قانون مكافحة جرائم تقنية المعلومات الكويتي: دراسة مقارنة

د. بوقرين عبد الحليم*

الملخص:

أصدر المشرِّع الكويتي القانون رقم (63) لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات، وبذلك يكون قد التحق بركب الدول الساعية بجدية لمكافحة هذا النوع من الإجرام، في حين لا تزال بعض الدول الأخرى متردِّدة أو تصدر بعض النصوص المحتشمة التي لا تفي بالغرض في كثير من الأحيان.

ومن خلال دراستنا لهذا القانون، وجدنا أن المشرِّع الكويتي عمل جاهداً على توفير الحماية الجزائية من مختلف الجرائم الإلكترونية، بل إننا نجده ينص على بعض الجرائم التي غفلت عنها الكثير من التشريعات المقارنة، وعلى الرغم من ذلك؛ فإن قانون مكافحة جرائم تقنية المعلومات الكويتي توجد فيه بعض النقائص التي تخلَّلت نصوصه التجريمية، كما أن المشرِّع الكويتي قد غفل هو الآخر عن ذكر بعض صور الجريمة الإلكترونية، وعن التطرق أيضاً إلى الجانب الإجرائي لهذا النوع من الجرائم، وقد حاولنا قراءة القانون قراءة تقويمية عن طريق مقارنته ببعض التشريعات المقارنة، وبالتحديد المشرِّع السعودي، والمشرِّع الجزائري، والاتفاقية العربية لمكافحة الجريمة المعلوماتية، لنخلص في الأخير إلى بعض النتائج والتوصيات.

* كلية الحقوق والعلوم السياسية – جامعة عمار ثليجي الاغواط – الجزائر

المقدمة:

في وقت يكاد كل شيء يكون فيه إلكترونياً وتصبح فيه جُلُّ معاملاتنا تتم عن بعد عن طريق إلكتروني، تظهر الجريمة المعلوماتية أو الإلكترونية لتضع حدوداً للرفاهية التي تمخضت عن استعمال وسائل تكنولوجيا الإعلام والاتصال، وتدفع بالدول إلى المسارعة في سن قوانين عقابية لحماية المعاملات الإلكترونية لتوفير الأمن المعلوماتي.

وها هو المشرِّع الكويتي يصدر القانون رقم (63) لسنة 2015، وهو من أحدث القوانين في هذا المجال، وتضمَّن (21) مادة موزَّعة على فصلين، حاول المشرِّع الكويتي من خلالها التطرق لمختلف صور الجريمة المعلوماتية، ووضع النصوص التجريمية المناسبة لها، وقد كان للمشرِّع الكويتي فرصة أكثر من غيره في سنِّ مثل هكذا قانون، حيث توجد أمامه العديد من التشريعات المقارنة التي تناولت مكافحة الجريمة المعلوماتية، وكذا العديد من الاتفاقيات الدولية على رأسها الاتفاقية العربية لمكافحة الجريمة المعلوماتية، واتفاقية بودابست لمكافحة الجريمة الإلكترونية. ولكن هل وفق المشرِّع الكويتي في سن قانون شامل لمختلف جوانب الجريمة المعلوماتية؟ وهل استفاد من ثغرات ونقائص القوانين المقارنة باعتباره قانون حديث النشأة؟

الإجابة عن هذه الإشكالية تكون من خلال قراءة في مواد القانون وتقييم نصوصه عن طريق بيان إيجابياته وسلبياته، وذلك وفق المبحثين التاليين:

المبحث الأول: التعليق على النصوص التجريمة لقانون جرائم تقنية المعلومات الكويتي.

المبحث الثاني: التعليق على الأحكام الخاصة بمكافحة جرائم تقنية المعلومات.

المبحث الأول

النصوص التجريمة لقانون جرائم تقنية المعلومات الكويتي

قبل أن نبدي ملاحظاتنا حول الجرائم الواردة في قانون مكافحة جرائم تقنية المعلومات الكويتي، نشير إلى أن المشرِّع الكويتي لم يكن موفقاً في عَنْونة هذا النوع من الجرائم، فعبارة (تقنية المعلومات) تدل على أنظمة تشغيل المعلومات ولا تشمل المعلومات، ونفس الملاحظة توجه إلى المشرِّع الجزائري الذي عنْون هذه الجرائم بـ (الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات)، وكأن الأمر يتعلق بحماية الأنظمة فقط دون المعلومات أو المعلومات الموجودة داخلها، لذلك فإن التسمية المعتمدة من طرف المشرِّع السعودي أقرب للصواب وأشمل وهي (قانون مكافحة الجريمة المعلوماتية)، ومع ذلك نجد أيضاً أن مصطلح معلوماتية لا يشمل كل الجرائم التي تقع في عالم افتراضي، وإنما تقتصر على الجرائم الماسة بالمعلومات، ومن هنا يكون الأصح تسمية هذا النوع من الجرائم بـ (الجرائم الإلكترونية).

المطلب الأول

المفاهيم الواردة في القانون

جاء في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الكويتي أنه: «تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية، المعنى الموضح قرين كل منها:

- البيانات الإلكترونية: بيانات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب آلي أو قواعد للبيانات .
- النظام الإلكتروني المؤتمت: برنامج أو نظام إلكتروني لحاسبٍ آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل، كلياً أو جزئياً، دون تدخل أو إشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة له.
- نظام المعالجة الإلكترونية للبيانات: نظام الكتروني لإنشاء أو إدخال أو استرجاع أو إرسال أو استلامٍ أو استخراج أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونياً.
- الشبكة المعلوماتية: ارتباط بين أكثر من منظومة اتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها.

- المستند أو السجل الإلكتروني: مجموعة بيانات أو معلومات يتم إنشاؤها أو تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو استقبالها كلياً أو جزئياً بوسيلة إلكترونية، على وسيط ملموس أو على وسيط إلكتروني آخر، وتكون قابلة للاسترجاع بشكل يمكن فهمه.

- الموقع: مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

- إلكتروني: كل ما يتصل بتكنولوجيا المعلومات، وذو قدرات كهربائية أو رقمية أو مغناطيسية أو بصرية أو رومغناطيسية أو وسائل أخرى مشابهة سلكية كانت أو لاسلكية، وما قد يُستحدث من تقنيات في هذا المجال.

- وسيلة تقنية المعلومات: أداة إلكترونية تشمل كل ما يتصل بتكنولوجيا المعلومات وله قدرات كهربائية أو رقمية أو مغناطيسية أو بصرية أو كهرومغناطيسية أو ضوئية أو وسائل أخرى مشابهة سلكية كانت أو لاسلكية وما قد يستحدث في هذا المجال.

- الجريمة المعلوماتية: كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون.

- الدخول غير المشروع: النفاذ المتعمَّد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني، من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان دون تفويض في ذلك أو بالتجاوز للتفويض الممنوح.

- نظام الحاسب الآلي: مجموعة برامج وأنظمة معلوماتية مُعَدَّة لتحليل المعلومات والبيانات والأوامر، وبرمجتها وإظهارها أو حفظها أو إرسالها أو استلامها، ويمكن أن تعمل بشكل مستقل أو بالاتصال مع أجهزة أو أنظمة معلوماتية أخرى.

- التوقيع الإلكتروني: البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو

إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في مستند أو سجل إلكتروني أو مضافة عليها أو مرتبطة بها بالضرورة، ولها طابع يسمح بتحديد هوية الشخص الذي وقَّعها ويميزه عن غيره.

- الالتقاط المعلوماتي: مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها، ويشمل ذلك المنقولة إلكترونياً.

- الاحتيال الإلكتروني: التأثير في نظام إلكتروني مؤتمت، أو نظام معلوماتي إلكتروني، أو شبكة معلوماتية، أو مستند أو سجل إلكتروني، أو وسيلة تقنية معلوماتية، أو نظام أو جهاز حاسب آلي، أو توقيع إلكتروني أو معلومات إلكترونية، وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير».

من بين أكثر القوانين جودة من حيث الصياغة نجد قانون مكافحة جرائم تقنية المعلومات الكويتي ولعل السبب في ذلك يعود إلى حداثة هذا القانون الذي صدر سنة 2015، ومع ذلك فإن المفاهيم التي تضمنها القانون لم تكن شاملة لكل جوانب الجرائم المعلوماتية.

بالرجوع إلى نص المادة السالفة الذكر نجد المشرِّع الكويتي يحاول شرح بعض المصطلحات المتعلقة بهذا النوع من الجرائم، وهو أمر يخدم مبدأ الشرعية، ويبعد القاضي الجنائي عن التفسير والقياس، ويسهل عليه الوصول إلى التكييف المناسب.

ولكن هل كانت هذه المفاهيم شاملة أم أن هناك مصطلحات كان على المشرِّع الكويتي تضمينها في الماد الأولى؟

لقد أسهب المشرِّع الكويتي في ذكر المفاهيم المتعلقة بالجرائم الإلكترونية أكثر من أي قانون آخر، وبإجراء مقارنة بسيطة بين هذه المفاهيم وتلك الواردة في القانون الجزائري أو السعودي أو الاتفاقية العربية نلحظ الدقة في التعبير عن المفاهيم

والدقة في شرحها[1]، ومع ذلك نلحظ وجود بعض النقائص نوردها فيما يلي:

- إن المشرِّع الكويتي ربط مفهوم الاحتيال الإلكتروني بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير[2]، وهو جانب الصواب قليلاً، وكان من الأفضل عدم ربط الاحتيال الإلكتروني بوجود قصد خاص كالحصول على منفعة أو الإضرار، حيث إنه من المعلوم أن الكثير من عمليات الاحتيال الإلكتروني ترتكب بدافع المتعة ومحاولة إثبات الذات والتحدي.

- لم يعرِّف المشرِّع الكويتي (التداخل) وهو فعلٌ يختلف عن الدخول غير المشروع، ويختلف أيضاً عن الالتقاط، وهو يتعلق بمحالة الجاني اعتراض الموجات والإشارات بقصد الاطلاع على محتواها، أو بقصد التشويش وهو ما يحدث عادة في البث التلفزيوني المشفّر.

- لم يعرِّف المشرِّع الكويتي (الوسيط في خدمة الإنترنت)؛ والوسيط له دور كبير في إيصال المعلومات أو توريدها أو حفظها، وهو يتحمل جزءاً من المسؤولية الجنائية عن بعض الجرائم الإلكترونية، ويعرِّفه المشرِّع الجزائري بأنه: «أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و /أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها[3].

(1) على سبيل المثال نجد المشرِّع الكويتي عرَّف البيانات الإلكترونية: بأنها بيانات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب آلي أو قواعد للبيانات، في حين نجد المشرِّع السعودي يستعمل مصطلح البيانات للدلالة على البيانات الإلكترونية، لذلك نجد أن التعبير الذي استعمله المشرِّع الكويتي أفضل لأنه مركز، كما أن المشرِّع السعودي لم يكن موفقاً كنظيره الكويتي في شرح هذه العبارة، حيث نجد أن التعريف المذكور أعلاه مختصر ودقيق، هذا ولم ينص المشرع الجزائري على هذا التعريف بينما نصت عليه الاتفاقية العربية لمكافحة الجرائم المعلوماتية تحت مسمي البيانات.

(2) حيث عرَّف المشرِّع الكويتي الاحتيال الإلكتروني بأنه: «التأثير في نظام إلكتروني مؤتمت أو نظام معلوماتي إلكتروني أو شبكة معلوماتية أو مستند أو سجل إلكتروني أو وسيلة تقنية معلوماتية أو نظام أو جهاز حاسب آلي أو توقيع إلكتروني أو معلومات إلكترونية وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير»

(3) بينما عرفته الاتفاقية العربية تحت مسمى مزود الخدمة بأنه: «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..، وللاستفادة أكثر يمكن إجراء مقارنة مع اتفاقية بودابست، هلالي عبد اللاه أحمد 2008، مكافحة الجرائم المعلوماتية، دار النهضة العربية، ط 01.

- لم يعرِّف المشرِّع الكويتي (الحاسب الآلي)، وإن كان جهاز الحاسب الآلي معروفاً، إلا أن معظم هذا النوع من الجرائم يتعلق به وبشبكة الإنترنت فيكون من الأفضل تعريف جهاز الحاسب الآلي، وهو ما فعله المشرِّع السعودي على خلاف المشرِّع الجزائري والاتفاقية العربية، حيث عرَّف جهاز الحاسوب في المادة الأولى فقرة (06) بأنه: «أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها أو إرسالها أو استقبالها أو تصفحها، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له».

المطلب الثاني

الجرائم الماسة بالأنظمة المعلوماتية والمواقع

تحت هذا العنوان سنحاول التطرق بالتحليل والنقد والتقويم للنصوص التجريمية المتعلقة بجرائم الدخول غير المشروع للأنظمة المعلوماتية والمواقع، أو تعطيل هذه الأنظمة والمواقع أو استغلالها في أنشطة غير مشروعة.

الفرع الأول

جرائم الدخول غير المشروع للأنظمة المعلوماتية والمواقع

تنص المادة الثانية من قانون مكافحة جرائم تقنية المعلومات الكويتي على أنه: «يعاقب بالحبس مدة لا تجاوز ستة أشهر، وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو إحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي، أو إلى نظامه، أو إلى نظام معالجة إلكترونية للبيانات، أو إلى نظام إلكتروني مؤتمت، أو إلى شبكة معلوماتية.

فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين، والغرامة التي لا تقل عن ألفي دينار، ولا تجاوز خمسة آلاف دينار أو إحدى هاتين العقوبتين.

فإذا كانت تلك البيانات أو المعلومات شخصية؛ فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين».

يحاول المشرِّع الكويتي من خلال هذه المادة حماية الأنظمة والبرامج من عمليات التطفل والقرصنة، عن طريق ما يُعرف بالدخول غير المشروع سواء كان الدخول في جزء من النظام أو كله وقد يتحقق ذلك من خلال الدخول بعد فوات الوقت المحدد للدخول[4].

وبإجراء مقارنة بين هذه الجريمة ونظيراتها عند المشرِّعين الجزائري والسعودي والاتفاقية العربية، نجد أن المشرِّع الكويتي لم يضف جديداً بخصوص هذه الجريمة، فقد غفل مثل نظرائه من المشرعين عن الكثير من السلوكيات التي تتشابه مع الدخول غير المشروع، وسنحاول الإشارة إليها فيما يلي :

- لم ينص المشرِّع الكويتي على فعل (البقاء) الذي يتحقق في حالة ما إذا كان الجاني مسموحاً له بالدخول لفترة زمنية، لكنه يتعمَّد البقاء بعد نفاذ تلك الفترة، ففي هذه الحالة يُعدُّ بقاؤه غير مشروع، وهو فعل لم يشر إليه المشرِّع السعودي، ولكن نص عليه المشرِّع الجزائري، حيث جاء في المادة (394 مكرراً) من قانون العقوبات أنه: «يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة

(4) حصل نقاش واسع في الولايات المتحدة الأمريكية حول عبارة «الدخول» وذلك سنة 1996 أمام محكمة كانساس العليا في قضية Allen، حيث حاولت التضييق من مفهوم الدخول، وتتلخص وقائع القضية في قيام المتهم Allen باستخدام حاسبه الآلي للاتصال بحاسب شركة الهاتف الجنوبية الغربية التي تتحكم في تحويل الاتصالات البعيدة المدى، حيث تلاعب المتهم بنظامها بطريقة تسمح بالاتصال الهاتفي مجاناً، وقد اتضح للمحققين أن Allen اخترق النظام عن طريق فك كلمته السرية، ومن ثمة إزالة الدليل على نشاطه بإلغاء السجلات..، وقد دافع المتهم عن نفسه أمام المحكمة بأنه لا يوجد دليل على دخوله إلى الحاسب الآلي للشركة، إلا أن الادعاء اعتمد على تعريف التشريع الواسع لعبارة «الدخول Access» والتي تقر بأن الدخول يعني الاقتراب أو إصدار أمر أو الاتصال بـ..أو أي أشياء أخرى تؤدي إلى استخدام مصادر الحاسب الآلي..، لكن المحكمة أجابت بأن هذا التعريف كان واسعاً يؤدي إلى القول بعدم دستورية التشريع لغموضه..، وانتهت المحكمة إلى أن المعنى الكامل والعادي يجب أن يطبق عوضاً عن الترجمة المشوهة للتعريف المتوافر...، والقول إن دخول المتهم إلى النظام يظهر في قيامه بالبحث عن كلمة العبور الخاصة بنظام الشركة المذكورة للوصول إلى المعلومات قول لا دليل عليه، وهو ما يؤدي إلى القول بعدم دخول المتهم إلى حاسبات الشركة. انظر: خليفة محمد، 2010، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، ص 140 وما بعدها.

انظر أيضا:

Samia Bet Ismail Kamoun، La formation du contrat de vente électronique et le droit commun des contrats، Revue Tunisienne de Droit، Centre de Publication Universitaire 2004،p 132.

مالية من 50.000 د.ج إلى 100.000 د. ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك».

وهو ما نصت عليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية حيث جاء في المادة (6/1) منها: "الدخول أو البقاء، وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به".

المشرِّع الكويتي نص في الفقرة الثانية من ذات المادة على تشديد العقوبة في حالة ترتب على فعل الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، لكنه لم يبيِّن عن أي معلومات يتكلم؛ هل المعلومات المتعلقة بسير النظام أو المعلومات المحفوظة داخل النظام؟ العديد من التشريعات ومنها التشريع الجزائري وبدرجة أقل المشرِّع السعودي، فصلت في هذه النقطة حيث نص قانون العقوبات الجزائري في مادته (394 مكرراً) في فقرتها الثانية أنه: "...تضاعف العقوبة إذا ترتَّب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتَّب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة: الحبس من ستة أشهر إلى سنتين والغرامة من 50.000د.ج إلى 150.000د.ج"، ومع ذلك نجد أن المشرِّع الجزائري لم يكن موفقا أيضاً، إذ يعتبر تخريب نظام اشتغال المنظومة في هذه الحالة واقعاً دون قصد، فالمجرم خرَّب النظام أثناء محاولته الدخول غير المشروع، ولم يخرِّب النظام من أجل الدخول، ومن هنا يكون المشرِّع الجزائري اكتفى بالنص على هذه الجريمة كظرف تشديد لجريمة الدخول في نظام المعالجة، في حين نجد المشرِّع الفرنسي نص على هذه الجريمة كظرف تشديد، وكذا بصفة مستقلة في المادة (323/2) من قانون العقوبات الفرنسي إذا كانت بالعمد، أي إذا تعمد الجاني تخريب المعلومات التي يشتغل بها النظام[5].

لذا يكون من الأفضل النص على فعل تخريب أو تعطيل عمل سير النظام كظرف تشديد في جريمة الدخول أو البقاء غير المشروع، وإدراج فقرة ثانية تنص على

(5) تنص بقية الفقرة وهي صياغة لا غبار عليها: «فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات، وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين. ويعاقب بذات العقوبة بحسب الأحوال كل من استعمل أياً مما ذكر مع علمه بتزويره أو فقده لقوته القانونية».

تجريم التخريب العمدي للمعطيات والمعلومات المتعلقة بسير الأنظمة، ثم النص على حماية المعلومات الموجودة داخل النظام، ومن خلال ما سبق وبالمقارنة مع ما نص عليه المشرِّع الكويتي في الفقرتين الأولى والثانية من المادة الرابعة نجد أنه يقصد البيانات الموجودة داخل النظام، وليس بيانات سير النظام، لذا يكون من الأفضل إعادة صياغة نص المادة لتتلاءم مع هذا المعنى.

- الملاحظ أيضاً أن المشرِّع الكويتي لم يُوفَّق عندما نص على حماية المعلومات سواء كانت عامة أو شخصية ضمن جريمة الدخول، حيث اعتبر المساس بهذه البيانات مجرد ظرف تشديد، ويكون من الأفضل لو نص على الجرائم الماسة بالبيانات المخزَّنة داخل الأنظمة والبرامج بصفة مستقلة، وذلك نظراً لتعدد وتنوع هذه الجرائم، فالأمر لا يتعلق فقط بمجرد المساس بهذه المعلومات بل هناك أشكال أخرى من الأفعال الماسة بالبيانات مثل:
- جريمة عدم اتخاذ الإجراءات الأولية لإجراء معالجة البيانات.
- جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة.
- جريمة المعالجة غير المشروعة للبيانات.
- جريمة تسجيل وحفظ بيانات شخصية، أو تتعلق بالماضي لأشخاص مصنفين.
- جريمة حفظ معلومات شخصية خارج الوقت المخصص به وفقاً للطالب.
- جريمة تغيير الغرض المحدد لجمع البيانات الاسمية.
- جريمة إفشاء بيانات اسمية للإضرار بصاحب الشأن.

كما نص المشرِّع الكويتي في الفقرة الأولى من المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من:

- ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون. فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة؛ الحبس مدة لا تجاوز عشر سنوات، والغرامة لا تقل عن

خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين. ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية..».

هنا ينص المشرِّع الكويتي على صورة أخرى للدخول غير المشروع إلى موقع أو نظام معلوماتي، والتي تتعلق بالحصول على بيانات أو معلومات حكومية سرية، وإن كانت صياغته غير موفقة على أساس أنها لا تشمل بعض الأفعال مثل الدخول من أجل الاطلاع أو الدخول من أجل إضافة معلومات.

أما الفقرة الثانية من ذات المادة فتنص: «زَوَّرَ أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً، أو نظام معالجة إلكترونية للبيانات، أو نظاماً إلكترونياً مؤتمتاً، أو موقعاً أو نظام حاسب آلياً، أو نظاماً إلكترونياً بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات..».

المشرِّع الكويتي وُفِّقَ إلى حدٍّ كبير في صياغة هذه الفقرة وإن كنا لا نتفق معه في العبارة الأخيرة والتي تناولت الوسيلة التي تتم بها الجريمة، وكان من الأفضل عدم النص على الوسيلة على اعتبار أن القانون الجنائي لا يعتد بالوسيلة في ارتكاب الجرائم، ثم لا يجب أن نربط ارتكاب الجريمة بوسيلة معينة خشية ظهور وسائل جديدة[6].

نشيد بالصياغة القانونية للمشرع الكويتي في نص الفقرة الثالثة(7) والرابعة[8]من المادة الثالثة، وندعو المشرِّع الجزائري ونظيره السعودي إلى الاقتداء به والنص

(6) جاء في الفقرة الثالثة: «غيّر أو أتلف عمداً مستنداً إلكترونياً يتعلق بالفحوصات الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية أو سهَّل للغير فعل ذلك أو مكنه منه، وذلك باستعمال الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات»، وإن كنا لا نحبذ ذكر الوسيلة في تجريم الأفعال.

(7) جاء في الفقرة الرابعة استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه .فإذا كان التهديد بارتكاب جناية أو بما يُعد مساساً بكرامة الأشخاص أو خادشاً للشرف والاعتبار أو السمعة كانت العقوبة الحبس مدة لا تجاوز خمس سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار، أو بإحدى هاتين العقوبتين.

(8) نص عليها المشرِّع السعودي في الفقرة الأولى من المادة الرابعة من قانون مكافحة الجرائم المعلوماتية.

على هاتين الجريمتين باعتماد ذات الصياغة القانونية، وإن كنا لا نتفق معه كثيراً في صياغة نص الفقرة الأخيرة من نص المادة الثالثة والتي جاء فيها: «توصَّل عن طريق شبكة المعلوماتية، أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال أو منفعة أو مستند أو توقيع على مستند، وذلك باستعمال طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه».

يتكلم المشرِّع الكويتي على النصب الإلكتروني وفي الحقيقة قليلة هي التشريعات التي نصت على هذه الجريمة بهذه الصياغة(9)، ومن الملاحظات البسيطة التي نبديها في هذا الشأن أن المشرِّع ذكر مصطلح «مال»، وكان من الأفضل لو أضاف عبارة «مهما كانت طبيعته»، حتى لا تثار إشكالية المال المادي والمال المعنوي، بالإضافة إلى أن المشرِّع الكويتي نسي أن يشير إلى بعض الطرق الأخرى للاحتيال ومنها: «الادعاء بوجود سلطة خيالية، أو اعتماد مالي خيالي»، وهذه الطرق من أكثر وسائل النصب انتشاراً، لذا ندعو المشرِّع الكويتي إلى تدارك ذلك.

والملاحظ أيضاً على هذه الجريمة؛ أن المشرِّع الكويتي لا يعترف بقيام جريمة الاحتيال الإلكترونية إلا إذا كانت الوسائل المستخدمة في الاحتيال من شأنها خداع المجني عليه، وإذا كان هذا الشرط معقولاً في جريمة النصب العادية، إلا أنه من الصعب تقبله في جريمة الاحتيال الإلكتروني على اعتبار أن العالم الإلكتروني عالم معقد يعتمد على المعرفة الجيدة بوسائل تقنية المعلومات وهو ما يجهله الكثير من مستعملي الفضاء الإلكتروني، ومن هنا كان من الأفضل عدم ربط قيام الجريمة بهذا الشرط وترك الحرية لقاضي الموضوع.

والملاحظ أيضاً، هو وجود تفاوت بين نص هذه الجريمة، وتعريف الاحتيال الإلكتروني الوارد في المادة الأولى من ذات القانون، حيث ربط المشرِّع الكويتي في تعريفه للاحتيال الإلكتروني بقصد الحصول على منفعة، في حين نجد نص المادة الثالثة الفقرة الأخيرة قد توسع ليشمل المال أو مستنداً أو توقيعاً على مستند، وربما يكون نص المادة هو الأصوب حتى لا يفلت مجرم من العقاب.

(9) المرجع السابق قانون مكافحة الجرائم المعلوماتية السعودي.

الفرع الثاني

جرائم تعطيل الأنظمة أو المواقع

نص المشرِّع الكويتي في الفقرة الأولى من المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات أنه: «يعاقب بالحبس مدة لا تجاوز سنتين، وبغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار، أو بإحدى هاتين العقوبتين كل من: أعاق أو عطَّل عمداً الوصول إلى موقع خدمة إلكترونية، أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات الإلكترونية بأي وسيلة كانت، وذلك عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات..».

لقد تميَّز المشرِّع الكويتي بالنص على هذا السلوك المجرَّم بهذه الصياغة، إذ لا نجد لها مثيلاً عند المشرِّع الجزائري، أما المشرِّع السعودي فقد نص على هذا السلوك المجرَّم، ولكن صياغة المشرِّع الكويتي أفضل [10]، ولا نبدي أي ملاحظة حول الصياغة القانونية للفقرة، وإن كنا نتمنى لو أضاف المشرِّع الكويتي مصطلح «منع» في هذه الجريمة.

أما الفقرة الثانية من المادة الرابعة فقد جاء فيها: «أَدْخَلَ عمداً عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها، أو دخل موقعاً في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع، أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه أو إيقافه أو تعطيله..».

هنا يحاول المشرِّع الكويتي حماية شبكة الإنترنت وموقعها، لكنه لم يكن موفقاً عندما استعمل مصطلح «أَدْخَلَ» وكان من الأفضل استعمال عبارة «إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها»، حتى تكون الصياغة شاملة لكل الحالات الممكنة.

أما فيما يخص حماية المواقع الإلكترونية فقد أسهب المشرِّع الكويتي في ذكر الأفعال التي يمكن أن تشكل السلوك المجرَّم وقد أحسن صنعاً، على خلاف المشرِّع

(10) قارن ما بين الفقرة الأولى من المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات الكويتي، والفقرة الثالثة من المادة الخامسة من قانون مكافحة الجرائم المعلوماتية السعودي.

السعودي الذي لم يكن دقيقاً عندما نص على حماية المواقع الإلكترونية[11]، بينما نجد المشرِّع الجزائري قد غفل عن هذه الجرائم.

الملاحظ أن المشرِّع الكويتي لم ينص في المادة الثانية على المساس العمدي بالبيانات المتعلقة بسير النظام المعلوماتي، وإنما نص عليه كظرف تشديد إذا تم بغير قصد، وهو في هذه الجريمة يتدارك الأمر لكنه قصر التجريم على المواقع الإلكترونية دون غيرها، وكان من الأفضل أن تشمل الجريمة بقية الأنظمة المعلوماتية.

المطلب الثالث

جرائم الاستخدام غير المشروع للأنظمة المعلوماتية والمواقع

نص المشرِّع الكويتي على هذه الجرائم من المادة الرابعة إلى غاية المادة العاشرة، وهي تتعلق باستخدام الأنظمة المعلوماتية والمواقع للاعتداء على المراسلات أو المقدسات الدينية ورموز الدولة أو الأموال والأمن.

الفرع الأول

جريمة الاعتداء على المراسلات أو الآداب أو الأموال باستعمال وسيط إلكتروني

جاء في الفقرة الثالثة من المادة الرابعة السالفة الذكر ما يلي: «تنصت أو التقط أو اعترض عمداً، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات..»[12].

لقد أحسن المشرِّع الكويتي صنعاً ومن قبله المشرِّع السعودي عندما نص على هذا السلوك المجرَّم، الذي لم يفطن إليه المشرِّع الجزائري، والذي يتعلق بالتصنت أو التقاط أو اعتراض الموجات أو الترددات، خاصة تلك المتعلقة بالبث التلفزيوني المشفر، وهو ما يعرف «بإحداث التداخل»، الذي يكون الهدف منه التشويش الذي تعاني منه بعض القنوات التلفزيونية المعروفة.

(11) المادة الخامسة من قانون مكافحة الجرائم المعلوماتية السعودي.

(12) جاء في نهاية الفقرة: «... فإذا أفشى ما توصل إليه يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين».

أما الفقرة الرابعة من المادة الرابعة فقد جاء فيها: «كل من أنشأ موقعاً أو نشر أو أنتج أو أعدَّ أو هيأ أو أرسل أو خزَّن معلومات أو بيانات، بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات وكان ذلك من شأنه المساس بالآداب العامة، أو أدار مكاناً لهذا الغرض».

يحاول المشرِّع الكويتي من خلال هذه الفقرة حماية الأخلاق والآداب العامة من نشر المواد الإباحية، وقد أسهب مرة أخرى في ذكر المصطلحات التي تعبر عن مختلف صور السلوك المجرم من الإنشاء إلى النشر والإنتاج والإعداد والتهيئة أو الإرسال أو التخزين، ولكن الشيء الملاحظ أن المشرِّع الكويتي قد ربط كل هذه السلوكيات بالمعلومات أو البيانات، وتجاهل الصور أو الفيديوهات كمادة يتم إعدادها وعرضها لذلك كان من الأفضل لو نص على عبارة: «ما من شأنه» مكان عبارة «معلومات أو بيانات»، حتى تكون الجريمة شاملة لكل الصور، ثم إن المشرِّع الكويتي ذكر عبارة «بالآداب العامة»، وكان من الأفضل لو أضاف لها عبارة «والنظام العام والقيم الدينية والحياة الخاصة»، وهو ما نص عليه المشرِّع السعودي الذي كانت صياغة لهذه الجريمة أفضل[13]، وكذا الاتفاقية العربية لمكافحته الجرائم المعلوماتية[14].

ثم لا بد من إضافة مصطلح «اشترى» بعد مصطلح «خزَّن»، حتى تطال الجريمة المشتري أيضاً، وبدرجة أقل يستحسن إضافة مصطلح «البيع» بعد مصطلح «العرض».

وجاء في الفقرة الأخيرة من المادة الرابعة ما يلي: «كلُّ من حرَّض أو أغوى ذكراً أو أنثى لارتكاب أعمال الدعارة والفجور، أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، فإذا كان الفعل موجهاً إلى حدث فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين».

يحاول المشرِّع الكويتي في هذه الحالة توسيع دائرة التجريم لتشمل المحرِّض على أعمال الفجور والدعارة باستخدام الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات، وهي التفاتة طيبة من المشرِّع الكويتي، ولكن الغريب أنه شدَّد العقوبات

(13) الفقرتان الأولى والثالثة من المادة السادسة من قانون مكافحة الجرائم المعلوماتية السعودي.
(14) المادة 12 من الاتفاقية.

فيما تعلق التحريض بحدث، ولم يشدِّد العقوبات في الفقرة الرابعة إذا تعلق الأمر بأفعال مخلة بالآداب متعلقة بالأحداث، مع أن جل التشريعات تنص على ذلك.

وقد جاء في المادة الخامسة من قانون مكافحة جرائم تقنية المعلومات الكويتي أنه: «يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن ألف دينار ولا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية .فإذا ترتَّب على استخدامها الحصول على أموال الغير، أو على ما تتيحه هذه البطاقة من خدمات، يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين».

نقف هنا للإشادة بالصياغة القانونية لهذه المادة التي نفتقدها في الكثير من التشريعات العربية، والأمر هنا يتعلق بحماية بطاقات الائتمان التي تعد من أكثر وسائل الدفع عرضة للقرصنة والتزوير، وعلى ذكر التزوير نلحظ أن المشرِّع الكويتي لم ينص على تزوير بطاقة الائتمان، وربما السبب أن نص الفقرة الثانية من المادة الثالثة يغني عن ذلك.

الفرع الثاني

جريمة الاعتداء على الأمن العام باستعمال وسيط إلكتروني

نص المشرِّع الكويتي على مجموعة من الجرائم والمتعلقة في مجملها بالأمن العام وذلك في المواد من السادسة إلى العاشرة، ودعونا نشير في البدء أنه لا إشكاليات تثار بشأن الصياغة القانونية للمادتين السادسة[15]، والسابعة[16]، فمن

(15) التي جاء فيها: «يعاقب بحسب الأحوال بالعقوبة المنصوص عليها في البنود 1، 2، 3 من المادة (27) من قانون المطبوعات والنشر المشار إليه، كل من ارتكب عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات المنصوص عليها في هذا القانون أحد الأفعال بحسب الأحوال المبينة بالمواد (19، 20، 21) من القانون المشار إليه».

(16) التي جاء فيها: « يعاقب بالعقوبة المقررة بالمادة 29 فقرة أولى من القانون رقم 31 لسنة 1970 بتعديل بعض أحكام قانون الجزاء رقم 16 لسنة 1960، كل من ارتكب أحد الأفعال المنصوص عليها بالمادة 28 من قانون المطبوعات والنشر المشار إليه عن طريق الشبكة المعلوماتية، أو باستخدام وسيلة من وسائل تقنية المعلومات المنصوص عليها في هذا القانون».

خلالها يحاول المشرِّع حماية المقدسات الدينية[17]، ورموز الدولة ووحدتها، وإن كنا نطالب بتعديل المادة (20) من قانون المطبوعات والنشر التي تمنع التعرض لشخص الأمير، وذلك بإضافة عبارة: «ورؤساء وملوك الدول وأعضاء البعثات الدبلوماسية».

والملاحظة المثارة أيضاً هو مسالة الإحالة، حيث يحيل المشرِّع الكويتي إلى نصوص قانونية ورادة في قانون المطبوعات والنشر، وكذا القانون المعدل لقانون الجزاء، وهو أمر غير محبذ خاصة من طرف القضاة، وكان من الأفضل إدراج الأفعال المنصوص عليها في تلك القوانين في المادتين بدل الإحالة إليها أو إلى عقوباتها.

ومع ذلك ندعو التشريع الجزائري، وكذا السعودي بالنص على هذه الجرائم والاقتداء بالمشرِّع الكويتي، ونشير إلى أن الاتفاقية العربية لمكافحة الجريمة المعلوماتية لم تشر إلى هذه الجرائم.

وجاء في المادة الثامنة من قانون مكافحة جرائم تقنية المعلومات الكويتي أنه :«يعاقب بالحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن عشرة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعاً أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات المنصوص عليها في هذا القانون، بقصد الاتجار بالبشر أو تسهيل التعامل فيهم، أو ترويج المخدرات أو المؤثرات العقلية وما في حكمها، أو تسهيل ذلك في غير الأحوال المصرح بها قانوناً».

يحاول المشرِّع الكويتي مواجهة جريمة الاتجار بالبشر وهي من أخطر الجرائم ضد الإنسانية، وكذا جريمة ترويج المخدرات أو المؤثرات العقلية لما لها من آثار سلبية على الفرد والمجتمع.

غير أن هناك بعض الجرائم الأخرى كان من الأفضل لو نص عليها المشرِّع الكويتي في هذه المادة نظراً لخطورتها أيضاً، وهي جريمة إنشاء موقع أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات بقصد الاتجار بالأعضاء البشرية أو تهريب المهاجرين..، وهي جرائم لم ينص عليها

(17) عبد الحليم بوقرين، 2015، الحماية الجنائية لشخص الرسول ﷺ، مجلة الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط / الجزائر، العدد 08، ص 01.

المشرِّع السعودي ولا المشرِّع الجزائري ولا حتى الاتفاقية العربية لمكافحة الجريمة المعلوماتية.

في حين نصت المادة التاسعة من قانون مكافحة جرائم تقنية المعلومات الكويتي على أنه: «يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، كل من قام عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات، بغسل أموال أو بتحويل أموال غير مشروعة أو بنقلها أو بتمويه أو بإخفاء مصدرها غير المشروع، أو قام باستخدامها أو اكتسابها أو حيازتها مع علمه بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع علمه بمصدرها غير المشروع، وذلك بقصد إضفاء الصفة المشروعة على تلك الأموال».

قليلة جداً هي التشريعات التي تفطَّنت لتجريم تبييض الأموال الذي يتم عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات، حيث يعتبر المشرِّع الكويتي من بين السبَّاقين في تجريم مثل هذه الأفعال، فالجناة على حدٍّ تعبير البعض في جرائم غسل الأموال قد اتجهوا إلى ارتكاب جرائمهم عن طريق الوسائط الإلكترونية وأهمها استعمال الحاسب الآلي وشبكة الإنترنت وبرامج الاختراق التي يمارسها الجناة لحسابات البنوك والقدرة على التلاعب بها ونقلها وتحويلها عن بعد، فلا بد أن تستعمل الأجهزة المصرفية الأنظمة المضادة لهذا الاختراق، وأن تراقب حركة الحسابات إلكترونياً سواء حركات السحب أو الإيداع أو التحويل أو النقل من الداخل أو الخارج أو العكس[18].

وحتى لا نبخس المشرِّع الكويتي حقه من الثناء فإن نص المادة السابعة كان ممتازاً في صياغته، فهو شامل لكل صور التجريم المتعلقة بتبييض الأموال عن طريق وسيط إلكتروني.

هذا وقد أصدر المشرِّع الجزائري النظام رقم (12 / 03) المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، حيث جاء الباب السادس منه تحت عنوان

(18) مراد رشدي، 2007، غسل الأموال عبر الوسائل الإلكترونية، مقال منشور على الموقع التالي: http://www.f-law.net/law/threads/1802 تاريخ الاطلاع 2016/03/19 على الساعة 23:15 بتوقيت غرينتش.

التحويلات الإلكترونية ووضع الأموال تحت التصرف، ونصت المادة (17) منه على ما يلي: «يتعيَّن على المصارف والمؤسسات المالية والمصالح المالية لبريد الجزائر في إطار التحويلات الإلكترونية مهما كانت الوسيلة المستعملة و/ أو وضع الأموال تحت التصرف أن تسهر على التحقق بدقة من هوية الآمر بالعملية والمستفيد بالإضافة إلى عنوانيهما .

يجب أن يحوز مسيرو نظام الدفع والمتعاملون المباشرون أو غير المباشرين على جهاز آلي لاكتشاف الزبائن والعمليات ويتعلق الأمر بالهيئات أو الأشخاص المسجلين في القوائم المعدة مسبقا[19]».

جاء في المادة العاشر من قانون مكافحة جرائم تقنية المعلومات الكويتي أنه :»يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعاً لمنظمة إرهابية، أو لشخص إرهابي، أو نشر عن أيهما معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، ولو تحت مسميات تمويهية، لتسهيل الاتصالات بأحد قياداتها أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية».

في رأينا المتواضع نص هذه المادة قد يخلق إشكاليات كثيرة من حيث التطبيق، لأمر بسيط وهو صعوبة تحديد المقصود بالمنظمات الإرهابية أو الشخص الإرهابي، والسؤال الذي قد يطرح هو على أي أساس يحكم القاضي على منظمة بأنها إرهابية أو على شخص بأنه إرهابي؟ والحل يكمن في رأينا في تحديد المقصود بالعمل الإرهابي والمنظمات الإرهابية، وذلك بإضافة عبارة كل من «أنشأ موقعاً لمنظمة أو شخص يسعى للقيام بأعمال إرهابية..»، وهنا إما يذكر الأفعال التي تشكل العمل الإرهابي أو على الأقل ذكر عبارة «كما هو محدد..»، وهنا يشير إلى المادة التي تعاقب على الجريمة الإرهابية في قانون الجزاء.

كما ندعو المشرِّع الكويتي إلى إضافة عبارة: «أو تمويل التدريب عليها» بعد «عبارة أو تمويلها»، كما ندعوه أيضاً إلى إضافة فقرة إلى نص هذه المادة تعاقب على إنشاء

(19) النظام رقم 12/03 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية عدد 12 سنة 2013، الجزائر.

موقع لبث النعرات والفتن بين أحزاب أو طوائف مكونة للمجتمع.

هذا ولم ينص المشرِّع الجزائري على مثل هذه الجريمة ونص عليها كل من المشرِّع السعودي[20]، وكذا الاتفاقية العربية لمكافحة الجريمة المعلوماتية[21].

المطلب الرابع

جرائم لم يتفطن لها المشرِّع الكويتي

على الرغم من أن قانون مكافحة جرائم تقنية المعلومات الكويتي حديث الصدور ويمتاز بصياغة ممتازة ولو شابته بعض النقائص، إلا أن هناك بعض الجرائم لم يتضمنها القانون، ونخصُّ بالذكر الأفعال المتعلقة بتصميم أو صنع أو الاتجار بمعطيات أو برامج تستعمل في الجرائم الإلكترونية، وكذا الأفعال المتعلقة بحيازة أو نشر أو استعمال المعطيات المتحصل عليها من الجرائم الإلكترونية، وهذه الجرائم لم ينص عليها المشرِّع السعودي أيضاً، ولكن نص عليها المشرِّع الجزائري الذي قدَّر أن تجميع عدد من المعطيات المستعملة لارتكاب هذا النوع من الجرائم من شأنه أن يرفع درجة الخطر التي تشكلها، مما يؤدي إلى إمكانية ارتكاب هذه الجرائم، بل وتسهيل ارتكابها، وهذا النوع يسمى بالتجريم الوقائي.

وقد جاء في المادة (394 مكرراً2) من قانون العقوبات ما يلي: «يعاقب بالحبس من شهرين إلى ثلاث سنوات، وبغرامة مالية من 1000.000 د.ج إلى 5.000.000 د.ج كل من يقوم عمداً وعن طريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة، أو معالجة، أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.»

وهو ما نصت عليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية في نص المادة

(20) المادة السابعة من قانون مكافحة الجريمة المعلوماتية السعودي.
(21) المادة 15 من الاتفاقية.

(09) منها حيث جرمت هذه المادة كلاً من:

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

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

- كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأيٍّ من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

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

المبحث الثاني

الأحكام الخاصة بمكافحة جرائم تقنية المعلومات

المواد المتبقية من قانون مكافحة جرائم تقنية المعلومات الكويتي تناولت الأحكام المتعلقة بالجرائم المذكورة آنفاً، كظروف التشديد والتخفيف والعقوبات التكميلية إلخ...، ولكن إذا كان المشرِّع الكويتي قد أنهى قانونه عند هذه الأحكام، فإن هناك جوانب وأحكاماً أخرى قد غفل عنها سنحاول ذكرها من خلال هذا المطلب.

المطلب الأول

الأحكام الواردة في قانون مكافحة جرائم تقنية المعلومات

الفرع الأول

ظروف التشديد والتخفيف

جاء في المادة (11) من قانون مكافحة جرائم تقنية المعلومات الكويتي ما يلي: «لا تقل عقوبة الحبس أو الغرامة التي يحكم بها عن نصف حدِّها الأقصى إذا اقترنت الجريمة بأي من الظروف الآتية:

- ارتكاب الجريمة من خلال عصابة منظمة؛
- شغل الجاني وظيفة عامة وارتكابه لها مستغلاً سلطته أو نفوذه؛
- التغرير بالقُصّر ومن في حكمهم من ناقصي الأهلية أو استغلالهم؛
- صدور أحكام سابقة من المحاكم الوطنية، أو الأجنبية بموجب الاتفاقيات المصادق عليها بإدانة الجاني بجرائم مماثلة».

وقد أحسن المشرِّع الكويتي بالنص على ظروف التشديد هذه، إذ إن الكثير من هذه الجرائم قد تتم وفق مخطط من طرف منظمة، أو عادة ما تقع من أشخاص يشتغلون في وظيفة تسهل لهم ارتكابها.

وتنص الفقرة الثانية من المادة المذكورة أعلاه على ظروف التخفيف حيث أجازت للمحكمة أن تعفي من العقوبة كل من بادر من الجناة بإبلاغ السلطات المختصة بالجريمة قبل علمها بها وقبل البدء في تنفيذ الجريمة، فإن كان الإبلاغ بعد العلم بالجريمة وقبل البدء في التحقيق تعيّن للإعفاء من العقوبة أن يكون من شأن الإبلاغ ضبط باقي الجناة في حالة تعددهم، وإن كنا نرى أنه كان من الأفضل لو كان الإعفاء من العقوبة مرتبطاً بالقبض على الجناة، وليس مرتبطاً بالعلم بالجريمة وبدء التحقيق، لأن هذا النوع من الجرائم يصعب إثباته ولا يتم الإبلاغ عنه عادة، لذا فنحن بحاجة إلى فتح المجال والترغيب وليس العكس.

الفرع الثاني

الأحكام الخاصة بالعقوبات

نص المشرِّع الكويتي على التكميلية في المادة الثالثة عشر حيث جاء فيها: "يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجرائم أو الأموال المتحصلة منها. ويجوز الحكم بإغلاق المحل أو الموقع الذي ارتكب فيه أي من هذه الجرائم إذا كان ارتكابها قد تم بعلم مالكها لمدة لا تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية، أو بحق المضرور في التعويض المناسب .ويكون الحكم بإغلاق المحل أو الموقع وجوبياً إذا تكرَّر ارتكاب أي من هذه الجرائم بعلم مالكها".

في هذه الحالة يتكلم المشرِّع الكويتي عن إمكانية فرض بعض العقوبات التكميلية والمتمثلة في المصادرة والإغلاق، وما يمكن أن نلاحظه هنا هو أن المشرِّع الكويتي جعل الحكم بهذه العقوبات جوازياً، وهو أمر لا يستقيم مع خطورة هذه الجرائم، فالأموال والوسائل التي استعملت في ارتكاب هذه الجرائم يجب أن تصادر، والمواقع والمؤسسات الضالعة فيها يجب أن تغلق، إذا لم نقل في كل الجرائم، فعلى الأقل أخطرها مثل الإرهابية والإباحية والماسة برموز الدين والدولة.

ثم إن المشرِّع الكويتي لم ينتبه إلى عقوبة تكميلية مهمة جداً وهي نشر الحكم لأنه يساهم في تعريف الناس بهؤلاء المجرمين وهذه المؤسسات أو المواقع.

وقد نص المشرِّع الجزائري على وجوب فرض عقوبتي المصادرة والغلق، وغَفَلَ هو الآخر عن عقوبة نشر الحكم حيث جاء في المادة (394 مكرراً4): "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، في حين نجد تشابها كبيراً ما بين نص المشرِّعين الكويتي والسعودي في هذا الخصوص[22].

هذا وقد نصت المادة الرابعة عشرة على ما يلي: «مع عدم الإخلال بالمسؤولية الجزائية الشخصية لمرتكب الجريمة، يعاقب الممثل القانوني للشخص الاعتباري بذات العقوبات المالية المقررة عن الأفعال التي تُرتكب بالمخالفة لأحكام هذا القانوني، إذا ثبت أن إخلاله بواجبات وظيفته أسهم في وقوع الجريمة مع علمه بذلك. ويكون الشخص الاعتباري مسؤولاً عما يحكم به من عقوبات مالية أو تعويضات إذا ارتكبت الجريمة لحسابه أو باسمه أو لصالحه».

كل التشريعات اتجهت نحو تحميل الشخص الاعتباري المسؤولية الجزائية التي تتناسب مع طبيعته، وهنا نجد المشرِّع الكويتي يكرِّس ذلك عن طريق فرض تحمُّل الشخص الاعتباري ما يحكم به من عقوبات مالية أو تعويضات إذا ارتكبت الجريمة لحسابه أو باسمه أو لصالحه، لكن الأمر الغريب والذي لا نجده في التشريعات المقارنة هو عدم تغليظ الغرامات بالنسبة للشخص المعنوي، حيث ساوى المشرِّع الكويتي بينه وبين الشخص الطبيعي، وهو أمر غير مستساغ نظراً للفارق في الذمة المالية بينهما.

هذا وقد نص المشرِّع الجزائري على العقوبة المقررة للشخص المعنوي في حالة ارتكابه لإحدى الجرائم الإلكترونية في نص المادة (394 مكرراً 4) حيث جاء فيها: «يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي»، بينما لا نجد نصاً مماثلاً في قانون مكافحة الجرائم المعلوماتية السعودي[23].

(22) المادة الثالثة عشر من قانون مكافحة الجرائم المعلوماتية السعودي.

(23) أكدت الاتفاقية على ضرورة معاقبة الشخص الاعتباري، لكنها لم تشر إلى مقدار العقوبة حيث =

أما المادة الثامنة عشرة من ذات القانون فتنص على أنه: «تسقط الدعوى الجزائية المنصوص عليها في هذا القانون بحسب مدة العقوبة، فإن كانت بحدود الثلاث سنوات فتسقط خلال سنتين، وإن كانت تتجاوز الثلاث سنوات فتسقط خلال خمس سنوات من يوم وقوع الجريمة، ولا تُسمع دعوى التعويض إذا لم يتم رفعها خلال ثلاث سنوات من تاريخ علم المضرور، ما لم تكن الدعوى الجزائية قائمة فيبدأ ميعاد عدم السماع من تاريخ انقضائها أو صدور حكم نهائي فيها».

الملاحظة التي نبديها على هذه المادة هو أنه كان على المشرِّع الكويتي أن يستثني بعض الجرائم الخطيرة من مسألة تقادم الدعوى الجزائية خاصة تلك المتعلقة بالإرهاب وتلك الماسة برموز الدين والدولة والاتجار بالبشر.

أما المادة (19) فهي تتعلق بالمعاقبة على الشروع في هذه الجرائم عن طريق تطبيق أحكام المادة (46) من قانون الجزاء، بالإضافة إلى أنها سمحت للقاضي بإبعاد الأجنبي عن الكويت بعد الانتهاء من تنفيذ عقوبته، وإبلاغ الأمر للسلطة الإدارية لتنفيذه.

الفرع الثاني

أحكام الجانب الإجرائي لقانون مكافحة جرائم تقنية المعلومات الكويتي

ما يؤخذ على المشرِّع الكويتي أنه لم يتطرق بالتفصيل للجهاز الخاص بمتابعة هذا النوع من الجرائم إلا ما ورد في المادة الخامسة عشرة والتي جاء فيها: «للموظفين الذين يصدر بتحديدهم قرار من الوزير المختص ضبط الجرائم التي تقع بالمخالفة لأحكام هذا القانون وتحرير المخالفات عنها، وإحالتها إلى النيابة العامة، وعلى جميع الجهات ذات الصلة تقديم التسهيلات اللازمة لهؤلاء الموظفين».

كنا نتمنى أن ينص المشرِّع الكويتي على جهاز أو هيئة وليس مجرد الإشارة إلى موظفين، لأن هذا النوع من الجرائم ذو طبيعة خاصة يتطلب وجود ضبطية أو جهاز خاص وموظفين ماهرين يتمتعون بكفاءة عالية في مجال تكنولوجيا

= جاء في المادة (20) منها: «تلتزم كل دولة طرف مع مراعاة قانونها الداخلي بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا».

الإعلام والاتصال وتقنية المعلومات، وهو ما فَطِنَ له المشرِّع الجزائري عندما نص على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك بموجب المرسوم الرئاسي رقم (15 / 261) الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[24].

ومن المهام الموكلة للهيئة نذكر ما يلي:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية .
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

وتتكون الهيئة من عدة أجهزة نذكرها باختصار:

(24) المرسوم الرئاسي الجزائري رقم 15 / 261 المؤرخ في 08 أكتوبر 2016، جريدة رسمية عدد 53.

- **لجنة مديرة تضطلع بالمهام التالية[25]:**

1- توجيه عمل الهيئة والإشراف عليه ومراقبته. 2 – دراسة كل مسألة تخضع لمجال اختصاص الهيئة لاسيما ما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية، 3 – ضبط برنامج عمل الهيئة وتحديد شروط وكيفية تنفيذه، القيام دورياً بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة. 4 – اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. 5 – دراسة مشروع النظام الداخلي للهيئة والموافقة عليه. 6 – دراسة مشروع ميزانية الهيئة والموافقة عليه. 7 – دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه

- إبداء رأيها في كل مسألة تتصل بمهام الهيئة، وتقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.

- مديرية عامة تتولى المديرية العامة بالصلاحيات الآتية[26]:

1 – السهر على حسن سير الهيئة. 2 – السهر على تنفيذ برنامج عمل الهيئة، 3 – تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها، 4 – تحضير اجتماعات اللجنة المديرة، 5 – تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية، 6 – تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية.

- **مديرية للمراقبة الوقائية واليقظة الإلكترونية:**

تتولى ما يلي:

1 – تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن

(25) تتكون من: الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا يعينهما المجلس الأعلى. ويعين ممثل رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي.

(26) يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي وتنهى مهامه حسب الأشكال نفسها.

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع ساري المفعول، 2 – إرسال المعلومات المحصَّل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، 3 – تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم، 4 – جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، 5 – تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائياً أو بناءً على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– مديرية للتنسيق التقني:

تتولى مديرية التنسيق التقني ما يلي:

1 – إنجاز الخبرات القضائية في مجال اختصاص الهيئة، 2 – تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها، 3 – إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، 4 – القيام بمبادرة منها أو بناء على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها 5 – تسيير منظومة الإعلام للهيئة وإدارتها.

في بقية المواد يتكلم المشرِّع الكويتي على أن تطبيق العقوبات المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات لا يخل بأية عقوبات أشد ينص عليها قانون الجزاء أو أي قانون آخر، وهو أمر منطقي يعكس نيَّة المشرِّع الكويتي في الحد من هذه الجرائم الخطيرة[27].

أما المادة السابعة عشرة فجاءت على النحو التالي: «تختص النيابة العامة وحدها، دون غيرها، بالتحقيق والتصرف والادعاء في جميع الجرائم المنصوص عليها في هذا القانون».

(27) المادة السادسة عشر من القانون.

إذا سلمنا بأن النيابة العامة هي الجهة الوحيدة المخوَّل لها التصرف في الدعوى العمومية والمطالبة بتوقيع العقوبات، فإن مسألة التحقيق في هذا النوع من الجرائم تحتاج إلى إعادة نظر، نريد أن نقول إن أعضاء النيابة العامة بتكوينهم العادي من الصعب عليهم التحقيق فيها نظراً لتعلقها بمسائل تقنية، لذلك فإن مسألة التحقيق في هذه الجرائم يجب أن تُسند إلى جهات مختصة وخبراء في هذا النوع من الإجرام ويكون ذلك تحت إشراف النيابة العامة.

المطلب الثاني

دعوة المشرِّع الكويتي للنص على الأحكام الإجرائية للجرائم المعلوماتية

لم ينص المشرِّع الكويتي على الجانب الإجرائي للجرائم المعلوماتية بالشكل اللازم، فهذه الجرائم تتطلب وجود إجراءات خاصة نظراً لكونها تقع في عالم افتراضي، وهو ما يخلق العديد من الصعوبات من الناحية التطبيقية، ويجعل الإجراءات العادية عاجزة عن إثبات هذه الجرائم والوصول إلى المجرمين.

الفرع الأول

لابد من الفصل في مشكلة الاختصاص

الجرائم المعلوماتية جرائم عابرة للحدود، فقد تقع في دولة وتتحقق نتائجها في دول مختلفة، وهو ما يثير مشكلة الاختصاص بالنسبة للموظفين المؤهلين للبحث والتحري وكذا القضاء.

وقد تصدت الاتفاقية العربية لمكافحة الجريمة المعلوماتية لهذه الإشكالية ونصت في مادتها الثلاثين على أنه: «تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية، وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت :

أ) في إقليم الدولة الطرف.

ب) على متن سفينة تحمل علم الدولة الطرف.

ج) على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د) من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها، أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ) إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة (31) الفقرة (1) من هذه الاتفاقية[28]، في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.
- إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلَّت الجريمة بأمنها، أو صالحها، ثم الدولة التي وقعت الجريمة في إقليمها، ثم الدولة التي يكون الشخص المطلوب من رعاياها، وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم".
- ومن هنا ندعو المشرِّع الكويتي للنص على مسألة الاختصاص كون أن لها علاقة بسيادة الدول ومبدأ المعاملة بالمثل.

الفرع الثاني

التفتيش الإلكتروني وحفظ المعطيات والترصد

إجراءات لابد من النص عليها

على خلاف العديد من التشريعات أصدر المشرِّع الجزائري القانون رقم 09/04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها، وهو قانون إجرائي ينص على عدة إجراءات مهمة تتناسب مع طبيعة الجريمة المعلوماتية.

1 – التفتيش الإلكتروني:

نظم المشرِّع الجزائري مسألة التفتيش الإلكتروني بموجب المادة (5) من القانون

(28) تتعلق الفقرة الأولى من نص المادة (31) بتسليم المجرمين بين الدول الأطراف.

09/04 حيث جاء فيها: «يجوز للسلطات القضائية المختصة، وكذا ضبّاط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة (4) أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها .

ب- منظومة تخزين معلوماتية .

في الحالة المنصوص عليها في الفقرة «أ» من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك.

إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة، ووفقاً لمبدأ المعاملة بالمثل .

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها».

ومع ذلك لم ينظم المشرِّع الجزائري التفتيش الإلكتروني بالشكل الكافي خاصة من حيث الشروط المتعلقة بالتفتيش كالميعاد والإذن القضائي وحضور المعني.

هذا وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على التفتيش الإلكتروني حيث جاء في 26 منها: «تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى :

(أ) تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها؛

(ب) بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.

- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها، بما يتوافق مع الفقرة (1 – أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول

قانوناً أو متوفرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى».

ومن هنا ندعو المشرِّع الكويتي لتنظيم مسألة التفتيش الإلكتروني كونه من بين الإجراءات المهمة في إثبات هذا النوع من الجرائم.

2- **ضبط الأدلة الإلكترونية:**

نظراً لخصوصية التفتيش والضبط في مجال الجرائم الإلكترونية، فإن المشرِّع قد أجاز للجهة المكلفة بالتفتيش الاستعانة بذوي الخبرة من مقدمي خدمة الإنترنت، وعند الانتهاء من عملية ضبط الموجودات أثناء التفتيش الإلكتروني في إحدى الجرائم المعلوماتية، فإنه يتوجب على القائم بعملية التفتيش والضبط وضع هذه الموجودات المعنوية في دعائم، ولا يتم فتحها إلا بحضور صاحبها مصحوباً بمحاميه .

وهو ما نصت عليه المادة السادسة من القانون رقم 09/04 الجزائري حيث جاء فيها:«عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقاً للقواعد المقررة في قانون الإجراءات الجزائية .

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز والسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية .

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات[29]».

(29) هذا وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على مسالة ضبط المعلومات المخزنة حسب نص المادة 27 التي جاء فيها أنه: «1 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الاتفاقية.. هذه الإجراءات تشمل صلاحيات :

أ) ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات؛ =

إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (6) أعلاه لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[30]».

الفرع الثالث

الترصد الإلكتروني

من بين الإجراءات المهمة التي لم ينص عليها قانون مكافحة جرائم تقنية المعلومات الكويتي إجراء مراقبة الاتصالات الإلكترونية أو ما يعرف بالترصد الإلكتروني، وقد نص المشرِّع الجزائري على هذا الإجراء بموجب المادة الثالثة من القانون رقم 09/04 سالف الذكر، حيث جاء فيها: «مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية [31]، وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات

= ب) عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها؛
ج) الحفاظ على سلامة معلومات تقنية المعلومات المخزنة؛
د) إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.
2 – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين 2 و1 من المادة السادسة والعشرين من هذه الاتفاقية».

(30) يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك..، انظر المادة الثامنة من القانون رقم 09/04 .

(31) نشير أن قانون الإجراءات الجزائية ينص على إجراءات اعتراض المراسلات والتقاط الصور وتسجيل الأصوات وهنا المادة تشير إلى أنه يتم تطبيق الشروط المنصوص عليها في قانون إجراءات الجزاءات، وبالتحديد المادة 65 مكرر5 حيث جاء فيها: «إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يلي:
– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية... ».

الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية».

ويمكن القيام بعمليات المراقبة الإلكترونية في الحالات الآتية:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطن .

ج –لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة .

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة « أ « من هذه المادة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[32].

الفرع الرابع

التعاون الدولي ضرورة حتمية

لا يمكن لأي دولة مهما بلغت من قوة التطور التكنولوجي والصرامة في قوانينها

(32) هذا وقد حثت الاتفاقية العربية الدول الأطراف على تبني الإجراءات التشريعية والضرورية بخصوص الجرائم المنصوص عليها في القانون الداخلي لتمكين السلطات المختصة من الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف أو التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية معلومات.. المادة 29 من الاتفاقية.

أن تواجه هذا النوع من الجرائم وحدها، ومن ثم وجب على كل الدول النص وتذليل إجراءات التعاون فيما بينها، وبالرجوع إلى قانون مكافحة جرائم تقنية المعلومات، لكننا لا نجد المشرِّع الكويتي يشير إلى مسألة التعاون الدولي رغم أهميتها.

هذا وقد نص المشرِّع الجزائري على التعاون الدولي في مكافحة الجريمة الإلكترونية، حيث إنه وفي إطار التحريات أو التحقيقات القضائية الجارية لمعاينة هذه الجرائم وكشف مرتكبيها سمح المشرِّع للسلطات المختصة بتبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني .

كما أجاز المشرِّع في حالة الاستعجال – مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل – قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها[33].

كما نص المشرِّع الجزائري على أنه تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل[34].

نشير إلى أن الاتفاقية العربية خصصت العديد من المواد لتنظيم مسالة التعاون الدولي نظراً لأهميتها، وقد حثَّت جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى يمكن لغايات التحقيقات، أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم[35].

(33) المادة 17 من قانون رقم 09/04.
(34) المادة 18 من قانون رقم 09/04
(35) الفصل الرابع من الاتفاقية.

الخاتمة:

على الرغم من النقائص الموجودة في قانون مكافحة جرائم تقنية المعلومات الكويتي، إلا أنه يُعد بحق من أكثر القوانين التي حاولت التطرق لمختلف صور جريمة المعلوماتية، والتي غفلت عنها الكثير من التشريعات المقارنة، وحتى يكون هذا القانون متكاملاً من جميع النواحي فإننا ندعو المشرِّع الكويتي للأخذ بالاقتراحات التالية:

- تعديل النصوص القانونية لبعض الجرائم تفادياً لوجود أي ثغرة كما هو مبيَّن في الورقة البحثية أعلاه.
- تجريم بعض الصور الأخرى للجريمة الإلكترونية وبالتحديد تصميم أو صنع أو الاتجار بمعطيات أو برامج تستعمل في الجرائم الإلكترونية، وكذا الأفعال المتعلقة بحيازة أو نشر أو استعمال المعطيات المتحصل عليها من الجرائم الإلكترونية.
- النص على الجانب الإجرائي للجرائم المعلوماتية كالاختصاص، والتفتيش الإلكتروني، والأدلة الإلكترونية، والترصد الإلكتروني، والتعاون الدولي في هذا المجال.
- إنشاء جهاز أو هيئة خاصة للوقاية من جريمة المعلوماتية ومكافحتها.
- إعداد وتدريب قضاة متخصصين للفصل في مثل هذه الجرائم.

المراجع:

كتب ومقالات وأبحاث باللغة العربية:

- خليفة محمد، 2010، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة.
- عبد الحليم بوقرين، 2015، الحماية الجنائية لشخص الرسول ﷺ، مقالة منشورة في مجلة الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط / الجزائر، العدد 08.
- مراد رشدي، 2007 غسل الأموال عبر الوسائل الإلكترونية، مقال منشور على الموقع التالي: http://www.f-law.net/law/threads/1802 تاريخ الاطلاع 2016/03/19 على الساعة 23:15 بتوقيت غرينتش.
- هلالي عبد اللاه أحمد، 2008، اتفاقية بودابيست لمكافحة الجرائم المعلوماتية، دار النهضة العربية، ط 01.

2 – قوانين واتفاقيات:

- الاتفاقية العربية لمكافحة الجرائم المعلوماتية.
- القانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات الكويتي.
- قانون الجزاء الكويتي.
- قانون النشر والمطبوعات الكويتي.
- قانون مكافحة الجرائم المعلوماتية السعودي.
- – قانون العقوبات الجزائري.
- قانون الإجراءات الجزائية الجزائري.
- القانون رقم 09/04 الجزائري لسنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجزائر، الجريدة الرسمية عدد 47.
- النظام رقم 12/03 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجزائر، الجريدة الرسمية عدد 12.
- المرسوم الرئاسي رقم 15/261 المؤرخ في 08 أكتوبر 2016، الذي يحدد تشكيلة وتنظيم وكيفية

سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجزائر، جريدة رسمية عدد 53.

3 – كتب ومقالات وأبحاث باللغة الفرنسية:

- Samia Bet Ismail Kamoun، 2004، La formation du contrat de vente électronique et le droit commun des contrats، Revue Tunisienne de Droit Centre de Publication Universitaire.
- Christine Bitouzet، 1999، Le commerce électronique de valeur pour lەentreprise، ed، Hernes science publication، Paris.

المحتوى: