفاقية العربية، في جريمة الدخول غير مشروع بتشديد العقوبة في حالة ما إذا ترتب عن فعل الدخول غير المشروع أو البقاء، إضافة إلى افعل تعديل أو النسخ أو التدمير البينات ووسائل تقنية المعلومات الحصول على معلومات حكومية سرية وهذا الظرف الأخير لم ينص عليه المشرع الجزائري.

- جرمت الاتفاقية أفعال الاعتداء على نظام تقنية المعلومات عن طريق تجريم التزوير والاحتيال باستخدام تقنية المعلومات

- حرصت الاتفاقية على تجريم الإباحية بنص خاص مع تشديد العقوبة في حالة إباحية الأطفال والقصر

- نصت الاتفاقية على تجريم جميع صور الجرائم المتعلقة بالإرهاب وتلك الجرائم المتعلقة بالجريمة المنظمة في حالة ارتكابها باستخدام تقنية المعلومات

- خلو الاتفاقية من نص يجرم الانتفاع بغير وجه حق، خدمات الاتصالات وقنوات البث باستخدام تقنية المعلومات.

- ومما يلاحظ على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الغموض وعدم الوضوح في تحديد بعض الجرائم، مثلما ورد في المادة 13 منها تحت عنوان الجرائم الأخرى المرتبطة بالإباحية، حيث تضمن هذا العنوان جريمة المغامرة والاستغلال الجنسي دون تحديد صور الاعتداء أو ذكر المقصود بمصطلح المغامرة؛ هل هي جريمة؟ أو أن الأمر يتعلق بخطأ عرضي، أو يقصد بها جريمة المقامرة التي

نصت عليها معظم تشريعات الدول العربية. وعليه إذا كان الأمر بتعلق بخطأ فيجب العمل على تصحيح مصطلح المغامرة الوارد في المادة 13 بمصطلح المقامرة.

- كذلك في المادة 14 نصت الاتفاقية على جريمة الاعتداء على حرمة الحياة الخاصة ولم تحدد الاتفاقية العربية مظاهر الاعتداء على حرمة الحياة الخاصة، بل ذكرت أنها ترتكب بواسطة تقنية المعلومات.

وعليه يمكن الخروج من هذه الدراسة ببعض التوصيات:

1- ضرورة تفعيل نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 المصادق عليها في 2014 بموجب المرسوم الرأسي رقم 14-252

2- ضرورة أخذ المشرع الجزائري بنص المادة الحادية عشر(11) من الاتفاقية العربية لسنة2014 الخاصة بجريمة الاحتيال المعلوماتي، حيث يعتبر نص هذه المادة أكثر النصوص دقة في التعبير عن حقيقة الاحتيال في مجال تقنية المعلومات

3- إسراع المشرع في سن تشريع خاص بجريمة الإباحية المرتكبة بواسطة تقنية المعلومات، تماشيا مع مبدأ الشرعية الجزئية.

ضرورة تكفل المشرع بسن قوانين تحمي أدوات الدفع الإلكتروني من الاستعمال غير المشروع كما ورد في نص المادة الثامنة عشر(18) من الاتفاقية العربية لسنة2014.

الهوامش:

(1) انظر المادة الثانية من الاتفاقية لعربية لمكافحة جرائم تقنية المعلومات

(2) وقع على الاتفاقية بتاريخ 2010/12/21 م بالقاهرة، وصادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 8 سبتمبر 2014م(الجريدة الرسمية للجمهورية الجزائرية ،العدد 57 ،المؤرخة في 28 سبتمبر 2014م).

(3) المادة 1/2 "أ" من اتفاقية فيينا لقانون المعاهدات 1969، التي انضمت إليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 87/222 المؤرخ في 1987/10/13(الجريدة الرسمية العدد 42، سنة 1987).

(4) انظر جمال عبد الناصر مانع، القانون الدولي العام- المدخل والمصادر- ، دار العلوم للنشر والتوزيع، ص64.

(5) انظر المادة الأولى من الاتفاقية لعربية لمكافحة جرائم تقنية المعلومات

(6) انظر المادة الثانية من الاتفاقية لعربية لمكافحة جرائم تقنية المعلومات

(7) عرف قانون مكافحة جرائم تقنية المعلومات لسلطنة عمان في الفصل الأول المادة1/ب تقنية المعلومات ب" الاستخدام العلمي للحوسبة و الإلكترونيات والاتصالات المعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة" مرسوم سلطاني رقم2011/12 الجريدة الرسمية العدد 929.

(8) انظر، محمد خليفة، (خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها)، دراسات وابحاث، جامعة زياني عاشور الجلفة، العدد01، المجلد01، ص 370-389.

(9) محمد حماد مرهج الهيتي، جريمة الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش- دراسة في ضوء التشريع الفرنسي-، مجلة كلية الحقوق جامعة النهرين

http://www.iasj.net/iasj?func=issueTOC&isId=4404&uiLanguage=ar11/ 2016/03/29 21h.

(10) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت-الجريمة المعلوماتية- دار الثقافة للنشر والتوزيع، الطبعة الأولى الاصدار الثالث، ص26.

http://www.iasj.net/iasj?func=issueTOC&isId=4404&uiLanguage=ar11/ 2016/03/29 21h.

(11) أنظر: رامي حليم،(جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات)، دراسات وأبحاث، جامعة زيان عاشور بالجلفة، العدد1، المجلد1،سنة 2009، ص343.

(12) أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة السابعة عشر، دار هومة، الجزائر ،2014 ص449.

(13) يقصد بكلمة سرية كما جاء في قانون الإمارات العربية لمكافحة جرائم تقنية انظمة المعلومات : أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو إفشائها إلا بإذن مسبق ممن يملك هذا الإذن

(14) تنص المادة 8 " كل من تنصت أو التقط أو اعترض بدون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها، يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين".

(15) زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى عين امليلة الجزائر، سنة 2011، ص 66

(16) انظر نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدي، عين امليلة، الجزائر 2012، ص226.

(17) انظر المادة 11 من المرسوم السلطاني رقم2011/12 الجريدة الرسمية لسلطنة عمان العدد 929.

(18) عبد الفتاح بيومي حجازي، مكافحة جرائم الانترنت في القانون العربي النموجي، ص 120 وما بعدها نقلا عن علي حسن الطوالبة، الجرائم الإلكترونية، جامعة العلوم التطبيقية، كلية الحقوق مملكة البحرين ط الأولي 2008 ص148.

(19) انظر المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

(20) معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن (مذكرة ماجستير)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، ص46.

(21) معتوق عبد اللطيف، المرجع نفسه، ص48

(22) أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الانترنيت، دار المطبوعات الجامعية الاسكندرية سنة 2009 ص 160.

(23) باسم شهاب جرائم المال والثقة العامة، بيرتي للنشر، الجزائر، 2013، ص 170.

(24) معتوق عبد اللطيف، مرجع سابق، ص41.

(25) علي حسن الطوالبة، مرجع سابق، ص179.

(26) نبيل صقر، مرجع سابق، ص238.

(27) علي حسن الطوالبة، مرجع سابق ص278.

(28) معتوق عبد اللطيف، مرجع سابق ص63.

(29) النسخة الصادرة عن مجلس جامعة الدول العربية ونسخ الدول المصدقة على الاتفاقية مثال الإمارات العربية وسلطنة عمان وجمهورية مصر العربية.

(30) معتوق عبد اللطيف، مرجع سابق ص76.

(31) أحسن بوسقيعة، مرجع سابق، ص127 وما بعدها.

(32) القانون 06-23 المؤرخ في 20 ديسمبر 2006، ج ر رقم 84، ص23.

(33) أسامة بن غانم عبيد، حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والأنترنت، المجلة العربية للدراسات الأمنية و التدريب المجلد 32 العدد 46 ص 71.

(34) أسامة بن غانم عبيد، مرجع سابق ص17.

(35) معتوق عبد اللطيف، مرجع سابق ص71.

(36) المرجع نفسه، ص71.

(37) باخوية دريس، جرائم الإرهاب في دول المغرب العربي(تونس، الجزائر، والمغرب أنموذجاً) مجلة دفاتر السياسة والقانون، العدد الحادي عشر 2014 ص101.

(38) أنظر المادة 1/19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 57 بتأريخ 2014/09/28.

(39) أحسن بوسقيعة، مرجع سابق ، ص449.

(40) نفس المرجع، ص450.

(41) اضيفت المواد بالقانون رقم 01/09 المؤرخ في 25 فبراير 2009 الجريدة الرسمية عدد 15 ص6.

(42) la loi n°92-597 du 1er juillet 1992relative au code de la propriété intellectuelle J.ORF n°153 du 3/7/1992 p8801.

(43) الأمر 03-05 الصادر بتاريخ 2003/17/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر73-14، ج ر عدد44 بتاريخ 2002/07/23.

(44) معتوق عبد اللطيف، مرجع سابق ص75

(45) نصت المادة المادة 13 مرسوم بقانون اتحادي رقم 5 لسنة2012 لدولة الإمارات العربية المتحدة لمكافحة جرائم تقنية المعلومات الجرائم التي تقع على هذا النوع من وسائل الدفع يعاقب بالحبس والغرامة ...كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة، أو أي وسيلة أخرى من وسائل الدفع الالكتروني، وذلك باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي ويعاقب بذات العقوبة كل من:

صنع أو صمم أي وسيلة من وسائل تقنية المعلومات، أو برنامج معلوماتي، يقصد تسهيل أي من الأفعال المنصوص عليها في الفقرة الأولي من هذه المادة.

استخدم بدون تصريح بطاقة ائتمانية أو الكترونية أو بطاقة مدينة أو أي وسائل أخرى للدفع الالكتروني، بقصد الحصول.

لنفسه أو لغيره، على أموال أو أملاك الغير أو الاستفادة مما تتيحه من خدمات يقدمها الغير.

قبل التعامل بهذه البطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الالكتروني مع علمه بعدم مشروعيتها.