المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الثاني - الإصدار الثامن عشر
تأريخ الإصدار: 20 أبريل 2021م

جرائم الاعتداء على الشبكة المعلوماتية في التشريعات العربية

(دراسة تحليلية مقارنة بالتشريع الإماراتي)

Crimes of assault on the information network in Arab legislations

(An analytical study compared to the UAE legislation)

إعداد/ أ.د. إمام حسنين خليل عطا الله

أستاذ القانون الجنائي، المركز القومي للبحوث الجنائية، أستاذ القانون الجنائي، جامعة زايد، الإمارات العربية المتحدة

Email: Imam.Attallah@zu.ac.ae

ملخص الدراسة

تعد الشبكة المعلوماتية من المصالح الحيوية التي تتطلب الحماية القانونية في أعلي مستوياتها وهي الحماية الجنائية؛ من خلال تجريم وعقاب مختلف صور المساس أو الاعتداء أو مجرد التأثير على الشبكة المعلوماتية، ويتحدد مدى نجاح تلك الحماية بقدر أحاطتها بتلك الصور من خلال نصوص تجريميه منضبطة.

والدراسة الراهنة تتناول، من خلال منهج وصفي تحليلي وفي إطار مقارن، موقف التشريعات الجنائية في عدد من الدول العربية من التجريم والعقاب على مختلف صور المساس أو الاعتداء أو مجرد التأثير على الشبكة المعلوماتية، بالنظر إلى أهمية تلك الحماية في عصر المعلومات وانتشار استخدام صور الذكاء الاصطناعي في العديد من المجالات الخدمية.

وسوف تكون المقارنة على أكثر من مستوى ومجال حيث ستتم مقارنة خطة المشرع الإماراتي في التجريم والعقاب على مستوى وطني، ما بين القانون الاتحادي الملغي رقم 2 لسنة 2006، والمرسوم بقانون الاتحادي الحالي رقم 5 لسنة 2012، لبيان الجوانب المستحدثة في التجريم والعقاب، وسياسات الإعفاء والتخفيف والتشديد، كما ستتم المقارنة مع التشريعات الوطنية في عدد من الدول العربية الأخرى، ومنها السعودية، والسودان والمملكة الأردنية الهاشمية، وسلطنة عمان، وقطر، ومملكة البحرين، ودولة الكويت، كنماذج للتشريعات العربية. كما ستكون المقارنة مع ما ورد في الاتفاقية الأوربية الخاصة بجرائم الكمبيوتر لعام 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 والتي صدقت عليها دولة الإمارات العربية المتحدة عام 2011، والمقارنة كذلك مع ما ورد بوثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية 2013.

الكلمات المفتاحية: جريمة، عقوبة، الحماية الجنائية، جريمة تقنية معلومات، شبكة معلوماتية

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الثاني - الإصدار الثامن عشر
تأريخ الإصدار: 20 أبريل 2021م

Crimes of assault on the information network in Arab legislations

(An analytical study compared to the UAE legislation)

Abstract

The information network is one of the vital interests that require legal protection at its highest level, which is criminal protection; Through the criminalization and punishment of various forms of abuse or assault or merely affecting the information network. The criminal protection success is determined to the extent that it is surrounded by these images through the Texts of criminalization and punishment.

The study deals with, according to a descriptive analytical approach and a comparative framework, the criminal legislations in a number of Arab countries regarding criminalization and punishment of various forms such as prejudice, assault or just affecting the information network, regarding the importance of this protection in the information age and the widespread use of artificial intelligence forms In many service areas.

The comparison will be on more than one level and field, as the Emirati legislator's plan for criminalization and punishment will be compared on a national level, between the repealed Federal Law No. 2 of 2006, and the current Federal Decree Law No. 5 of 2012, to show the new aspects of criminalization and punishment, and the exemption and mitigation policies. Emphasis will be placed on the comparison with national legislation in a number of other Arab countries, including Saudi Arabia, Sudan, the Hashemite Kingdom of Jordan, the Sultanate of Oman, Qatar, the Kingdom of Bahrain, and the State of Kuwait, as models for Arab legislation. The comparison will also be with what was stated in the European Convention on Computer Crimes for year 2001, and the Arab Convention to Combat Information Technology Crimes, year 2010, which the United Arab Emirates ratified in 2011, and the comparison also with what was mentioned in the Riyadh document for the unified system (law) to combat information technology crimes for countries The Cooperation Council for the Arab States of the Gulf 2013.

Keywords: Crime, Punishment, criminal protection, IT crime, information network

مقدمة:

تعد الشبكة المعلوماتية هي الأساس في الذكاء الاصطناعي والمحرك له، ومن ثم فالتمتع بخدمات الذكاء الاصطناعي يفرض ضرورة توفير الحماية للشبكة المعلوماتية لضمان استمرار تشغيلها وحمايتها من عمليات التحايل والاحتيال والاختراق، ولا شك أن أعلي درجات الحماية تتمثل في الحماية الجنائية، سواء في جانبها الموضوعي أو الإجرائي، ومن ثم حرص المشرع الإماراتي، والذي كان من أول من سن تشريعا لمكافحة جرائم تقنية المعلومات، علي توفير حماية متكاملة للشبكة المعلوماتية، بدءا من تعريف المقصود بها ووصولا إلي تجريم مختلف صور الاعتداء عليها في أي صورة من صور الاعتداء التي تتناسب مع طبيعتها، مثل الاحتيال أو التحايل أو الاختراق بأية وسيلة، وقد تابعه في ذلك عدد من التشريعات العربية اللاحقة.

أولاً: أهمية الدراسة

تبدو أهمية هذه الدراسة في أن القانون هو حائط الصد الأول في مواجهة إساءة استخدام وسائل تقنية المعلومات والاعتداء على الشبكات المعلوماتية الالكترونية، وهو السبيل الذي انتهجته الدول المتقدمة وتبنته الاتفاقيات الدولية والإقليمية لمكافحة هذا النوع من الإجرام المستحدث والمتنامي، يضاف إلى ذلك الانتشار الواسع والملحوظ للتكنولوجيا المتقدمة ووسائل الاتصال في الدول العربية، خاصة خلال العقد الأخير من هذا القرن وفي بعض الدول الخليجية على وجه الخصوص مثل دولة الإمارات العربية، والبحرين، والسعودية، وقد صاحب هذا الانتشار ضعف الوعي لدي غالبية مستخدمي شبكة المعلومات الدولية بمخاطرها، وقلة مستويات الجاهزية التقنية والقانونية لمكافحة جرائم تقنية المعلومات، ومن ثم يمكن إدراك أهمية دراسة وتحليل الحماية الجنائية للشبكة المعلوماتية في التشريع الإماراتي كنموذج تشريعي عربي متقدم وسابق على غيره من التشريعات، وتم تعديله بشكل كلي بعد مرور أقل من ست سنوات على العمل به، وذلك في إطار مقارن، بالنظر إلى أن القانون الجنائي (عقوبات وإجراءات) – سواء كان عاما أو خاصا - هو القادر على توفير أكبر قدر ومستوى من الحماية ضد مخاطر هذه الجرائم التي أصبح المجتمع العربي أكثر عرضة لمخاطرها والوقوع ضحية لأعمالها المتعددة والمتنوعة والمتطورة، الأمر الذي يفرض ضرورة مراجعة التشريعات بشكل دوري ومنتظم لتكون قواعدها مسايرة للتطور المتلاحق في مجال التكنولوجيا واستخدام وسائل تقنية المعلومات.

ثانياً: مشكلة الدراسة

تثير الدراسة الراهنة إشكالية بحثية تتمثل في مدى توافق واتساق توجه التشريعات الجنائية العربية في الشبكة المعلوماتية مع الاتجاهات الدولية والإقليمية والتشريعات المقارنة في هذا الشأن؛ سواء من حيث الإطار العام للتجريم، أو أنواع العقوبات التي تبناها كل تشريع بالتطبيق على المشرع الجنائي الإماراتي. كما تبدو الإشكالية البحثية كذلك في مدى الحاجة إلى المراجعة الدورية لتشريعات مكافحة جرائم تقنية المعلومات لتكون أكثر توافقاً مع التطورات التكنولوجية التي يشهدها المجتمع العربي، ولتوفر أكبر قدر من الحماية من خطر الوقوع في براثن هذه الجرائم واستغلال مرتكبيها المحترفين الولع العام بالتكنولوجيا المتقدمة في العديد من المجتمعات العربية وخاصة المجتمع الإماراتي، حيث يتميز هؤلاء المجرمون بقدر عال من الذكاء المعلوماتي والخبرة بوسائل التقنية، التي تجعل من الصعوبة ملاحقتهم بعد ارتكاب الجريمة.

ثالثاً: أهداف الدراسة

يتمثل الهدف الرئيسي في هذه الدراسة في الوقوف على مدى كفاية وكفاءة التشريعات الجنائية العربية التي صدرت لتوفير الحماية للشبكة المعلوماتية، وذلك بالتطبيق علي التشريع الإماراتي، حيث تعد دولة الإمارات العربية المتحدة هي صاحبة فكرة القانون الاسترشادي العربي لمكافحة جرائم تقنية المعلومات عام 2003، كما أنها الدولة العربية الأولي التي أصدرت تشريعا مستقلا في هذا الشأن عام 2006، ثم ما لبثت أن ألغته بالمرسوم بقانون الاتحادي رقم 5 لسنة 2012، كتجربة تشريعية عربية فريدة تفيد في بيان مدى التطور الذي لحق السياسة الجنائية التي تبناها هذا المشرع في هذا المرسوم، مقارنة بالقانون الاتحادي رقم 2 لسنة 2006 في ذات الشأن، الأمر الذي يمكن أن يفيد الدول العربية الأخرى علي صعيد تطوير تشريعاتها النافذة في شأن مكافحة جرائم تقنية المعلومات، أو إصدار تشريعات جديدة في هذا الشأن.

ويتفرع عن هذا الهدف الرئيسي جملة أهداف فرعية تتمثل في:

1-بيان أحكام جرائم تعطيل الشبكة المعلوماتية وإعاقة الوصول إليها.

2- دراسة أركان جرائم الاحتيال والتحايل على الشبكة المعلوماتية.

3- دراسة جريمة الحصول على شفرة الدخول لتقنية المعلومات.

4- دراسة أحكام جريمة إنتاج برامج معلوماتية والتقاط الاتصالات عبر الشبكة المعلوماتية.

رابعاً: المفاهيم الأساسية في الدراسة

تتضمن الدراسة عددا من المفاهيم التي يجب بيان مدلولها وفحواها والتي ستسهم في دراسة وتحليل جوانب الحماية الجنائية للشبكة المعلوماتية، وذلك على النحو التالي:

1- المعلومات الإلكترونية

أولت التشريعات الجنائية العربية في مجال التقنية المعلومات أهمية كبيرة للملومات والبيانات، وإن اختلفت في التعبير عنها، ففي حين استخدم المشرع الإماراتي مصطلح (المعلومات الإلكترونية)، استخدمت بعض التشريعات مصطلح (البيانات أو المعلومات) مثل نظام مكافحة جرائم المعلوماتية السعودي لعام 2007، والمشرع السوداني في قانون جرائم المعلوماتية لعام 2007 أيضا، وعرف المشرع الأردني في قانون جرائم أنظمة المعلومات (المعلومات) وعرفه باختصار بأنها " البيانات التي تمت معالجتها وأصبح لها دلالة "، في حين أفاضت التشريعات الأخرى في تحديد مفهومها، ومدت الحماية إلي ما يمكن نقله أو تخزينه أو انتاجه أو توليده. إلخ بالحاسوب أو أي وسائط إلكترونية أخري، وهو ما تبنته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، وساوت بعض التشريعات العربية بين المعلومات الإلكترونية والبيانات من حيث الحماية الجنائية مثل تشريع سلطنة عمان رقم 12 لسنة 2011، وهو ما تبنته وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية،

والمشرع القطري في القانون رقم 14 لسنة 2014 بشأن مكافحة الجرائم الإلكترونية، في حين تبني المشرع البحريني في القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات مصطلح (المعلومات)، وله ذات المضمون الوارد بالتشريعات الأخرى التي تبنت مصطلح (المعلومات الإلكترونية). وفي المقابل تبني المشرع الجزائري مصطلحا مغايرا (معطيات معلوماتية) في القانون رقم 9 لسنة 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها، وتعني "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

ونحن من جانبنا نفضل استخدام لفظ "البيانات" بدلاً من مصطلح "المعلومات الالكترونية" أو " المعلومات "، الذي نعتقد أنه لا يضيف جديداً، خاصة أنه ذات اللفظ الذي تبنته الاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة 2010 في البند رقم (3) من المادة الثانية منها، كما استخدمه قانون الإمارات العربي الاسترشادي، والاتفاقية الأوربية لجرائم الكمبيوتر لعام 2001 في المادة الأولى، والعديد من التشريعات العربية السابق الإشارة إليها، وفي هذا توسيع لنطاق الحماية للبيانات التي يتم معالجتها أو القابلة للمعالجة عبر وسائل تقنية المعلومات، دون تطلب أن تكون (معلومة) أو (معلومة إلكترونية)، وذلك في ضوء أهمية وخطورة البيانات القابلة للمعالجة المعلوماتية.

ولم يختلف تعريف المصطلح "المعلومات الالكترونية" في القانون الاتحادي رقم 2 لسنة 2006 عما ورد في المرسوم بقانون الاتحادي رقم 5 لسنة 2012، فهي "أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها". وهو تعريف يتفق في العديد من جوانبه مع ما ورد من تعريف" للبيانات أو المعلومات " في التشريعات العربية الأخرى.

وبذلك فإن المشرع الجنائي في الدول العربية، في مجال تقنية المعلومات، يضيق من نطاق الحماية الجنائية للبيانات، من خلال تطلبه أن تكون المعلومات – لتكتسب وصف الالكترونية – قابلة للتخزين والمعالجة والتوليد والنقل معاً بوسائل تقنية معلومات، ولم يكتف بواحدة من تلك العمليات: "التخزين، أو النقل، أو المعالجة، أو التوليد"، بل تطلبها معاً، وكان من الأفضل استخدام حرف العطف "أو" ليدل على المغايرة بدلاً من حرف العطف "و" الذي يدل على المماثلة وضرورة اجتماع هذه العمليات لإكساب المعلومة الوصف الالكتروني، وهو ما يتفق مع مبدأ الشرعية في التجريم والعقاب وعدم التوسع في تفسير النصوص الجنائية.

وقد وفر المرسوم بقانون الاتحادي رقم 5 لسنة 2012 الحماية الجنائية لبعض المصالح الجديرة بالحماية، والتي لم تكن موجودة في القانون الاتحادي الملغي رقم 2 لسنة 2006 مثل "المحتوى" ويقصد به "المعلومات والبيانات والخدمات الالكترونية"، و "المنشآت المالية أو التجارية أو الاقتصادية" وهي المنشآت التي تكتسب هذا الوصف بموجب الترخيص الصادر لها من جهة الاختصاص في الدولة"، بل إنه وفر الحماية ضد "مواد إباحية الأحداث" والتعدي علي "العنوان البروتوكولي للشبكة المعلوماتية" و ضد أعمال "الالتقاط" و "الإساءة"، وجميعها مصالح تم حمايتها بموجب نصوص القانون المتعلقة بالتجريم والعقاب، ومن ثم وجب التقيد بالمعاني التي أعطاها لها القانون في المادة[1].

2- **البرنامج المعلوماتي**:

حرصت التشريعات العربية علي توفير الحماية الجنائية للبرامج المعلوماتية، ومن فقد حددت مفهوم للبرنامج المعلوماتي محل الحماية، فقد أطلق عليه المشرع السعودي مصطلح " برامج الحاسب الآلي "، في حين وفر المشر الأردني الحماية ل " البرامج" وهي مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات، وهو معني يقترب من مفهوم " البرنامج المعلوماتي " كما ورد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، وما ورد لذات المصطلح في المرسوم السلطاني العماني، والمشرع القطري أيضا. والمصطلح الذي استخدمه المشرع الأردني " البرامج "، هو ذاته الوارد في وثيقة الرياض، وهو مجموعة الأوامر والتعليمات القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة ما. هذا في حين خلي تشريع كل من: السودان، الجزائر، سوريا، البحرين والكويت من هذا المصطلح، واقتصر البعض منها على تعريف النظام المعلوماتي أو نظام الحاسب الآلي.

وقد أبقى المرسوم بقانون الاتحادي رقم 5 لسنة 2012، على مصطلح " البرنامج المعلوماتي " كما كان عليه الحال في القانون الملغي رقم 2 لسنة 2006، وهو بذات المفهوم الوارد في الاتفاقية العربية ووثيقة الرياض والتشريعات العربية الأخرى التي وفرت حماية جنائية له بوصفه إحدى المصالح الجديرة بالحماية الجنائية، وقد استخدم المرسوم هذا المصطلح في المادة رقم (10) منه، ومع هذا فقد كنا نفضل:

أ- استخدام حرف "أو" للمغايرة والشمول، والاكتفاء بواحدة دون اشتراط اجتماع الكل "البيانات أو التعليمات أو الأوامر".

ب- إضافة عبارة "القابلة للمعالجة" بعد عبارة "قابلة للتنفيذ" لتشمل لفظ "البيانات" أيضا.

ج- إضافة عبارة "عن طريق الشبكة المعلوماتية" و "إحدى" قبل عبارة "وسائل تقنية المعلومات"، حتى يكون أعم وأشمل لأي وسيلة، وكذلك للشبكة المعلوماتية على السواء دون تطلب أن تكون أكثر من وسيلة.

د- استبدال عبارة "للحصول على نتيجة محددة" بعبارة "لإنجاز مهمة"، وحيث إنها أوضح وأكثر تحديداً من الإطلاق الوارد في العبارة المستخدمة.

هـ - إضافة عبارة "أو التي يتم إعدادها" لتكون أشمل، وجرياً على ما استخدمته الاتفاقية الأوربية في هذا الخصوص.

ومن ثم يمكن أن يكون تعريف **البرنامج المعلوماتي على أنه "مجموعة من البيانات أو التعليمات أو الأوامر أو التوجيهات القابلة للمعالجة أو التنفيذ عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات المعدة أو التي يتم إعدادها للحصول على نتيجة محددة".**

3- **"نظام المعلومات الالكتروني"**:

استخدم المشرع الإماراتي في المرسوم الحالي لفظ "نظام" بدلاً من لفظ "نظم" - الذي كان وارداً في القانون الاتحادي الملغي رقم 2 لسنة 2006 - رغم أن القانون الأخير لم يكن يستخدم قط في مواده عبارة أو مصطلح "نظم المعلومات الالكتروني"،

ولكنه استخدم لفظ "النظام" في المادة (22) فقط، وكانت الصياغة اللغوية لمصطلح "نظم المعلومات الالكتروني"، غير دقيقة، فصفة "الالكتروني" لا تعود على "نظم" ولا على "المعلومات" على السواء، ومع هذا فقد كنا نفضل استخدام مصطلح "النظام المعلوماتي" حيث أنه يتفق مع ما ورد في قانون الإمارات العربي الاسترشادي، والاتفاقية الأوربية، والاتفاقية العربية في هذا الشأن، كما تبناه المشرع السعودي من قبل، وتبعه المشرع في سلطنة عمان، والمشرع القطري " نظام معلوماتي"، بمعني مجموعة برامج وأدوات تستخدم في معالجة وإدارة البيانات والمعلومات الإلكترونية، كما استخدم كل من المشرع السوداني والمشرع الأردني من بعده مصطلح " نظام المعلومات " بذات المفهوم، وعبر عنه المشرع الجزائري، ومن بعده المشرع السوري بمصطلح " منظومة معلوماتية "، وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وعلي حد تعبير المشرع السوري " مجموعة متسقة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها "، وهو تعريف شكلي لا يشمل ما يقوم به النظام المعلوماتي من وظائف هي التي تدفع المشرع لحمايته. وقد استخدم المشرع الكويتي مصطلح " نظام الحاسب الآلي "، وهو " مجموعة برامج وأنظمة معلوماتية معدة لتحليل المعلومات والبيانات والأوامر وبرمجتها وإظهارها أو حفظها أو إرسالها أو استلامها، ويمكن أن تعمل بشكل مستقلاً وبالاتصال مع أجهزة أو أنظمة معلوماتية أخرى." كما استخدم مصطلح "النظام الإلكتروني المؤتمت"، بمعني برنامج ونظام الكتروني لحاسب آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل، كلياً أو جزئياً، دون تدخل أو إشراف اي شخص طبيعي في الوقت الذي يتم فيها لتصرف أو الاستجابة له.

وهناك مصطلح " نظام المعالجة الإلكترونية للبيانات"، بمعني نظام الكتروني لإنشاء أو إدخال أو استرجاع أو إرسال أو استلام أو استخراج أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونياً. كما عبر المشرع البحريني عنه ب " نظام تقنية المعلومات".

أما مصطلح " نظام المعلومات الإلكتروني " فقد استخدمه المشرع الإماراتي، وهو ما أخذت به وثيقة الرياض للقانون الموحد لمكافحة جرائم تقنية المعلومات، ومن جانبنا نقترح إضافة كلمة "أجهزة" مع "أدوات"، ليشمل أجهزة الحاسب، واستخدام حرف "أو" للمغايرة بين المعالجة والإدارة، وقد جاء التعريف لهذا المصطلح في المرسوم بقانون الاتحادي رقم 5 لسنة 2012 أكثر تحديدا، ومتفقاً إلى حد كبير مع الملاحظات السابقة.

4- "الشبكة المعلوماتية":

الشبكة المعلوماتية أو " شبكة المعلومات " أو " الشبكة "، وهي: ترابط من الأجهزة الحاسوبيّة والمنظومات المعلوماتيّة يسمح بتبادل المعلومات أو التّشارك فيها بين مرسِل ومستقبِل أو مجموعة من المستقبلين، وفق إجراءات محدَّدة، كانت محل اهتمام من جانب كل التشريعات الجنائية العربية المتعلقة بمكافحة جرائم تقنية المعلومات ما عدا المشرع البحريني، والمشرع الجزائري، كما أن المشرع السوري تناول تفصيلا ما يتم عبر الشبكة بالحماية الجنائية، حيث وفر الحماية لمجموعة من المصالح المتعلقة بالشبكة، مثل التواصل علي الشبكة، ومقدم الخدمات علي الشبكات، ومقدمي خدمات التواصل والاستضافة والنفاذ إلي الشبكة، حيث حدد مفهوم لكل منها، علي النحو التالي:

التّواصل على الشّبكة: استخدام الشّبكة، أو أيّ منظومة معلوماتيّة مشابهة، لوضع معلومات أو خدمات، ليس لها طابع المراسلات الشّخصيّة، في متناول عامّة الجمهور أو فئة منه، بحيث يمكن لأيّ فرد الوصول إليها باتّباع إجراءات محدَّدة.

مقدِّم الخدمات على الشّبكة: أيّ من مقدّمي الخدمات الذين يعملون في إطار التّواصل على الشّبكة؛ ومن أصنافهم: مقدّم خدمات النّفاذ إلى الشّبكة، ومقدّم خدمات التّواصل على الشّبكة، ومقدّم خدمات الاستضافة على الشّبكة.

مقدّم خدمات التّواصل على الشّبكة: مقدّم الخدمات الذي يتيح التّواصل على الشّبكة، وذلك عن طريق موقع إلكتروني أو أكثر، أو أيّ منظومة معلوماتيّة مشابهة.

مقدّم خدمات الاستضافة على الشّبكة: مقدّم الخدمات الذي يوفّر، مباشرة أو عن طريق وسيط، البيئة والموارد المعلوماتيّة اللازمة لتخزين المحتوى، بغية وضع موقع إلكتروني على الشّبكة؛ ويُسمّى اختصاراً المضيف.

مقدّم خدمات النّفاذ إلى الشّبكة: مقدّم الخدمات الذي يتيح للمشتركين لديه النّفاذ إلى الشّبكة والوصول إلى المعلومات والخدمات المتوفّرة عليها.

كما عرف القانون الكويتي الشبكة المعلوماتية بأنها "ارتباط بين أكثر من منظومة اتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها".

وقد جعل المرسوم بقانون الاتحادي رقم 5 لسنة 2012 مصطلح " الشبكة المعلوماتية " أكثر تحديداً. من ذلك التعريف الذي ورد في القانون الاتحادي الملغي؛ حيث جعله "ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات"، بعد أن كان ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات أو تبادلها".

ومع هذا فقد أغفل المرسوم بقانون الاتحادي رقم 5 لسنة 2012 ذكر كلمة "وصلة"، وهو ما استخدمته الاتفاقية الأوربية، كما أن الوصلات يمكن أن تكون مرتبطة داخل الأرض بأسلاك أو كابلات، وبدون أسلاك (لاسلكي – قمر صناعي)، ومن ثم كان يمكن إضافة عبارة "أيا كان وسيلته أو مجاله الجغرافي"، وهي تعود على الوصلة أو الارتباط، حيث يمكن أن تكون الشبكة محددة جغرافيا (محلية)، أو تغطي مساحة واسعة.

كما كان من الأفضل إضافة عبارة "أو بين أكثر من نظام أو برنامج أو شبكة معلوماتية"، لعموم التعريف، ولأن الشبكتين يمكن أن ترتبطا فيما بينهما؛ فالإنترنت شبكة دولية تتكون من عدة شبكات متصلة فيما بينها، وتخضع جميعا لذات الأحكام، كما توجد أنواع أخرى من الشبكات. متصلة أو غير متصلة بالأنترنت -قادرة على تداول المعلومات، ويمكن أن تكون نظم المعلومات متصلة بشبكة بمثابة منافذ أو كوسيلة لتسهيل نقل المعلومات مثل "جهاز راوتر أو أجهزة مماثلة"، والمهم أن يتم الحصول على المعلومات أو تداولها أو تبادلها أو نقلها على الشبكة، وذلك اتساقا مع الاتفاقية الأوربية، وتفسيرها في هذا الشأن.

كما كان من الأفضل لدقة وشمول التعريف إضافة عبارة "البيانات أو المعلومات أو نقلها أو تداولها"، حيث أن البيانات أعم، كما أن الأمر لا يقتصر فقط على التبادل، ولكن يدخل فيه نقل البيانات وتداولها. وهذا الأمر ينطبق على باقي التشريعات العربية محل الدراسة والتي أوردت تعريفات مختصرة " للشبكة المعلوماتية"، بما لا يوفر لها الحماية التي تتناسب مع أهميتها.

ومن ثم نقترح أن يكون التعريف على النحو التالي: الشبكة المعلوماتية هي "وصلة أو ارتباط بين وسيلتين أو أكثر من وسائل تقنية المعلومات، أو بين أكثر من نظام أو برنامج أو شبكة معلوماتية أيا كانت وسيلته أو مجاله الجغرافي للحصول على البيانات أو نقلها أو تداولها أو تبادلها".

5- "الموقع الالكتروني":

حرصت غالبية التشريعات الجنائية العربية محل الدراسة علي حماية المواقع الإلكترونية، وتوسعت في مفهومها لتضم الحسابات الشخصية للأفراد علي مواقع التواصل الاجتماعي لتوفير أكبر قدر من حماية الخصوصية المعلوماتية، فعرفه المشرع السعودي بأنه " مكان إتاحة البيانات علي الشبكة المعلوماتية من خلال عنوان محدد، وهو ذات المفهوم الذي تبناه المشرع السوداني، والمشرع الأردني من بعده، والمشرع العماني، والمشرع القطري، وأخيرا المشرع الكويتي، كما تبنته بذات المفهوم الاتفاقية العربية ووثيقة الرياض للقانون الموحد لمكافحة جرائم تقنية المعلومات، أما المشرع السوري فقد توسع في مفهوم الموقع الإلكتروني بأنه " منظومة معلوماتيّة، لها اسماً وعنوان يعرِّفها، وتتضمّن معلومات أو خدمات يمكن الوصول إليها عن طريق الشّبكة، وبخاصة الإنترنت." كما وفر حماية أيضا لعناصر من الموقع الإلكتروني بشكل أكثر تحديد، حيث حدد مفهوم دقيق لكل من تلك العناصر، على النحو التالي:

اسم موقع إلكتروني: مجموعة من الرموز الأبجديّة والرّقميّة، مخصّصة ومسجَّلة وفق قواعد محدَّدة، وتدلّ على موقع إلكتروني على الشّبكة، وبخاصة الإنترنت، وتسمح بالوصول إليه.

نطاق على الإنترنت: زمرة من أسماء المواقع الإلكترونية على الإنترنت، تخضع لسلطة إداريّة واحدة، وتندرج تحت اسم واحد هو اسم النطاق.

اسم النّطاق العُلوي: أوسع نطاق ينتمي إليه موقع إلكتروني ما على الإنترنت، ويُكوِّن الحقل الأخير من اسم هذا الموقع.

اسم النّطاق العُلوي الوطني: اسم نطاق عُلوي قياسي تندرج تحته جميع المواقع الإلكترونية أو موارد الإنترنت التي تديرها سلطة واحدة ذات صبغة وطنيّة.

اسم النّطاق العُلوي السّوري: اسم النّطاق العُلوي الوطني للجمهورية العربية السّورية؛ وهو ".سورية" و ".sy"، أو أيّ نطاق إضافيّ يُعتمد لاحقاً.

وفي المقابل فلم يول المشرع البحريني اهتماما ملحوظا بالموقع الإلكتروني بوصفه مصلحة جديرة بالحماية، ومن قبله المشرع الجزائري الذي اقتصر على حماية " الاتصالات الإلكترونية ".

وقد جعل المرسوم بقانون الاتحادي رقم 5 لسنة 2012 هذا المصطلح أكثر تحديداً بأن أضاف إليه كلمة "الالكتروني" عما ورد في القانون الاتحادي رقم 2 لسنة 2006. كما قيد المعلومات المتاحة عليه بأن تكون معلومات الكترونية، وذكر أمثلة للمواقع مثل: مواقع التواصل الاجتماعي مثل فيس بوك، توتير،..... الخ، والصفحات الشخصية، والمدونات، وهذا لإضفاء مزيد من الحماية لكل من يستخدم شبكة المعلومات الدولية، سواء بشكل فردي أو بشكل جماعي.

6- **"الالتقاط المعلوماتي"**:

عرفته الاتفاقية العربية بأنه " مشاهدة البيانات أو المعلومات أو الحصول عليها " وتطلب المشرع السعودي أن يكون ذلك دون مسوغ نظامي صحيح، وهو ما لم يشترطه المشرع السوداني في الالتقاط، وتبعه في ذلك المشرع العماني، ووثيقة الرياض، والمشرع القطري. في حين حدده المشرع الكويتي بأنه " **الالتقاط المعلوماتي" وهو مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها، ويشمل ذلك المنقولة الكترونياً.**

وعلى الجانب الآخر لم تتضمن تشريعات الجزائر والأردن وسوريا والبحرين تعريفا للالتقاط، على الرغم من اهتمام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ووثيقة الرياض بهذه المصلحة التي يجب توفير الحماية الجنائية منها لكونها تمثل اعتداءا على الخصوصية، خاصة وأن هذه التشريعات صدرت في أوقات متقاربة مع الاتفاقية العربية أو بعدها.

وقد تبنى المرسوم الاتحادي الإماراتي رقم 5 لسنة 2012، التعريف الوارد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد كان القانون الملغي يستخدم هذا المصطلح دون أن يضع له تعريفاً محدداً، فحسناً فعل المشرع بوضع تعريف محدد له، وهذا على الرغم من ورود هذا اللفظ "الالتقاط" في قانون الإمارات العربي الاسترشادي.

وكنا نفضل أن يضاف إلى المشاهدة أيضا الاستماع إلى البيانات أو المعلومات، بالإضافة للحصول عليها، ليكون التعريف أكثر دقة وشمولاً، ويتفق أكثر مع التشريعات العربية التي أوردته.

7- **المحتوي المعلوماتي:**

لم تهتم غالبية التشريعات الجنائية محل الدراسة، بتوفير حماية جنائية للمحتوي المعلوماتي، فلم يورده المشرع السعودي ضمن المصالح الأولي بالحماية، وتبعه في ذلك كل من المشرع الجزائري، والأردني، والسوري، والقطري والكويتي، وهو ما تبناه المشرع الإماراتي في القانون الملغي رقم 2 لسنة 2006. وهذه التشريعات تتبني الوثائق العربية ذات الصلة في هذا الشأن ومن أهمها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، ووثيقة الرياض للقانون الموحد لمكافحة جرائم تقنية المعلومات في دول مجلس التعاون لدول الخليج العربية لعام 2013.

وفي المقابل أورده قانون جرائم المعلومات السوداني لعام 2007، وأطلق عليه " المحتوي " دون وصفه بالمعلوماتي، ويقصد به محتوي المادة الإلكترونية سواء كان ذلك المحتوي نص أو صورة أو صوت أو فيديو أو ما في حكمها. وهو ذات منهج المشرع العماني والذي ربط بين مفهوم المحتوي والقانون الذي يجرمه، فعرفه بأنه " موضوع البيانات أو المعلومات الإلكترونية محل التجريم بموجب أحكام هذا القانون،

أيا كان شكل ذلك المحتوي نصا مكتوبا أو صوتا أو صورة أو صوتا وصورة ". كما عرف المشرع السوري **المحتوى** بأنه " المعلومات أو الخدمات التي يمكن الوصول إليها وتداولها في إطار التّواصل على الشّبكة". كما عرف المشرع البحريني " بيانات المحتوي " بأنها بيانات وسيلة تقنية المعلومات، خلافاً لبيانات خط السير، يتم إرسالها كجزء من اتصال. وعرفه المشرع الإماراتي في المرسوم بقانون الاتحادي رقم 5 لسنة 2012، بأنه " المعلومات والبيانات والخدمات الإلكترونية ".

خامسا: منهج الدراسة

الدراسة تعتمد على منهجين أساسين أولهما: هو المنهج الوصفي التحليلي، ويستخدم في وصف وتحليل خطة المشرع الجنائي في التجريم والعقاب بشأن جرائم الاعتداء على الشبكة المعلوماتية، بالإضافة إلى وصف وتحليل الأحكام المشتركة لهذه الجرائم واستخلاص جوانب القوة والضعف في السياسة الجنائية إزائها.

والمنهج الثاني هو المنهج المقارن، وسوف تكون المقارنة على أكثر من مستوى ومجال حيث ستتم مقارنة خطة المشرع الإماراتي في التجريم والعقاب على مستوى وطني، ما بين القانون الاتحادي الملغي رقم 2 لسنة 2006، والمرسوم بقانون الاتحادي الحالي رقم 5 لسنة 2012، لبيان الجوانب المستحدثة في التجريم والعقاب، وسياسات الإعفاء والتخفيف والتشديد، كما ستتم المقارنة مع التشريعات الوطنية في عدد من الدول العربية الأخرى، خاصة نظام مكافحة الجرائم المعلوماتية السعودي لعام 2007، والتشريع السوداني بشأن مكافحة جرائم تقنية المعلومات لعام 2007، وقانون جرائم أنظمة المعلومات لسنة 2010 في المملكة الأردنية الهاشمية، والمرسوم السلطاني بإصدار قانون مكافحة جرائم تقنية المعلومات في سلطنة عمان رقم 12 لعام 2011، وقانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية بدولة قطر، وقانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات بمملكة البحرين، والقانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات بدولة الكويت، كنماذج للتشريعات العربية، فضلا عن المقارنة مع ما ورد في الاتفاقية الأوربية الخاصة بجرائم الكمبيوتر لعام 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 والتي صدقت عليها دولة الإمارات العربية المتحدة عام 2011، والتي كانت نتاجا لقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لعام 2003، والمقارنة كذلك مع ما ورد بوثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية 2013.

كما ستعرض الدراسة للأحكام القضائية الصادرة عن محاكم دولة الإمارات العربية المتحدة من المحكمة الاتحادية العليا، ومحكمة نقض أبو ظبي، ومحكمة تمييز دبي بشأن جرائم تقنية المعلومات، سواء في ظل القانون الاتحادي الملغي رقم 2 لسنة 2006 أو المرسوم بقانون الاتحادي الحالي رقم 5 لسنة 2012، وكذلك بعض الأحكام القضائية بشأن جرائم المعلوماتية في المملكة العربية السعودية للعام القضائي 2013 /2014، والتي استطاع الباحث جمعها من خلال موقع وزارة العدل السعودية الإلكتروني.

سادسا: نطاق وتقسيم الدراسة:

لا شك لأن الاعتداء علي الشبكة المعلوماتية يبدأ منذ الدخول أو محاولة الدخول إليها بطريق غير مشروع ويشمل البقاء فيها دون إذن أو مبرر مشروع، وهو ما حرصت جميع التشريعات الجنائية العربية علي رصد العقوبات له، بيد أن نطاق هذه الدراسة يتحدد ببيان وتحليل موقف التشريعات الجنائية العربية إزاء الأفعال التي تتجاوز مرحلة محاولة الدخول أو الدخول أو البقاء في الشبكة المعلوماتية، إلي مرحلة تعطيل وإعاقة الشبكة المعلوماتية عن العمل، أو التحايل عليها أو التقاط الاتصالات من خلالها، بما يؤثر علي عمل منظومة الذكاء الاصطناعي أيضا، وذلك في إطار مقارن مع عدد من التشريعات الجنائية العربية.

وعلى ذلك سوف تقسم الدراسة على المحاور التالية:

المحور الأول: جرائم تعطيل الشبكة المعلوماتية وإعاقة الوصول إليها.

المحور الثاني: جرائم الاحتيال والتحايل على الشبكة المعلوماتية.

المحور الثالث: جريمة الحصول على شفرة الدخول لتقنية المعلومات.

المحور الرابع: جريمة إنتاج برامج معلوماتية والتقاط الاتصالات عبر الشبكة المعلوماتية.

المحور الأول

جرائم تعطيل الشبكة المعلوماتية وإعاقة الوصول إليها

عاقب المشرع الإماراتي في المرسوم بقانون الاتحادي رقم 5 لسنة 2012 على نوعين من الأفعال التي يترتب على كليهما التأثير في الشبكة المعلوماتية أو النظام المعلوماتي هما: إعاقة الوصول إلى الشبكة المعلوماتية، وتعطيل الشبكة أو إيقافها عن العمل. وقد وردت هذه الجرائم في المادة 5 من القانون الاتحادي الملغي رقم 2 لسنة 2006[2]. وهذه المادة كانت تشبه المادة (3) من الاتفاقية الأوربية لمكافحة جرائم الكمبيوتر لعام 2001، والمادة السابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، والمادة (7) من قانون الإمارات العربي الاسترشادي، حيث تطلبت الاتفاقية العربية تجريم الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي وسيلة فنية وقطع بث أو استقبال بيانات تقنية المعلومات، وكان المشرع الإماراتي العربي أكثر توسعاً حيث عاقب كل من أعاق أو شوش أو عطل عمدا الوصول إلى الخدمة أو الدخول للأجهزة.

وقد تطلبت الاتفاقية الأوربية في فعل التعطيل أو الإعاقة أن يكون عمديا وبدون وجه حق، ليخرج التعطيل أو الإعاقة المصرح بهما قانونا، أو بناء على أمر أو إذن من المشتركين في البث لأغراض الرقابة، أو لمصلحة الأمن الوطني، أو لدواعي كشف الجرائم، وكذلك بالنسبة للأعمال التجارية. كما أن المادة (7) من قانون الإمارات العربي الاسترشادي أضافت فعل "التشويش" إلى التعطيل والإعاقة ليدخل في مجال التجريم. والمادة السابعة من الاتفاقية العربية أضافت إلى النتائج المترتبة على أفعال التعطيل والإعاقة "قطع بث أو استقبال بيانات تقنية المعلومات"،

وهو ما أشارت إليه الاتفاقية الأوربية "بالبث المغناطيسي الكهربائي الصادر من نظام معلوماتي"، وهذا من شأنه أن يغطي المطالبات بتجريم الانتفاع بخدمات الاتصال أو قنوات البث المسموعة أو المرئية.

ورغم أن قانون الإمارات العربي الاسترشادي جرم كل من انتفع بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو ما في حكمها بخدمات الاتصال، وذلك على استقلال، ومع هذا فقد كان إيرادها ضمن تلك المادة يأتي في مكانه الصحيح لاتصالها بموضوع الإعاقة أو التشويش في أغلب الحالات.

وقد كانت وثيقة الرياض للقانون الموحد، أكثر تفصيلا حيث فرقت في مادتين متتاليتين (9، 10) بين الإعاقة والتعطيل العمدي للوصول إلى الخدمة أو للدخول إلى الأجهزة والبرامج ومصادر البيانات من جانب، وبين ايقاف تقنية المعلومات عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو اتلاف أو تغيير البرامج والبيانات والمعلومات من خلال إعداد أو إدخال ما من شأنه ذلك عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات من جانب آخر، فإذا لم يتحقق الايقاف أو التعطيل أو التأثير الوارد على البيانات والبرامج تكون الجريمة جنحة عقوبتها الحبس، أما إذا تحقق شيء من ذلك أصبحت جناية عقوبتها السجن.

وتجريم الوثيقة لإعاقة الوصول للخدمة أو الدخول لوسيلة تقنية معلومات هو من باب التجريم التحوطي لحماية وضمان انتفاع الأضرار والمؤسسات بالخدمات المعلوماتية، وقد اشترطت المادة (9) أن يتم ذلك بأية وسيلة ولكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، كما أن المادة (10) تشترط أن يتم إدخال ما من شأنه ايقاف أو تعطيل الشبكة المعلوماتية عن العمل عن طريق الشبكة ذاتها أو إحدى وسائل تقنية المعلومات وأن يكون ذلك عمدا.

وعلى صعيد التشريعات الجنائية العربية بشأن مكافحة جرائم المعلومات، فقد جرم البندان (2، 3) من المادة الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي لعام 2007 إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو نسخ البرامج أو البيانات الموجودة، أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها، وكذلك إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت، وعاقبت على هذه الأفعال بالسجن مدة لا تزيد على أربع سنوات وغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين.

وبالمثل فقد أفرد المشرع السوداني المادتين (8، 9) لتجريم أفعال إيقاف أو تعطيل أو إتلاف البرامج أو البيانات أو المعلومات (م 8)، وكذلك إعاقة أو تشويش أو تعطيل الوصول إلى الخدمة (م 9)، وفرض للجرائم الواردة في المادة (8) عقوبة السجن ست سنوات أو الغرامة أو كلاهما معا، وللأفعال الواردة في المادة (9) عقوبة السجن مدة لا تجاوز سنتين والغرامة أو إحدى هاتين العقوبتين.

أما المشرع الأردني فقد جمع في المادة (4) من القانون المؤقت لجرائم أنظمة المعلومات عام 2010 العديد من صور التجريم تتلخص في إدخال أو نشر أو استخدام برنامج عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو مسح أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو الغاؤه أو اتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو

انتحال شخصية مالكه دون تصريح، وجعل عقوبة ذلك الحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة والغرامة من 200 إلى 1000 دينار أو إحدى هاتين العقوبتين.

كما عاقب المرسوم السلطاني رقم 12 لسنة 2011 العماني، في المادة (9)، بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من أدخل عمدا وبدون وجه حق في نظام معلوماتي أو شبكة معلوماتية أو وسائل تقنية المعلومات ما من شأنه إيقاف أي منها أو تعطيله عن العمل أو ألغي أو غير أو عدل أو شوه أو أتلف أو دمر البرامج أو البيانات أو المعلومات الالكترونية المستخدمة أو المخزنة في أي منها مع علمه بأن ذلك من شأنه إيقافها أو تعطيلها عن العمل، وذلك باستخدام وسائل تقنية المعلومات، كما عاقب في المادة (10) بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على سنتين وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألفي ريال عماني أو بإحدى هاتين العقوبتين، كل من أعاق أو عطل عمداً ودون وجه حق الوصول إلى خدمات مزود الخدمة أو الدخول إلى نظام معلوماتي أو وسائل تقنية المعلومات، وذلك باستخدام وسائل تقنية المعلومات.

وبالمثل خصص المشرع السوري المادة (17) من المرسوم التشريعي رقم (17) لسنة 2012 لجريمة اعاقة الوصول إلى الخدمة، حيث عاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة ألف إلى خمسمائة ألف ليرة 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 بأي وسيلة كانت الوصول إلى الخدمات أو البرامج أو المواقع الالكترونية أو مصادر البيانات أو المعلومات عليها، وبذلك فإن المشرع السوري لم يستلزم أن تكون إعاقة الدخول إلى المنظومة المعلوماتية أو إعاقة الوصول إلى الخدمات والبيانات والمعلومات التي توفرها تلك المنظومة – لم يستلزم – أن يكون باستخدام وسيلة تقنية المعلومات أو الشبكة المعلوماتية، ومن ثم يخضع لهذه الجريمة من يقوم بقطع الكابل الخاص بشبكة المعلومات بطريق العمد.

أما المشرع في دولة الكويت في القانون (63) لسنة 2015 فقد خصص البندين (1، 2) من المادة (4) لتجريم وعقاب كل من أعاق أو عطل عمدا الوصول إلى موقع خدمة الكترونية أو الدخول إلى الأجهزة والبرامج أو مصادر البيانات أو المعلومات الالكترونية بأي وسيلة كانت وذلك عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات، وكذلك كل من أدخل عمدا عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شأنه ايقافها عن العمل أو تعطيلها.

ومع هذا لم يتضمن كل من القانون البحريني رقم 60 لسنة 2014، ونظيره القطري رقم 14 لسنة 2014 بشأن مكافحة جرائم تقنية المعلومات – لم يتضمن أي منهما – نصا يجرم هذه الأفعال علي الرغم من ثبوت أهمية تجريمها بصورة واضحة في الوقت الراهن بدليل تمكن جماعة نسبت نفسها لما يعرف بتنظيم الدولة الإسلامية (داعش)، المصنف إرهابيا وفقا لقوانين العديد من الدول والمنظمات الدولية والإقليمية، حيث تمكنت تلك الجماعة من إيقاف الموقع الإلكتروني الخاص بقناة فرنسية (قناة الناس الخامسة التليفزيونية)، فضلا عن تمكنها من وقف بث القناة علي مستوي العالم لمدة زمنية، حتي تمكنت من استعادة الإرسال،

وقد تزامن ذلك مع وقف بث القنوات الفضائية المصرية التي تبث إرسالها من مدينة الإنتاج الإعلامي في مدينة السادس من أكتوبر، لمدة تزيد علي خمس ساعات نتيجة عمل إرهابي أيضا ولكنه تم بوسيلة تقليدية ؛ من خلال تفجير محولات الطاقة الكهربائية التي تغذي المدينة الإعلامية، ورغم وحدة النتيجة في الحالتين – وقف بث القنوات الفضائية ومواقعها الإلكترونية – إلا أن كل حالة تمت بوسيلة مختلفة أحدهما بدائية والأخرى إلكترونية، بما يدلل علي أهمية الانتباه للهجمات الإرهابية المستحدثة والتي يمكن أن تطال مصالح أكثر حيوية وذات أهمية استراتيجية.

وسوف نعرض لهاتين الجريمتين في المرسوم بقانون الاتحادي الإماراتي رقم 5 لسنة 2012 على النحو التالي:

أولاً: جريمة إعاقة أو تعطيل الوصول إلى تقنية المعلومات

جرم المشرع في المادة 8[3]، من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع الكتروني أو نظام معلومات الكتروني، وفرض لذلك عقوبة الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم، أو إحدى هاتين العقوبتين.

ومن ثم فقد جاءت خلوا من أي ضوابط؛ فلم تتطلب أن يكون الفعل عمديا مثل غالبية التشريعات العربية، أو بدون تصريح، كما لم تتطلب وسيلة معينة للتعطيل أو الإعاقة، مثل المشرع الكويتي ومن ثم فيجوز استخدام أي وسيلة، كما أنها تعاقب على مجرد التشويش على الشبكة المعلوماتية أو نظام المعلومات الالكتروني، كما أنها لم تتطلب حدوث نتيجة معينة على فعل الإعاقة أو التعطيل، ومن ثم فإنه يكفي حدوث الإعاقة أو تعطيل الوصول إلى الشبكة أو الموقع الالكتروني.

وجريمة إعاقة أو تعطيل الوصول للشبكة المعلوماتية جريمة عمدية بالأساس، حتى ولو لم يتطلب المشرع أن تقع عمدا أو بدون تصريح، ومن ثم يلزم لقيامها توافر القصد الجنائي لدى الجاني بعنصريه العلم والإرادة، ويجب أن ينصرف علمه إلى فعل التعطيل أو الإعاقة، وإلى أن هذا ينصب على شبكة معلوماتية أو موقع الكتروني أو نظام معلومات الالكتروني.

والجريمة المنصوص عليها في المادة (8) من الجنح، ومن ثم يعاقب على الشروع فيها، بمقتضى نص المادة (40) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، بنصف العقوبة المقررة للجريمة التامة، وتخضع في أحكام العقاب عليها لذات الأحكام التي سبق ذكرها بصدد جرائم الدخول غير المشروع.

ثانياً: جريمة إيقاف أو تعطيل تقنية المعلومات

وردت هذه الجريمة في المادة (10)[4]، من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، وتتضمن تجريم إيقاف الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات.

1- **الركن المادي:** يتمثل الركن المادي في هذه الجريمة في إدخال برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، بشرط أن يؤدي ذلك إلى إيقاف الشبكة أو تعطيلها أو تدميرها أو نسخ أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الالكتروني أو البيانات أو المعلومات.

وهذه الجريمة سبق النص عليها في المادة (6)[5]، من القانون الاتحادي الملغي رقم 2 لسنة 2006، وفي تلك المادة لم يكن المشرع يتطلب أن يتم إيقاف أو تعطيل الشبكة عن طريق استخدام وسيلة معينة، سوى أن يتم ذلك عبر الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، حيث يدخل الجاني عبرها ما من شأنه إيقافها عن العمل أو تعطيلها، وكذلك لم يكن يتطلب حدوث نتيجة معينة وهو إيقاف الشبكة عن العمل أو تعطيلها أو تدمير البرامج أو المواقع.

ومن ثم فقد كان السلوك الإجرامي فيها يتمثل في إدخال أي شيء من شأنه إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها، وقد كان حكماً خاصاً بالشبكات فقط دون غيرها.

وقد ورد النص على تجريم هذه الأفعال في المادة (4) من الاتفاقية الأوربية، والمادة الثانية من الاتفاقية العربية، والبند 2 من نظام مكافحة الجرائم المعلوماتية السعودي لعام 2007، والمادة (8) من قانون جرائم المعلوماتية السوداني لعام 2007، وضمها المشرع الأردني في قانون جرائم أنظمة المعلومات لعام 2010 ضمن الأفعال العديدة المجرمة في المادة (4). المادة (9) من المرسوم السلطاني رقم 12 لسنة 2011 في سلطنة عمان، وفي المادة (4) من التشريع الكويتي على النحو السابق توضيحه، في حين لم يتضمنها أي من القانون البحريني أو القطري.

وقد تطلبت الاتفاقيتان الأوربية والعربية، بصدد هذه المادة، أن ترتكب الأعمال عمدا وبدون وجه حق، وذلك أن دواعي أمن وحماية نظام المعلومات قد تتطلب إدخال ما من شأنه تدمير بعض البيانات، أو يكون ذلك بناء على إذن المالك أو صاحب حق الاستغلال، أو يتم تعديل البيانات بغرض تسهيل الاتصالات أو تأمينها أو حمايتها، وهذا ما تداركه المشرع الإماراتي في المادة (10)، من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، حيث تطلب أن يكون إدخال البرنامج عمداً وبدون تصريح. كما أن النص في الاتفاقية يسمح للدول الأطراف بأن تشترط للتجريم في هذه المادة حدوث ضرر جسيم، وهو ما لم يكن وارداً في النص الملغي، رغم أنه يعتبر الفعل من الجنايات ويشبه السلوك الإجرامي فيه نظيره في المادة السابقة، فقد جاء المرسوم بقانون الاتحادي رقم 5 لسنة 2012، مشترطا أن يتم إيقاف الشبكة المعلوماتية أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو الموقع أو البيانات أو المعلومات، وجميعها صور للضرر لازمة لقيام الجريمة المعلوماتية، بل إن الاتفاقية الأوربية في نص المادة (4) منها ميزت في فقرتين بين المساس بسلامة البيانات، والمساس بسلامة النظام ذاته، وهو ما يعرف "بتخريب المعلوماتية"، وتطلبت أن يترتب على الأفعال بعض الأضرار، مثل إبطاء سير عمل النظام، أو بعض البرامج التي ترسل حجم كبير من الرسائل دفعة واحدة لجهة محددة لتعطيل النظام بها.

ومن ثم يمكن القول إنه بتعديل هذه المادة أصبح المشرع الجنائي الإماراتي أكثر توافقا مع الاتفاقيات الدولية والإقليمية في شأن مكافحة جرائم تقنية المعلومات خاصة في تجريم أفعال الإعاقة والتعطيل للشبكة المعلوماتية أو نظام المعلومات الالكتروني، من حيث:

أ. اشتراط أن يحدث فعل الإعاقة أو التعطيل عمداً وبدون تصريح.

ب. اشتراط أن تتم أفعال الإعاقة أو التعطيل عن طريق إدخال برنامج معلوماتي وليس عن أي طريق آخر، وفي هذا حماية وضمان لمبدأ الشرعية الجنائية.

ج. اشتراط أن يترتب على الإعاقة أو التعطيل ضرر معين حدد المشرع صور هذا الضرر حصراً، احتراما أيضا لمبدأ الشرعية، فهذه الجريمة من الجرائم ذات النتيجة أو الجرائم المادية التي يتطلب المشرع لقيامها تحقق نتيجة مادية ملموسة هو الإضرار بتقنية المعلومات على النحو الوارد بنص المادة (10) من المرسوم، وهو ما لم تشترطه باقي التشريعات العربية محل الدراسة.

2-الركن المعنوي: تطلب المشرع العمد صراحة في هذه الجريمة، في فعل إدخال البرنامج المعلوماتي، وهذا القصد العام ينطوي على العلم بعناصر وماديات الجريمة وانصراف الإرادة إلى ارتكاب فعل الإدخال؛ ومن ثم يجب أن يعلم الجاني بأنه يقوم بإدخال برنامج معلوماتي، وينصرف علمه أنه يقوم بذلك في شبكة معلوماتية أو نظام معلومات الكتروني.... الخ، كما أن هذه الجريمة تتطلب قصداً خاصاً وهو اتجاه نية الجاني إلى إتلاف أو تعطيل الشبكة المعلوماتية أو نظام المعلومات الالكتروني أو أي وسيلة من وسائل تقنية المعلومات، أو الإضرار بها على النحو الوارد بالقانون، فإذا وقفت إرادة الجاني عند حد التعطيل أو الإعاقة للشبكة فلا تكتمل الجريمة في نموذجها الحالي، ويمكن أن يتحقق بها جريمة التعطيل السابق الإشارة إليها، فلابد أن يكون لديه نية الأضرار.

3-العقوبة: هذه الجريمة جناية عقوبتها - إذا تمت على النحو السابق وحدثت نتيجتها - هي السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم، أو إحدى هاتين العقوبتين، أما إذا لم تحدث النتيجة المطلوبة وهي الإضرار بالشبكة المعلوماتية بإيقافها أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام، أو الموقع الالكتروني، أو البيانات أو المعلومات، فتكون العقوبة هي السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين.

وبالنظر إلى كون هذه الجريمة جناية فقد كان من حسن السياسة التشريعية ألا يتم الجمع في العقوبة المقررة لها بين السجن والغرامة على وجه التخيير بينهما، وإن كان يجوز الجمع، ولكن على وجه الوجوب، وذلك أن الغرامة عقوبة أصلية في الجنح فقط، ومع هذا يمكن تقريرها في الجنايات، حيث أن العقوبات الأصلية في الجنايات التعزيرية هي الإعدام والسجن المؤبد والسجن المؤقت وفقا لنص المادة (28) من قانون العقوبات الاتحادي الإماراتي[6]، أما عقوبة الغرامة فهي أصلية في الجنح والمخالفات فقط، وهي إلزام الحكومة عليه أن يدفع للخزينة المبلغ المحكوم به، وحدها الأدنى في الجنح يزيد عن ألف درهم، وفي المخالفات لا تزيد على ألف درهم، وحدها الأقصى في الجنح ثلاثين ألف درهم والجنايات مائة ألف درهم، ما لم ينص القانون على خلافه وفقا لنص المادة (71) من قانون العقوبات الاتحادي[7].

ويثور التساؤل إذا اختار القاضي الحكم بالغرامة في الجناية السابقة، حال عدم تحقق النتيجة، والتي حددها المشرع بما لا يجاوز خمسمائة ألف درهم ولم يحدد حدها الأدنى ولا يوجد حد أدنى للغرامة في الجنايات، ومن هنا نتساءل عن الحد الأدنى الذي لا يجوز للقاضي النزول عنه عند الحكم في هذه الجناية بالغرامة؟ وعلى أي أساس يستند في الوصول إلى هذا الحد؟ حيث حدد القانون حدها الأدنى في المخالفات والجنح فقط، وحدها الأقصى في الجنح والجنايات فقط، ما لم ينص القانون على خلاف ذلك.

ونعتقد أنه في ظل خروج هذا النص - من ناحية تفريد العقوبة - عن القواعد المستقرة في التجريم والعقاب فإنه يلزم التدخل بتعديله بحذف التمييز بين السجن والغرامة، أو على الأقل تحديد حد أدنى للغرامة في الجناية المذكورة حال عدم تحقق نتيجتها.

ونعتقد أنه لحين إجراء هذا التعديل فإنه لا يجوز أن يقل الحد الأدنى للغرامة عن ثلاثين ألف درهم وهو الحد الأقصى للغرامة في الجنحة، ومن ثم فالأخذ بالقواعد العامة في القانون الجنائي توجب على القاضي أن يحكم بالغرامة التي لا تقل عن ثلاثين ألف درهم ولا تجاوز خمسمائة ألف درهم، حال تخلف تحقق النتيجة المذكورة في المادة (10) من المرسوم.

وهذه الجناية لا تخضع للإعفاء من العقاب أو تخفيف العقوبة المنصوص عليه في المادة (45) من المرسوم، لأنه لم يعتبرها من الجرائم الماسة بأمن الدولة وفقا لنص المادة (44) منه إلا إذا ارتكبت الجريمة المذكورة لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، وفقا للفقرة الثانية من المادة (44) من المرسوم، إضافة إلى اعتبار ذلك ظرفا مشددا في ذات الوقت لهذه الجريمة وفقا لنص الفقرة الثانية من المادة (46) من المرسوم.

وقد أفرد المشرع في الفقرة الأخيرة من المادة (10) من المرسوم عقوبة مخففة هي الحبس والغرامة أو إحدى هاتين العقوبتين، لأي فعل عمدي يقصد به إغراق البريد الالكتروني بالرسائل أو إيقافه عن العمل أو تعطيله أو إتلاف محتويات، وفي ذلك حماية للخصوصية المعلوماتية المتمثلة في البريد الالكتروني للشخص أو الهيئة، وحماية لهذا البريد الذي يحوي رسائل خاصة.

والعقاب هنا على اتجاه إرادة الجاني من خلال فعل متعمد إلى التأثير على البريد الالكتروني، حتى لو لم يحدث هذا التأثير بالفعل.

المحور الثاني

جرائم الاحتيال والتحايل على الشبكة المعلوماتية

حرصت بعض التشريعات العربية علي أن تورد تعريفا محددا لجريمة الاحتيال الإلكتروني، الاحتيال المعلوماتي، حيث عرفت وثيقة الرياض للقانون الموحد الاحتيال المعلوماتي بأنه" التأثير في نظام المعلومات الالكتروني أو وسيلة تقنية المعلومات عن طريق البرمجة أو التدخل أثناء تطبيق البرنامج أو إدخال بيانات غير صحيحة أو غير مكتملة أو بأية طريقة أخرى."، وتبعه المشرع الكويتي في تعريف جريمة الاحتيال الإلكتروني بأنها " 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."، ولكن لم يتم استخدام مصطلح " التحايل "، كما حرصت العديد من تشريعات الدول العربية علي تجريم افعال الاحتيال والتحايل الإلكتروني أو المعلوماتي.

وقد وردت جريمة الاحتيال المعلوماتي في المادة (10) من قانون الإمارات العربي الاسترشادي،

كما حرصت الاتفاقية الأوربية على النص عليها في المادة (8) تحت مسمى "جريمة النصب المتعلقة بالكمبيوتر" واشترطت ارتكاب أفعال عمدية وبغير حق وأن ينتج عنها إلحاق خسارة بملكية شخص آخر، عن طريق إدخال أو تبديل أو محو أو تدمير لبيانات الكمبيوتر، أو أي تدخل في وظيفة منظومة الكمبيوتر بقصد احتيالي أو غير أمين للحصول على منفعة اقتصادية لصالح الشخص ذاته أو لصالح الغير. وأوردتها الاتفاقية العربية في المادة الحادية عشرة تحت مسمى "جريمة الاحتيال" وهي التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير، عن طريق إدخال أو تعديل أو محو أو حجب المعلومات أو البيانات أو التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها، أو تعطيل الأجهزة أو البرامج والمواقع الالكترونية، ولا شك أن هذه الصيغة تعبر عن حقيقة الاحتيال المعلوماتي. كما أن وثيقة الرياض للقانون الموحد أوردت المادتين 14 و15 لمعالجة أعمال الاحتيال التي تتم عبر وسائل تقنية المعلومات، فعاقبت في المادة 14 "كل من استولى أو تحصل لنفسه أو لغيره على مال منقول أو منفعة أو على سند أو توقيع هذا السند عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بطريقة احتيالية أو باتخاذ أسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك منشأته خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن (.....) وبالغرامة التي لا تقل عن (.....) أو بإحدى هاتين العقوبتين. وجرمت استخدام الاحتيال المعلوماتي بالمعني الوارد في الوثيقة في الاستيلاء على أموال وسندات مملوكة للغير، سواء استولي عليها الشخص لنفسه أو لغيره".

أما على صعيد التشريعات الجنائية العربية الخاصة بمكافحة جرائم تقنية المعلومات، فقد نص على هذه الجريمة البند (1) من المادة الرابعة من نظام مكافحة الجرائم المعلوماتية السعودي لعام 2007، حيث عاقب كل من استولى لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة". كما جرم المشرع السوداني الاحتيال وانتحال الشخصية أو صفة غير صحيحة في المادة 11 من قانون جرائم المعلوماتية لعام 2007، حيث عاقب كل من يتوصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة، بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند، وذلك بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا.

كما عاقب المشرع العماني على هذه الجريمة، بمقتضى المادة (13) من المرسوم السلطاني رقم 12 لسنة 2011، كل من أدخل أو عدل أو غير أو أتلف أو شوه أو ألغى بيانات أو معلومات الكترونية في نظام معلوماتي الكتروني أو حجبها عنه أو تدخل في وظائفه أو أنظمة تشغيله أو عطل وسائل تقنية المعلومات أو البرامج أو المواقع الالكترونية عمدا ودون وجه حق بقصد التحايل والتسبب في إلحاق الضرر بالمستفيدين أو المستخدمين لتحقيق مصلحة أو الحصول على منفعة لنفسه أو لغيره بطريقة غير مشروعة، وشدد المشرع العقاب إلى السجن المؤقت إذا كان النظام المعلوماتي خاص بجهة حكومية أو مصرف أو مؤسسة مالية. ومن ثم يكون هذا النص أكثر توافقا مع نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. كما خصص المشرع السوري المادة 21 من المرسوم التشريعي لجريمة " الاحتيال عن طريق الشبكة "، وفرض عقوبة الحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سوريّة، كلّ من استولى، باستخدام الأجهزة الحاسوبيّة أو الشّبكة، على مال منقول أو عقار، أو معلومات أو برامج ذات قيمة ماليّة،

أو سند يتضمّن تعهّداً أو إبراء أو أيّ امتياز ماليّ آخر، وذلك عن طريق خداع المجني عليها وخداع منظومة معلوماتيّة خاضعة لسيطرة المجني عليه، بأيّ وسيلة كانت، وتكون العقوبة الاعتقال المؤقّت، والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سوريّة، إذا وقعت الجريمة على ثلاثة أشخاص فأكثر، أو إذا تجاوز مبلغ الضّرر مليون ليرة سوريّة، أو إذا وقع الاحتيال على مصرف أو مؤسّسة ماليّة. ولا تطبّق الأسباب المخفّفة التّقديريّة إلاّ إذا أسقط المضرور حقّه الشّخصي.

وتضمن القانون القطري رقم 14 لسنة 2014 جريمة الاحتيال الإلكتروني في المادة (11)، ضمن الفصل الثالث منه مع جريمة التزوير، علي نحو ما أوضحنا سابقا، والتي نصت علي أن " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

1- استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي.

2- تمكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، من الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو التوقيع عليه، بطريق الاحتيال، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة ".

كما تضمن القانون البحريني رقم 60 لسنة 2014 النص على هذه الجريمة في المادة(8)، ضمن الفرع الثاني، المعنون ب (الجرائم ذات الصلة بوسائل تقنية المعلومات)، حيث عاقب بالحبس من توصل – دون مسوغ قانوني – إلي الاستيلاء علي مال مملوك للغير أو حصل علي أي مزية لنفسه أو لغيره أو إلي توقيع سند أو إلغاؤه أو إتلافه أو تعديله، باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية، وذلك من خلال أي فعل مما يلي:

1- إدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تعديل أو تغيير أو تحريف أو حجب بيانات وسيلة تقنية المعلومات. وهذه الألفاظ جميعا يقصد بها – وفق ما أورده المشرع نفسه في المادة (1) – لفظ "الإتلاف"، ومن ثم كان يكفي أن يذكره بديلا عنها جميعا، حيث لا يوجد ما يبرر تكرارها كما هي مرة أخرى.

2- القيام بأي تدخل في عمل نظام تقنية المعلومات....."

فالفعل الإجرامي في هذه الجريمة ÷و اتخاذ اسم كاذب أو صفة غير صحيحة، أو الاستعانة بالطرق الاحتيالية علي النحو الوارد في قانون العقوبات ووفق ما استقر عليه الرأي بشأنها فقها وقضاء. ويشترط لقيام النموذج القانوني لهذه الجريمة أن يتم السلوك الإجرامي فيها بوسيلة من الوسيلتين اللتين حددهما المشرع، وهما "الإتلاف" بإتلاف بيانات وسيلة تقنية المعلومات، أو " التدخل في عمل نظام تقنية المعلومات ". ومن ثم يتم الوصول لنتيجة محددة مادية وملموسة هي الاستيلاء على مال مملوك للغير، أو الحصول على أي مزية لنفسه أو لغيره، أو الوصول إلى توقيع سند أو إلغاؤه أو إتلافه أو تعديله. ويكفي إحدى تلك النتائج لقيام الجريمة.

أما المشرع الكويتي والذي أورد تعريفا "الجريمة الاحتيال الإلكتروني " فلم يورد نموذجا تجريميا لها ضمن مواده، واقتصر علي البند(5) من المادة (3)، من القانون رقم 63 لسنة 2015، والذي يعاقب كل من توصل عن طريق الشبكة 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 وانتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، والعقوبة هي الحبس مدة لا تجاوز ثلاث سنوات وغرامة من ثلاثة آلاف إلي عشرة آلاف دينار، أو إحدى هاتين العقوبتين.

وخلافا للتشريعات السابقة، لم يتضمن قانون جرائم أنظمة المعلومات الأردني لعام 2010 نصا يعاقب على جريمة الاحتيال المعلوماتي، وإنما تضمنت المادة (4) ضمن ما تضمنته من أفعال مجرمة، تجريم " إدخال أو نشر أو استخدام برنامج عن طريق الشبكة المعلوماتية..... بهدف تغيير موقع إلكتروني..... أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح "، وهذا التجريم لا يتعلق بالاحتيال المعلوماتي وفقا للمستقر عليه في التشريعات الجنائية العربية، وإنما يتعلق بانتحال الصفة، وهو أمر مختلف تماما عن الاحتيال.

وفي ضوء ما سبق وبدراسة موقف المشرع الإماراتي نجد أنه ميز في المرسوم بقانون الاتحادي رقم 5 لسنة 2012 بين نوعين من الجرائم هما جريمة الاحتيال وجريمة التحايل، حيث وردت الثانية في المادة (9) منه، ووردت الأولى في المادة (11)، وجريمة التحايل جديدة لم يكن القانون الاتحادي الملغي رقم 2 لسنة 2006 ينص عليها؛ وتتضمن التحايل على العنوان البروتوكولي للإنترنت باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها.

والاحتيال مصطلح قانوني محدد مستقر في قانون العقوبات وهو مرادف لجريمة النصب؛ فالغش، أو الاحتيال، أو النصب هي تعبيرات تستخدم بمعان مترادفة بالرغم من أنها تتمايز في الحقيقة من الوجهة اللغوية أو الدلالات الاصطلاحية، فالقانون المصري على سبيل المثال يستخدم تعبير النصب [8].

وسوف نتناول جريمتي الاحتيال والتحايل المعلوماتي، على النحو التالي:

الفرع الأول: جريمة الاحتيال الالكتروني.

الفرع الثاني: جريمة التحايل الالكتروني.

الفرع الأول

جريمة الاحتيال الالكتروني

الاحتيال في اللغة هو طلب الحيلة، وفي الاصطلاح هو الغش والخداع الذي يعمد إليه شخص للحصول من الغير بدون حق على فائدة أو ميزة [9].

وعادة لا يتجه المشرع إلى وضع تعريف واضح ومحدد لجريمة الاحتيال، وإنما يكتفي بالنص على وسائل هذه الجريمة والأشياء التي ترد عليها، وهذا ما اتجه إليه كل من المشرع الأردني ونظيره المصري، إلا أنه يمكن تعريف الاحتيال بوجه عام بأنه أي سلوك يقوم به الجاني من أجل خداع المجني عليه وإيهامه بما يخالف الواقع من أجل الاستيلاء على أمواله [10]،

وكذلك يمكن تعريف الاحتيال بأنه جريمة تؤدي إلى الإضرار بملكية الغير بالحصول من هذا الأخير الذي يملكها على النقل الإرادي لماله عن طريق خداعة [11].

بينما عرفت محكمة النقض المصرية النصب بأنه "احتيال وقع من المتهم على المجني عليه بقصد خداعة والاستيلاء على ماله فيقع المجني عليه ضحية الاحتيال الذي يتوافر باستعمال طرق احتيالية أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة أو التصرف في مال الغير ممن لا يملك التصرف فيه"[12].

والطرق الاحتيالية من العناصر الأساسية الداخلة في تكوين الركن الماي وفي ذلك قضت المحكمة الاتحادية العليا بأنه ""لما كان من المقرر أن جريمة النصب كما هي معرفة به في المادة 399 من قانون العقوبات الاتحادي يتطلب لتوافرها أن يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعة والاستيلاء على ماله فيقع المجني عليه ضحية هذا الاحتيال الذي يتوافر بالاستعانة بطرق احتيالية، أو باتخاذ اسم كاذب أو صفة غير صحيحة، كما أن الاستعانة بشخص آخر أو بأخرين على تأييد أقواله، وادعاءاته المكذوبة للاستيلاء على مال الغير يرفع كذبه إلى مصاف الطرق الاحتيالية الواجب تحققها في جريمة النصب. والطرق الاحتيالية بالمعنى المتقدم من العناصر الأساسية الداخلة في تكوين الركن المادي في الجريمة "[13].

أما مفهوم الاحتيال المعلوماتي، فلم يوجد تعريف واضح ومعتمد له، لذلك فقد تعددت التعريفات، ومنها:

"حث الحاسب الآلي على تغيير بعض الحقوق بأي وسيلة كانت، بهدف الحصول على ربح غير مشروع على حساب شخص آخر، فوظيفة الحاسب الآلي تكمن في مساعدة الجاني على إتمام فعل الاحتيال"[14].

ويرى البعض "إن الاحتيال المعلوماتي يتحقق كلما كانت هناك نية تحقيق ربح مادي غير مشروع للجاني ينتج عنه خسارة مادية تلحق بالمجني عليه وكان استخدام الحاسوب وسيلة لارتكاب الاحتيال أو تسهيله أو تعجيل تنفيذه"[15].

أما التعريف الذي أقرته هيئة الأمم المتحدة للاحتيال المعلوماتي في التوصية رقم (R9/89) المتبناة من المجلس الأوربي فهو "أنه الإدخال أو المحو أو التعديل أو كبت البيانات أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص آخر بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر". إلا أن هذا التعريف انتقد بأنه واسع النطاق، كما أن تعداده لأساليب هذه الجريمة قد يجعله قاصراً عن الإحاطة بما قد يظهر من صور جديدة لهذه الجريمة مستقبلاً [16].

ومن ذلك أيضا التعريف الذي ارتكزت عليه لجنة أوديت البريطانية وهو "كل سلوك احتيالي وخداعي يهدف الشخص بواسطته كسب فائدة أو مصلحة مادية"[17].

ومما سبق يتضح بجلاء أن الاحتيال يختلف تماما عن التحايل؛ من حيث أن الاحتيال له وسائل وطرق محددة ينص عليها القانون لا يتصور أن يقع بدونها، وهي تدخل في الركن المادي للجريمة، سواء كانت تقليدية أو معلوماتية، في حين أن التحايل هو مصطلح عام لا توجد له وسائل محددة.

وهذا ما عبر عنه المشرع في المادة (4) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012 "باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى"، ومن ثم تصبح الوسيلتان الواردتان بالمادة واردتان على سبيل المثال وليس الحصر، في حين حدد المشرع الوسائل في المادة (11) من المرسوم التي من خلالها يتم الاحتيال وهي، استخدام طرق احتيالية؛ وقد أسهم الفقه والقضاء في تحديد هذا المصطلح بشكل كبير حتى أضحى محدداً وواضحاً، بالإضافة إلى وسائل أخرى مثل: اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة، بشرط أن يتم ذلك عن طريق الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات.

وإذا كان تجريم التحايل مستحدث في المرسوم بقانون الاتحادي رقم 5 لسنة 2012، فإن تجريم الاحتيال في المادة (11) من المرسوم سبق أن تبناه المشرع في المادة (10) من القانون الملغي رقم 2 لسنة 2006[18].

أولا: الركن المادي:

يتكون الركن المادي في جريمة الاحتيال من استخدام طرق احتيالية ينتج عنها الحصول على المال، وفي ذلك قضت المحكمة الاتحادية العليا "جريمة الاحتيال كما هي معرفة في المادة 399 من قانون العقوبات الاتحادي تتطلب لتوافرها ان يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعة والاستيلاء على ماله فيقع المجني عليه ضحية الاحتيال الذي يتوافر باستعمال طرق احتيالية أو باتخاذ اسم كاذب أو صفة غير صحيحة متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم"[19].

فإذا لم يتوافر عنصر الاحتيال، فلا جريمة، كما لو كان المجني عليه عالما بحقيقة التصرف، وفي ذلك قضت المحكمة الاتحادية العليا بأنه "من المقرر أن جريمة الاحتيال لا تقوم الا على الغش والاحتيال الموجه إلى المجني عليه لخدعه وسلب ماله فإذا لم يكن هناك احتيال بل كان تسليم المال ممن سلمه عن بينه بحقيقة الامر فلا جريمة"

ويجب أن يكون من شأن الطرق الاحتيالية الايهام بواقعة غير حقيقية وأن يستبين الحكم مدى العلاقة بين الطرق الاحتيالية والايهام الذي حدث للمجني عليه"[20].

ويجب أن يتم التحديد على وجه الدقة الطرق الاحتيالية من خلال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وهو ما يتفق مع مبدأ الشرعية، وما هو مأخوذ به في نصوص جرائم الاحتيال من ضرورة تحديد الطرق الاحتيالية بدقة؛ كما أنه يشترط العمد وعدم مشروعية التوصل، لتخرج الأفعال التي تعد من قبيل الخطأ أو الأفعال التي تتم استخداما لحق مقرر قانونا. كما أنه يضيف الإلغاء أو الإتلاف للأفعال، لأنها تصيب السندات وكذلك المعلومات طالما تمت بطريقة احتيالية، وقد وردت في نص المادة (399 ع.أ)[21].

ثانيا: الركن المعنوي: جريمة الاحتيال من الجرائم العمدية التي تتطلب توافر القصد الجنائي العام، الذي يتكون من العلم والإرادة، حيث يجب أن ينصرف علم الجاني إلى ماديات الجريمة وتتجه إرادته إلى ارتكابها،

ولكن في الاحتيال يجب أن ينصرف علم الجاني إلى الوسيلة الاحتيالية المنصوص عليها، عكس التحايل، كما أن الاحتيال يتطلب قصداً خاصاً هو نية الحصول على مال منقول أو منفعة أو على سند أو توقيع هذا السند، في حين أن التحايل لا يتطلب هذا القصد الخاص.

الفرع الثاني

جريمة التحايل الالكتروني

هذه الجريمة الكترونية بحتة؛ حيث أن التحايل فيها يتم على العنوان البروتوكولي للإنترنت وليس على إنسان، فالهدف ليس خداع أي شخص ولكن خداع شبكة الانترنت ذاتها. وهي جريمة مستحدثة لم يكن ينص عليها القانون الاتحادي الملغي رقم 2 لسنة 2006، ولم ترد في قانون الإمارات العربي الاسترشادي أيضا، ولكنها وردت – بصيغة أخرى – في المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تحت مسمى "جريمة إساءة استخدام وسائل تقنية المعلومات"، حيث عاقبت في البند (2) على "حيازة أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المتعلقة بالدخول غير المشروع، وكذلك إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير هذه البرامج، وهذه بلا شك لا تتعامل مع حقيقة التحايل المعلوماتي". كما أن المشرع السوري في المرسوم رقم (17) لسنة 2012 أورد في المادة 19 منه جريمة " تصميم البرمجيات الخبيثة واستخدامها"، حيث عاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سوريّة، كلّ من يقوم بتصميم البرمجيّات الخبيثة وترويجها لأغراض إجراميّة. كما عاقب بالحبس من ستّة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سوريّة، كلّ من استخدم البرمجيّات الخبيثة، أيّاً كان نوعها، وبأيّ وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبيّة أو المنظومات المعلوماتيّة أو الشّبكة. وهذه الأفعال لا تطوي بالضرورة على تحايل معلوماتي، وإن كان يمكن أن يدخل فيها في بعض الحالات.

وقد ربط كل من المشرع البحريني ونظيره القطري – وجريا على نهج الاتفاقية العربية – بين تجريم تلك الأفعال وجرائم الدخول غير المشروع لوسيلة تقنية المعلومات. فقد أورد المشرع القطري في المادة الثالثة المتضمنة في الفصل الأول من القانون رقم 14 لسنة 2014، والمعنون " جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية "، تلك الأفعال وتحققها كظرف مشدد لجريمة الدخول غير المشروع، حيث نصت تلك المادة علي أن " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك.

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، **أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة**

المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكه أو القائم على إدارته".

وعاقب المشرع البحريني في القانون رقم 60 لسنة 2014، في المادة (6)، الواردة في الفرع الأول منه، والمعنون " الجرائم الواقعة على أنظمة وبيانات وسيلة تقنية المعلومات "، عاقب على إنتاج أو استيراد أو شراء أو بيع، أو عرض للبيع أو الاستخدام، أو توزيع أو تداول أو حيازة أو نشر، أو إتاحة:

أ-أداة – بما في ذلك أي برنامج – تم تصميمها أو تحويرها بصفة أساسية لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد (2،3،4،5) من القانون، والمشرع يعرف " البرنامج " بأنه مجموعة تعليمات معبرا عنها بكلمات أو رموز أو بصورة أخرى، إذا تضمنتها أي من الوسائط التي يمكن قراءتها آليا، تكون قادرة علي جعل وسيلة تقنية المعلومات تؤدي عملا معينا أو تحدث نتيجة محددة.

ب-كلمة مرور أو شفرة دخول أو أي رمز دخول أو أية بيانات وسيلة تقنية معلومات أخرى مماثلة، يمكن بواسطتها الدخول إلي نظام تقنية المعلومات أو أي جزء منه. وتطلب المشرع أن يكون ارتكاب أي من الأفعال السابقة بقصد ارتكاب أي من الجرائم المنصوص عليها في المواد من (2) حتى (5)، وتلك الجرائم تتعلق بالخول غير المشروع لوسيلة تقنية المعلومات أو إتلاف بياناتها، أو التقاط أو اعتراض أو التنصت على تلك البيانات، أو استخدامها في التهديد والابتزاز.

هذا في حين لم تتضمن التشريعات ذات الصلة في كل من السعودية، والسودان، والأردن، والكويت، نصوصا مشابهة لذلك النص الوارد في المرسوم بقانون اتحادي رقم 5 لسنة 2012.

وإذا كانت المادة (9)[22] ، من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، قد أوردت هذه الجريمة ولم تحدد وسائل التحايل على العنوان البروتوكولي للإنترنت فإنه يدخل فيها ما سبق، حيث أن استخدام البرامج والأدوات هي من الوسائل الشائع استخدامها في هذا التحايل، كما أن المادة ذكرت وسيلتين على سبيل المثال هما: استخدام عنوان وهمي، أو استخدام عنوان عائد للغير، والهدف من ذلك هو ارتكاب جريمة أيا كان نوعها، أو مدى جسامتها، وسواء واردة في المرسوم بقانون الاتحادي رقم 5 لسنة 2012، أو قانون العقوبات الاتحادي، أو في قانون عقابي آخر، وقد يكون القصد هو الحيلولة دون اكتشاف تلك الجريمة بعد ارتكابها، سواء ارتكبت من قبل ذات الشخص أو من شخص آخر.

والركن المعنوي المتطلب هنا أيضا هو القصد الجنائي المتمثل في العلم والإرادة، فالتحايل لا يكون إلا عمدياً، ولم تُحَدَدَ له وسائل معينة عكس الاحتيال، فيكفي أن ينصرف علم الجاني إلى التحايل بغض النظر عن وسيلته، ولكن يجب أن تنصرف نيته إلى ارتكاب جريمة ما حتى لو لم تتحقق بالفعل أو إلى الحيلولة دون اكتشافها من خلال هذا التحايل.

والعقوبة المقررة هي الحبس والغرامة أو إحدى هاتين العقوبتين، حيث أن المشرع قد حدد حداً أدنى للحبس في جريمة الاحتيال، بحيث لا يقل عن سنة، في حين أطلق عقوبة الحبس في التحايل بين حديها الأدنى شهر والأعلى ثلاث سنوات،

كما وضع المشرع الحدين الأدنى والأقصى لمبلغ الغرامة في جريمة الاحتيال لتتراوح ما بين مائتين وخمسين ألف درهم ومليون درهم، في حين أنها في جريمة التحايل تتراوح بين مائة ألف درهم وثلاثمائة ألف درهم فقط، ولكن عقوبة الغرامة في الجريمتين تخييرية مع الحبس.

المحور الثالث

جريمة الحصول على شفرة الدخول لتقنية المعلومات

هذه الجريمة ليست كجريمة الدخول غير المشروع السابق تناولها، حيث لا يجرم المشرع فيها فعل الدخول غير المشروع في ذاته، وإنما يجرم المشرع مقدمات هذا الفعل والتي تكون بطريقة معينة، هي الحصول على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى بدون تصريح، للدخول إلى وسيلة تقنية معلومات، أو موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلوماتية، أو معلومات الكترونية.

وقد ورد النص عليها في البند (1) من المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي تطلبت العقاب على إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير كلمة سر نظام معلومات أو شفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما، بقصد استخدامه لأية من جرائم الدخول غير المشروع في النظام المعلوماتي. فجاءت هذه المادة لتكمل حلقات الحماية الجنائية للدخول غير المشروع من خلال حماية أكواد وشفرات الدخول على الأنظمة والبرامج، ومن ثم فقد كان من الأوفق من ناحية الترتيب أن تأتي ضمن جرائم الدخول غير المشروع.

كما حرصت وثيقة الرياض للقانون الموحد على النص عليها في المادة (12)، والتي عاقبت كل من تحصل بطريقة غير مشروعة على رقم أو شفرة أو كلمة السر(المرور) أو أية وسائل أخرى للدخول إلى البرامج أو نظام المعلومات الالكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات (بالحبس).....(وبالغرامة).....(أو بإحدى هاتين العقوبتين).

ويعاقب بذات العقوبة كل من أعد أو أنتج أو باع أو اشترى أو استورد أو عرض أو أتاح أو روج بأية طريقة برامج أو أدوات أو أجهزة مصممة أو مكيفة لأغراض ارتكاب جرائم تقنية المعلومات أو كلمات سر أو رموز تستخدم لفك التشفير أو لدخول موقع أو نظام المعلومات الالكتروني بصورة غير مشروعة.

ولم يرد تجريم لمثل هذه الأفعال في الاتفاقية الأوربية المتعلقة بالكمبيوتر لعام 2001، وكذلك لم ترد نصوص خاصة بها في قانون جرائم أنظمة المعلومات الأردني لعام 2010، ومن قبله النظام السعودي لمكافحة الجرائم المعلوماتية لعام 2007 والقانون السوداني لمكافحة جرائم المعلوماتية لذات العام. بل إن القانون القطري رقم 14 لسنة 2014، والقانون الكويتي رقم (63) لسنة 2015، لم يتضمناها رغم حداثة إصدارهما.

في حين أن المشرع في سلطنة عمان نقل النص الوارد في الاتفاقية العربية، وخصص له الفصل الثالث من المرسوم السلطاني رقم 12 لسنة 2011، والذي يتضمن مادة وحيدة برقم (11) تحت ذات العنوان "إساءة استخدام وسائل تقنية المعلومات"،

حيث عاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على خمسة عشر ألف ريال عماني أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو بيع أو شراء أو استيراد أو توزيع أو عرض أو إتاحة برامج أو أدوات أو أجهزة مصممة أو مكيفة لأغراض ارتكاب جرائم تقنية المعلومات، أو كلمات سر أو رموز (شفرات) تستخدم لدخول نظام معلوماتي آخر أو حاز أدوات أو برامج مما ذكر، وذلك بقصد استخدامها في ارتكاب جرائم تقنية معلومات". وقد حذا المشرع البحريني في القانون 60 لسنة 2014 حذو المشرع في سلطنة عمان؛ وربط – كما أوضحنا سابقا – بين تلك الأفعال وجرائم الدخول غير المشروع، بل ربطها بالجرائم الأخرى، على نحو ما أشرنا سابقا.

وقد سبق أن أوضحنا أن المشرع السوري في المرسوم رقم (17) لسنة 2012 أورد في المادة 19 منه جريمة " تصميم البرمجيات الخبيثة واستخدامها"، حيث عاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سوريّة، كلّ من يقوم بتصميم البرمجيّات الخبيثة وترويجها لأغراض إجراميّة. كما عاقب بالحبس من ستّة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سوريّة، كلّ من استخدم البرمجيّات الخبيثة، أيّاً كان نوعها، وبأيّ وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبيّة أو المنظومات المعلوماتيّة أو الشّبكة.

وقد أورد المشرع الإماراتي هذه الجريمة في المادة (14) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، ولم يسبق النص عليها في القانون الاتحادي الملغي رقم 2 لسنة 2006. واستجاب المشرع بهذه المادة للعديد من المطالبات بتوفير حماية أكبر للمرافق الحيوية في الدولة وبياناتها، للمحافظة على دوام واستمرار عمل هذه المرافق بكفاءة.

وإذا كان التفسير الموسع لكلمة "الإفشاء" يفيد بأنها تدخل من بين الأفعال التي يتوصل بها للدخول للنظام المعلوماتي، والتي كانت واردة في الفقرة الأولى من المادة (2) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012، فإن هذا النص تبدو فائدته في توفير حماية لكلمات المرور ذاتها وتجريم السعي للحصول عليها بكافة الطرق.

ولم يكن قانون الإمارات العربي الاسترشادي يتضمن نصا خاصا بهذه الجريمة كذلك، ومن ثم فهي جريمة مستحدثة في التشريع الإماراتي تضمنتها المادة (14) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012 والتي تنص على أن "يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل، بدون تصريح، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلوماتية أو معلومات الكترونية.

ويعاقب بذات العقوبة كل من أعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات، أو روج بأي طريقة روابط لمواقع الكترونية أو برنامج معلوماتي، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون".

وقد كان من الأفضل اعتبار استخدام كلمة المرور أو الشفرة في إحداث ضرر بعد ذلك هو ظرف مشدد للعقوبة الأصلية، وفي هذه الحالة يمكن أن تكون الغرامة نسبية بالنسبة إلى حجم الضرر لأنه هو مناط التجريم في هذه الحالة.

وعقوبة هذه الجريمة هي الحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو إحدى هاتين العقوبتين، وهي جريمة عمدية يتطلب القانون لقيامها توفر القصد الجنائي العام المتمثل في العلم والإرادة.

ولكن هذه المادة لا تعاقب على تسهيل الحصول على الرقم السري أو الشفرة، ومن ثم فهو يدخل في نطاق المساهمة الجنائية بطريق المساعدة السابقة إذا أدى إلى الحصول فعلا على كلمة المرور أو الشفرة، في حين أن تجريمه على استقلال كان سيعتبره جريمة قائمة بذاتها وهذا كان أوفق من حيث تأمين حماية كاملة لكلمات المرور والشفرات والأرقام السرية.

ولم يشترط المشرع لتمام الجريمة الدخول إلى وسيلة تقنية المعلومات ومن ثم إذا تم الحصول على كلمة المرور أو الشفرة وتم الدخول مثلا فإنه يكون دخول غير مشروع يخضع للعقاب الوارد كذلك في المادة (2) من المرسوم، ونكون بصدد تعدد مادي للجرائم المرتبطة وتطبق عليه جريمة قواعد الارتباط المادي.

المحور الرابع

جرائم إنتاج برامج معلوماتية والتقاط الاتصالات عبر الشبكة المعلوماتية

سوف نعرض لهذه الجرائم في فرعين، على النحو التالي:

الفرع الأول: جريمة انتاج برامج معلوماتية لغرض إجرامي.

الفرع الثاني: جريمة اعتراض أو التقاط الاتصالات عبر الشبكة المعلوماتية.

الفرع الأول

جريمة انتاج برامج معلوماتية لغرض إجرامي

تضمنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جريمة " إساءة استخدام وسائل تقنية المعلومات"، في المادة التاسعة منها، حيث جرمت انتاج أو بيع أو شراء أو توزيع أو توفير أية أدوات أو برامج مصممة أو كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلوماتيا بقصد استخدامها لارتكاب أو تكون مكيفة لغايات ارتكاب الجرائم المبينة بالمواد من السادسة إلى الثامنة بها، وكذلك جرمت حيازة أية أدوات أو برامج مذكورة لذات الغرض. أما وثيقة الرياض للقانون الموحد فلم تتضمن تجريما لشيء مما ذكر. كما لم يتمنها كل من التشريع السعودي والتشريع السوداني، ولم يتضمن القانون القطري رقم 14 لسنة 2014 نصا مماثلا، رغم حداثة صدوره وأهمية الأفعال محل التجريم. كما لم يتضمن قانون الإمارات العربي الاسترشادي نصا بهذا الشأن، لأنه كان في فترة سابقة على الاتفاقية العربية، وعلى ذات النهج سار المشرع الكويتي في القانون رقم 63 لسنة 2015.

وقد تضمن المرسوم بقانون الاتحادي بدولة الإمارات رقم 5 لسنة 2012 في الفقرة الثانية من المادة (14) هذه الجريمة والتي كانت هناك مطالبات بتضمينها في القانون، وكنا نود أن يفرد لها المشرع نصا مستقلا،

حيث عاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات أو دمج بأي طريقة لمواقع الكترونية أو برنامج معلوماتي أو أي وسيلة تقنية معلومات، مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون، وهو ما نص عليه المشرع العماني وورد في الاتفاقية العربية في المادة التاسعة منها.

ولا شك أن إنتاج أو توزيع أو توفير أو تبادل هذه البرامج أو بعضها أو استيرادها أو تصديرها أو الاتجار بها بأي شكل ينبغي تجريمه للحد من ارتكاب الجرائم المعلوماتية.

وقد تضمن القانون البريطاني، بشأن إساءة استخدام الحاسب الآلي والصادر في يونيو 1990، نصا يجرم كل من صنع أو هيأ أو أمد أو قدم أو وفر برامج أو بيانات أو أدوات بقصد المساعدة في ارتكاب جريمة مما سبق، وكل من حاز أو حصل على شيء مما سبق بذات القصد، كما أن الاتفاقية الأوربية تضمنت نصا مشابها في المادة (9) منها.

كما تضمن القانون البحريني رقم 60 لسنة 2014 نصا مشابها في البند (أ) من المادة (6) يجرم فعل من قام بإنتاج أو استيراد أو شراء أو بيع أو عرض للبيع أو الاستخدام، أو توزيع أو تداول أو حيازة أو نشر أو إتاحة، أداة – بما في ذلك أي برنامج – تم تصميمها أو تحويرها بصفة أساسية لغرض أو بقصد ارتكاب جرائم محددة؛ وهي جرائم الخول غير المشروع، واتلاف البيانات، والتنصت والالتقاط، وإرسال بيانات تتضمن تهديدا، والمنصوص عليها في المواد 2،3،4،5 من القانون.

وقد ينظر إلى السلوك الإجرامي في هذه الجريمة على أنه اشتراك في جريمة الدخول أو الإعاقة، ومع ذلك فهو فعل قائم بذاته معاقب عليه، حتى ولو لم تقع جريمة الدخول أو التشويش أو التنصت، ومن ثم يتصور أن يكون هناك اشتراك في هذا الفعل ذاته، أما لو اعتبرناه مجرد اشتراك فإن القاعدة أنه "لا اشتراك في الاشتراك".

وللإحاطة بتجريم الأفعال المتعلقة بهذا الموضوع، نقترح أن يكون النص على النحو التالي:

"كل من أنتج أو صنع أو هيأ أو باع أو اشترى أو استورد أو وزع أو أمد أو قدم أو وفر أي برنامج أو أنظمة أو معلومات أو بيانات أو شفرة دخول أصلية أو مشابهة أو غير ذلك بقصد استخدامها في ارتكاب أو المساعدة في ارتكاب جريمة من الجرائم السابقة أو يسهل ذلك للغير، يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن الحد الأقصى المقرر لغرامة الجريمة التي كان يقصد ارتكابها أو المساعدة فيها".

الفرع الثاني

جريمة اعتراض أو التقاط الاتصالات عبر الشبكة المعلوماتية

هذه الجريمة لم ترد في الاتفاقية الأوربية المتعلقة بالكمبيوتر لعام 2001، ولكن أوردتها المادة 8 من قانون الإمارات العربي الاسترشادي لعام 2003، حيث عاقبت على التنصت والالتقاط والاعتراض لما هو مرسل عن طريق الشبكة المعلوماتية.

كما يمكن القول إن هذه الجريمة متضمنة في المادة الرابعة عشرة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، والتي تطلبت تجريم أفعال الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات ولا شك أن الأفعال السابقة تمثل اعتداء على حرمة الحياة الخاصة، كما أنها متضمنة صراحة في المادة السابعة التي تطلبت تجريم الاعتراض غير المشروع والمتعمد لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات. كما حرصت وثيقة الرياض للقانون الموحد على النص عليها في المادة (11)، والتي تفرض العقاب على كل من تنصت أو التقط أو اعترض عمدا، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، حيث قررت عقابه (بالحبس....) (وبالغرامة)....(أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن( ) إذا أفشى ما تم التنصت عليه أو التقاطه أو اعتراضه.

وعلى صعيد التشريعات الجنائية العربية، فقد تضمن البند (1) من المادة الثالثة من نظام مكافحة الجرائم المعلوماتية السعودي لعام 2007 تجريم التنصت والالتقاط والاعتراض لما هو مرسل عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي (قانوني) صحيح. كما خصص المشرع السوداني المادة (6) منه لجريمة" التنصت أو التقاط أو اعتراض الرسائل "، حيث عاقبت بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معا، كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها، دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة.

كما أوردها المشرع الأردني في المادة (5) من قانون جرائم أنظمة المعلومات لعام 2010 فعاقب على التنصت والالتقاط والاعتراض، دون أن يحدد - أي من التشريعين السعودي أو الأردني - المقصود بكل من تلك الألفاظ الثلاثة.

وعاقب المرسوم السلطاني رقم 12 لسنة 2011 في المادة الثامنة منه كل من اعترض عمدا وبدون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الالكتروني المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو تنصت عليها، ومن ثم فقد عاقب على أفعال الاعتراض، وقطع البث أو الاستقبال، والتنصت، ولم يعاقب على "الالتقاط"، على الرغم من أنه أورد تعريفا له في المادة (1) من المرسوم بأنه "مشاهدة البيانات أو المعلومات الالكترونية أو الحصول عليها"، وهو معنى لا يتوافر في الأفعال المجرمة وهي الاعتراض والقطع والتنصت. وهو بذلك يساير النص الوارد في المادة السابعة من الاتفاقية العربية السابق الإشارة إليها. كما خصص المشرع السوري البند(أ) من المادة (18) المتضمنة جريمة " اعتراض المعلومات "، حيث عاقبت بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سوريّة، كلّ من اعترض أو التقط قصداً، بوجه غير مشروع، المعلومات المتداولة على منظومة معلوماتيّة أو الشّبكة، أو تنصّت عليها.

كما عاقب المشرع القطري في القانون رقم 14 لسنة 2014 عي هذه الأفعال بمقتضي المادة (4)، والتي تنص علي أن " يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور ".

كما عاقب المشرع البحريني في القانون رقم 60 لسنة 2014 على هذه الأفعال بالمادة (4)، حيث فرض عقوبة الحبس والغرامة التي لا تجاوز مائة ألف دينار أو إحدى هاتين العقوبتين، على كل من تنصت أو التقط أو اعترض دون مسوغ قانوني مستخدما وسائل فنية، إرسالا غير موجه للعموم لبيانات وسيلة تقنية معلومات، سواء كانت البيانات مرسلة من نظام تقنية المعلومات أو إليه أو ضمنه، ويشمل هذا الإرسال أي انبعاثات لمواجهات كهرومغناطيسية من نظام تقنية المعلومات تحمل معها هذه البيانات.

والمشرع البحريني يشترط بذلك أن تتم الأفعال المجرمة أو أحدها باستخدام وسائل فنية، فإذا لم تستخدم هذه الوسائل فلا قيام للجريمة، في حين أن التشريعات الأخرى لم تشترط أو تتطلب استخدام وسيلة محددة في التنصت أو الاعتراض أو الالتقاط.

كما أفرد المشرع الكويتي في القانون رقم 63 لسنة 2015 البند 3- من المادة (4) لهذه الجريمة، حيث عاقب بالحبس مدة لا تجاوز سنتين وغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين كل من تنصت أو التقط أو اعترض عمداً، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات. 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.

وبذلك يتضح حرص التشريعات الجنائية العربية على تجريم الأفعال التي تمس الخصوصية عبر الشبكة المعلوماتية، لضمان حرية انتقال وتداول البيانات التي لا يرغب أصحابها في اطلاع الغير عليها.

وقد كان يمكن في ظل القانون الاتحادي الإماراتي الملغي رقم 2 لسنة 2006 أن يطلق على هذه الجريمة "جريمة التنصت المعلوماتي"، حيث كان المشرع يعاقب في المادة الثامنة منه كل من تنصت أو التقط أو اعترض عمداً بدون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

ولكن بعد إلغاء هذا القانون، فقد جرم المشرع في المادة (15) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012 فعلي الاعتراض والالتقاط العمديين فقط، ولم يجرم فعل التنصت، وهو بلا شك يختلف عن المصطلحين الواردين بالمادة، حيث أن التنصت يعني الاستماع بعناية وتركيز، وبشكل غير مشروع (خلسة أو بطريق الحيلة). وتنص المادة (15) على أن " يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمدا وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية.

فإذا أفشى أي شخص المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق فإنه يعاقب بالحبس مدة لا تقل عن سنة واحدة".

وهذه المادة تشبه المادة (380) [23]، من قانون العقوبات الاتحادي، التي وردت في الفصل السادس من الباب السابع من الكتاب الثاني تحت عنوان "الجرائم الواقعة على السمعة، القذف والسب وإفضاء الأسرار"، وهي تشكل إحدى جرائم الاعتداء على حرمة الحياة الخاصة، الجرائم الواقعة على الأشخاص". وتعاقب هذه المادة كل من استرق السمع في مكالمة هاتفية. ومن ثم تتميز هذه المادة عن المادة (380) في الركن المادي لكل منهما؛ فهو في المادة (15) الالتقاط أو الاعتراض،

وفي المادة (380) هو فض برقية بغير رضا من أرسلت إليه، أو استراق السمع في مكالمة هاتفية، وهو ما لا ينطبق على استراق السمع عبر الشبكة المعلوماتية.

ولم يكن المشرع في القانون الملغي يعاقب على إفشاء المعلومات التي حصل عليها الشخص عن طريق التقاط أو اعتراض الاتصالات، فتدارك ذلك في المرسوم بقانون الاتحادي رقم 5 لسنة 2012، وعاقب على ذلك بالحبس مدة لا تقل عن سنة واحدة.

ويمكن القول إنه تمت الاستفادة من نص المادة (2/380) بخصوص المادة الماثلة، بتجريم إفشاء ونشر مضمون ما تم اعتراضه أو التقاطه عبر الشبكة المعلوماتية، بإضافة فقرة ثانية للمادة (15)، وقد كان يمكن تشديد العقاب في حالة إفشاء المعلومات التي تعد من الأسرار سواء المتعلقة بشخص طبيعي أو معنوي، مثل إفشاء سر إصابة لاعب كرة محترف مما يؤدي إلى خسارة فادحة له ولناديه.

أما المشرع الإماراتي فقد عاقب فقط على "الالتقاط" و "الاعتراض"، ولم يعاقب على التنصت أو القطع، كما أنه حدد مفهوم الالتقاط في المادة (1) أيضا على النحو السابق الإشارة إليه.

وقد كان المشرع الإماراتي متفردا بجعل إفشاء المعلومات التي تم الحصول عليها ظرفاً مشدداً لتلك الجريمة، حيث جعل الحد الأدنى لعقوبة الحبس سنة، ولم يجعل الحبس تخييريا مع الغرامة فجعله عقوبة وحديدة لإفشاء المعلومات التي تم الحصول عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق.

إلا أن المشرع البحريني تبع نظيره الإماراتي في هذا الشأن؛ اعتبر إفشاء الإرسال أو جزء منه الناتج عن التنصت أو الالتقاط أو الاعتراض ظرفا مشددا يخضع لقواعد التشديد المنصوص عليها في قانون العقوبات البحريني، الأمر الذي لم يتضمنه أي من التشريعات السابقة.

ونحن من جانبنا لا نرى مبرراً لحذف التنصت من مجال التجريم في التعديل الجديد للتشريع الإماراتي، حيث ينبغي توفير المزيد من الحماية للاتصالات التي تتم عبر الشبكة المعلوماتية وحماية الخصوصية المعلوماتية بشكل كبير، أسوة بموقف المشرع الجنائي في حماية الخصوصية المادية للإنسان على مستوى شخصه وسكنه ومتعلقاته الخاصة.

وجريمة التقاط أو اعتراض الاتصالات جريمة عمدية، ويجب أن يكون ذلك بدون تصريح مسبق فلا يكفي الإذن اللاحق للإعفاء من العقوبة.

وفي ذلك تقول محكمة تمييز دبي بأنه "إذ كانت المادة 8 من القانون رقم 2006/2 في شأن مكافحة جرائم تقنية المعلومات الملغي والتي تشبه المادة (15) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012 تنص على أنه ((كل من تصنت أو التقط أو اعترض عمدًا بدون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالحبس وبالغرامة أو إحدى هاتين العقوبتين)) ولما كان الثابت من أقوال الشهود واعتراف الطاعن كما يبين من الأوراق ومن مدونات الحكم الابتدائي المؤيد بالحكم المطعون فيه أن الطاعن قد التقط دون وجه حق عمدًا ما هو مرسل لشركة..... المجني

عليها وحاول استثمار ذلك لمصلحته الخاصة بأن رد على بعض العملاء طالبًا منهم مخاطبة الشركة التي يعمل بها إضرارًا بالشركة المجني عليها فمن ثم تكون كافة أركان الجريمة المسندة إلى الطاعن قد توافرت مما يتعين مساءلته عنها جنائيًا ومدنيًا ويكون كافة ما ينعاه في طعنه لا يعدو أن يكون جدلاً موضوعيًا في تقدير محكمة الموضوع واستنباط معتقدها مما لا يجوز إثارته أمام محكمة التمييز"[24].

كما أن الإفشاء في هذه الجريمة هو ظرف مشدد، حيث تكون العقوبة هي الحبس فقط لمدة لا تقل عن سنة واحدة، ويكون الإفشاء بأي وسيلة ولأي عدد من الأشخاص حتى لو كان شخصاً واحداً، فلا يشترط أن يكون بطريق الإعلام أو الإعلان أو الدعاية أو النشر، ولا يشترط في المعلومات التي تم إفشائها أن تكون سرا بطبيعتها أو بمقتضى القانون وهذا توسع محمود في الحماية للمعلومات التي يتم تداولها عبر شبكة المعلومات، ومن ثم كان يمكن اعتبار سرية المعلومات ظرفاً مشدداً في هذه الحالة.

ويخضع العقاب على هذه الجريمة لذات الأحكام السابق الإشارة إليها، من حيث الإعفاء أو التخفيف أو التشديد، وكذلك يكون هناك عقاب على الشروع في التقاط أو اعتراض الاتصالات عبر الشبكة المعلوماتية بنصف العقوبة المقررة.

كما إنه في إطار تجريم الأفعال السابقة كنا نأمل أن يتضمن المرسوم بقانون الاتحادي رقم 5 لسنة 2012، نصا يجرم أيضا إنتاج وحيازة الفيروسات وكلمات المرور بهدف استخدامها في ارتكاب جرائم أو تسهيل ارتكابها خاصة جرائم تقنية المعلومات الواردة في المرسوم المشار إليه، حيث ظهرت مطالبات عديدة بشأن تجريم حيازة برامج أو فيروسات من شأنها أن تستخدم في ارتكاب أي من الجرائم الواردة في قانون مكافحة جرائم تقنية المعلومات، على أن يكون التجريم للحيازة المجردة مع توافر العلم بأنها صالحة لارتكاب الجريمة؛ أسوة بما ورد في الاتفاقية العربية والمرسوم السلطاني العماني حيث يكفي توافر قصد استخدامها في ارتكاب الجريمة، حتى لو لم تقع، بل يكفي العلم أنها تستخدم في ذلك، طالما كانت حيازتها دون وجه حق.

والجريمة المقترحة تدخل ضمن جرائم التشويش والتعطيل والالتقاط، لأن كلمات المرور والشفرات هي الأدوات لذلك. ومن ثم نقترح أن يكون هناك نص مادة مضاف برقم (14 مكرر) إلى المرسوم بقانون الاتحادي رقم 5 لسنة 2012 ينص على أن "كل من حاز أو أحرز كلمة مرور أو شفرة أو برنامج أو فيروسات أو غيرها بقصد استخدامها أو مع العلم أنها تستخدم في ارتكاب جريمة مما سبق أو سهل ذلك للغير يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين.

الخاتمة والتوصيات

إن الدراسة التحليلية المقارنة للتشريعات الجنائية العربية في مجال مكافحة جرائم الاعتداء علي الشبكة المعلوماتية والتي هي الأساس في عمل الذكاء الاصطناعي، تظهر جوانب من الاتفاق وأخري من الاختلاف بين تلك التشريعات؛ فقد حرصت جميع التشريعات الجنائية العربية علي بيان المصالح الجنائية الجديرة بالحماية في صدر كل منها ؛ من خلال بيان المعاني المحددة للمصطلحات الواردة بكل منها، وكان أهمها: المعلومات الإلكترونية، والبرامج المعلوماتي، ونظم المعلومات الإلكترونية، والشبكة المعلوماتية، والمحتوي المعلوماتي ..إلخ، علي نحو ما أوضحنا في الدراسة.

كما أن التشريعات أولت عناية خاصة بتجريم الأفعال التي تؤدي إلى وقف أو تعطيل تقنية المعلومات، وأفعال التنصت والالتقاط لما يتم خلالها، وهو ما تناولته الدراسة بالشرح والتحليل في إطار مقارن بين التشريعات والوثائق الدولية والإقليمية ذات الصلة.

وفي ضوء التحليل والمقارنة فقد خلصت الدراسة إلى عدة توصيات، على النحو التالي:

1- فيما يتعلق بجريمة الاحتيال المعلوماتي، نقترح – منعا لحدوث اختلاف في أسس وقواعد التجريم بين التشريعات الجنائية العربية - الأخذ بالنص الوارد في المادة الحادية عشرة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث أنه أكثر تعبيرا عن حقيقة الاحتيال المعلوماتي من بعض النصوص الواردة بالتشريعات العربية، أو الأخذ بالنص المعدل والمقترح لهذه المادة، وهو " كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في إدخال أو تعديل أو محو أو حجب البيانات أو المعلومات، أو تدخل في وظيفة أنظمة التشغيل أو الاتصالات أو حاول تعطيلها أو تغييرها أو قام بتعطيل الأجهزة أو البرامج أو المواقع أو الأنظمة المعلوماتية أو تلاعب فيها دون وجه حق وبنية الاحتيال وكان من شأن ذلك خداع المجني عليه والاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند أو تعديله أو إتلافه أو إلغاؤه أو تحقيق مصالح أو منافع غير مشروعة لنفسه أو للغير، يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ..... ولا ..... أو بإحدى هاتين العقوبتين".

وبصيغة أخرى "كل من توصل عمدا وبدون وجه حق إلى الاستيلاء على أموال منقولة أو عروض أو سندات أو مخالصات أو معلومات أو برامج أو أي متاع منقول لنفسه أو للغير، وبنية الاحتيال عن طريق إدخال أو تعديل أو محو أو حجب أو إتلاف أو مسح للمعلومات أو البيانات المخزنة على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أو عن طريق التدخل في وظيفة أنظمة التشغيل أو الاتصالات أو تعطيلها أو تغييرها أو تعطيل الأجهزة أو البرامج أو المواقع أو الأنظمة المعلوماتية أو التلاعب فيها بأي شكل، يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن. ..... ولا تجاوز. ..... أو بإحدى هاتين العقوبتين.

وتكون العقوبة السجن الذي لا يزيد على خمس سنوات إذا كان النظام المعلوماتي أو البرامج أو المواقع أو وسيلة تقنية المعلومات خاصة بجهة حكومية اتحادية أو محلية أو مؤسسة مالية أو اقتصادية أو تجارية".

2- أن تجرم التشريعات الجنائية العربية مقدمات الدخول غير المشروع لتقنية المعلومات، والتي تكون بطريقة معينة، هي الحصول على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى بدون تصريح، للدخول إلى وسيلة تقنية معلومات، أو موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلوماتية، أو معلومات الكترونية ؛ حيث لم تتضمن التشريعات في كل من: السعودية، السودان، الأردن، قطر، الكويت، نصا تجريميا بهذا الشأن، ومن ثم يمكن الاستهداء بالتجريم الوارد بالمادة 14 من المرسوم بقانون الاتحادي الإماراتي رقم 5 لسنة 2012، مع الأخذ في الاعتبار جعل أفعال الفقرة الثانية منها ظرفاً مشدداً للعقوبة الواردة في فقرتها الأولى، وتجريم تسهيل الحصول على الشفرة أو الرمز للدخول، أو تعديلها وفقاً للنص التالي:

"كل من حصل أو استولى أو توصل بأي طريقة على كلمة المرور أو الشفرة الخاصة ببرنامج أو نظام أو موقع معلوماتي أو أية وسيلة من وسائل تقنية المعلومات عمدا وبدون وجه حق أو سهل ذلك للغير بقصد استخدامها لارتكاب أي من الأفعال

الواردة في المادة (2) من هذا المرسوم بقانون أو أية جريمة أخرى يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو إحدى هاتين العقوبتين. فإذا ترتب على ما سبق الإضرار بالنظام أو البرنامج أو وسيلة تقنية المعلومات أو البيانات أو المعلومات المخزنة على أي منها أو بمستخدميها أو المستفيدين منها أو مالكيها أو أصحاب الحق في استغلالها أو ترتبت أية خسارة مادية لأي شخص طبيعي أو معنوي تكون العقوبة هي الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن ضعف قيمة ما ترتب من ضرر أو إحدى هاتين العقوبتين".

3- وضع نص مستقل في التشريعات الجنائية العربية محل الدراسة – أسوة بالمشرع السوري - لتجريم إنتاج أو تصميم برامج معلوماتية لغرض إجرامي، والتي وردت في الفقرة الثانية من المادة (14) من المرسوم بقانون اتحادي لدولة الإمارات رقم 5 لسنة 2012. ويمكن اقتراح نص ليكون على النحو التالي:

"كل من أنتج أو صنع أو هيأ أو باع أو اشترى أو استورد أو وزع أو أمد أو قدم أو وفر أي برنامج أو أنظمة أو معلومات أو بيانات أو شفرة دخول أصلية أو مشابهة أو غير ذلك بقصد استخدامها في ارتكاب أو المساعدة في ارتكاب جريمة من الجرائم السابقة أو يسهل ذلك للغير، يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن الحد الأقصى المقرر لغرامة الجريمة التي كان يقصد ارتكابها أو المساعدة فيها".

4- إحكام التجريم الخاص بالأفعال التي تمثل اعتراض أو التقاط للاتصالات عبر الشبكة المعلوماتية، وتفعيل حماية الخصوصية المعلوماتية، من خلال تشديد العقاب على إفشاء ما هو مرسل إذا كان سراً بذاته أو بموجب القوانين أو اللوائح أو الأوامر، سواء كان الشخص طبيعي أو معنوي، وذلك على النحو التالي:

"كل من تنصت أو التقط أو اعترض عمدا، بدون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، فإذا قام من تنصت أو اعترض أو التقط بإفشاء ما هو مرسل دون إذن صاحبه سواء بنفسه أو بواسطة غيره وكان من شأن ذلك إلحاق الضرر به أو بأسرته تكون العقوبة الحبس الذي لا تقل مدته عن ستة أشهر والغرامة التي لا تقل عن. ..... ولا تجاوز. ..... أو إحدى هاتين العقوبتين.

فإذا كان ما هو مرسل وفقا للفقرة السابقة يعد سرا بذاته أو بموجب القوانين أو اللوائح أو الأوامر أو القرارات أو التعليمات الإدارية لشخص طبيعي أو معنوي وهو يعلم أو كان يجب عليه أن يعلم بذلك، تكون العقوبة الحبس لمدة لا تقل عن سنة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو إحدى هاتين العقوبتين، دون حاجة لإثبات الضرر".

5. أن تتضمن التشريعات الجنائية العربية محل الدراسة، نصا يجرم إنتاج وحيازة الفيروسات وكلمات المرور بهدف استخدامها في ارتكاب جرائم أو تسهيل ارتكابها، خاصة جرائم تقنية المعلومات الواردة في تلك التشريعات.

هوامش الدراسة

(1) المنشآت المالية أو التجارية أو الاقتصادية: أي منشأة تكتسب وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة.

الكتروني: ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو مؤتمتة أو ضوئية أو ما شابه ذلك.

مواد إباحية الأحداث: أي صور أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو أفعال جنسية حقيقة أو افتراضية أو بالمحاكاة لحدث لا يتجاوز الثامنة عشر من عمره.

العنوان البروتوكولي للشبكة المعلوماتية: مُعرف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات، ويتم استخدامه لأغراض الاتصال.

سري: أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو بإفشائها إلا بإذن مسبق ممن يملك هذا الإذن.

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها.

الإساءة: كل تعبير متعمد عن أي شخص أو كيان يعتبره الشخص العادي مهيناً أو ماساً بشرف او كرامة ذلك الشخص أو الكيان.

(2) **تنص المادة (5) من القانون الاتحادي رقم 2 لسنة 2006 على أن:**

"كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين".

(3) **تنص المادة (8) على أن:**

"يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع الكتروني أو نظام معلومات الكتروني".

(4) **تنص المادة (10) من المرسوم رقم 5 لسنة 2012، على أن:**

"يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمدا وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات الكتروني

أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الالكتروني أو البيانات أو المعلومات.

وتكون العقوبة السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين إذا لم تتحقق النتيجة.

وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الالكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته".

(5) **تنص المادة 6 من القانون الاتحادي الملغي رقم 2 لسنة 2006 على أن:**

"كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها يعاقب بالسجن المؤقت وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين".

(6) **تنص المادة (28) من قانون العقوبات الاتحادي على أن:**

"الجناية هي الجريمة المعاقب عليها بإحدى العقوبات الآتية:

1- أية عقوبة من عقوبات الحدود أو القصاص فيما عدا حدي الشرب والقذف.

2- الإعدام.

3- السجن المؤبد.

4- السجن المؤقت. "

(7) **تنص المادة (71) من قانون العقوبات الاتحادي على أن:**

"عقوبة الغرامة هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن مائة درهم ولا أن يزيد حدها الأقصى على مائة ألف درهم في الجنايات وثلاثين ألف درهم في الجنح وذلك كله ما لم ينص القانون على خلافه".

(8) يونس خالد مصطفى، جرائم الحاسوب، الجامعة الأردنية، دار الثقافة للتوزيع والنشر، عمان، الأردن، 1994، ص 177.

(9) نائلة قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2005، ص 419.

(10) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص 163.

(11) كورنو جيرار، معجم المصطلحات القانونية، ص 80.

(12) مشار إليه في: عفيفي كامل عفيفي، مرجع سابق، ص 161.

(13) المحكمة الاتحادية العليا، الطعن رقم 489 لسنة 2014، جزائي، جلسة الثلاثاء 2014/12/30.

(14) نائلة قورة، مرجع سابق، ص 425.

(15) نهلا المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 188.

(16) محمود عبانه، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص 54 - 55.

(17) يونس خالد مصطفى، جرائم الحاسوب، الجامعة الأردنية، دار الثقافة للتوزيع والنشر، عمان، الأردن، 1994، ص 178.

(18) **تنص المادة (10) من القانون الاتحادي الملغي رقم 2 لسنة 2006 على أن:**

"كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين العقوبتين".

(19) المحكمة الاتحادية العليا، الطعنان رقما 400، 546 لسنة 2013، جزائي، جلسة الثلاثاء 2014/03/18.

(20) **تنص المادة (399) من قانون العقوبات الاتحادي على أن:**

"يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو صفة غير صحيحة متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم، ويعاقب بالعقوبة ذاتها كل من قام بالتصرف في عقار أو منقول يعلم أنه غير مملوك له أو ليس له حق التصرف فيه أو تصرف في شيء من ذلك مع علمه بسبق تصرفه فيه أو التعاقد عليه وكان من شأن ذلك الإضرار بغيره.

وإذا كان محل الجريمة مالاً أو سندًا للدولة أو لإحدى الجهات التي ورد ذكرها في المادة (5) عد ذلك ظرفًا مشددًا.

ويعاقب على الشروع بالحبس مدة لا تجاوز سنتين أو بالغرامة التي لا تزيد على عشرين ألف درهم ويجوز عند الحكم على العائد بالحبس مدة سنة فأكثر أن يحكم بالمراقبة مدة لا تزيد على سنتين ولا تجاوز مدة العقوبة المحكوم بها".

(21) **تنص المادة (399) من قانون العقوبات الاتحادي على أن:**

"يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو صفة غير صحيحة متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم، ويعاقب بالعقوبة ذاتها كل من قام بالتصرف في عقار أو منقول يعلم أنه غير مملوك له

أو ليس له حق التصرف فيه أو تصرف في شيء من ذلك مع علمه بسبق تصرفه فيه أو التعاقد عليه وكان من شأن ذلك الإضرار بغيره.

وإذا كان محل الجريمة مالاً أو سندًا للدولة أو لإحدى الجهات التي ورد ذكرها في المادة (5) عد ذلك ظرفًا مشددًا.

ويعاقب على الشروع بالحبس مدة لا تجاوز سنتين أو بالغرامة التي لا تزيد على عشرين ألف درهم ويجوز عند الحكم على العائد بالحبس مدة سنة فأكثر أن يحكم بالمراقبة مدة لا تزيد على سنتين ولا تجاوز مدة العقوبة المحكوم بها".

(22) **تنص المادة (9) من المرسوم بقانون الاتحادي رقم 5 لسنة 2012 على أن:**

"يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من تحايل على العنوان البروتوكولي للإنترنت باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها".

(23) **تنص المادة (380) من قانون العقوبات الاتحادي على أن:**

"يعاقب بالغرامة التي لا تقل عن ثلاثة آلاف درهم من فض رسالة أو برقية بغير رضاء من أرسلت إليه أو استرق السمع في مكالمة هاتفية.

ويعاقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر أو بالغرامة التي لا تقل عن خمسة آلاف درهم إذا أفشى الرسالة أو البرقية أو المكالمة لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك إلحاق الضرر بالغير".

(24) الطعن رقم 344 لسنة 2008 جزاء، محكمة التمييز – المكتب الفني، مجموعة الأحكام والمبادئ القانونية الصادرة في المواد الجزائية عام 2008 – جزاء، العدد التاسع عشر.

DOI: doi.org/10.52133/ijrsp.v2.18.1