

واقع مكافحة الجريمة الالكترونية

أ. رزيقة حيزير

كلية علوم الإعلام والاتصال جامعة الجزائر 3

Razika.hizir@gmail.com

Résume

L'auteur expose dans cette étude, le phénomène de La cybercriminalité qui désigne les infractions pénales commises en ligne via les réseaux de communications électroniques et les systèmes d'information, et s'agit d'un problème a différentes formes et sans frontières, et il dresse un aperçu général sur les moyens techniques et juridiques et les mesures prises par les États et la communauté internationale pour y faire face.

مقدمة

في الوقت الذي ساهمت فيه الثورة التكنولوجية في خلق بيئة حديثة تشهد جملة من التسهيلات والتطورات المذهلة والمتعددة في مختلف الميادين والمجالات أهمها تقريب المسافات بين الشعوب، نجم عن سوء استخدام ثروتها أثارا سلبية كثيرة معادية لنشاطات المجتمعات التي اقتحمتها أنواع جديدة من الاعتداءات والجرائم والمجرمين. وظهر ما يسمى اليوم بالجريمة المعلوماتية criminalité la informatique أو الجريمة السيبرانية la cybercriminalité التي تباينت وتعددت تسمياتها وتعريفها بتعدد وتباين النظم القانونية والثقافية بين الدول¹؛ ما أدى إلى عدم الاتفاق على مصطلح موحد للدلالة عليها (...) أو وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصرها في مجال ضيق². لكنّها تبقى تمثل المخالفات التي تُرتكب "ضدّ الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد

إيذاء سمعة الضحية أو الحاق أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام ما تقدمه شبكة الانترنت لتحقيق أغراض شخصية أو مكاسب مالية، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر.³

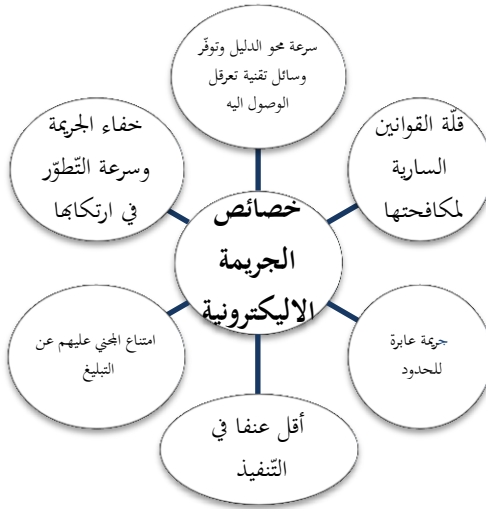
من هنا تبرز أهمية الاشكالية الرئيسية لموضوع الدراسة التي تحاول كشف أهم التحديات القانونية ومختلف الآليات الدولية لمكافحة الجرائم الالكترونية، وذلك عبر تقديم لمحة عن الظاهرة ومحاولة رصد أهم المحاولات التشريعية والتدابير لصدها وفقا للسؤال المحوري حول: ما هو واقع مكافحة الجرائم الالكترونية ؟

أولا : الجريمة الالكترونية أو التهديد الجديد

في الوقت الذي تُعتبر فيه شبكة الانترنت وسيلة للاتصال والتّقارب وتبادل المعلومات والمنافع بين المجتمعات، أصبحت في نفس الوقت بمنافعها أداة تزوير وتضليل ولُب الرّذيلة والتّعدي على حقوق الآخرين، ووسيلةً لظاهرة إجرامية جديدة لم تشهدها المجتمعات البشرية من قبل.

1. خصائص الجريمة الالكترونية: تستمد الجريمة الالكترونية خصائصها من خصائص الانترنت التي أضحت وسيلة مثالية لتنفيذ العديد من الجرائم والأفعال غير المشروعة والعابرة للحدود؛ إذ لم يعد هناك أية حدود مرئية أو مسموعة تقف أمام نقل المعلومات بسرعة، وبسهولة مذهلة، وبكميات كبيرة. و"السهولة في نقل المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل في دولة أخرى"⁴ كما يمكن ارتكابها أثناء وجود الضحية على شبكة الانترنت دون أن يلحظها أو يدري بوقوعها. فهي لا تتطلب جهدا أو عنفا مقارنةً بالجرائم التقليدية، كما تتميز بسرعة محو الدليل. ولا يُبلغ عنها في أغلب الأحيان إمّا بسبب عدم اكتشافها من قبل الضحايا أو خوفا من التشهير. وتتميّز الجرائم المعلوماتية بطبيعتها الناعمة *soft crime*، فهي تعتمد على البراعة التقنية للمجرم في التعامل مع جهاز الحاسوب بعيدا عن العنف.

ونذكر أنّ أوّل حالة اعتداء أمني على شبكة النت سُجلت سنة 1988. حيث قام الطّالب روبرت موريس من جامعة "كرونل" بتطوير فيروس عرف لاحقا بفيروس موريس، بعدما استغلّ ثغرة في نظام البريد الاليكتروني المستخدم آنذاك ممّنه من استنساخ نفسه ونقل نسخ إلى عدد كبير من الحواسيب المتّصلة بالشّبكة محدثا شللا في جميع الأجهزة التي أصابها.⁵ وعلى العموم يمكن اختزال أهم خصائص الجريمة المعلوماتية في الشّكل الموالي.



الشّكل رقم 1 يوضّح خصائص الجريمة المعلوماتية

2. أنواع الجريمة الإلكترونية: تتمّ الجريمة المعلوماتية من خلال جهاز الحاسوب المرتبط بشبكة الانترنت وبتقنيات عالية ما يشتّت جهود التّحريات والتّنسيق الدّولي لتعقب أثارها ويضفي عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية؛ ويكون جهاز الكمبيوتر قلب هذه الجريمة من عدّة جوانب:⁶

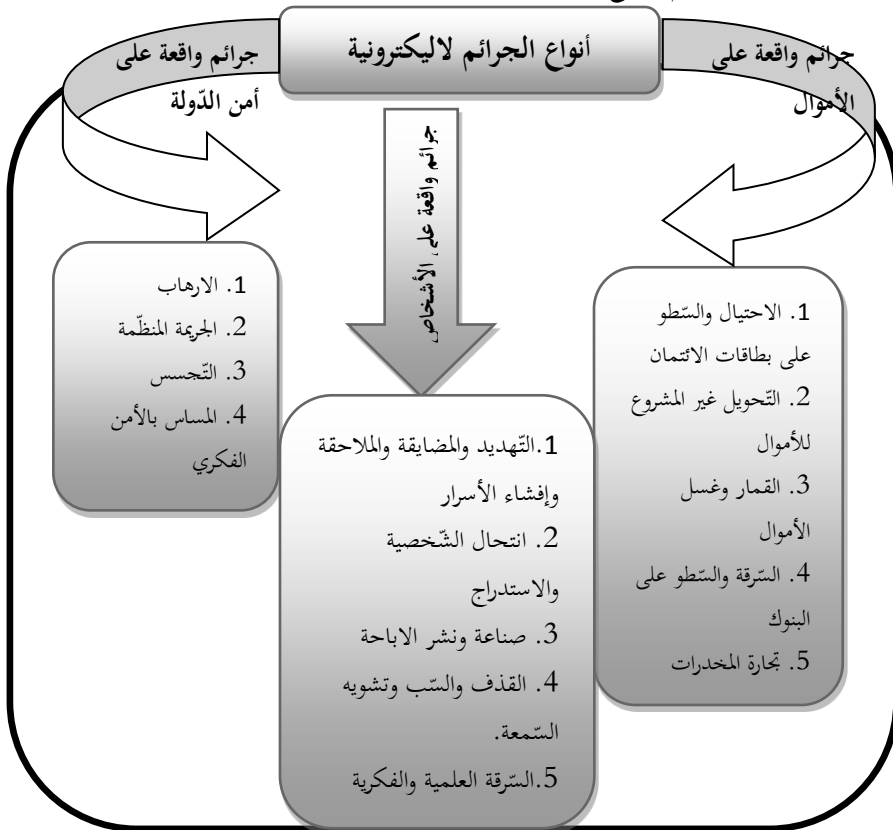
❖ الكمبيوتر هدفا للجريمة: l'ordinateur est la cible يصبح الحاسوب هدفا للفعل الاجرامي في حالة الدّخول غير المصرّح به إلى النظام، أو عند زراعة الفيروسات لتدمير المعطيات والملفات المخزّنة أو تعديلها أو الاستيلاء عليها...

❖ الكمبيوتر أداة لارتكاب الجريمة: l'ordinateur est l'instrument يعتبر الحاسوب أداة مستغلّة في الجرائم المعلوماتية بأنواعها المختلفة على غرار الاستيلاء

على الأموال من خلال إجراء تحويلات غير مشروعة أو استخدامه في عمليات التزوير أو الاستيلاء على أرقام بطاقات ائتمان وتحويل الأموال، كما يمكن أن يستخدم الكمبيوتر في جرائم القتل...

❖ **الكمبيوتر بيئة الجريمة:** يمكن للكمبيوتر أن يكون بيئة خصبة تحتضن الجريمة في حالة استخدامه كأداة لتخزين البرامج المقرصنة فيه أو في حالة استخدامه لنشر المواد غير القانونية، أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية وغيرها من الجرائم.

❖ **الكمبيوتر أداة لاكتشاف الجريمة:** ولأنه سيف ذو حين فإن الكمبيوتر يستخدم على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، ليلعب دورا رئيسيا في الكشف عن الجرائم وتتبع خطوات فاعليها...



الشكل رقم 2 يوضح بعض أنواع الجريمة الالكترونية

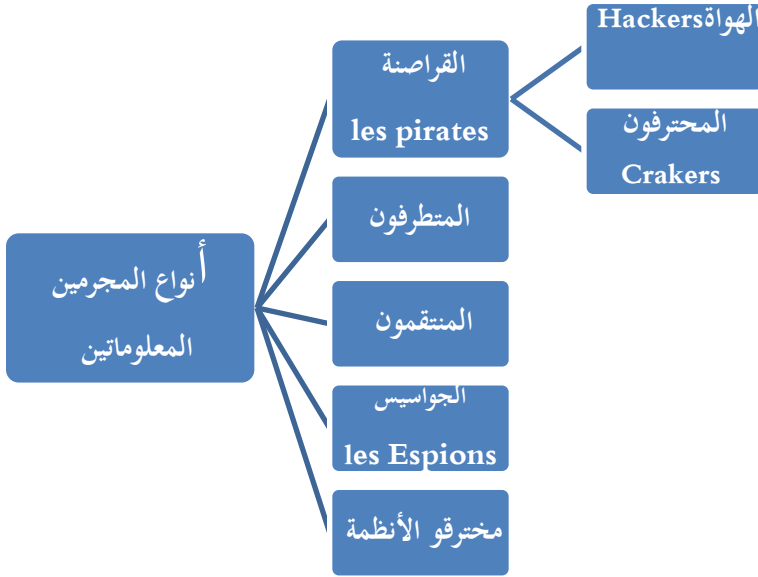
3. المجرم الإلكتروني: إن المجرم المعلوماتي يتسم بخصائص تميزه عن المجرم التقليدي. فالجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها، ولكن الأمر يختلف بالنسبة للجرائم المعلوماتية؛ إذ يتمتع المجرم الإلكتروني بالمهارة والمعرفة والدكاء. وتختلف دوافع الجريمة المعلوماتية من مجرم إلى آخر، فقد تدفع الرغبة في التعلم وقهر النظام المعلوماتي وإثبات الذات أو الرغبة في الانتقام أو المتعة والتحدي أو حب المال والثراء أو التنافس السياسي والاقتصادي والتسابق العسكري بين الدول... إلى ارتكاب الجرائم.⁷

من جهته مكن الفضاء الإلكتروني من خلق فرص جديدة للمجرمين لارتكاب جرائم مثل القرصنة، والاحتيال، وتخريب أجهزة الكمبيوتر أو سرقة المعلومات أو العبث بها، الاتجار بالمخدرات... بل استفادوا من الشبكة في تبادل الأفكار والمعلومات والخبرات الاجرامية في ما بينهم، والتي تضمن لهم القيام بجرائمهم بعيدا عن أعين الأمن وأجهزة مكافحة الجرائم المعلوماتية. إذ يعقد المجرمون مؤتمرات تسمح لهم بابتكار طرق ووسائل من أجل ارتكاب جرائمهم لم تستطع التشريعات مواكبة سرعة تطورها. وتتحدد طبيعة المتهم طبقا للدرجة العلمية والمستوى الثقافي والتعليقي في التعامل مع التكنولوجيا الحديثة، لأنه يرتكب الجريمة في حدود ما لديه من قدرات.⁸

وتجدر الإشارة أنه عقد أول مؤتمر سنة 1990 بأوروبا شارك فيه مراهقون نوابغ في المعلوماتية من كل أنحاء العالم هدف إلى تبادل الأفكار فيما بينهم وتعليم بعضهم البعض طرق اقتحام أنظمة الحواسيب في الدول الأخرى وتنمية مهاراتهم واكتساب الخبرة. وتكرّر عقد مثل هذه المؤتمرات خاصة بمدينة "لاس فيغاس" بالولايات المتحدة، حيث ينظم سنويا مؤتمر يسمى DEFCON يجمع المراهقين من كل أنحاء العالم،⁹ لتبادل المعلومات والشفرات الخبيثة ما يؤدي إلى تكوين شبكات عالمية من القرصنة.

ومن أشهر الجرائم التي ارتكبت في الولايات المتحدة تلك التي اقترفها المراهق "دينيس موران" (17 سنة)، والتي تحولت لاحقا إلى قضية رأي عام لاختلافها عن بقية الجرائم وللخسائر التي تسببت فيها. إذ قام المراهق الذي سعى نفسه "كوليو"

بشن سلسلة من الهجمات الالكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الانترنت. فأقلقت العمليات التخريبية "لكوليو" من بداية سنة 1999 وحتى بداية 2000 المسؤولين عن هذه المواقع.¹⁰ ويمكن حصر أنواع المجرمين الاليكترونيين في الشكل رقم 3:

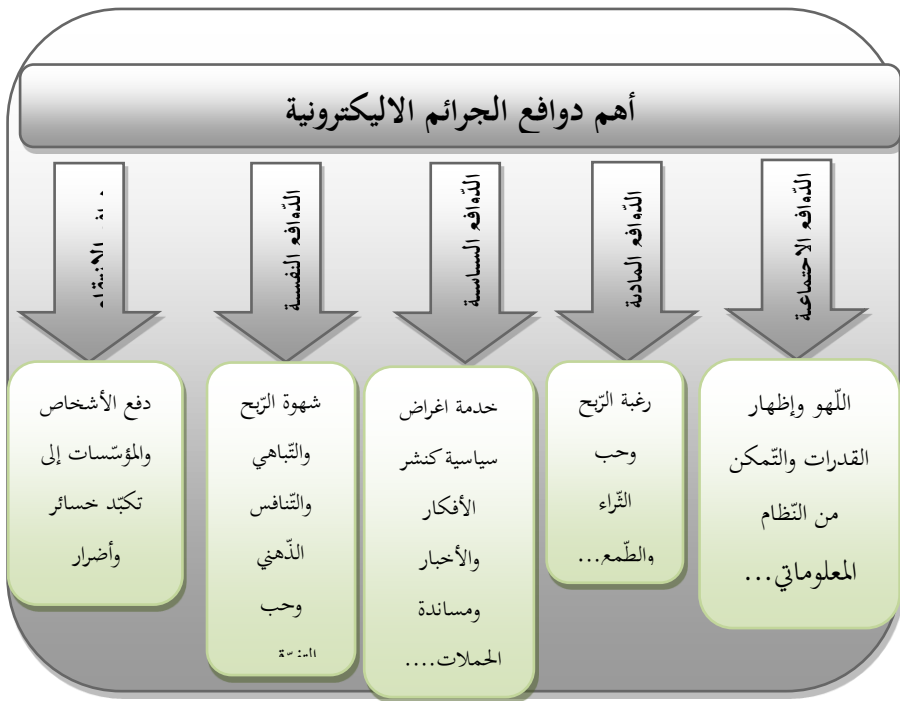


الشكل رقم 3 يوضح أنواع المجرمين الاليكترونيين

4. دوافع الاجرام الاليكتروني: تتلخص أسباب الجرائم الإلكترونية بأنها ظاهرة اجتماعية متوافقة مع انتقال نشاطات المجتمعات من الواقع الفعلي (المادي) إلى المجتمع الرقمي أو الافتراضي، الذي أفرز تناقضات اجتماعية واقتصادية وسياسية... واسعة وسهل الوصول للمستهدفين بسرعة في ظل الفرص المتاحة لارتكابها كضعف الرقابة وقلة الخطورة على الجناة، وهذا يهدف الكسب غير المشروع رغبة في الثراء، أو في الشهرة أو في الانتقام...¹¹ ويوجه مرتكبو الجرائم المعلوماتية كل ما لديهم من خبرات ومهارات تكنولوجية نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية، وذلك إما بسرقة تلك الأموال أو بتحويلها للحساب الشخصي داخل البنك...¹² كما يتملك بعض مجرمو المعلوماتية شعور بالبحث عن

القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية. ففي بعض الأحيان وجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي. من جهة أخرى قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة في قهر الأنظمة الإلكترونية والتغلب والتفوق عليها.

كما يمكن لدوافع المزاح والدعابة والتسلية أن تورط الشخص ويقوم بتصرفات دون قصد إحداث جرائم. أو تنتج عنها نتائج ترقى إلى درجة الجريمة لأنه من الطبيعي أن الشخص الذي يقوم بمسح مجموعة من الملفات من جهاز شخص آخر، وكانت هذه الملفات تحتوي على معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دعابة، بل إن هذا التصرف في حقيقته هو جريمة إتلاف وتخريب متعمد.¹³ ويختزل الشكل الموالي دوافع الجريمة المعلوماتية.



الشكل رقم 4 يوضح أهم دوافع الجريمة المعلوماتية

ثانيا: تحديات مواجهة الجريمة الالكترونية

نجم عن سوء استخدام ما حملته الثورة التكنولوجية أثارا سلبية أثرت على حقوق الأفراد وحرياتهم، وسببت خسائر مادية ومعنوية معتبرة. لذلك سعت المجتمعات إلى الحد من لجريمة الالكترونية التي طرحت اشكالات قانونية واجتماعية واقتصادية معقدة. فكما واكب المجتمعات تطوّر الجريمة التقليدية والتّصدي لها وردعها عن طريق سن قوانين وتشريعات دأبت على فعل نفس الشّيء مع الجريمة المعلوماتية من خلال وضعها في اطار قانوني ومحاولة ايجاد مختلف الطّرق والتدابير السّليمة لمكافحتها. وتجسّدت بداية مكافحة الجرائم المعلوماتية بتطبيق النّصوص القانونية المتوقّرة بمختلف أنواعها، وذلك تباديا لإفلات الجاني من العقاب لاسيما في الحالات التي تلبس فيها هذه الجريمة ثوب بعض الجرائم التقليدية كالسرقة والنّصب والتّزوير وخيانة الأمانة.¹⁴

1. الجهود الدّولية للحدّ من الجرائم الالكترونية: لم يقف المجتمع الدّولي المعاصر مكتوف الأيدي أمام تناسل الجرائم المعلوماتية، إذ يعمل على محاربتها عبر مختلف الهيئات والمنظمات العالمية والإقليمية، مرشدا بذلك جهود ومحاولات مختلف الدّول في سنّ القوانين والتّشريعات الدّاخلية وانهاج تدابير وآليات لصدّ الجرائم المستحدثة. وتبدّل منظمة الأمم المتحدة جهودا معتبرة وكثيرة في مكافحة الجريمة المعلوماتية لا يمكن ذكرها كلّها في هذا المقام، فهي تؤكد في كلّ مؤتمراتها وأشغالها على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التّعاون للحدّ من انتشار هذه الجريمة العصرية ودائمة الفرار من الآليات القانونية، بدءا بالمؤتمر السّابع الذي انعقد سنة 1985 إلى غاية المؤتمر الثاني عشر لسنة 2010. إضافة إلى المؤتمر الخامس عشر للجمعية الدّولية لقانون العقوبات وذلك تحت إشراف الأمم المتحدة عام 1994، الذي نتج عنه عدّة توصيّات وقرارات ذات الصّلة بالجرائم المعلوماتية.¹⁵

وتوصّلت في مؤتمرها الثّامن حول جرائم الانترنت إلى دعوة الدّول الأعضاء لاتخاذ التّدابير وكلّ الاجراءات الممكنة لتحديث القوانين والتّشريعات وضرورة اتخاذ تدابير أمنية ووقائية، كنشر الوعي في الأوساط الشّعبية والتّعاون مع مختلف المنظّمات

لحماية مصالح الدول وحقوق الضحايا. وعقدت أيضا اتفاقية في شهر ديسمبر 2000 تهدف إلى مكافحة سوء استخدام التكنولوجيا لأغراض إجرامية. إذ توافد ممثلون من رؤساء ورؤساء حكومات عن 124 دولة إلى صقلية، لتوقيع هذه المعاهدة الدولية. التي التزموا فيها بتجريم عمليات غسل الأموال، والفساد، وعرقلة عمل العدالة... كما وقّرت المعاهدة إطار عمل لمصادرة عائدات الجريمة المنظمة، والممتلكات أو المعدات المستعملة في الأعمال الإجرامية وحجزها، وضمت أحكامًا خاصة بالتعاون الدولي على هذا الصعيد.¹⁶

وفي سنة 2010 ناقش المؤتمر الثاني عشر مختلف تطورات الجريمة المعلوماتية والعدالة الجنائية، وهذا بعدما كانت قد عقدت ورشة عمل حول التشريعات السببرانية سنة 2008.¹⁷ ووصفت الأمم المتحدة الجريمة المعلوماتية في إحدى تقاريرها لسنة 2012 على أنها جريمة عصرية متشعبة ومتعددة الجوانب والطبقات تستخدم الجماعات الإجرامية فيها العديد من مزايا العولمة، مثل سهولة الاتصالات وسرعتها والتحرّكات المالية والسفر الدولي... وهذا يعني أنّ التحقيق في الجريمة المنظمة ومقاضاة مرتكبيها ومعاقبتهم صارت أكثر تعقيدا، ومع بذل الدول جهودا لمكافحة الجريمة المعلوماتية، اكتسب التعاون الدولي بشأن المسائل الجنائية مزيدا من الأهمية.¹⁸

من جهتها تعمل المنظمة العالمية للملكية الفكرية وهي إحدى الوكالات الهامة التابعة للأمم المتحدة، على دعم الملكية الفكرية وحماية الملكية الصناعية والأدبية والفنية، وذلك من خلال توفير لحماية القانونية للبرامج المعلوماتية وقواعد البيانات بعقد اتفاقيات دولية تهدف إلى تطوير التشريعات على غرار قوانين حق المؤلف ووضع عقوبات على كلّ محاولات التزوير في العلامات التجارية أو محاولات القرصنة...¹⁹

وإلى جانب الجهد الكبير المبذول من قبل الاتحاد الدولي للاتصالات في إطار برنامج الأمن المعلوماتي العالمي المعلن عنه من قبل الأمين العام للإتحاد عام 2007، والذي يرمي إلى تحقيق عدة أهداف أبرزها استحداث نموذج تشريعي لمكافحة الجريمة المعلوماتية يمكن تطبيقه عالميا بفضل قابليته للاستخدام والتلاؤم مع التّدابير

التشريعية القائمة على الصّعيدين الوطني والإقليمي،²⁰ تعقد سنويا منظمة التعاون الاقتصادي والتنمية عددا من الملتقيات وورش العمل المعمّقة ذات العلاقة بالمجال بغية وضع معايير أمنية وقانونية لمواكبة تطوّرات جرائم الانترنت.

وساهمت أيضا منظمة الشرطة الجنائية الدولية Interpol التي تأسست سنة 1923، في مكافحة الجريمة المنظّمة من خلال تزويد الدّول الأعضاء بمعلومات مهمة عن المجرمين المطلوبين للعدالة، مركزة اهتمامها على الجريمة المنظّمة ذات الصّلة بغسل الأموال.²¹ وعقدت هذه المنظمة عدّة اجتماعات وندوات حول الجريمة المعلوماتية، كان أوّل اجتماع نظمته وشاركت فيه 50 دولة، يتمحور حول الجريمة المعلوماتية في 19 إلى 20 أفريل 1995 أين تمّ اتفاق الدّول الأعضاء على اتخاذ قرار يتعلّق بمكافحة الجرائم المالية عبر الدول وتعزيزها في التعاون الدّولي. وأوصت الأنتربول الدول الأعضاء بتبنيّ مسائل تضمّنّها تشريعاتها الداخليّة على غرار اتخاذ الإجراءات الكفيلة بمنع استخدام التكنولوجيا في غسل الأموال؛ ضرورة تأكد الأجهزة المعنية بالرقابة والإشراف على المصارف والمؤسسات المالية، من وجود برامج كافية لدى هذه الجهات لمكافحة غسل الأموال؛ تعاون المنظمة مع الدّول العربيّة والإسلامية في مجال تسليم المجرمين ومصادرة الأموال غير المشروعة...²²

كما نُظمت أشغال الاجتماع الثالث في 9 و10 ماي 1996 ناقش فيه المشاركون طبيعة هذه الجريمة المستحدثة وجميع التدابير الجبوية المتخذة لصدّها. ثم عقد اجتماع شهر سبتمبر 1998 بمقر المنظمة (مدينة ليون الفرنسية) شارك فيه 108 ممثلا عن 36 دولة واتفق فيه المشاركون على نقاط عديدة تخصّ طرق مكافحة الجريمة العابرة للحدود.²³

2. الجهود الاقليمية لصدّ الجريمة المستحدثة: لعب الإتحاد الأوروبي Union Européenne دورا فعّالا في مجال مكافحة الجريمة المعلوماتية حيث أثمرت جهوده عن ميلاد أولى المعاهدات الدّولية الخاصة بمكافحة الجرائم المعلوماتية بالعاصمة المجرية بودابست عام 2001، وتلخّصت أهداف اتفاقية "بودابست" على أهمية التعاون الاقليمي والدّولي وتحقيق التّوازن بين حقوق الانسان وإجراءات مواجهة جرائم المعلوماتية وأهم العقوبات، وتعتبر هذه الاتفاقية التي شهدت انضمام

العديد من الدول إلى جانب دول الاتحاد الأوروبي كالولايات المتحدة والفلبين وكندا وجنوب افريقيا واليابان... بمثابة الدليل القانوني لمكافحة الجريمة المعلوماتية لدى مختلف التشريعات المحلية.²⁴ كما أنشأ الاتحاد الأوروبي أجهزة تساعد على مكافحة هذا النوع من الجرائم، من بينها جهاز اليوروبول والمركز الأوروبي لمكافحة الجريمة المعلوماتية والذي أفتتح في جانفي 2013.

كما اهتمت مجموعة الدول الصناعية الثمانية الكبرى (G8)، التي تضم كل من الولايات المتحدة، اليابان، ألمانيا، فرنسا، بريطانيا، إيطاليا، كندا، روسيا، بمكافحة الجريمة المعلوماتية من خلال إنشاء هيئة العمل المعنية بالإجراءات المالية منذ قمة باريس الاقتصادية سنة 1989.²⁵ فضلا عن إنشاء مجموعة أخرى بعد اجتماع الحكومات السبع في كندا سنة 1995، التي هدفت إلى مكافحة الجريمة المنظمة عبر الدول. ثم عقدت قمة الحكومات السبع في مدينة ليون الفرنسية في شهر جوان 1996، أين تبنت عدّة توصيات أهمها: تشجيع الدول على تسليم المجرمين عن طريق المعاهدات والتشريعات، وتشجيع دوائر الهجرة على مكافحة الجريمة المعلوماتية ومحاربة تهريب الأجانب، التشديد على ضرورة تبادل المعلومات عن تحركات المجرمين عبر الحدود، والنظر في اتخاذ تدابير تشريعية لمصادرة العائدات غير المشروعة المتأتية من الاتجار بالمخدرات وغير ذلك من الجرائم الخطيرة أو ضبطها، ووضع اليد على الأصول حسب الحاجة، وتوفير ترتيبات مؤقتة كتجميد الأصول أو ضبطها.²⁶

وفي نفس السياق أنشئت منظمة الدول الأمريكية Organisation des Pays Américains سنة 1986 لجنة لمراقبة استعمال المخدرات أطلقت عليها لجنة البلدان الأمريكية لمكافحة تعاطي المخدرات CICAD التي ساهمت في دفع الدول الأعضاء إلى خفض الطلب على العقاقير المخدرة غير المشروعة، ومنع استعمالها، ومكافحة الإنتاج والاتجار غير المشروع بها. وفي سنة 1991 قدمت نفس المنظمة مشروع قانون لمكافحة غسل الأموال، وافقت عليه الدول الأعضاء في شهر مارس 1992. وصاقت الدول الأعضاء على تبني التوصيات التي أصدرتها في مجال مكافحة

غسل الأموال. لتنظم منظّمة الدول الأميركية سنة 1996 بعد سلسلة من النّشاطات إلى اتفاقية مكافحة الفساد والرّشوة الصّادرة عن الأمم المتحدة.²⁷

من جهته صدر مجلس وزراء الدّاخلية والعدل العرب، المنعقد بمقر الأمانة العامة لجامعة الدّول العربية بالقاهرة في شهر ديسمبر 2010، القانون الجزائي الموحد كقانون عربي نموذجي نصّ في الباب السّابع على الجرائم ضدّ الأشخاص ووجوب حمايتهم من جرائم الانترنت. كما تمّ في مجال الملكية الفكرية ابرام الاتفاقية العربية لحماية حقوق المؤلّف حيث نصّت على توفير الحماية القانونية للبرامج المعلوماتية وعلى حثّ وتشجيع الدّول الأعضاء على ضرورة تطوير تشريعاتها الجزائية لمواجهة جرائم التكنولوجيا.²⁸

3. بعض الجهود المحلية لمكافحة الجرائم الالكترونية: شهدت الولايات المتحدة الأميركية صدور أول قانون لمواجهة جرائم الحاسب الآلي سنة 1984 الذي جرّم فعل إتلاف الحاسب الآلي ونظمه وما يحتويه من معلومات، ليخضع فيما بعد لعدّة تعديلات سنة 1986 ثمّ عام 1994 ثمّ سنة 1996. وتم من خلاله تجريم الابتزاز المعلوماتي وتحديد العقوبة بناء على عدة اعتبارات تتعلّق بوجود النية عند المتهم بتحقيق الرّبح المادي وإلحاق الضّرر بالضّحية...²⁹ وبعدها أقرّت وزارة العدل الأميركية تصنيفا جديدا لجرائم الكمبيوتر سنة 2000 يشمل أفعال السّطو على البيانات بالانجار بكلمة السّر، وحقوق الطّبع وعمليات القرصنة، سرقة الأسرار وتزوير الماركات التّجارية، وتزوير العملة، نشر الصّور الجنسية الفاضحة واستغلال الأطفال، والاحتيال، وتهديدات القنابل بواسطة شبكة الأنترنت، الإتجار بالأسلحة النّارية والمتفجّرات والمخدرات وغسل الأموال عبر الشّبكة.³⁰

كما سعت الجهود الفرنسية لمكافحة هذا النّسل الجديد من الجريمة من خلال صدور قانون 1988 الذي يعرّم بعض جرائم الحاسوب. ليعدّل سنة 1994 بنص القانون الجديد الذي أقرّ تجريم محاولات المساس بأنظمة المعالجة الآلية للمعطيات بمختلف أشكال الاعتداء كفعل دخول أو البقاء بطريقة احتيالية في كلّ أو جزء من نظم المعالجة الآلية للمعطيات وعاقبت على ذلك بالحبس مدة سنتين وغرامة مالية بقيمة 30.000 أورو، أما إذا نتج عن ذلك حذف أو تعديل للمعطيات

الموجودة في النظام أو تعديل للمعطيات الموجودة في النظام أو تعريف لمجريات النظام فتكون العقوبة الحبس لمدة ثلاث سنوات والغرامة بقيمة 45.000 أورو... ونصّت المادة 323 من نفس القانون على عقوبات تكميلية إلى جانب العقوبات الأصلية في حالة اقتراف الأفعال الاجرامية كحرمان المجرم من الحقوق العائلية والمدنية ومنعه ممارسة الوظائف العامة، ومصادرة المواد التي استخدمت في ارتكاب الجريمة. وإذا كان الفعل المجرم ارتكب من طرف إحدى المؤسسات فيكون العقاب بالإغلاق والطرّد من الصفقات العامة ونشر الحكم حسب شروط من قانون العقوبات الفرنسي.³¹

وبعدها صدر سنة 2004 القانون المتعلّق بالثقة في الاقتصاد والذي شدّد العقوبات على المعاملات الاقتصادية لحمايتها من خطر فقدان الثقة بين المتعاملين، كما وضع أحكاما جزائية لتنظيم عملية تشفير الوثائق المعلوماتية، حيث سمح بالقيام بعملية التّشفير لكن بعد تقديم طلب الرّخصة من السّلطات المختصة، وحدّد عقوبات تتراوح بالحبس سنتين مع دفع غرامة مالية قيمتها 30.000 أورو لكلّ من يخالف هذه الأحكام، كما شدّد العقوبة على كلّ من يستعمل الوسائل المادية المعدّة لهدف التّشفير لارتكاب أو تسهيل ارتكاب الجرائم.³²

أما على المستوى الجهود العربية فقد عملت على تطوير بنيتها التشريعية لمواكبة تطور ومكافحة جريمة المعلوماتية. إذ شهد التشريع الإماراتي جهودا معتبرة لمكافحة الجريمة الإلكترونية، من خلال صدور قانون سنة 2006 حمل بين طياته جملة من المصطلحات ذات الدلالة القانونية على غرار المعلومات الإلكترونية، البرنامج المعلوماتي، نظام المعلوماتي الإلكتروني، الشبكة المعلوماتية، المستند الإلكتروني، الموقع، البيانات الحكومية.³³ ونص على مجموعة من أنواع الجرائم المعلوماتية كجريمة اختراق المواقع والأنظمة الإلكترونية، وجرم كذلك الأفعال التالية: العبث بالفحوص الطّبية باستخدام الانترنت وكذلك القيام بالتّصنّت أو الاعتراض مرسل عن طريق الشّبكة المعلوماتية واستخدام الانترنت في الابتزاز والتّهديد وعاقب على هذه الأفعال بعقوبة السّجن مدة عشر سنوات إذا كان التّهديد بارتكاب جنائية أو

إسناد أمور خادشة للشرف. كما نصّ أيضا على جرم بعض الأفعال كالسرقة والاحتيال والاستيلاء على سندات أو على بيانات البطاقات الإلكترونية...³⁴

من جهته اهتمّ المشرّع المصري بمكافحة الجرائم المعلوماتية من خلال سنّ قانون مكافحة الجرائم المعلوماتية في أوت 2005 الذي اعتمد على النصوص التقليدية بخصوص بعض الجرائم كالتزوير والاحتيال والسرقة...³⁵ وجرّم رغم كأول قانون صدر حول التوقيع الإلكتروني، بعض الأفعال المتعلقة بالنظم المعلوماتية، وأفعالا تتعلق بالحصول على توقيع أو وسيط أو محور الكتروني بدون وجه حق، أو اعتراضه أو تعطيله عن أداء وظيفته. وعرف النص الوسيط الإلكتروني بأنّه "أداة وأدوات أو أنظمة إنشاء التوقيع الإلكتروني فهو نظام معلوماتي يساعد على إنشاء التوقيع الإلكتروني وإصدار المحرّرات الإلكترونية".³⁶

وأما التشريع الأردني فقد لجأ للجرائم الانترنت، بعدما صادقت الأردن وتونس على اتفاقية تسمح بإمكانية استخدام التوقيع الإلكتروني تسهيلات للمعاملات الإلكترونية الجديدة.³⁷ في وقت شهدت فيه تونس صدور أول تشريع تعرّض لجرائم المبادلات التجارية الإلكترونية سنة 2000. حيث نصّت المادة 48 من القانون التونسي على كلّ ما يتعلّق بالشّفرة الخاصة بالتوقيع الإلكتروني، كما جرّم القانون فعل اختراق منظومة معلوماتية وفك رموز الشفرة أو كلمة السر ونشرها واستعمالها بدون وجه حق، إذ يعاقب المجرم بالحبس لمدة تتراوح بين ستّة أشهر إلى سنتين مع دفع غرامة مالية تتراوح بين ألف وعشرة آلاف دينار تونسي.³⁸

4. الجهود التشريعية الجزائرية لمكافحة الجريمة الالكترونية: شهدت الجزائر على غرار باقي الدول حركة متسارعة في مجال الاجرام الالكتروني خاصة أمام الاستعمال الواسع لشبكة الانترنت وضعف المراقبة والمتابعة الدورية والشاملة. بالمقابل حاول المشرّع الجزائري تدارك الفراغ القانوني في مجال الاجرام المعلوماتي بتعديل قانون العقوبات سنة 1997 من خلال الأمر رقم 10/97 المتضمن تجريم كلّ أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات من خلال المواد 394 إلى 394 مكرر 7.³⁹ وعدّل قانون العقوبات مرة أخرى عام 2006 بموجب القانون المؤرّخ في 20 ديسمبر 2006، وذلك مع ازدياد الوعي بخطورة هذا

التّوع المستحدث من الإجرام لا سيما مع ارتفاع نسبة مستخدمي الانترنت، وذلك بتجريم أفعال الاعتداءات الواردة على منتجات الإعلام الآلي. ونذكر أنّ الجزائر عقدت في 25 أكتوبر 2003 اتفاقية دولية ثنائية جزائرية -فرنسية تتضمّن التّعاون في مجال الأمن ومكافحة الاجرام المنظم، ودخلت بنود هذه الاتفاقية حيز التّنفيد بصدور العدد 77 من الجريدة الرّسمية في 9 ديسمبر 2007. كما انضمت إلى العديد من الاتفاقيات الدّولية التي تهدف إلى مكافحة الجريمة المعلوماتية على غرار اتفاقية لحماية الملكية الصّناعية واتفاقية "بارن" Berne لحماية المصنّفات الأدبية والفنية (سبتمبر 1986) والاتفاقية العالمية حول حقوق المؤلّف.

ثمّ صدر في شهر أوت 2009 القانون المتضمّن لموضوع القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الاعلام والاتصال ومكافحتها والذي دخل حيز التّنفيد بصدور العدد 47 من الجريدة الرسمية في أوت 2009.⁴⁰ والذي جاء بالعديد من الآليات لمكافحة الجريمة المعلوماتية كتفتيش المنظومة المعلوماتية، وحجز المعطيات وإنشاء الهيئة الوطنية للوقاية ومكافحة الجرائم المتّصلة بتكنولوجيا الاعلام والاتصال، فضلا عن النص على التّعاون الدّولي في مجال المساعدة وتبادل المعلومات للكشف عن الجرائم المستحدثة المنصوص عليها في القانون رقم 04-09.

وإلى جانب محاولة صد الجريمة الالكترونية من خلال قانون العقوبات صدر المشرّع قوانين خاصة على غرار قانون حماية التّأمينات الاجتماعية رقم 01/08 المؤرخ في 23 جانفي 2008، الذي يشدد العقوبة على الاستخدام غير المشروع للبطاقة الالكترونية للمؤمّن عليه اجتماعيا، أو أي محاولات أخرى كالتّعديل أو الحذف الكلّي أو الجزئي للمعطيات التقنية أو الادارية المدرجة في البطاقة الالكترونية.⁴¹

في الختام يمكن القول أنّه في ظلّ جهود مختلف الأنظمة لصدّ واحتواء وكشف حقيقة الجريمة الالكترونية وتحديد طبيعتها ونطاقها، تبقى هذه الجريمة في تطوّر وفرار مستمر، ما يستعجل تباين محاولات تعريفها وتطوّرات خصائصها وأخطارها على المجتمعات الحديثة. لاسيما وأنّه يُنتظر أن ترتفع احصائيات سنة 2011 التي

كشفت أنّ هناك على الأقل 2,3 مليار شخص كانوا متصلين بشبكة الانترنت، نسبة 60 % من المستخدمين يعيشون في الدول المتقدمة ونسبة 45 % كانوا من فئة الشباب الأقل من 25 سنة، خلال سنة 2017 التي ستشهد حسب الخبراء ارتفاعا ملفتا في عدد مستخدمي الانترنت. بينما يُنتظر أن يرتفع عدد الأجهزة المتصلة بشبكة الانترنت سنة 2020 بنسبة 70 % أي بنسبة تفوق عدد سكان الأرض بست مرات.⁴² الأمر الذي سيعقد من مهام التشريعات ويحدث اضطرابات تصعب تصوّر نطاق الجريمة المعلوماتية وتتبع آثار الأدلة التي تدين الخارجين عن القانون.

الهوامش:

¹ Liang Jiansheng, *Criminalité informatique*, ENSSIB, France, 1999, p 20

² محمد علي عريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة، الإسكندرية، 2004، ص 8.

³ ذياب موسى البداينة، "الجرائم الإلكترونية: المفهوم والأسباب"، ورقة مقدمة في الملتقى العلمي للجرائم المستحدثة في ظلّ التغيرات والتحوّلات الإقليمية والدولية، 2014 ، الاردن، مداخلة متوقّرة على الموقع الإلكتروني: <http://repository.nauss.edu.sa> تاريخ التصقّح يوم 25 فيفري 2017 على الساعة 23.00.

⁴ نهلاء عبد القادر المومني، "الجرائم المعلوماتية"، دار الثقافة للنشر والتوزيع، ط 1، عمان، 2008.

⁵ نهلاء عبد القادر المومني، مرجع سابق الذكر، ص 58.

⁶ Liang Jiansheng, op.cit, pp 23-27 .

⁷ نهلاء عبد القادر المومني ، مرجع سابق الذكر، صص 77- 80 .

⁸ أيمن عبد الحفيظ، "الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية دون دار للنشر، 2008، ص 11.

⁹ نفس المرجع، ص 27.

¹⁰ نفس المرجع، ص 25.

¹¹ ذياب موسى البداينة، مرجع سابق الذكر

¹² أيمن عبد الحفيظ، مرجع سابق الذكر، ص 18.

¹³ نفس المرجع، ص 20.

¹⁴ محمد سامي الشوا، "ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية، القاهرة، 1988، ص 30.

¹⁵ Liang Jiansheng, op.ci, p 30.

¹⁶ Anmonka Jeanine-Armelle Tano-Bian, "La répression de la cybercriminalité dans les États de l'Union européenne et de l'Afrique de l'Ouest", Thèse pour le Doctorat en Droit Public, Université Sorbonne, Paris, 2015, p 42.

¹⁷ Liang Jiansheng, op.ci, p 36.

¹⁸ تقرير "مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية"، 10 جويلية 2012، وثيقة متوقّرة على الموقع الإلكتروني: <http://www.amlu.gov.jo> شوهد يوم 20 03 2017 على الساعة 18.00.

19. Anmonka Jeanine-Armelle Tano-Bian, op.cit, p 138.

20. Ibid, p 140.

21. Ibid, p 55.

22. Liang Jiansheng, op.ci, p 56.

23. Liang Jiansheng, op.ci, p57.

24. Anmonka Jeanine-Armelle Tano-Bian, op.cit, p 205.

25. Liang Jiansheng, op.ci, p 55.

26. Liang Jiansheng, op.ci, p 48.

27. Phil Butler, "Crime Cybernétique, fraude financière et blanchissement d'argent : comprendre nouveau paysage des menaces", tiré du site : taccelus.thomsonreuters.com, le 27 02 2017 à 10.06.

Phil Butler هو خبير لدى الأمم المتحدة من المكلفين بمكافحة الاحتيال، وهو مدير العلاقات الخارجية بالمركز الجامعي بـ Newcastle.

28. محمد علي عريان، مرجع سابق الذكر، ص 39.

29. Phil Butler, op.cit

30. Ibid

31. Liang Jiansheng, op.ci, p 30.

32 Ibid, p 33.

33. خالد ممدوح إبراهيم ، " أمن الجريمة الإلكترونية " ، الدار الجامعية، الإسكندرية ، 2008 ، ص ص 5-6.

34. عبد الله عبد الكريم عبد الله، " جرائم المعلوماتية والأنترنترنت"، منشورات الحلبي الحقوقية، بيروت، 2007، صص 63-79.

35. عبد الفتاح بيومي الحجازي ، "التوقيع الالكتروني في النظم القانونية المقارنة"، دار الفكر الجامعي، الإسكندرية، 2005، ص 556.

36. نفس المرجع، ص 556.

37. عبد الله عبد الكريم، مرجع سابق الذكر، ص 85.

38. نفس المرجع، ص 85.

39. تقرر المواد 394 إلى 394 مكرر 7 من قانون العقوبات الجزائري جملة من العقوبات بالحبس ودفعت الغرامات المالية لمن يرتكب جريمة اليكترونية. حيث تنص المادة 394 مكرر على معاقبة "بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 10.000 د.ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك." لتتضاعف العقوبة إذا "ترتب عن ذلك أي حذف أو تغيير أو تخريب في المعطيات وفي نظام أشغال المنظومة إلى الحبس من ستة أشهر إلى سنتين وغرامة تتراوح من 50.000 إلى 150.000 د.ج." أما المادة 394 مكرر 1 فتعاقب "بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 إلى 2000.000 د.ج كل من أدخل بطريقة الغش معطيات في نظام أو أزال أو عدّل بطريقة الغش المعطيات التي يتضمنها". في حين تعاقب 394 مكرر 2 "بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000 إلى 5000.000 د.ج كل من يقوم عمدا وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في

هذا القسم . بالإضافة إلى حياة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصّل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

وتضاعف المادة 394 مكرر 3 العقوبة المنصوص عليها في هذا القسم في حالة استهداف "الدّفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات أشد". وتخصّ المادة 394 مكرر 4 معاقبة الشّخص المعنوي الذي يرتكب "إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرّات الحدّ الأقصى المقرر للشّخص الطّبيعي". في حين تعاقب المادة 394 مكرر 5 بالعقوبات المقرّرة للجريمة ذاتها" كل من شارك في مجموعة أو في اتفاق تألّف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسّد أو عدّة أفعال مادية ". كما تصدر المادة 394 مكرر 6 الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها، أو اغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها . " وتعاقب كذلك المادة 394 مكرر 7 الشروع في ارتكاب الجائحة المنصوص عليها في هذا القسم بالعقوبات المقرّرة على الجائحة ذاتها."

40. الجريدة الرسمية، العدد 47، الصادرة بتاريخ 16 أوت 2009، (المواد 5 و6 و7 و13 و16 من القانون رقم 09-

04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

41. الجريدة الرسمية، العدد 4، الصادرة بتاريخ 27 جانفي 2008، (القانون 01/08 المتعلّق بال تأمينات

الاجتماعية الصادر في 2008/01/23)

42. Groupe d'experts, " étude approfondie sur la cybercriminalité", UNODC, Vienne, 25-28 février 2013, p 2.