ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

الجرائم المستحدثة في قانون مكافحة الجريمة المعلوماتية في الجمهورية العربية السورية

د. أصالة كيوان كيوان
عميد كلّية الحقوق، جامعة الشام الخاصة ASP - فرع اللاذقية ، اللاذقية، الجمهورية العربية السورية
البريد الالكتروني: a.k.fol.LAT@aspu.edu.sy

الكلمات المفتاحية	Received:05/10/2024	ID No. 2768
الجريمة المعلوماتية – الثورة التكنولوجية – وسائل التواصل الاجتماعي- البرمجيات الخبيثة.	Accepted:23/11/2024	(PP 357 - 376)
	Published:30/03/2024	https://doi.org/10.21271/zjlp.22.sp.16

الملخّص

بالرغم من المزايا الكبيرة التي حققتها ثورة المعلومات التي يعيشها العالم بأجمعه وعلى جميع الأصعدة، وفي شتى مجالات الحياة المعاصرة. فإن هذه الثورة التكنولوجية المتنامية رافقها بالمقابل جملة من الانعكاسات السلبية بسبب سوء استخدام هذه التقنية المتطورة واستغلالها لتسهيل ارتكاب العديد من الظواهر الجرمية لا وبل تم استغلال هذه التقنية لارتكاب جرائم مستحدثة لم تكن لولا هذه الثورة التكنولوجية.

فالجريمة ظاهرة اجتماعية مرتبطة بالإنسان وعرفت منذ القدم، وتطورت وتعقدت أشكالها وتنوعت مناهجها ووسائلها مع تقدم المجتمعات، ومع الثورة التكنولوجية التي نعيشها في العصر الحاضر فقد أخذت ظاهرة الإجرام بعداً دولياً وأصبحت عابرة للقارات وليس فقط للدول الأمر الذي يستدعي إعادة النظر في التشريع الداخلي لكل دولة ومواكبة هذا التطور الهائل. وفي هذه الدراسة سنحاول بشكل مختصر أن نوضح تطور التشريعات السورية وكيف عالجت تطور ظاهرة الجريمة المعلوماتية وذلك من خلال عرض الجرائم المعلوماتية المستحدثة في التشريع السوري.

الكلمات المفتاحية: الجريمة المعلوماتية – الثورة التكنولوجية – وسائل التواصل الاجتماعي- البرمجيات الخبيثة.

المقدمة

الجريمة المعلوماتية لها مسميات عدة منها: (جرائم الحاسوب والإنترنت- الجريمة الإلكترونية - جرائم التقنية العالية -الجريمة الإلكترونية -الجريمة السايبرية). وقد تباينت الصور الإجرامية لظاهرة الجرائم الإلكترونية وتشعبت أنواعها فمنها ما يتصل بالاعتداء على ذات النظام الالكتروني، ومنها ما يتعلق بالاعتداء على المعلومات ومنها أيضاً الاحتيال الإلكتروني، والتزوير الإلكتروني، وجرائم الاعتداء على الحق في الخصوصية وجرائم الاعتداء على التحويلات المالية الالكترونية. وتضم أشكالاً أخرى يصعب حصرها.

فالجرائم الإلكترونية ظاهرة عالمية ونوع مختلف عن الجرائم العادية وخصوصاً في ظل التطور الهائل لوسائل الاتصال الحديثة والثورة المعلوماتية التي يعيشها عصرنا الحالي فقد أصبح انتشار وتوسع إطار الجرائم المعلوماتية أمراً واقعاً مما دعا المشرع السوري إلى سن «قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية» الصادر بالمرسوم التشريعي

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

رقم (17) لعام 2012، والذي وضح بشكل كامل الجرائم التي قد ترتكب بحق الأفراد والمؤسسات نتيجة العمل على الحواسيب والانترنت والشبكات والتطبيقات، حيث يتم بموجب القانون تحديد عقوبات بحق مرتكبي هذه الجرائم وتضمن بعض التعليمات الخاصة بمزودات الخدمة وجزاء مخالفتها وغيرها.

ولكن تشهد الحياة اليومية تطوراً متسارعاً في مجال تقنية المعلومات وبما أن البيئة الإلكترونية روادها عديدون جداً فقد وجد بعض المجرمين التقنيين في هذه البيئة مجالاً خصباً لارتكاب صور متعددة من الجرائم الالكترونية عبر وسائل الاتصال الحديثة. وبما أن المشرع السوري يحاول دائما تلبية متطلبات العصر ومواكبته فقد أصدر في 25 آذار عام 2018 المرسوم التشريعي رقم 9 حيث نص المرسوم على إحداث محاكم جزائية مختصة بالنظر في هذه الجرائم وإحداث نيابة عامة ودوائر تحقيق. وفي عام 2022 صدر القانون رقم 20 والذي يعيد التأطير القانوني لمفهوم الجريمة المعلوماتية ليشمل العديد من صور وأشكال السلوك الإجرامي المرتبط بالمعلومات ونظم المعلومات والتي بدأت تشهد تزايداً كبيراً في المجتمع السوري.

أهداف الدراسة: تهدف هذه الدراسة إلى التعريف أولاً بماهية الجريمة المعلوماتية، وأركانها وأنواعها، ثم عرض تجربة المشرع السوري في مجابهة هذه الجريمة وذلك من خلال تحليل النصوص القانونية التي استحدثت عدد كبير من الجرائم التي لم تكن موجودة قبل ومواكبة التشريع السوري للتطور السريع والمتزايد لهذه الجرائم. وذلك بهدف الحفاظ على حقوق الأشخاص في المجتمع الدولي والداخلي السوري على السواء ولسد الثغرات في وجه التطور السريع لجرائم المعلوماتية.

منهج البحث: ستعتمد هذه الدراسة على المنهج التحليلي المقارن وذلك من خلال تحليل ومقارنة النصوص القانونية التي ناقشت موضوع الدراسة وذلك من خلال خطة البحث التالية:

المبحث الأول: ماهية الجريمة المعلوماتية وفقاً للقانون السوري

المطلب الأول: تعريف وخصائص الجريمة المعلوماتية

المطلب الثاني: أركان الجريمة المعلوماتية وأنواعها.

المبحث الثاني: التشريعات السورية في مواجهة الجريمة المعلوماتية.

المطلب الأول: الجرائم المستحدثة في المرسوم التشريعي رقم 17 لعام 2012

المطلب الثاني: التعديلات التشريعية التي تضمنها القانون رقم 20 لعام 2022

المبحث الأول

ماهية الجريمة المعلوماتية وفقاً للقانون السوري

إن اتساع حجم شبكة الإنترنت وسهولة الوصول إليها، والتزايد المستمر في استخدام هذه الشبكة، ودخول تقنية المعلومات جميع مجالات الحياة تقريباً، جعل منها مسرحاً لكثير من الأفعال الإجرامية. خصوصاً في السنوات القليلة الماضية. فمعظم الجرائم التقليدية أصبحت ترتكب عبر الإنترنت كالسب والشتم والتهديد وغيرها، إضافة إلى أن هذه الشبكة لم تسلم بحد ذاتها من اعتداءات المجرمين التي تناولت أنظمتها ومعلوماتها كجريمة إعاقة خدمة الانترنت واعتراض المعلومات المرسلة عبر الشبكة وغيرها. ولذلك سنوضح في هذا المبحث تعريف هذه الجريمة وخصائصها وفقاً للقانون السوري في المطلب الأول ثم ننتقل لتوضيح أركانها وأنواعها في المطلب الثاني كما يلي:

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

المطلب الأول

تعريف وخصائص الجريمة المعلوماتية

الجرائم المعلوماتية هي صنف جديد من الجرائم، انتقل بالجريمة من صورها التقليدية إلى أخرى إلكترونية. هذه الجريمة سنوضح تعريفها أولاً ثم خصائصها كما يلي:

أولاً: تعريف الجريمة المعلوماتية: المعلوماتية مصطلح مشتق من المعلومة أو المعلومات وفنياً هناك علاقة بين البيانات والمعلومات، فالبيانات هي مجموعة من الحقائق أو المشاهدات، أو القياسات التي تكون عادة في شكل حروف أو أرقام أو أشكال خاصة توصف أو تمثل فكرة أو موضوعاً أو هدفاً أو شرطاً أو أية عوامل أخرى، وتمثل هذه البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات. فالبيانات تعد مصطلحاً عاماً لكل الحقائق والأرقام والرموز والحروف فهي معطيات أولية يمكن معالجتها وإنتاجها عن طريق نظم المعلومات[1].

أما الإنترنت فهي " عبارة عن آلية اتصال مكونة من مفاتيح وأسلاك وأماكن تخزين للبيانات، ودواعم توصيل، و روابط اتصال، تعمل في بوتقة واحدة بفضل بروتوكول الإنترنت (TCP/IP). فالإنترنت تحتوي على عدة تطبيقات ووسائل للتواصل مثل البريد الإلكتروني e-mail والماسنجر messenger والتي تستعمل في أفق الإنترنت، ولكنها ليست هي والإنترنت شيئاً واحداً. فالإنترنت تشبه الطريق التي تكون بين المدن، في حين أن تلك التطبيقات المذكورة وعلى رأسها الوبّ، هي أنواع وسائل المواصلات التي تستخدم هذه البنية الأساسية، مثل السيارات أو الحافلات أو الدراجات النارية"[2] أو بتعبير آخر هي شبكة تتألف من عدد كبير من الحواسيب المتوضعة عبر العالم، والمترابطة مع بعضها البعض، والتي تستخدم في تواصلها بروتوكول تراسل الإنترنت[3].

ونتج عن التحكم البشري في هذه النظم ثورة سميت بالثورة الصناعية أو الثورة المعلوماتية. وتزايد استخدام الحواسيب كأداة لتخزين ومعالجة واسترجاع المعلومات.

وتعد جريمة " دودة موريس" التي تعود واقعتها إلى 12 / 11/ 1988، هي الجريمة الأولى التي ارتكبت عبر الإنترنت حسب التاريخ القانوني، حيث استطاع الشاب " موريس" أن ينشر فيروس إلكتروني تمكن من مهاجمة آلاف الحواسيب عبر الإنترنت، وقد تسبب بأضرار بالغة، أبرزها: توقف آلاف الأنظمة عن العمل، وتعطيل الخدمة ...وقد قدرت الخسائر لإعادة إصلاح هذه الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار[4].

ومنذ ذلك الحين بدأ البحث في هذه الظاهرة الإجرامية لفهم طبيعتها وخصائصها ومعرفة كيفية الحد منها فتم تعريفها بأنها " الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت،

---

[1] - د. هدى حامد قشقوش (2000)، الإتلاف غير ألعمدي لبرامج وبيانات الحاسب الالكتروني، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، ص 887.

[2] - القاضي الدكتور إيهاب السنباطي (2007)، موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ص87 – 80.

[3] - د.طارق الخن (2018)، جرائم المعلوماتية، منشورات الجامعة الافتراضية السورية ، ص4.
متوفرة على الرابط:https://pedia.svuonline.org

[4] - د. علي جبار الحسيناوي (2009)، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، ص10.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

وبواسطة شخص على دراية فائقة"[1]. وفي تعريف آخر " كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها"[2]. وفي تعريف آخر أيضاً" تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها"[3].

ونلاحظ أن كل التعاريف تشترك بالفكرة الأساسية وهي أنها جرائم تقع على شبكة الإنترنت أو بواسطتها وطبعاً الحاسب هو الوسيلة للوصول إلى شبكة الانترنت لذلك لا بد من التمييز بين جريمة الحاسوب وجريمة الإنترنت، فجريمة الحاسوب هي التي ترتكب بواسطة الحاسوب أو على مكوناته المعنوية، فقد ترتكب من خلال حاسوب واحد أو من خلال شبكة داخلية تضم عدة حواسيب دون أن يكون هناك ولوج إلى الإنترنت، كما هو الحال في الجرائم التي تهدف إلى سرقة معلومات الحاسوب أو إتلافها. أما جرائم الإنترنت فإن شرطها الأساسي هو اتصال الحاسوب بالإنترنت، فالحاسوب هو الوسيلة التي لا مفر منها للولوج إلى هذه الشبكة[4].وللدلالة على كلا الجريمتين سواء الحاسوب أو الإنترنت نلاحظ أن المشرع السوري استخدم مصطلح الجريمة المعلوماتية ليشمل جرائم الإنترنت وجرائم الحاسوب في مصطلح جامع شامل لهما وقد عرف الجريمة المعلوماتية في المادة الأولى من قانون مكافحة الجريمة المعلوماتية السوري رقم 17بأنها:

"جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة" ونلاحظ أنه المشرع السوري وضع تعريفاً عاماً وشاملاً للجريمة المعلوماتية في القانون رقم 17 ثم عاد ونظم هذه الجريمة في القانون رقم 20 بشكل أدق ويتناسب مع التطور التكنولوجي بقوله: " سلوك مجرَّم وفقاً لأحكام هذا القانون يقترف بواسطة وسائل تقانة المعلومات، يستهدف المعلومات أو نظم المعلومات أو يرتبط بإضافة محتوى رقمي على الشبكة".

فيتم ارتكاب الجريمة المعلوماتية بإحدى وسائل تقانة المعلومات وتستهدف واحدا مما يلي:

_ المعلومات أو المحتوى الرقمي الموجود على وسائل تقانة المعلومات.

_ اختراق أو تعطيل المنظومات المعلوماتية مثل السيرفرات أو الراوترات أو أي جهاز مرتبط على الشبكة أو أجهزة الموبايل بقصد تعطيلها أو الإضرار بها أو إخراجها من الخدمة أو إعاقة الوصول إليها.

_إضافة محتوى رقمي على الشبكة يشكل جرم ضمن الجرائم المذكورة في القانون مثل (ذم أو قدح أو تحقير أو يمس هيبة الدولة...الخ)

ثانياً: خصائص الجريمة المعلوماتية: نظراً لارتباط الجريمة الإلكترونية بجهاز الحاسوب، وشبكة الإنترنت بصفة عامة، ووسائل التواصل الاجتماعي بصفة خاصة، فقد أضفى عليها ذلك مجموعة من الخصائص المميزة لها عن خصائص الجريمة التقليدية، ومن هذه الخصائص مايلي:

1_ جريمة غير مقيدة بالحدود الجغرافية: فمن الممكن أن تكون جريمة داخلية عندما تقع كاملة في نطاق إقليم دولة معينة. وربما تكون دولية عندما يكون أحد أطرافها شخصاً دولياً. فقد أعطى انتشار شبكة الإنترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود المكان، لذلك فإن من السهولة بمكان أن يكون

---

[1] - المحاميان منير وممدوح الجنبيهي (2005)، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ص13.

[2] - المحامي محمد أمين الشوابكة(2006)، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ص10.

[3] - نبيلة هبة هروال (2007)، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ص30.

[4] - د. طارق الخن، مرجع سابق، س10.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

المجرم في بلد ما والمجني عيه مقيم في بلد آخر. وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها، وحيث أن التشريعات الداخلية متفاوتة فيما بين كل دولة من دول العالم تظهر العديد من المشاكل حول صاحب الاختصاص القضائي لهذه الجريمة وإشكالات أخرى متعلقة بإجراءات الملاحقة القضائية.

2_ جريمة صعبة الاكتشاف والإثبات: تكمن صعوبة إثبات مثل هذه الجريمة أنها لا تترك في الغالب أثراً مادياً ظاهراً يمكن ضبطه، وذلك بسبب إمكانية حذف الآثار المعلوماتية المستخدمة في ارتكاب الجريمة خلال ثوان. هذا فضلاً عن أن الجاني من الممكن أن يستخدم اسماً مستعاراً أو أن يرتكب جريمته من خلال إحدى مقاهي الإنترنت.

3_ يتصف المجرم فيها بالذكاء والمعرفة التقنية: تعد المهارة التقنية والذكاء من أبرز الصفات التي يجب أن يتحلى بها المجرم، فالمجرم يمتلك وسائل التدمير الناعمة كالفيروسات ولا يستخدم العنف مثل الجرائم التقليدية ولذلك أطلق عيها البعض مسميات عديدة منها الجرائم النظيفة، الجرائم الناعمة. إلا أن ذلك لا يعني ضرورة أن يكون مجرم الإنترنت على قدر كبير من العلم في هذا المجال، فالواقع العملي أثبت أن أشهر مجرمي الإنترنت لم يحصلوا على مهاراتهم التقنية عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المضمار[1].

المطلب الثاني

أركان الجريمة المعلوماتية وأنواعها

لكل سلوك إجرامي عقوبة تتناسب مع الخطورة الكامنة في نفس فاعل الجريمة وتلك معادلة طبيعية عادلة ولازمة لنجاة البشرية واستقرارها في حياة آمنة مطمئنة، فكل جريمة لها أركانها الخاصة بها حددها المشرع لمعاقبة كل من ينتهج السلوك الإجرامي إذا انتفى أحدها لا تقوم الجريمة ولا يبقى لها وجود ولا تترتب على الفعل المسؤولية الجنائية وهذه الأركان تختلف من جريمة إلى أخرى بحسب نوعها وطبيعتها، ولذلك سنحدد هذه الأركان في الجريمة المعلوماتية أولاً ثم ننتقل لنوضح أنواع هذه الجريمة ثانياً، كما يأتي:

أولاً: أركان الجريمة المعلوماتية: إذا كانت الجرائم العادية تتكون من أركان تتصل فيما بينها حيث أن غياب أي ركن منها يؤدي إلى زوال النموذج الإجرامي للفعل، فإن جرائم تقنية المعلومات تتطابق مع الجرائم العادية وبذلك فهي تتكون من الأركان الآتية:

1_ الركن المادي: إن طبيعة الركن المادي بالجريمة المعلوماتية تثير بعض الإشكاليات لأن مفهوم أو مناط التجريم ينصب على نظام إلكتروني يساء استعماله أو يتم اقتحامه على نحو غير مشروع، بما يكون لذلك الاستعمال أو الاقتحام من أثر مادي ملموس يظهر إما في صورة تدمير للمعلومات، وهو ما يثير إمكانية الإتلاف العمدي للمنقولات، أو السرقة وذلك عن طريق إساءة استعمال بطاقات الائتمان مثلاً. فالسلوك الإجرامي في الجريمة المعلوماتية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي، أو تلك التي يتم إدخالها للحاسب الآلي، وصعوبة المشكلة أو السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة[2]. أي الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك مادياً بها، تماما مثل التيار الكهربائي الذي يسري في توصيلة

[1] - د. نائلة عادل محمد فريد قورة (2005)، جرائم الحاسوب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ص57

[2] - سميرة معاشي (2011)، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد 7، جامعة محمد خيضر بسكرة، الجزائر، ص280.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

دون أن نراه[1]. أما في الجريمة التقليدية فالسلوك الإجرامي بوصفه عنصراً في الركن المادي فيتم رؤيته والتأكد منه كفعل القتل أو السرقة.

فالنشاط أو السلوك المادي في الجريمة المعلوماتية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الإنترنت، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته. ولكي يتوافر الركن المادي في الجريمة المعلوماتية، فلا بد من حصول النتيجة الإجرامية على أن ترتبط بالسلوك الإجرامي بعلاقة سببية. لذلك يتعين تحليل السلوك الإجرامي في الجريمة المعلوماتية في كل نوع من أنواعها بشكل مستقل.

2_ الركن المعنوي: إذا كان الركن المادي للجريمة هو الوجه الخارجي المحسوس للسلوك المكون لها فإن ركنها المعنوي هو الوجه الباطني أو النفساني لهذا السلوك الذي لا يتعدى انتساب السلوك الإجرامي إلى نفسية صاحبه فهو الرابطة النفسية بين الفعل والفاعل وقد يتخلف هذا الانتساب النفسي حين يصبح جسم الإنسان أداة في يد قوة خارجية عنه وتفلت سيطرة صاحبه عليه. على أن كيفية انتساب السلوك إلى نفسية صاحبه ليست واحدة، فحين ينتج السلوك حدثا إجرامياً ما يحتمل أن تكون نفسية صاحب متخذه من هذا الحدق موقفاً من ثلاثة مواقف وهي[2]:

_ إما الإرادة الدافعة إلى تحقيق الحدث (هو ما يسمى القصد المباشر)

_ وأما الإرادة المؤيدة لوقوعه (وهو ما يسمى القصد غير المباشر)

_وأما محض الإرادة الخاملة (وهو ما يسمى الإهمال وعدم المبالاة)

ولكل حالة من هذه الحالات أحكامها في تحديد الركن المعنوي للجريمة ففي الوقت الذي يتطلب فيه الركن المعنوي إرادة كاملة متجهة نحو تحقيق السلوك الإجرامي وعلم كامل بكافة عناصره فهنا يتحقق العمد في ارتكاب الجريمة أما إذا كان السلوك ناتجا عن إهمال وعدم انتباه وعدم مراعاة القوانين والأنظمة فإن الفاعل يكون قد ارتكب خطأ قد يحاسب عليه القانون.

وهذا التحليل للركن المعنوي في الجرائم التقليدية ينطبق على الجرائم المعلوماتية فالفاعل عندما يرتكب جريمة من هذه الجرائم يجب أن تتوافر العلاقة النفسية بين الفعل والفاعل في صورة علم بكل عناصر السلوك المادي وإرادة متجهة نحو هذه العناصر ولهذا نجد أن توافر الركن المعنوي في الجريمة المعلوماتية يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها.

3_ الركن القانوني: وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب للجرائم المعلوماتية في ماورد النص عليه في قانون مكافحة الجريمة المعلوماتية السوري.

ثانياً: أنواع الجريمة المعلوماتية:

تقسم جرائم المعلوماتية إلى نوعين[3]: الأول: الجرائم التقليدية التي ترتكب بواسطة نظم المعلومات وخاصة شبكة الإنترنت، وهي تلك الجرائم التي كانت موجودة قبل عصر المعلومات، ولكن بعد ظهور هذه التقنية وانتشار الشبكات أصبحت ترتكب بواسطتها، فراحت تبدو وكأنها جرائم جديدة. ومن هذه الجرائم: جريمة التهديد بالقتل وجريمتي الذم والقدح التي ترتكب عبر البريد الإلكتروني، والجرائم المخلّة بالأخلاق والآداب العامة التي ترتكب عبر المواقع الإباحية وغير ذلك من الجرائم.

---

[1] - عبد الفتاح بيومي حجازي (2004)، جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ص148.

[2] - مجمود نجيب حسني (1971)، النظرية العامة للقصد الجنائي، دار النهضة العربية، ص90.

[3] - د. حسين بن سعيد الغافري (2009ـ)، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، ص79 و217.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

أما النوع الثاني: فهي الجرائم المستحدثة، ويقصد بها تلك الجرائم التي ظهرت في عصر تقنية المعلومات ولم تكن معروفة من قبل وخاصة بعد اختراع الإنترنت، ومن أمثلة هذه الجرائم: جريمة الدخول غير المصرح به إلى أنظمة الحاسوب أو المواقع الإلكترونية، وجريمة تعطيل أو عرقلة نظام معلوماتي، وجريمة إتلاف المعلومات عن طريق زرع الفيروسات وغيرها من الجرائم.

المبحث الثاني

التشريعات السورية في مواجهة الجريمة المعلوماتية

أضحى التطور التقني في مجال تقنية المعلومات مادة أساسية في حياة الإنسان الغني أو الفقير على حداً سواء لا يستطيع أحد الاستغناء عنها، وأصبح هذا الفضاء الواسع وعاء تضخ فيه كافة المعلومات والبيانات العامة والخاصة. وحوى الكثير من المنابر والصفحات العامة والخاصة والمدونات للتعبير عن الرأي والإعلان والتعليم والتوجيه والترغيب والترهيب. وصار بالمقابل مسرحاً لارتكاب جرائم ومخالفات لم تكن معروفه بشكلها الحالي قبل استخدام شبكة الانترنت وتطبيقاتها. وبالتالي أصبح لزاماً على المشرع وضع التقنيين اللازم والضروري لضبط استخدام الشبكة المعلوماتية ومراقبة محتواها. وهذا ما فعله المشرع في سورية بداية من خلال صدور المرسوم التشريعي رقم /17/ لعام 2012 المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

إلا أن التطور التقني فائق السرعة وما رافقه من انتشار واسع بشكل غير مسبوق للجريمة المعلوماتية بصور وأشكال حديثة ومبتدعة غير مسبوقة. كل ذلك دفع المشرّع السوري لإعادة النظر في التشريع الموجود والعمل على تحديثه بما يوافق التطورات الحاصلة، وبما يضمن توفير حماية أكبر للمصالح القانونية العامة والخاصة، وتنظيم الحريات في العالم الافتراضي والحد من إساءة استعمال الوسائل التقنية. وكان ذلك فعلاً بصدور القانون رقم 20 للعام 2022. وسيتم مناقشة هذا التعديلات كما يلي:

المطلب الأول

الجرائم المستحدثة في المرسوم التشريعي رقم 17 لعام 2012

نظراً لحداثة موضوع الجرائم الالكترونية نجد أن المشرع السوري عمد بداية في المرسوم التشريعي رقم 17 لعام 2012 إلى الوقوف على أهم الجرائم المستحدثة بسبب ثورة المعلوماتية، بحيث تناول هذه الجرائم بالتحليل وأفرد لها الفصل الثالث من هذا المرسوم، ولذلك سنناقش هذه الجرائم بالترتيب كما وردت في المرسوم، كما يلي:

1_ الدخول غير المشروع إلى منظومة معلوماتية

نصت المادة 15 على: " /أ/ يعاقب بالغرامة من عشرين ألفا إلى مئة ألف ليرة سورية كل من دخل قصدا بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع الكتروني على الانترنت دون ان يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك.

/ب/ وتكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل اليها أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها".

الواضح من هذا النص أن المشرع السوري لم يشترط أن ينجح الفاعل في الوصول إلى المعلومات المخزنة لتحقق هذه الجريمة، وإنما يكفي أن يدخل إلى النظام المعلوماتي، بطريقة غير مشروعة أي دون إذن أو ترخيص من الشخص المسؤول عن هذا النظام. كما يجب أن يكون قاصدا ذلك أي تتجه إرادته إلى هذا الدخول غير المشروع، فإذا اعتقد الفاعل

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

بناء على أسباب معقولة بأن له الحق في الدخول إلى النظام المعلوماتي فإن القصد الجرمي لا يتوفر لديه. بل يجب أن يتجه علم الجاني إلى أن فعله سيؤدي إلى الدخول إلى حاسوب أو منظومة معلوماتية أو موقع إلكتروني، ويجب أن يعلم بأن ليس له الحق أو الصلاحية في هذا الدخول.

وشدد المشرع السوري عقوبة الدخول غير المشروع في حال تم أخذ نسخة من المعلومات أو إتلافها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها.

2_ جريمة شغل اسم موقع الكتروني

نصت المادة (16) على: " يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من شغل اسم موقع الكتروني من دون علم صاحبه أو حد من قدرة مالك نطاق على الإنترنت على التحكم في هذا النطاق".

ويتمثل النشاط الجرمي في جريمة شغل اسم موقع إلكتروني من دون علم صاحبه بانتحال شخصية موقع إلكتروني، وهو شكل من أشكال سرقة الهوية على الإنترنت[1]. ويتم هذا الأسلوب عن طريق إنشاء مواقع مزيفة على شبكة الإنترنت، على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة، بحيث يبدو هذا الموقع المزيف وكأنه الموقع الأصلي المقدم لتلك الخدمة. ويقوم الجناة عادة بالحصول على البيانات الخاصة بالموقع الأصلي وعنوانه ورقمه عن طريق الإنترنت، ثم يستخدمون هذه البيانات لإنشاء الموقع المزيف بحيث يبدو للعيان شبيها بالموقع الأصلي، وبعد ذلك يقومون بتعديل البيانات السابقة على الموقع الأصلي، بحيث لا يكون على الإنترنت إلا موقع واحد بنفس العنوان. وهنا تظهر النتيجة الجرمية المتمثلة بالحد من قدرة صاحب الموقع من التحكم بموقعه[2]. ولكي تتحقق هذه الجريمة لابد من اكتمال ركنها المادي والمعنوي أي لابد أن تتجه إرادة الجاني إلى انتحال شخصية موقع إلكتروني دون علم صاحبه أو الحد من قدرة مالكه من التحكم به.

3_ جريمة إعاقة الوصول إلى الخدمة

نصت المادة (17) على: " يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من أعاق أو منع قصدا بأي وسيلة كانت الدخول إلى منظومة معلوماتية أو الشبكة أو عطلها أو أوقفها عن العمل أو أعاق أو منع قصدا باي وسيلة كانت الوصول إلى الخدمات أو البرامج أو المواقع الالكترونية أو مصادر البيانات أو المعلومات عليها".

اعتبر المشرع السوري إعاقة الوصول إلى منظومة المعلوماتية أو إلى الشبكة سواء كانت الإعاقة بشكل كامل أو بشكل جزئي ومهما كانت الوسيلة المرتكبة جريمة يعاقب عليها القانون في حالة توفر القصد الجرمي العام بعنصرية العلم والإرادة. فيجب أن تتجه إرادة الجاني إلى حرمان المجني عليه من الدخول إلى منظومة المعلومات أو الشبكة.

4_ جريمة اعتراض المعلومات

نصت المادة (18) على: " /أ/ يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من اعترض او التقط قصدا بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة أو تنصت عليها.

/ب/ يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من استخدم الخداع للحصول على معلومات شخصية او سرية من المستخدمين على منظومة معلوماتية أو الشبكة يمكن استغلالها لأغراض إجرامية".

---

[1] - د. طارق الخن، مرجع سابق، ص36.

[2] - د. جميل عبد الباقي الصغير (2003)، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، القاهرة، ص37.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

يتمثل السلوك الإجرامي في قيام الفاعل بالتدخل غير المشروع لمعرفة محتوى الاتصالات التي تتم عبر شبكات المعلومات داخل نظام المعلوماتية، أو بين أنظمة معلوماتية مختلفة حيث يقوم بالتقاط المعلومات المتضمنة في هذا الاتصال. ويختلف الدخول غير المصرح به إلى نظام المعلوماتية عن اعتراض هذه النظام من حيث النشاط الإجرامي في كل منهما، فالدخول إلى النظام لا يتأتى إلا بتشغيله للولوج إلى ما يحتوي عليه من معلومات، أما في حالة التقاط المعلومات عن طريق اعتراض النظام فإن عملية تشغيله تكون قد بدأت بالفعل بواسطة شخص آخر غير الجاني، واقتصر دور الفاعل على اعتراضه للوصول إلى المعلومات التي تتضمنها عملية الاتصال[1]. ولكن يتفق الدخول غير المصرح به إلى نظام المعلوماتية واعتراض هذه النظام من حيث أن الجريمتان تتطلبان القصد الجرمي العام بعنصرية العلم والإرادة. فيجب أن يعلم الفاعل أن ليس له الحق في اعتراض أو التقاط المعلومات أو التنصت عليها، ثم يجب أن تتجه إرادته إلى اعتراض هذه المعلومات.

وهناك وسيلة تستخدم في هذا المجال تعرف بالتقاط الموجات الكهربائية وهي جمع للمعلومات عن بعد، فمن الممكن جمع معلومات يتم إرسالها من أحد الحواسيب داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، حيث يتم التقاط الموجات الكهربائية التي تحيط بالحاسوب ثم يتم تحويلها إلى معلومات مقروءة على الشاشة[2].

5- جريمة تصميم البرمجيات الخبيثة واستخدامها

عرف المشرع السوري البرمجيات الخبيثة في المادة الأولى من المرسوم رقم 17 بقوله: " برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الالكترونية أو الشبكة أو تعطيل عملها أو تبطئته أو تخريب محتوياتها أو مواردها او جمع معلومات عنها أو عن مالكيها أو مستخدميها أو عن بياناتهم دون إذنهم أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بصورة غير مشروعة."

ونصت المادة (19) من نفس المرسوم على عقوبة تصميم أو ترويج أو حتى استخدام هذه البرمجيات بقصد الإضرار بأنظمة المعلومات بقولها: " أ_ يعاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية كل من يقوم بتصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية.

ب-يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية كل من استخدم البرمجيات الخبيثة أيا كان نوعها وبأي وسيلة كانت بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة". ونلاحظ تشدد المشرع السوري في عقوبة استخدام هذه البرمجيات لأن الآثار التي تنتج عنها غير محددة فشخصية المجني عليه وعدد الضحايا غير محدد وذلك نتيجة قدرة الفيروس على نسخ نفسه والانتقال من حاسب إلى آخر فمن الصعوبة السيطرة عليها بعد نشرها واستخدامها.

6_ جريمة إرسال البريد الواغل

عرف المشرع السوري في المرسوم رقم 17 في المادة الأولى البريد الواغل بقوله: " أي شكل من اشكال الرسائل مهما كان محتواها التي ترسل على الشبكة الى الغير دون رغبة المتلقي في وصولها إليه". ونصت المادة (20) من نفس المرسوم على: " يعاقب بالغرامة من عشرين ألفا إلى مئة ألف ليرة سورية كل من يقوم بإرسال بريد واغل الى الغير إذا كان المتلقي لا يستطيع إيقاف وصوله إليه أو كان إيقاف وصوله مرتبطا بتحمل المتلقي نفقة إضافية". ونلاحظ هنا أن المشرع السوري

[1] - أ. عباوي نجاة (2017)، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاتر السياسة والقانون، العدد16 لعام، ص285

[2] - د. نائلة عادل محمد فريد قورة، مرجع سابق، 350.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

لم يشترط أن يحتوي البريد الواغل على معلومات معينة حتى يتم تجريمه بل فقط اشترط لتحقق هذه الجريمة أن يكون المتلقي أو المرسل إليه غير قادر على إيقاف وصول الرسائل غير المرغوب فيها له، أو كان إيقاف وصولها مرتبط بتحمل المتلقي نفقات إضافية على نفقات الاشتراك بخدمة البريد الإلكتروني.

7_ جريمة الاحتيال عن طريق الشبكة

موضوع الاحتيال هو ذلك الشيء الذي يرد عليه التسليم الصادر من المجني عليه إلى المحتال نتيجة الغلط الذي أوقعه فيه[1]. والاحتيال عبر الشبكة لا يختلف عن الاحتيال التقليدي فالفعل نفسه هو فعل الخداع ولكن يمارسه الجاني عن طريق الشبكة أو الأجهزة الحاسوبية. وقد حدد المشرع السوري عقوبة الاحتيال عن طريق الشبكة بنص المادة 21 التي تضمنت:

" /أ/ يعاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية كل من استولى باستخدام الأجهزة الحاسوبية أو الشبكة على مال منقول أو عقار أو معلومات أو برامج ذات قيمة مالية او سند يتضمن تعهداً أو إبراءً أو أي امتياز مالي آخر وذلك عن طريق خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه بأي وسيلة كانت.

/ب/ وتكون العقوبة الاعتقال المؤقت والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية في الحالات التالية:

1- إذا وقعت الجريمة على ثلاثة اشخاص فأكثر.

2- إذا تجاوز مبلغ الضرر مليون ليرة سورية.

3- إذا وقع الاحتيال على مصرف أو مؤسسة مالية.

ج- ولا تطبق الاسباب المخففة التقديرية إلا إذا أسقط المضرور حقه الشخصي".

ونلاحظ أن المشرع شدد العقوبة إلى الاعتقال المؤقت في هذه الظروف الثلاثة بسبب خطورة الجاني فعندما يتعدد المجني عليهم، أو عندما يكون حجم الضرر كبيراً، أو عندما يكون المجني عليه ذو صفة مصرفية. ولا يؤخذ بالأسباب المخففة التقديرية إلا إذا أسقط المضرور حقه الشخصي.

8_ جريمة الاستعمال غير المشروع لبطاقات الدفع

عرف المشرع السوري في المادة الأولى من المرسوم رقم 17 بطاقة الدفع بقوله:" بطاقة ذات أبعاد قياسية تصدرها عادة المصارف أو المؤسسات المالية وما بحكمها وتستخدم في عمليات الدفع أو الائتمان أو سحب الأموال أو تحويلها عن طريق حساب أو محفظة مصرفية." ولهذه البطاقة أنواع متعددة منها (بطاقات سحب النقود، بطاقات وفاء، بطاقات الاعتماد، بطاقات الائتمان..) [2]. وقد شاع استخدام هذه البطاقات بشكل كبير في الآونة الأخيرة وأصبحت أكثر استخداماً وانتشاراً لذلك شدد المشرع السوري في

المادة (22) على عقوبة إساءة استعمال هذه البطاقة بقوله: " /أ/ يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية كل من حصل دون وجه حق على بيانات أو أرقام بطاقة دفع باستخدام الأجهزة الحاسوبية أو الشبكة.

/ب/ يعاقب بالحبس من ثلاث الى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية كل من:

[1] - د. محمود نجيب حسني (1998)، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، منشورات الحلبي الحقوقية، بيروت، ص382.

[2] - د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، مرجع سابق، ص15.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

1- قام بتزوير بطاقة دفع.

2- استعمل بطاقة دفع مزورة أو مسروقة أو مفقودة في الدفع أو سحب النقود".

9_ انتهاك حرمة الحياة الخاصة

الخصوصية كما عرفها المشرع السوري في المادة الأولى من المرسوم رقم 17 هي: " حق الفرد في حماية اسراره الشخصية والملاصقة للشخصية والعائلية ومراسلاته وسمعته وحرمة منزله وملكيته الخاصة وفي عدم اختراقها او كشفها دون موافقته". ونظراً لارتباط هذا الموضوع بالشخصية الإنسانية وعلاقاتها سواء العاطفية أو الصحية أو المدنية ...إلخ فقد شدد المشرع السوري عقوبة نشر إي معلومة (حتى لو صحيحة) دون رضاء صاحب العلاقة في المادة 23 التي نصت على: " يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه حتى ولو كانت تلك المعلومات صحيحة".

كما تضمن الفصل الخامس من هذا القانون الأحكام العامة المتعلقة بالجريمة المعلوماتية كالظروف المشدة التي تشمل جميع نصوصه التجريمية، والشروع، والعلنية، والمصادرة وغيرها من القواعد العامة المتعلقة بالجرائم التقليدية والنواحي الإجرائية.

المطلب الثاني

التعديلات التشريعية التي تضمنها القانون رقم 20 لعام 2020

نعيش اليوم في عصر التكنولوجيا وما يعرف بالعالم الافتراضي فلا يخلو منزل من حاسوب، ولا تخلو يد من هاتف ذكي أو جهاز لوحي. وبات التواصل من خلال العالم الافتراضي هو الطابع العام للمجتمعات كافة. حتى غدا هذا التواصل بديلاً فيما يتعلق بتقديم أغلب الخدمات العامة وحتى الخاصة عند البعض. ولذلك كان من الضروري أن يواكب المشرع السوري التطورات التقنية المتسارعة وذلك للحد من التجاوزات المسيئة على الشبكة التي تؤثر سلباً على الدولة والمجتمع. لذا تم العمل على إضافة تعديلات للمرسوم التشريعي رقم 17 لعام 2012 تتوافق مع التطورات في قطاع الاتصالات وتكنولوجيا المعلومات. تراوحت هذه التعديلات بين إضافات لجرائم مستحدثة لم ينص عليها المرسوم رقم 17 وبين مضاعفة عقوبات نص عليها بحيث تتدرج العقوبات والغرامات التي نص عليها القانون بحسب نوع الجريمة المعلوماتية بدءاً بالسجن لمدة شهر إلى السجن لمدة 15 سنة، بالإضافة إلى السجن المؤبد في بعض الحالات، في حين تتراوح الغرامات المالية عن العقوبات ما بين 200 ألف إلى 25 مليون ليرة سورية.

وجاءت الجرائم المعلوماتية مذكورة على سبيل الحصر في الفصل الرابع من القانون رقم 20 وبلغت 21 جريمة معلوماتية سنذكرها بالترتيب كما وردت في القانون كما يلي:

1_ تجاوز حدود الدخول المشروع

عاقب المشرع السوري في المادة 11 بغرامة من ثلاثمئة ألف ليرة سورية إلى أربعمئة ألف ليرة سورية كل من دخل إلى نظام معلومات، أو موقع إلكتروني أو حساب شخصي بشكل مشروع فتجاوز حدود هذا الدخول، وشدد العقوبة لتصبح الحبس من ثلاثة أشهر إلى ستة أشهر وغرامة من خمسمئة ألف ليرة سورية إلى سبعمئة ألف ليرة سورية إذا وقع التجاوز على نظام معلومات أو موقع إلكتروني أو حساب شخصي عائد لجهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة. ويقع على المضرور إثبات القرائن الدالة على الضرر الحاصل في تجاوز حدود الدخول المشروع وتقديم هذه القرائن لمحكمة الجريمة المعلوماتية.

أما إذا قام الفاعل بنسخ المعلومات التي وصل إليها، أو استخدمها، أو أفشاها، أو حذفها، أو قام بتعديلها فيعاقب بالحبس من ستة أشهر إلى سنة وغرامة من سبعمئة ألف ليرة سورية إلى مليون ليرة سورية وتشدد العقوبة لتصبح السَّجن

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

المؤقت من ثلاث سنوات إلى خمس سنوات، وغرامة من مليوني ليرة سورية إلى ثلاثة ملايين ليرة سورية إذا كانت المعلومات عائدة لجهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة.

أما إذا قام الفاعل بنسخ المعلومات التي وصل إليها ثم قام بحذفها من منظومة المعلومات أو الموقع أو الحساب الشخصي الذي دخل إليه بشكل غير مشروع فيُعاقب بالحبس من سنتين إلى ثلاث سنوات وغرامة من ثلاثة ملايين ليرة سورية إلى أربعة ملايين ليرة سورية.

وتشدد القانون السوري عند وقوع الجرم على الجهات العامة والمشتركة والمؤسسات المالية وذلك لحمايتها من تبعات الجريمة على أن يبقى للقضاء المختص تقدير قيمة الضرر الحاصل بناء على ادعاء من الشخص العادي أو الاعتباري.

2_ الدخول غير المشروع

يعاقب المشرع السوري في المادة 12 كل من يدخل (اختراقاً)[1] جهازاً حاسوبياً أو منظومة معلوماتية أو موقع إلكتروني أو حساب شخصي بدون تصريح أو موافقة مسبقة من صاحب المنظومة وبأي طريقة كانت سواء عن طريق الشبكة أو احتيالاً، بالحبس من شهر إلى ستة أشهر وغرامة من ثلاثمئة ألف ليرة سورية إلى أربعمئة ألف ليرة سورية. فهنا مجرد الدخول غير المشروع بدون إذن أو رضى صاحب العلاقة يشكل جريمة.

أما إذا قام الفاعل بنسخ المعلومات التي وصل إليها، أو استخدمها، أو أفشاها، أو حذفها، أو قام بتعديلها فيعاقب بالحبس من سنة إلى ثلاث سنوات وغرامة من مليون ليرة سورية إلى مليوني ليرة سورية.

أما إذا قام الفاعل بنسخ المعلومات التي وصل إليها ثم حذفها، أي قام بفعل السرقة، فيعاقب بالحبس من ثلاث سنوات إلى خمس سنوات وغرامة من خمسة ملايين ليرة سورية إلى ستة ملايين ليرة سورية

3_ شغل اسم موقع إلكتروني

عاقب المشرع السوري في المادة 13 كل من شغل اسم موقع إلكتروني دون رضا صاحبه بالحبس من ثلاثة أشهر إلى ستة أشهر وغرامة من ثلاثمئة ألف ليرة سورية إلى خمسمئة ألف ليرة سورية. وتُشدد العقوبة لتصبح الحبس من ستة أشهر إلى سنة وغرامة من مليون ليرة سورية إلى مليوني ليرة سورية إذا كان الموقع الإلكتروني عائداً لجهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة. وينطبق ذلك على كل من يقوم بشغل اسم موقع إلكتروني مسجل سواء على الشبكة داخل سورية أو خارجها.

4_ انتحال الحساب الشخصي

عاقب المشرع السوري في المادة 14 بغرامة من ثلاثمئة ألف ليرة سورية إلى خمسمئة ألف ليرة سورية كل من انتحل الحساب الشخصي للغير وذلك كأن يقوم المنتحل باستخدام البيانات الشخصية لشخص ما دون رضاه وإنشاء حساب على الانترنت على أحد التطبيقات التي يتم استخدامها. أما إذا استخدم الفاعل الحساب الشخصي المنتَحل كأن يرسل طلبات الصداقة باسمه بهدف الكسب غير المشروع أو الابتزاز أو أي فعل آخر بدون رضا صاحب الحساب الشخصي، فيعاقب بالحبس من ثلاثة أشهر إلى ستة أشهر وغرامة من مليون ليرة سورية إلى مليوني ليرة سورية.

5_ إعاقة أو منع الوصول إلى الخدمة

يُعاقب وفقاً للمادة 15 بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من ثلاثمئة ألف ليرة سورية إلى خمسمئة ألف ليرة سورية كل من عطل (سواء بشكل كلي أو جزئي) أو أوقف أو أعاق أو منع الدخول إلى الشبكة أو نظام معلومات، أو الوصول

[1] - ويطلق على هؤلاء الذين يدخلون إلى أنظمة الحاسب الآلي بدون تصريح بالمخترقين، وتختلف أهداف الاختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لسرقة أو تغيير أو إزالة معلومات معينة، وقد يقوم المخترق بجريمته بقصد إظهار قدراته على الاختراق وفي كلا الحالتين يعتبر هذا الدخول مجرم ومعاقب عليه قانونياً.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

إلى الخدمات أو الحساب الشخصي أو البرامج أو المواقع الإلكترونية أو مصادر المعلومات أو حدّ من قدرة مالك نطاق على التحكم به باستخدام إحدى وسائل تقانة المعلومات. سواء أكان ذلك بتخريب البرمجيات أو البيانات، أو بإغراق المنظومة المعلوماتية بما يفوق طاقتها الاستيعابية، أو قطع الاتصال عنها، أو أي وسيلة معلوماتية أخرى

6_ تصميم أو ترويج أو استخدام البرمجيات الخبيثة

يعاقب المشرع وفقا للمادة 16 بالحبس من سنة إلى ثلاث سنوات وغرامة من ثلاثة ملايين ليرة سورية إلى خمسة ملايين ليرة سورية كل من قام لغايات إجرامية:

1. بتصميم البرمجيات الخبيثة.
2. بترويج البرمجيات الخبيثة.

ويُعاقب بالسَّجن المؤقت من خمس سنوات إلى سبع سنوات وغرامة من ستة ملايين ليرة سورية إلى عشرة ملايين ليرة سورية كل من استخدم البرمجيات الخبيثة بقصد الإضرار بوسائل تقانة المعلومات أو نظم المعلومات أو الشبكة أو الحساب الشخصي. أما استخدام البرمجيات الخبيثة لدراستها من أجل أغراض البحث والعلم والتطوير، بهدف التصدي لها، فلا يدخل في نطاق تطبيق هذه العقوبة كما لا يدخل ضمن نطاق هذه المادة البرمجيات الخبيثة التي يتم تصميمها من قبل المبرمجين الهواة لأغراض التسلية وطالما لم يتم الترويج لها بهدف الكسب المادي أو بيعها ولا يدخل فيها البرمجيات التي يتم تصميمها وبيعها للكشف على البرمجيات الخبيثة مثل برامج مكافحة الفيروسات.

7_ إرسال رسائل غير مرغوب بها

يعاقب وفقاً للمادة 16 بغرامة من مئة ألف ليرة سورية إلى مئتي ألف ليرة سورية كل من يقوم بإرسال رسالة أو معلومات عبر الشبكة إلى الغير مهما كان محتواها بشكل متكرر دون رغبة المتلقي في استلامها، وكان غير قادر على إيقافها أو أن إيقاف وصولها مرتبط بتحمله نفقة إضافية. وأياً كان الغرض سواء الترويج أو التسويق أو الإزعاج، أو أي غرض آخر.

8_ اعتراض المعلومات

كل من اعترض أو التقط بوجه غير مشروع المعلومات المتداولة على نظام معلومات أو الشبكة، أو تنصت عليها باستخدام إحدى وسائل تقانة المعلومات يُعاقب وفقاً للمادة 18 بالحبس من ثلاثة أشهر إلى سنة وغرامة من خمسمئة ألف ليرة سورية إلى مليون ليرة سورية. وهذا ينطبق على كل شخص أقدم قاصداً، بوجه غير مشروع، على تلقي أو التقاط المعلومات المتداولة على منظومة معلوماتية أو على الشبكة، أو التنصت عليها، بوسائل معلوماتية، وذلك عند نقلها من أو إلى أو في منظومة معلوماتية، سواء جرى استغلال هذه المعلومات لاحقا أم لا، وهو ما يعرف بالتجسس الإلكتروني. ويفترض في هذا الفعل أيضاً أن تكون المعلومات المعنية غير متاحة أصلاً لاطلاع العامة عليها، أي لا يمكن الوصول إليها إلا من قبل المخولين بذلك

9_ الاحتيال المعلوماتي

يُعاقب وفقا للمادة 19 بالسَّجن المؤقت من ثلاث سنوات إلى خمس سنوات وغرامة من ثلاثة ملايين ليرة سورية إلى خمسة ملايين ليرة سورية كل من استخدم وسائل تقانة المعلومات للاستيلاء احتيالاً على معلومات أو برمجيات أو مال منقول أو عقار أو سند يتضمن تعهداً أو إبراءً أو أي امتياز مالي آخر مملوكاً أو عائداً للغير عن طريق الشبكة.

10_ إساءة الائتمان المعلوماتي

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

يعاقب وفقاً للمادة 20 بالحبس من سنة إلى ثلاث سنوات وغرامة من ثلاثمئة ألف ليرة سورية إلى خمسمئة ألف ليرة سورية كل من ائتمن على معلومات أو برمجيات نقلت إليه على سبيل الحيازة الناقصة بواسطة وسائل تقانة المعلومات إذا قام بتغيير حيازته إلى حيازة كاملة.

ويُعاقب بالحبس من ستة أشهر إلى سنة وغرامة من مئتي ألف ليرة سورية إلى أربعمئة ألف ليرة سورية كل من رفض إعادة معلومات أو برمجيات دخلت في حيازته غلطاً أو بصورة طارئة أو بقوة قاهرة بواسطة وسائل تقانة المعلومات. أي من تنتقل له حيازة الشيء بمقتضى سند من دون أن يخوله ذلك أي حق في الملكية، كما لو تم إرسال بريد الكتروني (عبر منظومة معلوماتية مرفق به ملف لتصميم برمجي ما) إلى شخص معين وبالخطأ دخل في حساب شخص آخر وقام الأخير بالاستيلاء عليه والاستفادة منه دون رده إلى صاحبه الأصلي رغم مطالبة صاحبها الأصلي بردها أو حذفها.

11_ انتهاك الخصوصية

يعاقب المشرع السوري وفقا للمادة 21 بالحبس من شهر إلى ستة أشهر وغرامة من خمسمئة ألف ليرة سورية إلى مليون ليرة سورية كل من قام بواسطة إحدى وسائل تقانة المعلومات بنشر معلومات على الشبكة تتعلق بالخصوصية من دون رضا صاحبها حتى لو كانت صحيحة. فلا يعتد بكون المعلومات المنشورة صحيحة أم لا، إذا كان نشرها قد تم من دون رضا الشخص المعني فمثلاً نشر خبر مرض أحد أفراد أسرة صديق له دون موافقته حتى لو كان المرض صحيح.

12_ الجرائم المتعلقة بالبطاقة الإلكترونية

يعاقب المشرع السوري وفقا للمادة 22 بالحبس من ستة أشهر إلى سنة وغرامة من مليوني ليرة سورية إلى ثلاثة ملايين ليرة سورية كل من حصل دون وجه حق باستخدام وسائل تقانة المعلومات أو الشبكة على معلومات بطاقة إلكترونية.

أما من قلَّد أو زيف أو زوّر بطاقة إلكترونية فيعاقب بالحبس من سنة إلى ثلاث سنوات وغرامة من ثلاثة ملايين ليرة سورية إلى أربعة ملايين ليرة سورية.

وكذلك يعاقب المشرع السوري كل من استعمل بطاقة إلكترونية مقلَّدة أو مزيفة أو مزورة إذا أفضى الاستعمال إلى تحقيق منفعة مادية أو كل من استعمل بطاقة إلكترونية مفقودة أو مسروقة أو سلمت له على سبيل الحيازة الناقصة إذا أفضى الاستعمال إلى تحقيق منفعة مادية.

13_ التسجيل غير المشروع

كل من استخدم وسائل تقانة المعلومات للحصول على تسجيلات صوتية أو مرئية أو التقط صوراً تخص أحد الناس من دون رضاه يعاقب وفقا للمادة 23 بالحبس من شهر إلى ستة أشهر وغرامة من خمسمئة ألف ليرة سورية إلى مليون ليرة سورية، وذلك كما في حال قيام أحد ما خلال اجتماع أو احتفال أو جلسة بتسجيل المكالمات الصوتية أو مكالمات الفيديو أو التقاط الصور لأشخاص دون علمهم أو رضاهم بقصد إثبات واقعة أو التهديد بالنشر للابتزاز أو التكسب المادي.

14_ الذم الإلكتروني

يُعاقب وفقاً للمادة 24 بغرامة من مئتي ألف ليرة سورية إلى ثلاثمئة ألف ليرة سورية كل من قام بإحدى وسائل تقانة المعلومات بذمّ أحد الناس بشكل غير علني باستخدام الشبكة.

يعاقب بالحبس من شهر إلى ثلاثة أشهر وغرامة من ثلاثمئة ألف ليرة سورية إلى خمسمئة ألف ليرة سورية كل من قام بإحدى وسائل تقانة المعلومات بذمّ أحد الناس بشكل علني على الشبكة. وتم التفريق بين العلنية والغير علنية في العقوبات لأن الذم على الشبكة يصل إلى عدد كبير من الناس وبسرعة كبيرة يفوق بأضعاف عددهم فيما لو تم الذم بين مجموعة من الأشخاص في الحياة العادية. والغاية الأساسية هي حماية الشرف والكرامة والاعتبار لدى الشخص مما يمسه

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

من أفعال خطيره من خلال إسناد وقائع قد تحتمل التصديق والاحتمال لدى السامع أو القارئ، ولما تتخذه من علنية تؤدي إلى سقوط شرف واعتبار وكرامة المجني عليه لدى فئة كبيرة من الناس.

15_ القدح أو التحقير الإلكتروني

يعاقب وفقاً للمادة 25 بغرامة من مئة ألف ليرة سورية إلى مئتي ألف ليرة سورية كل من قام بإحدى وسائل تقانة المعلومات باقتراف القدح أو التحقير بأحد الناس بشكل غير علني باستخدام الشبكة. كما يعاقب بالحبس من عشرة أيام إلى شهرين وغرامة من مئتي ألف ليرة سورية إلى ثلاثمئة ألف ليرة سورية كل من قام بإحدى وسائل تقانة المعلومات باقتراف القدح أو التحقير بأحد الناس بشكل علني على الشبكة.

16_ جرائم المساس بالحشمة أو الحياء

يُعاقب وفقا للمادة 26 بالحبس من ستة أشهر إلى سنة وغرامة من مليون ليرة سورية إلى مليوني ليرة سورية كل من قام بمعالجة صور ثابتة أو متحركة أو محادثات أو تسجيلات صوتية عائدة لأحد الناس بوسائل تقانة المعلومات لتصبح منافية للحشمة أو الحياء وقام بإرسالها له أو للغير أو عرضها عليه أو على الغير أو هدد بنشرها عن طريق الشبكة.

ويُعاقب بالحبس من سنتين إلى ثلاث سنوات وغرامة من ثلاثة ملايين ليرة سورية إلى أربعة ملايين ليرة سورية كل من هدد بالنشر أو نشر على الشبكة صوراً ثابتة أو متحركة أو محادثات أو تسجيلات صوتية منافية للحشمة أو الحياء عائدة لأحد الناس ولو حصل عليها برضاه، وتشدد العقوبة لتصبح السجن المؤقت من خمس سنوات إلى سبع سنوات وغرامة من أربعة ملايين ليرة سورية إلى خمسة ملايين ليرة سورية إذا وقع الجرم على قاصر.

17_ الجرائم الواقعة على الدستور

يعاقب وفقاً للمادة 27 بالاعتقال المؤقت من سبع سنوات إلى خمس عشرة سنة وغرامة من عشرة ملايين ليرة سورية إلى خمسة عشر مليون ليرة سورية كل من أنشأ أو أدار موقعاً إلكترونياً أو صفحة إلكترونية أو نشر محتوى رقمياً على الشبكة بقصد إثارة أفعال تهدف أو تدعو إلى تغيير الدستور بطرق غير مشروعة، أو سلخ جزء من الأرض السورية عن سيادة الدولة، أو إثارة عصيان مسلح ضد السلطات القائمة بموجب الدستور أو منعها من ممارسة وظائفها المستمدة من الدستور، أو قلب أو تغيير نظام الحكم في الدولة.

18_ النيل من هيبة الدولة

يعاقب وفقا للمادة 28 بالسجن المؤقت من ثلاث سنوات إلى خمس سنوات وغرامة من خمسة ملايين ليرة سورية إلى عشرة ملايين ليرة سورية كل من قام بإحدى وسائل تقانة المعلومات بنشر أخبار كاذبة على الشبكة من شأنها النيل من هيبة الدولة أو المساس بالوحدة الوطنية. وهنا يجب على القاضي التمييز بين حرية التعبير الذي سمح بالانتقاد والإشارة إلى أماكن الخلل في حال وجودها، وبين الجرائم المعلوماتية المتعلقة بالإساءة إلى الإدارة العامة أو القائمين عليها في أشخاصهم وشرفهم وحياتهم الخاصة.

19_ النيل من مكانة الدولة المالية

كل من أنشأ أو أدار موقعاً إلكترونياً أو صفحة إلكترونية أو نشر محتوى رقمياً على الشبكة بقصد إحداث التدني أو عدم الاستقرار أو زعزعة الثقة في أوراق النقد الوطنية أو أسعار صرفها المحددة في النشرات الرسمية يعاقب وفقاً للمادة 29 بالسجن المؤقت من أربع سنوات إلى خمس عشرة سنة وغرامة من خمسة ملايين ليرة سورية إلى عشرة ملايين ليرة سورية

20_ جرائم المخدرات والمؤثرات العقلية

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

كل من أنشأ أو أدار موقعاً إلكترونياً أو صفحة إلكترونية أو نشر محتوى رقمياً على الشبكة بقصد الاتجار بالمخدرات أو المؤثرات العقلية أو الترويج لها المنصوص عليها في الجداول الملحقة بقانون المخدرات يعاقب وفقاً للمادة 30 بالسجن المؤبد وغرامة من خمسة ملايين ليرة سورية إلى عشرة ملايين ليرة سورية

21_ جرائم الإساءة إلى الأديان والمقدسات والشعائر الدينية

كل من أنشأ أو أدار موقعاً إلكترونياً أو صفحة إلكترونية أو نشر محتوى رقمياً على الشبكة بقصد الإساءة إلى أحد الأديان أو أحد المقدسات أو الشعائر الدينية أو الحض على الكراهية أو التحريض على العنف يعاقب وفقاً للمادة 31 بالحبس من سنة إلى ثلاث سنوات وغرامة من ثلاثة ملايين ليرة سورية إلى ستة ملايين ليرة سورية.

هذا ويتولى في سورية فرع مكافحة جرائم المعلوماتية وظائف الضابطة العدلية بما يخص الجرائم المعلوماتية، والذي يتبع لإدارة الأمن الجنائي، ويقوم الفرع بالبحث، والتقصي، وجمع المعلومات، عن مرتكبي الجرائم الالكترونية وتقديمهم للقضاء، كما يتكون من عدة أقسام وهي: قسم التحقيق والمتابعة، وقسم الأدلة الرقمية، وغرف العمليات. كما تم إحداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات بالقانون رقم /9/ لعام 2018. وتنحصر مهمة هذه المحاكم في البحث بـ "جرائم المعلوماتية والاتصال"؛ ووفقاً للمادتين الأولى والثانية من القانون فإنه: تنشأ نيابة عامة، ودوائر تحقيق، ومحاكم جزائية بدائية، واستئنافية في كل محافظة، للنظر في جرائم المعلوماتية والاتصالات. كما يراعى عند اختيار القضاة المشار إليهم في هذا القانون أن يكونوا ممن تم تدريبهم على مكافحة جرائم المعلوماتية وجرائم الاتصالات أو ممن لديهم خبرة عملية في هذا النوع من القضايا.

الخاتمة

في نهاية هذه الدراسة وجدنا أن الجريمة المعلوماتية هي جريمة متطورة بشكل متسارع ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة وتتسم بأنها جريمة ذات طابع مادي، و تتمثل في كل سلوك غير قانوني مرتبط بأي شكل بالأجهزة الإلكترونية (حاسب – شبكة – انترنت – بطاقات ممغنطة ...الخ)، يتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة، وغالباً ما يكون هدف المجرم هو سرقة وقرصنة المعلومات الموجودة في الأجهزة، أو إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم المسروقة بالإضافة إلى استخدام أو تزوير البطاقات الممغنطة بهدف الكسب المادي. ونظرا لتسارع تطور هذه الجريمة فقد أقر مجلس الشعب السوري القانون رقم 20 في جلسته المنعقدة بتاريخ 17-3-2022، وصدر عن السيد رئيس الجمهورية بتاريخ 18 نيسان 2022 ليدخل حيز التنفيذ بعد شهر من صدوره، وقد جاء القانون رقم 20 في 50 مادة موزعة على 7 فصول. وجاءت الجرائم المعلوماتية مذكورة على سبيل الحصر في الفصل الرابع وبلغت 21 جريمة معلوماتية وهي : (تجاوز حدود الدخول المشروع-الدخول غير المشروع- شغل اسم موقع الكتروني – انتحال الحساب الشخصي- إعاقة أو منع الوصول إلى الخدمة – تصميم أو ترويج أو استخدام البرمجيات الخبيثة -إرسال رسائل غير مرغوب بها – اعتراض المعلومات -الاحتيال المعلوماتي – إساءة الائتمان المعلوماتي -انتهاك الخصوصية – التسجيل غير المشروع – الجرائم المتعلقة بالبطاقة الالكترونية – الذم الالكتروني -القدح أو التحقير الإلكتروني -جرائم المساس بالحشمة أو الحياء -الجرائم الواقعة على الدستور – النيل من هيبة الدولة – النيل من مكانة الدولة المالية -جرائم المخدرات والمؤثرات العقلية -جرائم الإساءة إلى الأديان والمقدسات والشعائر الدينية) وتتدرج العقوبات والغرامات التي نص عليها القانون بحسب نوع الجريمة

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

المعلوماتية بدءاً بالسجن لمدة شهر إلى السجن لمدة 15 سنة، بالإضافة إلى السجن المؤبد في بعض الحالات، في حين تتراوح الغرامات المالية عن العقوبات ما بين 200 ألف إلى 25 مليون ليرة سورية.

وبما أن هذه الجريمة عالمية وليست محلية فقط لذلك نقدم في نهاية هذه الدراسة مجموعة من المقترحات كما يلي:

- بما أن الجرائم المعلوماتية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة فالعالم أصبح بمثابة مدينة صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها. لذلك نقترح بأن تتجه الدول نحو سن نفس القوانين العقابية والوقائية الردعية لمحاربة الجريمة الإلكترونية، أو على الأقل التنسيق من خلال الاتفاقيات الدولية وتبادل الخبرات في هذا المجال بين الدول
- نلاحظ أن هناك تداخل بين جريمة إتلاف المعلومات وجريمة إعاقة الخدمة، فتعديل المعلومات أو إلغائها أو محوها يعد من وسائل إتلاف المعلومات كما يعد من وسائل إعاقة الوصول للخدمة. لذلك من الأنسب دمج الحالتين معاً في عقوبة شاملة لأي إعاقة أو اتلاف للمعلومة.
- نقترح العمل على تطوير عمليات جديدة لتحقيق السرية الرقمية وزيادة أمن المعلومات فهو أهم هدف في بناء طرق ووسائل الحماية كآليات إثبات الهوية وضمان السرية والأمان للمعلومات والبيانات المنقولة والمرسلة والمنشورة مثلها مثل أنظمة الأمان والحماية من الجرائم الإلكترونية المعتمدة في البنوك العالمية والوطنية، كالتشفير عن طريق كلمات السر، أو لوحات المفاتيح والرسومات الافتراضية التي تعتبر مهددة وغير آمنة بشكل نهائي، فقد يعرض أي خلل في هذه الأنظمة المستخدمين لخسائر فادحة. وبذلك يضمن مستخدمو الانترنت أمان معلوماتهم كما تضمن المؤسسات المختلفة خصوصية وحماية منتجاتها.
- نقترح نشر التوعية بين جميع شرائح المجتمع وذلك من خلال إلقاء محاضرات متكررة الهدف منها:

أ_ اتخاذ أعلى درجات الحيطة والحذر وعدم التهاون بالأفعال التي يقوم بها الأفراد أو ينشرونها على الشبكة المعلوماتية

ب- لا بد من الاطلاع على القانون كي لا يقعوا فريسة سهلة أمام جناة متخصصين. أو يرتكبوا عن وعي أو إهمال إحدى الجرائم المنصوص عليها قانوناً.

ج- يتوجب على الجميع الحفاظ على خصوصية بياناتهم وبالمقابل احترام خصوصية الغير. والحذر من السماح للغير باستخدام كلمات المرور الخاصة بالحسابات الشخصية العائدة لهم. كونها تعد ملكاً لهم وهم مسؤولون عن كل ما يصدر عنها، أو يتم من خلالها. ويقع عليهم إثبات خلاف ذلك في حال تم استخدام الحساب أو النشر عليه من قبل الغير.

د- توعية كل من يتعرض لأي محاولة ابتزاز أو تهديد عبر الشبكة، ألا يتردد بالإبلاغ عنها لفرع الجرائم المعلوماتية. حيث تتم متابعة كافة الشكاوى ذات الصلة بدقة ومهنية عالية. مما يضمن محاسبة المذنب وتحقيق الردع العام المنشود.

هـ - تنبيه الشرائح العمرية الصغيرة بأن الهدف من الشبكة المعلوماتية هو تنفيذ الأعمال بأقل جهد وتخزين البيانات والوصول للمعلومات بدقة وسرعة، وليست مجالا للتسلية وإضاعة الوقت وصولاً إلى ارتكاب الجرائم عن غير قصد.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

قائمة المراجع

- الكتب:

1- الدكتور إيهاب السنباطي، موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة،2007.

2- د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، القاهرة2003.

3- د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة2009.

4- سميرة معاشي، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد 7، جامعة محمد خيضر بسكرة، الجزائر2011.

5- د.طارق الخن، جرائم المعلوماتية، منشورات الجامعة الافتراضية السورية2018، متوفرة على الرابط: https://pedia.svuonline.org

6- أ. عباوي نجاة ، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاتر السياسة والقانون، العدد16 لعام 2017.

7- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر 2004.

8- د. علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري للنشر والتوزيع، عمان 2009.

9- المحاميان منير وممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية2005.

10- المحامي محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان2006.

11- محمود نجيب حسني، النظرية العامة للقصد الجنائي، دار النهضة العربية 1971.

12- د. محمود نجيب حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، منشورات الحلبي الحقوقية، بيروت 1998.

13- نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية2007.

14- د. نائلة عادل فريد قورة، جرائم الحاسوب الآلي الاقتصادية، الطبعة 1، منشورات الحلبي الحقوقية، بيروت 2005.

15- د. هدى حامد قشقوش ، الإتلاف غير ألعمدي لبرامج وبيانات الحاسب الالكتروني، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني2000.

- التشريعات القانونية:

1- قانون الجريمة المعلوماتية السوري رقم 20 لعام 2022

2- قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم 17 لعام 2012.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

ئەو تاوانانەی هاتوونەتەکایەوە لە یاسای بەرەنگاربوونەوەی تاوانی زانیاری لە کۆماری عەرەبی سوریا

د. ئەسالە کەیوان کەیوان
ڕاگری فاکەڵتی یاسا، زانکۆی شامی تایبەت (ASPU)، لقی لازقیە، لازقیە، سوریە
ئیمێل: a.k.fol.LAT@aspu.edu.sy

پوختە

سەرەڕای ئەو سوودە گەورەیەی شۆڕشی زانیاری بەدەستی هێناوە کە هەموو جیهان لە هەموو ئاستەکاندا و لە بوارە جیاجیاکانی ژیانی هاوچەرخدا بەخۆیەوە دەبینێت. ئەم شۆڕشە تەکنەلۆژیایە گەشەسەندووانە ژمارەیەک کاردانەوەی نەرێنی بەدوای خۆیدا هێنا بەهۆی خراپ بەکارهێنانی ئەم تەکنەلۆژیایە پێشکەوتووانە و بەکارهێنانیان بۆ ئاسانکاری بۆ ئەنجامدانی چەندین دیاردەی تاوانکاری و تەنانەت ئەم تەکنەلۆژیایە بۆ ئەنجامدانی تاوانی نوێ بەکارهێنرا کە بەبێ ئەم شۆڕشە تەکنەلۆژیایە نەدەبوو.

تاوان دیاردەیەکی کۆمەلایەتییە کە پەیوەستە بە مرۆڤەوە و هەر لە کۆنەوە ناسراوە و شێوەکانی پەرەی سەندووە و ئاڵۆزی و شێواز و ئامرازەکانی لەگەڵ پێشکەوتنی کۆمەڵگاکاندا گۆڕاوە و لەگەڵ شۆڕشی تەکنەلۆژیای ئێستادا کە ئێمە دەژین دیاردەی تاوان ڕەهەندێکی نێودەوڵەتی وەرگرتووە و بۆتە کێشەیەربڕ نەک تەنیا بۆ وڵاتان کە داوای پێداچوونەوە بە یاسای ناوخۆی هەر وڵاتێک دەکات و لەگەڵ ئەم پێشکەوتنە مەزنەدا بگونجێت. لەم تۆێژینەوەیەدا هەوڵ دەدەین بە کورتی پەرەسەندنی یاساکانی سوریا و چۆنیەتی مامەڵەکردنی لەگەڵ پەرەسەندنی دیاردەی تاوانی زانیاریدا ڕوون بکەینەوە بە خستنەڕووی ئەو تاوانە زانیارییانەی کە لە یاساکانی سوریادا پەرەیان پێدراوە.

وشە گرنگەکان: تاوانی زانیاری – شۆڕشی تەکنەلۆژیا – تۆڕە کۆمەڵایەتیەکان – زیانەوالە.

The Anti-Cybercrime Law in the Syrian Arab Republic and the difficulties of implementing it

Dr- Asala Kewan Kewan
The scientific stage/ Dean of the Faculty of Law / ASPU- Al Sham Private University / lattakia doctor of private law،lattakia, Syria.
Email: a.k.fol.LAT@aspu.edu.sy

Abstract

Despite the great advantages achieved by the information revolution that the entire world is experiencing at all levels and in various areas of contemporary life. On the other hand, this growing technological revolution was accompanied by a number of negative repercussions due to the misuse of this advanced technology and its exploitation to facilitate the commission of many criminal phenomena. Indeed, this technology was

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

exploited to commit new crimes that would not have occurred without this technological revolution.
Crime is a social phenomenon linked to humans and has been known since ancient times. Its forms have developed and become complex and its methods and means have diversified with the progress of societies, and with the technological revolution that we are experiencing in the present era, the phenomenon of crime has taken on an international dimension and has become transcontinental and not just countries, which requires reconsidering the internal legislation of each country and keeping up with it. This huge development. In this study, we will briefly attempt to explain the development of Syrian legislation and how it has dealt with the development of the phenomenon of cybercrime, by presenting the cybercrimes introduced in Syrian legislation.

Key words: Information crime - technological revolution - social media - Malware