جريمة التحايل على العنوان البروتوكولي
دراسة تحليلية في التشريع العقابي الإماراتي

الدكتور/ معاذ سليمان الملا(*)

ملخص:

انفرد المشرع العقابي الإماراتي في تجريم التحايل على العنوان البروتوكولي في إطار المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، وهي فلسفة تميل إلى ضبط سلوكيات المستخدمين أثناء استخدام شبكة الإنترنت لاسيما أن هذا السلوك يعد نافذة للعبور إلى شبكة الإنترنت العميق والمظلم حيث تقبع فيها الأنشطة الإجرامية بكافة أشكالها بما في ذلك الإجرام المنظم. ونحاول في هذا البحث دراسة موقف المشرع العقابي الإماراتي وإظهار فلسفته في تجريم هذا السلوك، ورغبته في تحقيق حماية فاعلة لمستخدمي شبكة الإنترنت، فاتبعنا منهجاً تحليلياً حيث قمنا بتقسيم الدراسة إلى مبحثين اثنين: الأول خصصناه لبيان ماهية العنوان البروتوكولي وطبيعته القانونية، والثاني استعرضنا فيه البنيان القانوني لتجريم التحايل على العنوان البروتوكولي، وصولاً إلى بعض النتائج والتوصيات.

مفردات البحث: تحايل - العنوان البروتوكولي- الإنترنت المظلم والعميق- جريمة- المشرع الإماراتي.

المقدمة

لا مراء من اعتبار الولوج إلى شبكة الإنترنت من الممارسات الضرورية التي لا يمكننا الاستغناء عنها في حياتنا اليومية بكافة ألوانها وأشكالها، إذ لم يعد شخصٌ على وجه الأرض كبيراً كان أو صغيراً إلا وقد ولج إليها بواسطة هاتفه المحمول أو حاسوبه الآلي أو حتى عبر أجهزة الألعاب الإلكترونية المتنوعة، ونلمس هذا الأمر من واقع ما أشارت إليه إحدى الدراسات من إدمان بني البشر على استخدام أدوات تقنية المعلومات وشبكة الإنترنت، حيث أظهرت أن عدد الأجهزة المتصلة بشبكة الإنترنت فاق عدد سكان الأرض(١).

وإذا كان ذلك إشارة واضحة للفوائد المتعددة التي تحظى بها أدوات تقنية المعلومات وشبكة الإنترنت، ولكن بالمقابل استطاع المتمتعون بالنزعات الإجرامية الاستفادة من أدوات تقنية المعلومات وشبكة الإنترنت وتوظيفها في أنشطتهم الإجرامية المختلفة من

(*) أستاذ القانون الجزائي المشارك بكلية القانون الكويتية العالمية - دولة الكويت

(١) للاطلاع على التقرير راجع الموقع الإلكتروني الخاص سكاي نيوز العربية على الرابط التالي:
https://www.skynewsarabia.com/technology/848802

خلال استغلال الثغرات التقنية والأمنية لشبكة الإنترنت، وليس ذلك فحسب؛ بل أصبحت شبكة الإنترنت البيئة الحاضنة للإجرام، أو بمعنى آخر الملاذ الآمن للجماعات الإجرامية تمارس فيها العديد من أنشطتها بالتخفي وراء ستار الظلام الافتراضي.

أولاً: موضوع البحث وأهميته

قد يضعنا موضوع البحث أمام تصور أن الحديث فيه سيكون فنياً بحتاً، وهذا صحيح إلى حد ما؛ لأن دراسته تتطلب منا الوقوف على ذلك، إلا أننا سنلجأ إلى تبسيط الفكرة بحيث تمكنا من استيعاب موضوع البحث الذي يتعلق تحديداً بآلية الارتباط بشبكة الإنترنت بواسطة أدوات تقنية المعلومات، وكيف يتم التحايل على الرابط الذي يمَكِن المستخدم من الدخول إلى عالم الإنترنت عبر ما يسمى بالعنوان البروتوكولي، فاللغة القانونية هي غايتنا الأساسية في طرح هذا الموضوع.

تنجلي أهمية هذا الموضوع فيما يتصل بحظر استخدام شبكة VPN وحجب بعض المواقع الإلكترونية في دولة الإمارات العربية المتحدة باهتمام البعض الذين رأوا أن هذا الحظر من شأنه أن يضيق من نطاق حرية الإعلام ويتعارض مع دستور الدولة الصادر سنة ١٩٧١.

ثانياً: نطاق البحث ومشكلته

يقول الخبير والباحث في مجال أمن المعلومات Donn B. Parker في عبارة استشهدنا بها كثيراً في كتابه المعروف بعنوان «Fighting Computer Crime» أو «مواجهة جرائم الكمبيوتر»، حيث قال: «نحن بحاجة إلى معرفة أكبر قدر ممكن حول إساءة استخدام أجهزة الكمبيوتر وآثارها لحماية معلوماتنا بشكل فعال، فمعرفة نقاط الضعف والضوابط وحدها ليست كافية» [٢]. هذه العبارة التي قيلت في تسعينيات القرن الماضي تؤكد لنا - وبحق- أننا لا زلنا نجهل بعض الجوانب التقنية أو الفنية عند استخدامنا لأدوات تقنية المعلومات وشبكة الإنترنت، أو نتجاهل هذه الجوانب ونكتفي باتخاذ إجراءات عقيمة، أو نتعمد إتيان بعض السلوكيات المخالفة التي تندرج تحت مفهوم الإساءة دون الشعور بمخاطر آثارها علينا، وانعكاسها - بطبيعة الحال- على واقع مجتمعاتنا.

(٢) "we need to know as much as possible about abuse and misuse of computers to effectively protect our information . knowledge of vulnerabilities and controls alone is not sufficient " .. Donn B. Parker. Fighting Computer Crime, a New Framework for Protecting Information, John Wiley & Son, New York, NY, USA ©1998, P81.

الأمر الذي يتطلب يقظة من المشرعين في إدراك هذه المخاطر ومواجهتها بشكل فعال بعد معرفة آثار الإساءات باتخاذ التدابير القانونية اللازمة التي تضمن حماية حقيقية للمستخدمين أثناء استخدامهم شبكة الإنترنت. وهذا بالفعل ما سلكه المشرع العقابي الإماراتي حينما جرم التحايل على العنوان البروتوكولي الذي قد يلج المستخدم عبر خدمات VPN أو TOR أو غير ذلك من تطبيقات أخرى تقود إلى العالم المجهول، أو كما يقال تارة أخرى بعالم الإنترنت المظلم أو العميق Dark or Deep Web، وهي المناطق التي تشكل تهديداً لأمن المجتمعات والدول على حد سواء؛ حيث تقبع فيها أخطر العصابات المنظمة التي تمارس الأنشطة غير المشروعة كالاتجار بالبشر والإرهاب والاتجار بالمخدرات والأسلحة وإلى غير ذلك من نماذج إجرامية أخرى.

ثالثاً: منهجية البحث وتقسيمه

اتبعنا في هذا البحث منهجاً تحليلياً للوقوف على مفهوم التحايل على العنوان البروتوكولي، فبدأنا بعرض ماهيته حيث تناولنا فيه مفهوم هذا العنوان وطبيعته القانونية والمخاطر التي تنم عنه، ثم بعد ذلك وضحنا البنيان القانوني لتجريم التحايل على العنوان البروتوكولي في المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، وناقشنا أيضاً التعديل الذي أجراه المشروع بموجب المرسوم بقانون اتحادي رقم ٢ لسنة ٢٠١٦ وإبراز غايته في هذا التعديل.

تحقيقاً لذلك قمنا بتقسيم البحث وفقاً للمنهجية المتبعة إلى مبحثين اثنين نوردهما على النحو الآتي:

المبحث الأول: ماهية التحايل على العنوان البروتوكولي

المبحث الثاني: موقف المشرع الإماراتي من التحايل على العنوان البروتوكولي

المبحث الأول
ماهية التحايل على العنوان البروتوكولي

تقسيم:-

يتطلب عرض فكرة التحايل على العنوان البروتوكولي الحديث أولاً عن مفهوم العنوان البروتوكولي وهذا هو المطلب الأول، وفي الثاني نستعرض طبيعته القانونية، ثم بعد ذلك نوضح في المطلب الثالث والأخير مخاطر هذا السلوك.

المطلب الأول
فكرة العنوان البروتوكولي وتعريفه

من منطلق دراستنا القانونية فإن عرضنا لمفهوم العنوان البروتوكولي سيكون بصورة بسيطة نبتعد فيه عن التعمق في المفهوم التقني الذي قد يخرجنا من مسار دراستنا، لذلك سوف نكتفي فقط بالإشارة إلى أهم الجوانب التقنية التي تساعدنا على استيعاب المفهوم العام للعنوان البروتوكولي.

أولاً: فكرة التحايل على العنوان البروتوكولي

التحايلَ في معجم اللغة العربية تحايل علي يتحايل، تحايُلاً، فهو مُتحايِل، والمفعول مُتحايَل عليه. ويقال اصطلاحاً تحايل على الرَّجلِ أو تحايل على الشَّيء أي سلك معه مسلك الحذق ليبلغ منه مأربَه «تحايل على القانون» أو داهنه وراوغه[٣]. وهو سلوك يشير إلى استخدام أساليب مخادعة ليتجاوز فيها الشخص مرحلة ما.

وفي البيئة المعلوماتية ظهر هذا المفهوم عند الولوج إلى شبكة الإنترنت عبر أدوات تقنية المعلومات المختلفة، فكل أداة يكون لها عنوان بروتوكولي عند استخدام شبكة الإنترنت، والعنوان البروتوكولي عبارة عن رقم تعريفي خاص لكل جهاز على حدة يتصل بالشبكة المعلوماتية (الإنترنت) سواء أكان الجهاز المتصل هاتفاً محمولاً أم حاسوباً آلياً أم غير ذلك من أدوات يمكن من خلالها الاتصال بهذه الشبكة، يكون التعريف بمكان وجود هذا الجهاز أو موقعه على الخارطة الجغرافية في الكرة الأرضية، وكل جهاز يتم منحه عنواناً خاصاً من قبل هيئة الإنترنت للأسماء والأرقام المخصصة (الآيكان ICANN)[٤]، ويتكون هذا العنوان

---

(٣) معجم اللغة العربية المعاصر، موقع المعاني الإلكتروني، كلمة البحث تحايل، راجع الرابط التالي: https://www.almaany.com/ar/dict/ar-ar/ تحايل

(٤) راجع: د. علاء التميمي عبده، التنظيم القانوني للعنوان البروتوكولي الموقع الإلكتروني كأحد عناصر الملكية الصناعية٢٠١٧، دار النهضة العربية، القاهرة، ص١٤٤. وراجع أيضاً:
Chris Reed, Computer Law, 7edition-2011, OXFORD UNIVERSITY, UK, P545.
وانظر أيضاً: الموقع الإلكتروني للمؤسسة على الرابط التالي:
http://archive.icann.org/tr/arabic.html

من ٣٢ رقماً مقسمة إلى أربع مجموعات كل مجموعة تحتوي على ٨ بت بأرقام عشرية يكون مداها من صفر وحتى ٢٥٥، وتوضيح ذلك يكون العنوان ١٣١,١٠٥,١٣,٣٠٠، وينقسم رقم IP إلى قسمين: رقم للشبكة و رقم عنوان للجهاز.

ويمكن تبسيط آلية الاتصال بشبكة الإنترنت بمثال وهو أنه إذا قمنا بكتابة عنوان قابل للقراءة نريد الولوج إليه عبر أجهزتنا وليكن موقع www.google.com على سبيل المثال، فإنه سيتم تحويل هذا العنوان إلى رقم تعريفي ١٣٩,١٣٠,٤,٥ يتم التعرف فيه على الجهاز المتصل، ومن ثم نصل إلى هذا الموقع بصرف النظر عن نطاقه داخلي أو عالمي، وبالتالي دون هذا العنوان لا يمكن لنا الاتصال عبر شبكة الإنترنت. وقد تطور العنوان البروتوكولي على مراحل عدة وصولاً إلى نسخته الجديدة وهو الجيل السادس IPv6 [٥]. والسؤال هنا كيف يمكن للمستخدم أن يتحايل على العنوان البروتوكولي ؟

العنوان البروتوكولي عبارة عن سلسلة أو مجموعة من الأرقام التي يمكن من خلالها تحديد هوية الجهاز المتصل عبر شبكة الإنترنت، أي أنه من خلال هذا العنوان يمكن تحديد اسم النطاق وتحديد اسم الجهة التي قامت بتسجيل النطاق وتحديد موقع الجهاز، وهو ما يعني إمكانية تتبع أو تقفي أثر الجهاز وصولاً إلى المستخدم الذي سيترك آثاراً ودلالات كثيرة تتصل به بشكل سجلات رقمية مؤتمتة كملفات الكوكيز (Cookies) التي تتضمن المواقع الإلكترونية الذي زارها، والوقت الذي قضاه فيها، والأمور التي بحث عنها عبر محركات البحث، وأيضاً المواد التي قام بتنزيلها، والرسائل التي أرسلها، والخدمات والبضائع التي قام بطلبها وشرائها، وحياته وهواياته وميوله، وآراءه على الشبكة، وإلى غير ذلك من تفاصيل دقيقة في الجانب الشخصي للمستخدم[٦].

لذلك تتفق معظم الآراء على أن حفظ هذه الملفات أو السجلات من شأنه أن يهدد

---

(٥) د. منال البلقاسي، المرجع السابق، ص٩٢و٩٣. وفي الفقه الانجليزي راجع:
Andrew Murray, Information Technology Law- The Law and Society, 3rd edition-2016, Oxford University Press, United Kingdom, P21-26.

وفي مراجع اللغة الفرنسية راجع:
Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haidara. Droit des activites numeriques, 1Edition, 2014, Dalloz, Paris, P743.

(٦) للمزيد من التفاصيل راجع: د. مروة زين العابدين، المرجع السابق، ص٣٣٣. وراجع أيضاً:
Peter Carey,op, cit, P198. And Donn B. Parker.op, cit, P89.

وفي مراجع اللغة الفرنسية:
Ludovic Pailler, Les réseaux sociaux sur internet et le droit au respect de la vie privée, 2012, Larcier, Belgique, P116.

خصوصية المستخدمين[٧]؛ الأمر الذي دفع البعض إلى إيجاد وسائل فنية تتيح لهم الالتفاف أو التحايل على العنوان البروتوكولي أشهرها على الإطلاق شبكة TOR وشبكة VPN. وتتفق هاتان الشبكتان في نظام عملهما من حيث توفير حماية لبيانات المستخدم عند الاتصال بشبكة الإنترنت، ومع ذلك يختلفان في الكيفية التي يتم فيها تحقيق الحماية للمستخدم وبياناته. سنحاول فيما يلي وباختصار شديد شرح كيفية حماية المستخدم وذلك على النحو التالي:

١ - **نظام شبكة** TOR [٨]: يقوم هذا النظام بحماية المستخدم من تحليل حركة مروره عند استخدام شبكة الإنترنت والاتصال من ثم بالسيرفر أو المتصفح الخاص بالشبكة لتنقله بعد ذلك إلى مقصده، وعند الاتصال تعمل هذه الشبكة على إخفاء هويته وموقعه بين الجهاز الذي يستخدمه أياً كان نوعه والمواقع الإلكترونية التي يزورها، وهذا يعني أنها تمنع مراقبة الغير عند زيارة المواقع في نقاط مختلفة بسبب طريقة توجيه حركة البيانات التي تخفي (IP)، وتمتاز هذه الشبكة بأنها تُدار من قبل أفراد متطوعين؛ الأمر الذي يصعب على أي منظمة أو حكومة أن تقوم بحجبها، كما أنها تمتاز بأنها مجانية، ويعاب على هذا النظام بأنه يبطئ عملية الاتصال، ويمكن أن تنكشف بياناته إذا لم يستخدم المستخدم اتصالاً من نوع HTTP، كما أن الوصول إليها لا يكون إلا عبر متصفح خاص بشبكة TOR.

٢ - **نظام شبكة** VPN [٩]: يقوم هذا النظام على السماح للمستخدمين باستعارة عنوان IP من السيرفر الخاص بشبكة VPN التي تقوم بتشفير جميع الاتصالات باستخدام الجهاز أياً كان نوع هذا الجهاز، ومن ثم تمريرها وما تحمله من بيانات من خلال نفق آمن تسمح للمستخدمين بتصفح المواقع الإلكترونية بشكل متخفٍ. وتخضع هذه الخدمة للمفاهيم المنصوص عليها في إطار المادة الأولى (خدمات

---

(٧) د. أشرف جابر سيد، المرجع السابق، ص٨٦. وراجع ذلك أيضاً لدى:
Ludovic Pailler, op, cit, P115. Et Fabrice Mattatia, Internet et les réseaux sociaux : que dit la loi ? 3e edition-2015, Eyrolles, Paris, P81-82.

(٨) Tor لفظ مختصر لعبارة (The Onion Router) وباللغة العربية التوجيه البصلي أي نسبة إلى ثمار البصل وطبقاته للمزيد من التفاصيل راجع التالي:
https://www.hotspotshield.com/ar/resources/tor-vs-vpn/

(٩) VPN اختصار لعبارة Virtual Private Network وهي شبكة اتصال افتراضية خاصة تعمل في نطاق شبكة الإنترنت، أي يكون الاتصال بها بعد الاتصال بشبكة الإنترنت. للمزيد من التفاصيل راجع التالي:
https://www.hotspotshield.com/ar/resources/tor-vs-vpn/

الاتصالات) من المرسوم بقانون اتحادي رقم ٣ لسنة ٢٠٠٣ وتعديلاته بشأن تنظيم قطاع الاتصالات، وقد عرفها قرار مجلس الوزراء رقم ٢١ لسنة ٢٠١٣ بشأن لائحة أمن المعلومات في الجهات الاتحادية، في البند ١٥ من المادة الأولى بأنها «شبكة تستخدم الإنترنت لتوفير طريقة للوصول إلى الشبكة التنظيمية المركزية بالجهة المعنية للمستخدمين المصرح لهم، وتطالب الشبكة عادة أن تتم المصادقة الآمنة من هؤلاء المستخدمين للتأكد من هويتهم قبل الدخول».

وتمتاز هذه الشبكة في عملها بأنها تخفي هوية المستخدم باستبدال العنوان البروتوكولي الأصلي بآخر غير معروف بحيث تتفادى الرقابة والقيود الجغرافية، وتشفر جميع أنواع البيانات عند الاتصال والانتقال عبر شبكة الإنترنت، وتمكن المستخدم من الوصول إلى المواقع المحجوبة، كما أن استخدامها يؤمن على الاتصالات اللاسلكية Wi-Fi. ولا يخلو هذا النظام من عيوب أيضاً حيث تسجل بعض أنواع تطبيقات VPN تاريخ تصفح المواقع أي أنها تخزن المواقع التي يقوم المستخدم بزيارتها.

ثانياً: تعريف التحايل على العنوان البروتوكولي

قيل بأن البروتوكول عبارة عن لغة يستخدمها جهاز الحاسب على الشبكة، مهمته تنظيم التخاطب مع الأجهزة الأخرى عبر مجموعة من الإجراءات التي تتحكم بالاتصال والتفاعل بين الأجهزة المختلفة عبر الشبكة[١٠]. وبروتوكولات الإنترنت عديدة[١١]، وما يعنينا في سياق دراستنا هو بروتوكول بيانات التعريف أو بروتوكول عناوين الإنترنت، وقد أطلق عليه اختصاراً (IP-address)، ويطلق عليه في الولايات المتحدة الأمريكية اختصاراً مصطلح (PII)[١٢]. وقد عرف المشرع الإماراتي العنوان البروتوكولي في البند ١٥ من المادة الأولى من المرسوم اتحادي بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، حيث نصت على أنه : «معرف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات، ويتم استخدامه لأغراض الاتصال». وعرفه البند (د) في المادة ٢ من التوجيه الأوروبي رقم ٢٠٠٦/٢٤ بشأن الاحتفاظ بالبيانات المعالجة عبر الاتصالات الإلكترونية، تحت

(١٠) د. منال البلقاسي، شبكات وأمن المعلومات، طبعة أولى ٢٠١٩، دار التعليم الجامعي، الإسكندرية، ص٩١.

(١١) هناك بروتوكولات عديدة تعمل في بيئة شبكة الإنترنت كبروتوكول التحكم والتحقق من صحة البيانات TCP وبروتوكول نقل صفحات الموقع الإلكتروني إلى أجهزة المستخدمين في الشبكة HTTP، وبروتوكول الصوت VOIP وبروتوكول التوجيه الديناميكي RIP وإلى غير ذلك من بروتوكولات.

(١٢) (IP-address) هي اختصارٌ لكلمة Internet Protocol، أما (PII) فهي اختصار لكلمة Personal Identifiable Information.

مصطلح معرف المستخدم وهو «معرفٌ فريدٌ يتم تخصيصه للأشخاص عند الاشتراك في خدمة الوصول إلى شبكة الإنترنت أو الاتصال عبرها أو التسجيل فيها»[١٣].

وبالنظر إلى هذين التعريفين نجد أن الاختلاف بينهما ينحصر في أن المشرع الإماراتي ينسب العنوان البروتوكولي إلى الجهاز أو الوسيلة المستخدمة في الاتصال بشبكة الإنترنت، لذلك نجده تبنى مصطلحاً فنياً وهو العنوان البروتوكولي للشبكة المعلوماتية وفق ما ورد في مادة التعريفات، في حين ينسب المشرع الأوروبي هذا العنوان إلى المستخدم الذي قد يكون شخصاً طبيعياً أو اعتبارياً، وهذا يعني أن المشرع الأوروبي يميل إلى اعتبار العنوان البروتوكولي كبيان شخصي على نحو ما سوف نراه. ومع ذلك يتفقان في أمرين اثنين: الأول أن العنوان البروتوكولي عبارة عن هوية محددة تتعلق بطرف معين (ينبثق منها الاختلاف السابق)، ويتفقان أيضاً في الغرض من العنوان البروتوكولي وهو الاتصال بشبكة الإنترنت أياً كان الغرض من الاتصال، إذ يستوي أن يكون الغرض منه عاماً أو خاصاً وذلك بحسب طبيعة الاستخدام.

ومن جانبنا فإننا نميل إلى ما ذهب إليه المشرع الإماراتي، كونه تبنى- وفق تصورنا- مصطلحاً ومفهوماً واسعين للعنوان البروتوكولي، فهو تعامل مع منطقية الاتصالات بشبكة الإنترنت، حيث رأى أن العنوان يتعلق بشكل مباشر بالجهاز وليس بالمستخدم، كون أنه ليس بالضرورة أن يكون الجهاز خاصاً بأحد الأشخاص بل قد يعود إلى أشخاص آخرين طبيعيين كانوا أم اعتباريين، ومثل ذلك مقهى الإنترنت أو الأجهزة الحكومية أو غير ذلك.

أما المشرع الأوروبي فقد استند في بيانه للعنوان البروتوكولي وبشكل مباشر إلى شخص المستخدم، وهذا المفهوم وفقاً للتصور السابق من الصعب معه تحديد هوية الشخص الذي ارتبط بشبكة الإنترنت، وإن كان بالإمكان تحديد الجهاز المتصل وموقعه. وذلك على اختلاف توجهه في الاتفاقية الخاصة بمكافحة الجرائم المعلوماتية الصادرة ٢٠٠١ ومذكرته التفسيرية، حيث عرف العنوان البروتوكولي ضمن بيانات حركة الاتصالات التي ترتبط بجهاز الكمبيوتر في البند (D) من المادة الأولى[١٤]. وقد تبنى المشرع العربي المفهوم ذاته في البند ٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة ٢٠١٠.

(١٣) Article 2 - Definitions ...'user ID' "means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;".

(١٤) عرف المشرع الأوروبي بيانات حركة الاتصالات بأنها «أي بيانات متعلقة باتصال عن طريق نظام معلوماتي والتي تنشأ عن نظام معلوماتي يشكل جزءاً في سلسلة اتصالات، توضح المنشأ، والوجهة، والمسار، والزمن، والتاريخ، والحجم، والمدة، أو نوع الخدمة الأساسية». وقد بينت الفقرة ٣٠ من المذكرة التفسيرية أن المنشأ يشير إلى عنوان بروتوكول الإنترنت (IP).
https://rm.coe.int/16800cce5b

ولم يُعرف المشرع الإماراتي المقصود بالعنوان البروتوكولي في المرسوم بقانون اتحادي رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات المُلْغىَ، كما لم يتناوله في التشريعات الإلكترونية الأخرى.

المطلب الثاني

الطبيعة القانونية للعنوان البروتوكولي

إذا كان العنوان البروتوكولي يحظى بأهمية في منهجية البناء والتطوير التقني، فإنه أيضاً يحظى بأهمية في الجانب القانوني من حيث تنظيم آلية التعامل فيه أو من خلاله عبر شبكة الإنترنت، وقد رأينا فيما سبق أن العنوان البروتوكولي يتصل بهوية محددة عبر جهاز إلكتروني، دون هذا العنوان لا يمكن للمستخدم الوصول إلى الموقع الإلكتروني.

وقد ثار خلاف في الفقه والقضاء حول الطبيعة القانونية لهذا العنوان، فمنهم من يرى بأن له طابعاً شخصياً للمستخدم، ومنهم من يرى خلاف ذلك:

أولاً: الاتجاه المؤيد للطابع الشخصي للعنوان البروتوكولي

استند هذا الاتجاه إلى لجوء القضاء إلى مطالبة مزودي خدمة الإنترنت في عدة قضايا بالكشف عن البيانات التي تحدد هوية مستخدمين ارتكبوا عدة جرائم عبر شبكة الإنترنت، وكان من بينها المطالبة بتحديد العنوان البروتوكولي، ورأوا أن هذا الأمر حتى ولو كان يشير بشكل غير مباشر للمستخدم إلا أن من شأنه أن يحدد هويته كمشترك، وهي بالتالي لا تختلف عن الاسم ورقم الهاتف والبريد الإلكتروني، ويترتب على ذلك عدم قدرة مزود الخدمة على معالجة هذا العنوان أي جمعه أو الاحتفاظ به إلا وفق الشروط والضوابط المقررة في التوجيه الأوروبي بشأن التعامل مع البيانات الشخصية.

وقد تعامل القضاء الأوروبي مع هذه الواقعة، فقد حسمت محكمة العدل الأوروبية هذا الأمر في الحكم الصادر عنها بتاريخ ١٩ أكتوبر ٢٠١٦ في الاستفسار المرفوع من المحكمة الفيدرالية الألمانية بشأن القضية رقم C582/14، حيث وجهت لها عدة استفسارات كان من بينها طبيعة العنوان البروتوكولي الديناميكية، وقد أثارت هذه المسألة النزاع بين Patrick Breyer والحكومة الألمانية الاتحادية سنة ٢٠١٤ بصفتها مشغلاً للمواقع الإلكترونية عبر

شبكة الإنترنت، لقيام الأخيرة بتسجيل وتخزين العنوان البروتوكولي الخاص به، وأيضاً تسجيل وتخزين عناوين البروتوكول لكل الزوار عند تصفحهم المواقع الإلكترونية، وذلك دون الحصول على موافقة مسبقة منهم على ذلك، وقد عللت الحكومة أن الهدف من هذا الإجراء هو حماية البيانات بموجب قانون Telemedia، فطالبها بالامتناع عن هذه الممارسة كونها تشكل تعدياً على بيانات شخصية للمستخدمين. إلا أن محكمة العدل الأوروبية اعتبرت العنوان البروتوكولي الديناميكي أيضاً من قبيل البيانات الشخصية، كما بينت أن قانون حماية البيانات في ألمانيا يتعارض مع المبادئ المقررة في اللائحة الأوروبية القديمة رقم ٩٥/٤٦ بشأن حماية معالجة البيانات الشخصية وتداولها(١٥).

والجدير ذكره أن هذا الرأي انقسم بدوره إلى اتجاهين أيضاً: حيث ذهب اتجاه إلى اعتبارها من قبيل البيانات التي تدخل في إطار الحق في الحياة الخاصة، أما الاتجاه الآخر ويرى أن البيانات الشخصية ليست متشابهة، بل هناك بيانات شخصية عادية ومثلها الاسم واللقب ورقم الهاتف ومكان السكن والاسم التجاري وغيرها، وهناك بيانات شخصية أخرى حساسة كالمعتقدات الدينية والسياسية والجينات الوراثية وإلى غير ذلك مما لا يرغب الشخص في الكشف عنه(١٦).

ثانياً: الاتجاه الرافض للطابع الشخصي للعنوان البروتوكولي

ذهب إلى أن العنوان البروتوكولي ليس من قبيل البيانات ذات الطابع الشخصي للمستخدم، تأسيساً على أن العنوان البروتوكولي لا يحدد هوية المستخدم بشكل مباشر بل يحدد الجهاز المتصل بشبكة الإنترنت، وقد تبنى القضاء الفرنسي في بادئ أحكامه هذا الرأي في بعض الأحكام الصادرة عنه(١٧). منها ما صدر عن محكمة استئناف باريس

(١٥) CJEU - JUDGMENT OF THE COURT (Second Chamber), 19 October 2016 http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN#Footnote

(١٦) راجع: د. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى ٢٠١٦، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، ص٧٩، ١٠٤، ٤٠٥. وانظر حول ذلك أيضاً لدى:
Peter Carey, Data Protection- A Practical Guide to UK and EU Law, 5ed-2018, OXFORD UNIERSITY PRESS, UK, P8, P20.

- وفي الفقه الفرنسي أيضاً لدى:
Guillaume Desgens-Pasanau, La protection des donnees personnelles, 2edition-2016, LexisNexis, Paris, P7.

(١٧) راجع: د. أشرف جابر السيد، الجوانب القانونية لمواقع التواصل الاجتماعي، الطبعة الأولى- ٢٠١٥، مركز النشر والترجمة لجامعة المجمعة، المملكة العربية السعودية، ص٨٥. وراجع حول ذلك أيضاً لدى:
Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haidara. Op, cit, P745.

بتاريخ ١٥ مايو٢٠٠٧ حيث بينت في حيثيات حكمها أن: «سلسلة الأرقام لا تشكل بيانات اسمية تحدد شخص المستخدم بقدر ما تحدد الجهاز»[١٨].

إلا أن المشرع الأوروبي حسم هذه المسألة في التوجيه الأوروبي الجديد رقم ٢٠١٦/٦٧٩ بشأن حماية معالجة البيانات الشخصية ونقلها، حيث شمل التوجيه العنوان البروتوكولي ضمن تعريف البيانات الشخصية في المادة ٤ منه، حيث بينت أن: «البيانات الشخصية تعني أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده (موضوع البيانات)؛ الشخص الطبيعي الذي يمكن تحديده هو الشخص الذي يمكن تحديده، بشكل مباشر أو غير مباشر، بشكل خاص بالرجوع إلى معرف مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف عبر الإنترنت أو إلى واحد أو أكثر من العوامل المحددة للفيزيائية، الفسيولوجية، الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي»[١٩].

ويبدو أن المشرع الأوروبي في هذا التعريف قد حاول أن يوازن بين الآراء الفقهية المختلفة، حيث أكد صراحة من خلال هذا التعريف أن العنوان البروتوكولي عبر شبكة الإنترنت سواء أكان ثابتاً أم متغيراً (ديناميكياً)[٢٠] يندرج تحت مفهوم البيانات الشخصية طالما كان بالإمكان تحديد هوية المستخدم، أو كانت هويته قابلة للتحديد.

ثالثاً: مدى اعتراف المشرع الإماراتي بالجانب الشخصي للعنوان البروتوكولي

يبدو أن صدور اللائحة الأوروبية الجديدة (GDPR)[٢١] رقم ٢٠١٦/٦٧٩ بشأن

(١٨) la cour d'appel de Paris, 13ème chamber, arrêt en date du 15 mai 2007. https://www.legalis.net/jurisprudences/cour-dappel-de-paris-13eme-chambre-section-a-arret-du-15-mai-2007/

(١٩) Article 2 – Definitions… personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(٢٠) العناوين البروتوكولية إما أن تكون ثابتة بمعنى أنها مسجلة لجهاز معين لدى مزود خدمة الإنترنت، فكلما ارتبط هذا الجهاز بشبكة الإنترنت يكون عنوانه ثابتاً، وقد يكون ديناميكياً أو متغيراً أي كلما ارتبط الجهاز بشبكة الإنترنت، كان له عنوان مختلف؛ لذلك لم يحدد المشرع الأوروبي هذه الطبيعة بالنسبة للعناوين البروتوكولية إذ اكتفى بالإشارة إلى صلة هذه العناوين بهوية المستخدم عبر شبكة الإنترنت. للمزيد من التفاصيل حول ذلك راجع بالتفصيل لدى:
Alain Bensoussan, Règlement européen sur la protection des données: Textes, commentaires et orientations pratiques, Édition : 2e edition 2018, Bruylant, P77-79.

(٢١) مقال نشر على صحيفة الاتحاد بعنوان/ حماية البيانات الشخصية، نشر بتاريخ ٢٧ يوليو ٢٠١٨. راجع الرابط الإلكتروني التالي:
https://www.alittihad.ae/wejhatarticle/99484/ حماية-البيانات-الشخصية

حماية معالجة البيانات الشخصية وتداولها ونفاذها في مايو عام ٢٠١٨ كان له وقعٌ واضحٌ بين دول العالم خصوصاً في دولة الإمارات العربية المتحدة؛ حيث تبين وجود مسعى من قبل الهيئة العامة لتنظيم قطاع الاتصالات بإعداد مشروع لحماية البيانات الشخصية. وهو ما حدا بنا إلى طرح سؤال في غاية الأهمية وهو هل دولة الإمارات العربية المتحدة بحاجة فعلاً إلى إعداد مشروع قانون لحمـاية البيانات الشخصية أم أن القوانين الموجـودة كفيلة بتحقيق تلك الحماية ؟

في وجهة نظرنا إن دولة الإمارات ليست بحاجة إلى إعداد مشروع جديد لحماية البيانات الشخصية؛ لأن لديها نماذج قانونية من الممكن الاعتماد عليها في تنظيم حماية البيانات مع إجراء بعض التعديلات التي تجعلها تتلاءم وتتواءم في الوقت ذاته مع اللائحة الأوروبية الجديدة، لاسيما وأن المشرع قرر حماية البيانات الشخصية في المادة ٢من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، فهو على الرغم من عدم نصه على تعريف محدد للبيانات الشخصية إلا أنه أشار بشكل غير مباشر إلى تقرير حمايتها في المادة ٢من أوجه كثيرة كالإلغاء أو الحذف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر، وقد شدد العقاب إذا كانت هذه الأفعال قد وقعت على بيانات شخصية(٢٢).

بجانب ذلك هناك نموذجان تشريعيان محليان وتحديداً في إمارة دبي وهما يتقاربان إلى حد كبير مع بنود اللائحة الأوروبية القديمة رقم ٩٥/٤٦ بشأن حماية البيانات، وهو القانون رقم ١ لسنة ٢٠٠٧ بشأن حماية البيانات في إمارة دبي (DIFC)، وقد عرف هذا القانون البيانات الشخصية بأنها: «أي بيانات تشير إلى شخص طبيعي يمكن التعرف

(٢٢) نصت المادة ٢ على أنه: «١- يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكتروني أو شبكة معلومات ، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. ٢- تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسين ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة ١ من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات .

٣ - تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة ٢ من هذه المادة شخصية» .

عليه». كذلك القانون رقم ٢٦لسنة ٢٠١٥ بشأن تنظيم نشر وتبادل البيانات[٢٣]، الذي نظم مسؤولية مزودي الخدمات عبر شبكة الإنترنت.

ومما لاشك فيه أن هذين النموذجين على وجه التحديد يمكن الاسترشاد بهما في إعداد لائحة لحماية البيانات الشخصية تتوافق مع اللائحة الأوروبية الجديدة، وتتوافق أيضاً مع كافة التشريعات الإلكترونية المعمول بها محلياً واتحادياً في دولة الإمارات العربية المتحدة.

المطلب الثالث

تقدير خطورة التحايل على العنوان البروتوكولي

قلنا أن التحايل يشير إلى قدرة المستخدم على تجاوز مرحلة ما، وفي بيئة الشبكة المعلوماتية يُشير التحايل إلى استخدام المستخدم أدوات تقنية المعلومات وتطبيقاتها من أجل تجاوز قيود الاستخدام، متخفياً بعنوان بروتوكولي آخر لفترة زمنية معينة طويلة كانت أم قصيرة. والسؤال هل يشكل ذلك إساءة تخالف قواعد الاستخدام الصحيح ؟ وما مدى خطورة ذلك ؟

أولاً: مدى اعتبار سلوك التحايل إساءة في استخدام أدوات تقنية المعلومات

لا يشكل سلوك التحايل إساءة بحد ذاته بقدر ما هو أسلوب يتيح للمستخدمين الانتقال عبر شبكة الإنترنت وتجاوز القيود التي قد تفرضها بعض الدول؛ لذلك يلجأ البعض إلى استخدام تطبيقات أو برامج معينة تمكنهم من الاختفاء عن الرقابة المفروضة في الشبكة عن طريق استبدال العنوان البروتوكولي المعرف للجهاز إلى عنوان بروتوكولي آخر يحصل عليه مستخدمو تلك التطبيقات أو البرامج.

والحقيقة أن كل دولة تختلف سياستها حول مدى اعتبار سلوك التحايل إساءة تتعارض مع قواعد الاستخدام الصحيح لأدوات تقنية المعلومات والشبكة المعلوماتية، ونقصد بالإساءة هنا إخلال المستخدم بضوابط الاستخدام السليم لهذه الأدوات على النحو الذي يترتب عليه مساس بحقوق وحريات الغير، أو تهديد النظام العام والآداب

(٢٣) لفظ (DIFC) اختصار لعبارة مركز دبي المالي العالمي، والجدير ذكره أن هذا القانون لم يعرب حتى الآن، فقد صدر باللغة الإنجليزية وظل كذلك حتى الآن. لمراجعة هذا القانون على الرابط الإلكتروني التالي:

http://www.difc.ae/download_file/49/196

العامة أو الإخلال بأمن الدولة وسيادتها. ويتوافق ذلك ما مع ذهب إليه البعض بأن الإساءة تعني استعمال أدوات تقنية المعلومات كجهاز الهاتف المحمول أو جهاز الحاسب الآلي أو غير ذلك من أجهزة تتصل بشبكة الإنترنت بطريقة تضر بالغير(٢٤). كذلك عرف المشرع الإماراتي الإساءة في المادة الأولى من المرسوم بقانون اتحادي بأنها كل تعبير متعمد عن أي شخص أو كيان يعتبره الشخص العادي مهيناً أو ماساً بشرف أو كرامة ذلك الشخص أو الكيان.

ولما كان التحايل سلوكاً يصعب معه القول بأن المستخدم يتعمد ذلك للإضرار بالغير، ذلك أن البعض يستخدمه من أجل الاتصال على الأقرباء، وقد يحدث أن يكون التحايل بشكل غير عمدي أثناء الولوج إلى المواقع الإلكترونية المختلفة، وهذا ما يتوافق- في رأينا- مع سياسة المشرع العقابي الإماراتي، إذ استلزم لتجريم سلوك التحايل أن يكون المستخدم قاصداً من سلوكه ارتكاب جريمة معينة.

ثانياً: مدى خطورة سلوك التحايل على العنوان البروتوكولي (نافذة على الجريمة)

قدمنا أن شبكتي TOR وVPN تقدمان خدمات مميزة للمستخدمين بحيث تمكنهم من التواصل المباشر والمرن والسريع والآمن مع المستخدمين عند استخدام شبكة الإنترنت للقيام بأنشطة متعددة تجارية وإعلانية وعسكرية، وأيضاً استخدامها في عمليات اتصالات عادية أو بالأحرى شخصية كالاتصال عبر تطبيقات الفايبر أو التانجو أو الواتساب وإلى غير ذلك من تطبيقات أخرى.

ومع ذلك هناك مخاطر عديدة على أمن المستخدم نفسه الذي لا يعلم درجة خطورة تحايله على العنوان البروتوكولي عند استخدامه لشبكة الإنترنت، لاسيما وأن سلوك التحايل أو التخفي قد يقوده إلى ما اشتهر بالبيئة الفاسدة للشبكة العنكبوتية، وتتمثل في الإنترنت المظلم Dark Web والإنترنت العميق Deep Web وهما يشكلان الجزء المخفي من منظومة شبكة الإنترنت، وهما عالمان يختلفان في درجة خطورتهما، فالأخير أقل خطورة من الأول إذ يحتوي على مواقع بعضها مشروع كمواقع لحماية الأرقام والحسابات السرية، ومواقع تضمن حماية التراسل في الدول الاستبدادية، وإلى غير ذلك مما يدخل في الإطار المشروع، كما أنها تحتوي على مواقع غير مشروع

(٢٤) د. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، ٢٠٠٣، ص١٧١.

تشكل في حقيقتها جرائم جنائية أهمها انتهاك حقوق الملكية الفكرية، أما الثانية ونقصد الإنترنت المظلم أو كما يقال بقبو شبكة الإنترنت فهي تحتوي على كافة الأشكال الإجرامية كتجارة المخدرات والمؤثرات العقلية وتجارة الأسلحة والمفرقعات والاتجار بالبشر وتجارة الأعضاء وأنشطة الإرهاب وغسل الأموال والجرائم الجنسية وغير ذلك من أنشطة[٢٥] أغلبها يدخل في نطاق الإجرام المنظم[٢٦].

فالعصابات الإجرامية المنظمة استطاعت استغلال التكنولوجيا الحديثة وبناء منصاتها المتنوعة على شبكة الإنترنت لتنفيذ أجنداتها وتمويلها عن طريق العملات الافتراضية بشكل آمن وسهل وسريع من خلال إخفاء هويتهم حتى عن أعين مزودي خدمات الإنترنت، أو تضليل الغير أو إيهامهم وراء ستار افتراضي، بحيث يصعب ملاحقتهم أو إثبات ما قاموا به، إذ يمكنهم طمس آثارها بسهولة. ولا ضير في القول بأن هذه الثورة دعمت أنشطة الإجرام المنظم في تدمير الأهداف وإلحاق خسائر طائلة بالضحايا[٢٧].

لذلك تعتبر شبكتا الإنترنت العميق والمظلم عالمين افتراضيين لا يمكن الوصول إليهما عبر محركات البحث العادية، بل عبر محركات بحث أخرى تحتوي على مواقع إلكترونية غير مفهرسة في نطاقات أخرى لا يمكن تتبعها عبر الشبكات المعمول بها في هاتين الشبكتين، ويقدر البعض أن هذه البيئة تشكل ما نسبته ٩٦٪ من الشبكة العنكبوتية، في حين استخدام الإنترنت العادي أو النظيف الذي يستخدمه الأفراد العاديون يشكل ٤٪[٢٨].

(٢٥) Michael Chertoff and Tobby Simon: The Impact of the Dark Web on Internet Governance and Cyber Security, Paper Series: No. 6 February 2015, P2.

(٢٦) Klaus Von Lampe, Organized Crime, Analyzing illegal Activities, Criminal Structures and Extra-legal Governance, 2016, Sage, 324.

(٢٧) للمزيد من التفاصيل راجع: د. عبد الصمد سكر، الجريمة المنظمة وآليات مكافحتها، الطبعة الأولى-٢٠١٨، دار النهضة العربية، مصر، ص٢٦ وما بعدها.

(٢٨) للمزيد من التفاصيل راجع: د. وليد بن صالح، الإنترنت المظلم والعملات الافتراضية: التحديات الجديدة للقانون الجنائي، بحث منشور في المؤتمر السنوي الخامس الدولي بعنوان/ التحديات المعاصرة للضمانات القانونية في عالم متغير، ٩-١٠ مايو ٢٠١٩، الجزء الثاني، مجلة كلية القانون الكويتية العالمية، الكويت، ص٣٩٠. وانظر أيضاً: تشيلسي أيه لويس، التخفي: نظرة متعمقة في شبكة تور (شبكة تخفي) وآثارها على أمن الحاسوب وحرية الرأي والتعبير في العصر الرقمي، مجلة معهد دبي القضائية، العدد (٥)، السنة (٣)، فبراير ٢٠١٥، دولة الإمارات العربية المتحدة، ص٢٣. وانظر أيضاً:
Kristin Finklea Dark Web, March 10, 2017 Congressional Research Service, USA, P2. www.crs.gov

وبالتالي يمكن القول أن هاتين الشبكتين بوابتان لمن يحملون قافية الشر خصوصاً العصابات الإجرامية المنظمة التي تتخذها موطناً لعملياتهم غير المشروعة، والولوج إليهما قد يعرض المستخدم إلى اعتداءات كثيرة يمكن إجمالها على النحو التالي:

١ - السماح للآخرين (الهاكرز) بالوصول إلى بياناته الشخصية من خلال النفاذ إلى جهازه ومن ثم المحتوى المخزن فيه كالصور والفيديوهات وأرقام حسابات وإلى غير ذلك، مما قد يؤدي ذلك إلى انتحال هويته أو تهديده أو ابتزازه أو تدمير بياناته أو سرقتها.

٢ - إذا كان استخدام الفرد لهاتين الشبكتين بغية إخفاء نفسه أو أفعاله- وهذا صحيح عملاً- عن الرقابة التي يمكن وصفها بالعادية، ولكنه بالمقابل سيكون مرصوداً لمجموعات احترافية تستطيع تحديد هويته ومكانه بدقة، بل ويمكن أن يكون أداة للجماعات الإجرامية.

٣ - لا يقتصر أمر الخطورة على الأفراد العاديين، بل أن الدولة وأمن مصالحها بكافة مجالاتها الاقتصادية والاجتماعية والسياسية والتنموية والدينية وغيرها في خطر مستمر.

ومن الوقائع المتعلقة في هذا الجانب ما حدث مؤخراً في دولة الإمارات العربية المتحدة، حيث تم إرسال رسائل مفبركة منسوبة لهيئة تنظيم الاتصالات تدعو مستخدمي أجهزة الهواتف المحمولة إلى دفع مخالفة قيمتها خمسة آلاف درهم[٢٩]. وواقعة أخرى ذكرتها صحيفة وول ستريت جورنال بأن إحدى الدول قامت بإرسال رسائل تهديدية إلى جنود منظمة حلف الشمال الأطلسي (الناتو)، وقد تبين أن هاكر استخدم عنواناً بروتوكولياً روسياً لإيصال تلك الرسائل عن طريق اختراق أنظمة الهواتف المحمولة[٣٠].

وانطلاقاً مما ذكر في هذا المبحث جاز لنا الوقوف على آلية تجريم التحايل على العنوان البروتوكولي الذي انفرد بها المشرع العقابي الإماراتي في إطار المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات.

---

(٢٩) مقال منشور على الموقع الإلكتروني الإمارات اليوم، بعنوان/ «تنظيم الاتصالات» تحقق في رسائل مفبركة حول منع استخدام شبكات VPN. راجع الرابط الإلكتروني التالي:
https://www.emaratalyoum.com/business/local/2018-01-25-1.1065037

(٣٠) Mohsin Qadir, "What is Spoofing?" An Average Internet User's Guide, March 31, 2018. PUREVPN.
https://www.purevpn.com/blog/what-is-ip-spoofing-scty/
https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402/

المبحث الثاني
موقف المشرع الإماراتي من التحايل على العنوان البروتوكولي

تقسيم:-

نعرض في هذا المبحث موقف المشرع الإماراتي من سلوك التحايل على العنوان البروتوكولي، واقتضى ذلك تقسيم المبحث إلى ثلاثة مطالب: الأول نبين فيه رؤية المشرع الإماراتي في تجريم التحايل على العنوان البروتوكولي، والثاني نوضح فيه أركان التجريم، أما الثالث والأخير فسوف نخصصه لبيان العقوبات والتدابير المقررة.

المطلب الأول
رؤية المشرع الإماراتي في تجريم التحايل على العنوان البروتوكولي

نحاول في هذا المطلب بيان رؤية المشرع الإماراتي في تجريم التحايل على العنوان البروتوكولي في إطار المرسوم بقانون اتحادي رقم٥ لسنة ٢٠١٢في شأن مكافحة جرائم تقنية المعلومات. ويتطلب ذلك بيان الأساس القانوني لتجريم هذا السلوك واستجلاء غاية المشرع.

أولاً: الأساس القانوني في تجريم التحايل على العنوان البروتوكولي

نصت المادة ٩ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات على أنه: «يعاقب بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليوني درهم، أو بإحدى هاتين العقوبتين، كل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها».

بالنظر إلى هذا النص نجد أن المشرع العقابي الإماراتي أراد أن يضع حداً لمشكلة لجوء مستخدمي الشبكة العنكبوتية إلى أدوات تقنية المعلومات للاختفاء أو التضليل أو غير ذلك من تعبيرات تتضمن القدرة على التستر أو إخفاء الهوية وراء الشبكة المعلوماتية لتنفيذ غايات إجرامية متفاوتة الخطورة، فهذا الأسلوب من الأساليب الفنية البحتة التي تتطلب قدراً من الذكاء في تنفيذها، خصوصاً وأن هناك مواقع ومنتديات منشورة على الملأ تتضمن

دلائل تعليمية لمستخدمي مواقع ومنتديات شبكة الإنترنت ومواقع التواصل الاجتماعي في كيفية تنفيذ بعض الأنشطة الإجرامية في بيئة شبكة الإنترنت[٣١]، وهناك - كما قلنا آنفاً - تطبيقات أو برامج معينة تمكن المستخدمين من التحايل على العنوان البروتوكولي.

ومما لاشك فيه أن ذلك قد يشكل خطراً حقيقياً على أمن المجتمع الاجتماعي والاقتصادي والسياسي، إذا لم توضع آلية للحد من تبعات الفوضى الإلكترونية، وبالتالي يأتي هذا التجريم متوافقاً مع التوجه العام في تعزيز الأمن الرقمي الذي تقدمه دولة الإمارات العربية المتحدة.

ولعل ذلك ما دفع المشرع الإماراتي إلى تعديل حكم هذه المادة في المرسوم بقانون اتحادي رقم ١٢ لسنة ٢٠١٦ [٣٢]، هو رغبته في ردع كل من أراد أن يتحايل ليس فقط على العنوان البرتوكولي بل ويتحايل على القانون، وقد تضمن هذا التعديل أمرين اثنين هما:

أولاً: يتعلق بالعقوبة المقررة للجريمة حيث كانت قبل تعديلها تعد من قبيل جرائم الجنح المعاقب عليها بالحبس، ولم يحدد المشرع مدتها، مما يعني أن القاضي سيعمل وفق ما تقرره القواعد العامة بشأن تحديد عقوبة الحبس، وتقرر المادة ٦٩ من قانون العقوبات الاتحادي الصادر سنة ١٩٨٧ أن عقوبة الحبس تكون بين الحد الأدنى وهو شهر واحد والحد الأقصى ثلاث سنوات. وبالنسبة لعقوبة الغرامة فقد كانت قبل التعديل تقرر أيضاً حدين: الأدنى هو مائة وخمسون ألف درهم، والأقصى لا يتجاوز خمسمائة ألف درهم، والغرامة وفقاً لذلك لا تخضع للقواعد العامة المقررة في المادة ٧١ المعدلة بمرسوم قانون اتحادي رقم ٧ لسنة ٢٠١٦ في شأن تعديل بعض أحكام قانون العقوبات رقم ٣ لسنة ١٩٨٧، حيث تقرر أن الحد الأدنى للغرامة هو ألف درهم، والحد الأقصى مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح[٣٣].

---

(٣١) هناك العديد من المواقع والمنتديات الإلكترونية التي تعرض محتويات تعليمية تمكن المستخدمين من تعلم طرق الاختراق أو تهكير الحسابات وكيفية الانتحال والسرقة الإلكترونية وإلى غير ذلك، كما أن هناك بعض المواقع توضح كيفية صنع الفيروسات المبرمجة.

(٣٢) تنص المادة ٩ قبل تعديلها على أنه: «يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين 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».

(٣٣) نصت المادة ٦٩ على أنه: «الحبس هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانوناً لهذا الغرض وذلك للمدة المحكوم بها، ولا يجوز أن يقل الحد الأدنى للحبس عن شهر ولا أن يزيد حده الأقصى على ثلاث سنوات ما لم ينص القانون على خلاف ذلك». أما المادة ٧١ فنصت =

ثانياً: وهو استعانة المشرع بلفظ آخر على خلاف ما كان ينص عليه، حيث كان المشرع يستخدم لفظ «الإنترنت» في النص السابق «... كل من تحايل على العنوان البروتوكولي للإنترنت..»، في حين النص الجديد استخدم لفظ آخر أكثر دقة وهو «الشبكة المعلوماتية»، فالمصطلح الأول وإن كان صحيحاً كونه يشير إلى شبكات الاتصالات، إلا أنه لم يرد لفظ الإنترنت ضمن ألفاظ وتعريفات المادة الأولى. وقد عرف المشرع الإماراتي الشبكة المعلوماتية في المادة الأولى من المرسوم بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بأنها: «ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات».

وقد ميز المشرع جريمة التحايل على العنوان البروتوكولي عن جريمة الاحتيال الإلكتروني المنصوص عليها في المادة ١١ [٣٤]، ونؤيد ما ذهب إليه البعض من أن هذا التمييز قائم على أساس اختلاف طبيعتهما، فالأولى جريمة إلكترونية بحتة لأن التحايل على العنوان البروتوكولي أو بمعنى آخر إن الخداع موجه لشبكة الإنترنت وليس إلى الشخص، وإن كان الأخير هو الهدف النهائي من الجريمة[٣٥]، أما جريمة الاحتيال الإلكتروني أو كما يقال تارة أخرى بالغش المعلوماتي فهي جريمة تتبع الأساليب العادية صحيح، وما يميزها عن الاحتيال التقليدي أن أدوات تقنية المعلومات تلعب دوراً رئيسياً فيها. فمن يقوم على سبيل المثال بالاتصال على آخرين لفك سحر أو الفوز بجائزة أو غير ذلك من ممارسات لا تستثني أحداً من مستخدمي الهاتف المحمول أو أدوات تقنية المعلومات، وبالتالي فإن المادة واجبة التطبيق هي المادة ١١ .

= على أنه: «عقوبة الغرامة : هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى على مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح ، وذلك كله ما لم ينص القانون على خلافه».

(٣٤) تنص المادة ١١على أنه: «يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات». وقد نص عليها المشرع في المادة١٠ من المرسوم بقانون رقم ٢ لسنة ٢٠٠٦ الملغى، وقد احتفظ المشرع في اعتبارها من قبيل جرائم الجنح، ولكن الاختلاف بينهما ينحصر في أمرين: الأول أن المشرع في المرسوم الملغى حدد الغاية من الاحتيال الإلكتروني وهو خداع المجني عليه، وقد استغنى المشرع عنها في المرسوم الجديد كما أنها لم ترد في المادة ٩، كذلك شدد في عقوبة الغرامة في المرسوم الجديد حيث كانت ثلاثين ألف درهم، في حين المرسوم الجديد يقرر عقوبة الغرامة بين الحدين كما هو واضح في النص.

(٣٥) أ. د. إمام حسنين عطا الله، جرائم تقنية المعلومات في التشريعات والصكوك العربية، طبعة أولى- ٢٠١٧- ١٤٣٩، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، ص٢٧٦.

ولا نؤيد ما ذهب إليه بعض الشراح من أن جريمة التحايل على العنوان البروتوكولي تتقارب مع نموذج جرائم الدخول غير المشروع، أو أنها تشكل إساءة عبر أدوات تقنية المعلومات[٣٦]؛ ذلك أن هذه النوعية من الجرائم سلوكها بحد ذاته جريمة، فمن يتحايل على عنوان بروتوكولي لإتمام عملية اتصال يختلف تماماً عمن يقوم باختراق موقع إلكتروني أو نظام معلوماتي. فالتحايل سلوك مشروع في بدايته لتبقى غاية المتحايل وما يبتغيه من ورائه، فقد يكون سلوكه مشروعاً من خلال وصوله إلى المواقع الإلكترونية بسبب الفضول، وقد يكون غير مشروع إذا كان المستخدم يقصد من سلوك التحايل ارتكاب جريمة خلف الستار المفترض عن طريق استبدال العنوان البروتوكولي، وسوف نوضح شروط قيام هذه الجريمة لاحقاً[٣٧].

ثانياً: غاية المشرع الإماراتي من تجريم هذا السلوك

يظهر تميز المشرع الإماراتي من هذه الناحية عن باقي المشرعين العقابيين بتخصيص نص يعنى بتجريم التحايل على العنوان البروتوكولي متى كان القصد منه ارتكاب جرائم مختلفة كسرقة العنوان البروتوكولي أو انتحال شخصية صاحب العنوان أو نشر الإشاعات أو لتضليل الرأي العام أو غير ذلك مما يضعنا أمام خطورة هذا السلوك، لتتضح رؤية المشرع وجديته في مواجهة هذه النوعية من الجرائم.

ويلاحظ أن البعض يرى أن نص المادة ٩ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ تتعارض مع بعض المبادئ الواردة في دستور دولة الإمارات العربية المتحدة الصادر سنة ١٩٧١ وتحديداً في المادتين٣٠ و٣١. فالمادة ٩ تضيق ما تقرره المادة ٣٠ التي تنص على أن: «حرية الرأي والتعبير عنه بالقول والكتابة، وسائر وسائل التعبير مكفولة في حدود القانون». وتنتهك ما ورد في المادة ٣١ التي تقرر بأن: «حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال وسريتها مكفولتان وفقاً للقانون»[٣٨].

---

(٣٦) أ.د. إمام عطا الله، المرجع السابق، ص٢٧٧ وما بعدها.

(٣٧) راجع: مقال منشور على الموقع الإلكتروني الاقتصادي، بعنوان/ الإمارات توضح طبيعة العقوبة المفروضة على مستخدمي VPN، نشر بتاريخ ٢ أغسطس ٢٠١٦، على الرابط الإلكتروني التالي:
https://aliqtisadi.com/804988-الإمارات-تحارب-الجرائم-الإلكترونية/

(٣٨) أشار المركز الدولي للعدالة وحقوق الإنسان بجنيف على هامش اليوم العالمي للصحافة لعام ٢٠١٧ إلى أن دولة الإمارات العربية المتحدة على الرغم من ضمانات حرية التعبير إلا أن السلطات فيها تقيد من ممارسة هذه الحرية بالنظر إلى التعديلات التشريعية الأخيرة بما فيها تعديل نص المادة ٩ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، وهي =

إلا أن هذا القول مردود عليه بأن المشرع الإماراتي يسعى كغيره من المشرعين العقابيين إلى حماية مجتمعه من خلال رسم ضوابط لممارسة هذه الحرية بما يتوافق مع سياسته الطموحة- إن جاز وصفنا لها- التي ترمي أيضاً وبموجب الدستور إلى ضمان تحقيق الموازنة بين حقوق سكان الاتحاد وواجباتهم المفروضة عليهم، وكان ذلك جلياً في المادة ٤٤ التي تعد ضابطاً لهذه الموازنة، حيث نصت على أن: «احترام الدستور والقوانين والأوامر الصادرة من السلطات العامة تنفيذاً لها ومراعاة النظام العام واحترام الآداب العامة، واجب على جميع سكان الاتحاد».

فغاية المشرع من هذا النص- وفق اعتقادنا- جاءت أيضاً لضمان حماية كيان الدولة ومقوماتها الأساسية من أي تأثيرات تنال منها، فالمشرع الإماراتي كغيره من المشرعين لن يقبل بثورة فيسبوك تحت غطاء حرية التعبير عن الرأي والفكر، وشواهد العصر كفيلة بالرد على ما تثيره شبكات التواصل الاجتماعي وغيرها من زعزعة لأمن الدول كافة، فسياسة اتخاذ التدابير الوقائية بحجب المواقع الإلكترونية المشبوهة ومواجهة الحسابات المضللة والوهمية التي تتخذ لنفسها منبراً لحرية التعبير عن الرأي والفكر وهي في حقيقتها مصدرٌ أساء استعمال هذا الحق بأن تم استخدامه لبث حالة الفوضى الإلكترونية وتأجيج الشارع من خلال نشر وبث الآراء المسمومة وإفساد عقول المستخدمين لاسيما الصغار منهم، وهذه السياسة ليست مقتصرة على دولة الإمارات فحسب؛ بل هي سياسة تتبعها جميع دول العالم، لاسيما وأن دولة الإمارات تحظى بمراكز متقدمة عالمياً في مؤشر التنافسية العالمية من بينها أداء مؤشر الأمن السيبراني[٣٩].

وعلى أية حال؛ فإن المشرع الإماراتي كان واضحاً في صياغته لنص المادة ٩ والتي انفرد بها عن غيره من المشرعين، إذ لم يترك البوابة مفتوحة- كما قلنا- للجريمة، بل حرص المشرع على الموازنة بين حرية استخدام الإنترنت والولوج في دائرة الجريمة، حيث جعل المشرع العقاب مقصوراً على من يتحايل على العنوان البروتوكولي فقط بقصد

= تحتل المرتبة ١٣ من بين الدول العربية في مؤشر حرية الإنترنت لعام ٢٠١٦. راجع: التقرير السنوي للمركز الدولي للعدالة بجنيف لعام ٢٠١٧:
http://echr.org.uk/ar/almnshwrat/aldwly-lldalt-astmrar-alanthakat-lhqwq-alansan-balamarat-wtjrym-almdafyn-nha

راجع: مؤشر حرية الإنترنت على الرابط التالي:
https://www.sasapost.com/internet-freedom-index-2016/

(٣٩) احتلت دولة الإمارات العربية المتحدة في مؤشر التنافسية لعام ٢٠١٨ المرتبة الأولى على المستوى الإقليمي والمرتبة السابعة على المستوى العالمي. للمزيد من التفاصيل راجع:
https://www.albayan.ae/across-the-uae/news-and-reports/2018-05-24-1.3273214

ارتكاب جريمة جنائية أياً كان شكلها، وبمفهوم المخالفة فإن العقوبة لن تطال من يتحايل على العنوان البرتوكولي دون قصد ارتكاب جريمة معينة.

المطلب الثاني

أركان تجريم التحايل على العنوان البروتوكولي ونطاق المسؤولية الجنائية عنها

كل جريمة جنائية تتطلب فضلاً عن ركنها الشرعي الذي آنفنا ذكره، ضرورة توافر ركنين آخرين هما الركن المادي والركن المعنوي، ويسبق توافر هذه الأركان بطبيعة الحال ضرورة تحقق شرط مفترض تقرره أحكام المرسوم بقانون رقم ٥ لسنة ٢٠١٢، وهو ارتكاب الجريمة بواسطة إحدى أدوات تقنية المعلومات لسريان أحكامه.

أولاً: الشرط المفترض

الشرط المفترض كما عرفه بعض فقهاء القانون الجنائي بأنه الشرط الذي يفترض القانون وجوده قبل أو وقت مباشرة الجاني نشاطه، وبغيره لا يمكن وصف السلوك بأنه جريمة[٤٠]. ويتمثل الشرط المفترض هنا في الحالة التي يتطلبها القانون، أي اشتراط أدوات تقنية المعلومات والشبكة المعلوماتية.

فالقاسم المشترك بين جميع الجرائم الواردة في أحكام هذا القانون هو استخدام الجاني تلك الأدوات في تنفيذ الأنشطة الإجرامية سواء أكان محل الاعتداء من البيئة ذاتها ونقصد الشبكة المعلوماتية باعتبارها البيئة الحاضنة التي تربط كل الوسائل التقنية في مضمار واحد من بينها أعماق شبكة الإنترنت، أم كان محل الاعتداء تقليدياً يتضمن حقوقاً ومصالح محمية قد تقع على الأشخاص كالتهديد والابتزاز أم على الأموال كانتحال شخصية الغير في أبسط صورها، وإلى غير ذلك من نماذج أخرى تكون فيها الوسيلة المعلوماتية مجرد أداة لتنفيذ الجريمة.

لذلك تفترض جميع الجرائم المنصوص عليها في أحكام هذا القانون استخدام أدوات تقنية المعلومات من أجل ارتكاب النشاط الإجرامي، وهو ما ينصرف إليه موضوع دراستنا؛ إذ لا يمكن الولوج إلى شبكة الإنترنت والتحايل في عنوانه إلا بواسطة تلك الأداة، وبالتالي إذا انتفى هذا الشرط لا مجال للقول بتطبيق حكم المادة ٩ لانتفاء الأداة المستخدمة، وأيضاً كونها الأساس الذي يعول عليه في تطبيق هذا القانون .

(٤٠) د. محمود محمود مصطفى، شرح قانون العقوبات، طبعة ١٠، القسم العام، دار النهضة العربية، القاهرة، ١٩٨٣. ص٣٨.

ثانياً: الركن المادي

بالنسبة للركن المادي فقد لاحظنا أن المشرع حدد شكل التجريم بأن قيده في قيام الجاني بارتكاب سلوك التحايل على العنوان البروتوكولي، ولا يتأتى ذلك إلا باستخدام إحدى أدوات تقنية المعلومات أو برامجها كما وضحنا آنفاً.

وهذا السلوك يتصف بحذاقة الجاني لقدرته وإتقانه في ارتكاب السلوك الإجرامي المتمثل في التحايل عبر أدوات تقنية المعلومات أو برامجها، فهو لا يستهدف أشخاصاً بشكل مباشر بل يستهدف شبكة افتراضية عبر شبكة الإنترنت، وبالتالي يخرج من نطاق التجريم متى كان التحايل على موضوع آخر غير العنوان البروتوكولي، كالتحايل على النظام الإلكتروني للحاسوب الآلي أو التحايل على الهاتف المحمول، أو غير ذلك من طرق تكون المادة ١١ واجبة التطبيق على وقائعها متى توافرت شروطها. والنتيجة في هذه الجريمة لها مدلول قانوني يتمثل في الخطر الذي قد يلحق مصلحة المجتمع بسبب سلوك التحايل، فالتجريم الذي سعى إليه المشرع هو حماية تلك المصلحة من احتمال تعرضها للخطر، فلم يشترط ضرراً فعلياً عليها.

والسؤال الذي يطرح نفسه في هذا المقام هو متى يكون التحايل على العنوان البروتوكولي جريمة خاضعة لحكم المادة ٩ من قانون مكافحة جرائم تقنية المعلومات؟

الأصل- كما وضحنا- أن التحايل على العنوان البروتوكولي ليس جريمة بحد ذاته؛ لأن المستخدم فقط يلجأ إلى تغيير عنوانه البروتوكولي واستبداله بآخر، خصوصاً أن العنوان البروتوكولي ليس ثابتاً في جميع الأحوال، بل هناك برامج أو تطبيقات تجعل هذه العناوين متغيرة، فتمنح المستخدمين بموجب ذلك عناوين تعريفية مختلفة أيضاً؛ لذلك حدد المشرع طرق التحايل المجرمة، وهي إما:

أولاً: استخدام الجاني عنواناً وهمياً أي عنواناً تعريفياً لا يعود لشخصية حقيقية بل شخصية مستحدثة أو مستعارة أو وهمية يختبئ وراءها[٤١]، فالبعض يلجأ إلى استخدام برامج معينة كنا قد سلطنا الضوء عليها سابقاً لتغيير عنوانه أو استبدالها كاستخدام خدمات شبكة VPN لتشفير اتصالاته بغية إخفاء أو استبدال عنوانهم التعريفي بآخر.

(٤١) مقال منشور على مدونة جديد الإنترنت، وهو بعنوان/ إنشاء الكثير من الحسابات المزيفة على الفيسبوك بطريقة شرعية وبدون بريد إلكتروني، راجع الرابط الإلكتروني التالي:
http://newinternt.blogspot.com/2015/09/blog-post_19.html

ثانياً: استخدام الجاني عنواناً تعريفياً يعود لشخص آخر، أي انتحال عنوانه البروتوكولي كاستخدام موقع Iplogger على سبيل المثال، الذي يمكن المستخدم من تحديد هوية الشخص ومن ثم نسخ عنوانه، ليبدو وكأنه المستخدم. والصورة الأخيرة تحديداً تظهر لنا مدى قدرة الجاني المعرفية في التلاعب من خلال نسخ العنوان البروتوكولي العائد إلى شخص معين، فالأمر هنا لا يتعلق بصورة أو عنوان سكن أو بريد إلكتروني أو غير ذلك مما يمكن أن ينفذه المستخدم العادي، بل الموضوع يميل إلى الدقة في إتمام الجريمة.

ونلاحظ في هذا الجانب أن المشرع توسع في طرق التحايل على العنوان البروتوكولي بدلالة العبارة التي أوردها في النص «أو بأي وسيلة أخرى»، مستدركاً بذلك ما قد يظهر في المستقبل من أدوات أو برامج أو تطبيقات جديدة تمكن المستخدمين من إخفاء هويتهم أمام المستخدمين الآخرين، وأيضاً صعوبة تحديدهم من قبل جهات التحقيق.

ولم يحدد المشرع صفة القائم على ارتكاب جريمة التحايل على العنوان البروتوكولي، فيستوي وقوعها ممن لديه صفة الموظف من عدمه، ومن جانبنا نرى ضرورة الإشارة إلى الموظف سواء أكان في القطاع العام أم الخاص، واعتبارها ظرفاً مشدداً للعقاب إذا ارتكب هذا النشاط.

وتعتبر مواقع التواصل الاجتماعي بكافة أنواعها من النماذج الشبكية التي قد تمكن المسيئين من التحايل على العنوان البروتوكولي إما بإنشاء حساب وهمي، وقد كان موقع الفيسبوك من بين مواقع التواصل الاجتماعي التي تمتلئ بحسابات وهمية، هذا إلى جانب إمكانية استغلال المخترقين حسابات تعود لأشخاص آخرين في هذه المواقع أو الشبكات بسبب ثغراتها الأمنية، ويستطيع المستخدم العادي أيضاً إنشاء حساب وهمي على أي شبكة تواصل دون تحديد بياناته الشخصية[٤٢].

ثالثاً: الركن المعنوي

الركن المعنوي هو الركن الذي يتعلق بالكيان النفسي أو الداخلي للمستخدم لحظة ارتكاب سلوكه؛ فقد اشترط المشرع لقيام الجريمة أن يكون التحايل على العنوان

(٤٢) مقال منشور على مدونة جديد الإنترنت، وهو بعنوان/ إنشاء الكثير من الحسابات المزيفة على الفيسبوك بطريقة شرعية وبدون بريد إلكتروني، راجع الرابط الإلكتروني التالي:
http://newinternt.blogspot.com/2015/09/blog-post_19.html

الإلكتروني إما بقصد ارتكاب جريمة جنائية، بصرف النظر عما إذا كانت منصوصاً عليها في هذا القانون أو في أي قانون آخر، أو كان التحايل بقصد إخفاء آثارها، كمحو أو إخفاء المحتوى المعلوماتي من صور أو محادثات أو نصوص تتعلق بالجريمة، وينصرف مفهوم الإخفاء أو التستر إلى الإخفاء أو التستر على جناة آخرين لهم علاقة بالجريمة.

فالواضح أن جريمة التحايل على العنوان البروتوكولي من قبيل الجرائم العمدية، التي لا يمكن تصور وقوعها على خلاف ذلك؛ لأن لفظ التحايل يشير بحد ذاته إلى تعمد الجاني ارتكاب السلوك محل التجريم، ومن ثم تأخذ صفة العمد صورة القصد الجنائي العام القائم على عنصرين رئيسيين هما العلم والإرادة.

أما بالنسبة لعنصر العلم ويعني علم الجاني بأنه يخفي هويته بإحدى الطرق المبينة باستخدام أدوات تقنية المعلومات، كعلمه بأن هذا البرنامج من شأنه تشفير البيانات، وعلمه أيضاً بأن ذلك سيمكنه من ارتكاب جريمته دون الكشف عن هويته، أو إخفاء آثارها للحيلولة دون اكتشاف آثارها أو الكشف عن جناة آخرين، وبالتالي لا تقوم الجريمة قبل من اتصل عبر شبكة الإنترنت، وترتب على ذلك منحه عنواناً مغايراً لعنوانه الأصلي. أما الإرادة فتعني اتجاه إرادة الجاني بعد توافر العلم بها نحو تحقيق جريمته، فإذا انصرفت إرادته نحو أمر آخر على خلاف ما ورد في ذيل النص وهو عزمه على ارتكاب جريمة أو الحيلولة دون كشفها، فإن الجريمة لا تتحقق.

ولا أهمية للباعث أو الغرض على ارتكاب الجريمة، إذ لا يعتد القانون به في تكوين القصد الجنائي، وبالتالي يستوي أن يكون الباعث على ارتكابها شريفاً أو خبيثاً، طالما توافرت عناصر القصد على النحو السالف ذكره.

وتقدير قيام القصد الجنائي في هذه الجريمة من عدمه، وأيضاً تقدير أدلتها من المسائل التي تستقلها محكمة الموضوع دون معقب عليها.

المطلب الثالث

المسؤولية الجنائية والعقوبات والتدابير المقررة

على ضوء ما تقدم، فإن المسؤولية الجنائية للمستخدم تتحقق متى تحايل بقصد ارتكاب جريمة، وثمة أشخاص قد يساهمون في ذلك، ونقصد مزود الخدمة الذي قد يكون له دور في الجريمة، وتتحدد مسؤوليته استناداً لهذا الدور؛ لذلك سنتحدث في هذا المطلب عن نطاق المسؤولية الجنائية للمستخدم ومزود الخدمة، ثم بعد ذلك نبين العقوبات والتدابير المقررة.

أولاً: نطاق المسؤولية الجزائية

لا إشكال حول تحديد نطاق المسؤولية الجنائية للمستخدم في جريمة التحايل إذ يمكن الوقوف على مسؤوليته الشخصية بمجرد ثبوت ارتكاب جريمة بعد تحايله على العنوان البروتوكولي عملاً بمقتضى المادة ٩، ولكن الحديث يأخذ منحى آخر عن دور مزود خدمة الإنترنت (ISP)[٤٣]عن المخالفات التي قد ترتكب في محيطه أو في خوادمه، إذ لا يمكن تحديد هوية المستخدم المتحايل إلا من خلاله، فالمزود يملك قدرة فنية لتحديده لأنه هو من يسمح بالاتصال بشبكة الإنترنت عبر خوادمه. وإذا كانت مسؤولية المتحايل تتحدد بموجب ما ورد في حكم المادة ٩ ، فما هو إذن نطاق مسؤولية مزود الخدمة ؟ وهل تمتد مسؤوليته إلى عدم التزامه بتحديد هوية المستخدمين لديه ؟

لم يعرف المشرع الإماراتي المقصود بمزود خدمات الإنترنت حتى في تشريعه المُلْغِي الصادر سنة ٢٠٠٦، وقد عرفه المشرع الأوروبي في البند (C) من المادة الأولى في اتفاقية بودابست الصادرة ٢٠٠١ بشأن الجرائم المعلوماتية، حيث نصت على أن: «١. مقدم الخدمة يشير إلى كل كيان عام أو خاص يقدم لمستخدمي الخدمة إمكانية الاتصال عن طريق نظام معلوماتي. ٢. كل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلاً من خدمة الاتصال أو نيابة عن مستخدمي هذه الخدمة»[٤٤]. كما عرفته الاتفاقية العربية الصادرة سنة ٢٠١٠ بشأن مكافحة جرائم تقنية المعلومات بصياغة مشابهة لما جاء في الاتفاقية الأوروبية[٤٥].

وفي هذا الإطار نؤيد ما ذهب إليه جانب من الفقه من أن مفهوم مزود الخدمة قد تطور مع الطفرة التقنية المتلاحقة، حيث تجاوز نشاطه ليشمل إنشاء المنتديات والمواقع

---

(٤٣) (ISP) اختصاراً لعبارة Internet service provider وهي الشركات والمؤسسات التي تقدم خدمة الاتصال مع شبكة الإنترنت لقاء رسم اشتراك معين. د. منال البلقاسي، المرجع السابق، ص٧٢. وانظر أيضاً في المفهوم ذاته لدى كل من:
Peter Carey,op, cit, P18. And Donn B. Parker.op, cit, P89.

(٤٤) Article 1 –Definitions ….(c) "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and; ii- any other entity that processes or stores computer data on behalf of such communication service or users of such service'.

(٤٥) نص البند الثاني من المادة الثانية للاتفاقية العربية على أنه: «٢. مزود الخدمة: أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها».

والحسابات وإدارتها وتوريد المحتوى، أي أن مزود الخدمة يمارس عدة مهام في شبكة الإنترنت[٤٦]، فقد كانت في السابق تقام من قبل عدة جهات أو أشخاص في ذات البيئة[٤٧].

والحقيقة أن هذا المفهوم ينسجم تماماً مع ما ذهب إليه المشرع الإماراتي في إطار المادة ٣٩ من المرسوم بقانون محل البحث، حيث كانت صيغته موجهة إلى مالك الموقع أو مشغل الخدمة باعتبارهما مزودين للخدمة، وقد نصت هذه المادة على أنه: «يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين أي مالك أو مشغل لموقع إلكتروني أو شبكة معلوماتية خزن أو أتاح متعمداً أي محتوى غير قانوني ، مع علمه بذلك، أو لم يبادر بإزالة أو منع الدخول إلى هذا المحتوى غير القانوني، خلال المهلة المحددة في الإشعار الخطي الموجه له من الجهات المختصة، والذي يفيد بعدم قانونية المحتوى وأنه متاح على الموقع الإلكتروني أو شبكة المعلوماتية».

بالنظر إلى هذا النص نجده يقرر مسؤولية مزود الخدمة تجاه المحتوى المعلوماتي الذي ينشر أو يبث عبر الشبكة المعلوماتية، وقد حدد المشرع نطاق مسؤوليته في حالتين: الأولى إذا خزن المحتوى غير القانوني أو أتاحه للجمهور بنشره أو بثه عمداً سواء بنفسه أو بواسطة مستخدم مشترك لديه، ولا مناص في مثل هذه الأحوال من اعتبار المزود شريكاً في الجريمة المرتكبة عبر موقعه أو حسابه أو في بيئته متى ثبت علمه بطبيعة المحتوى، وذلك عملاً بمقتضى نص المادة ٤٥ من قانون العقوبات الاتحادي، حيث يتوافق سلوك المزود مع ما جاء في البند الثالث من المادة ٤٥ من مساعدة الفاعل عمداً بأي طريقة

(٤٦) مزود الخدمة مصطلح يطلق على كل من يقدم خدمة في بيئة شبكة الإنترنت، هناك عدة مزودين في بيئة الإنترنت، مزود خدمة الوصول ومورد معلومات ومتعهد إيواء. للمزيد من التفاصيل راجع: د. محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، الطبعة الأولى ٢٠١٦، دار النهضة العربية، القاهرة، ص١٣.

(٤٧) مزودو خدمة الإنترنت بحسب طبيعة العمل كانوا عدة جهات أو أشخاص يتعاملون مع المعلومات ونقلها إلى شبكة الإنترنت بموجب عقود بينهم تحدد التزاماتهم، وكان من يتولى خدمة الوصول إلى شبكة الإنترنت يطلق عليه متعهد الوصول، ومن يتولى نقل المحتوى إلى الشبكة يطلق عليه متعهد نقل المحتوى، ومن يستضيفها أي يأوي المحتوى المعلوماتي يطلق عليه متعهد الإيواء أو متعهد الاستضافة، وهناك أيضاً بحسب طبيعة العمل وتقسيمه من يقوم بتوريد المحتوى والذي قد يكون من بينهم المؤلف. وتختلف طبيعة تقسيماتهم بحسب ما تناوله الفقه، للمزيد من التفاصيل حول تقسيمات مزودي الخدمة وطبيعة أعمالهم راجع: د. حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها-دراسة مقارنة، طبعة أولى ٢٠١٧، مكتبة بدران الحقوقية، لبنان، ص٥٣٨ وما بعدها. وراجع أيضاً: في المراجع الإنجليزية لدى: Chris Reed, op, cit, P305. وراجع تعريف مزود خدمات الإنترنت في الفقه الفرنسي لدى :
Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haidara. Op, cit, P109 et P350.

أخرى في الأعمال المجهزة أو المسهلة أو المتممة لارتكاب الجريمة[٤٨]. ويختلف الموقف إذا كانت مشاركته بالتدخل عمداً كتوفير تطبيقات خاصة للتحايل، فإن المزود يسأل بوصفه فاعلاً أصلياً، عملاً بمقتضى المادة ٤٤ من قانون العقوبات. أما الحالة الثانية وتتمثل في عدم قيام مزود الخدمة بإزالة المحتوى أو منع الدخول إلى هذا المحتوى (حجبه) بعد إشعاره بمضمونه غير القانوني من قبل الجهات المختصة، وهي وفق ما ورد في المادة الأولى الجهات الاتحادية أو المحلية المعنية بشؤون الأمن الإلكتروني في الدولة.

وفي كلتا الحالتين سيخضع مزود الخدمة للعقوبة المنصوص عليها في المادة ٣٩ من المرسوم محل البحث. ولم يتناول في هذا الجانب مسؤولية مزود الخدمة عن عدم إبلاغ السلطات المختصة عن المخالفات إذا علم بنفسه أو بالإنذار الموجه إليه من الجمهور حول طبيعة المحتوى غير القانوني. كما لم يتناول مسؤوليته بشأن إخلاله بالحماية الفنية أو التقنية اللازمة لنظامه، وإلى غير ذلك من التزامات لم يشأ المشرع تحديدها على الرغم من أهميتها في بيئة الإنترنت.

هذا إلى جانب أن المشرع لم يُشر إلى التزام مزود الخدمة بتمكين السلطات المختصة من تحديد هوية المستخدم الذي ارتكب جريمة في موقعه أو حسابه، أو بمعنى آخر عدم تعاونه مع السلطات المختصة؛ ذلك أن ما نص عليه المشرع صراحة في المادة ٤٩ إنما يقتصر على إلزام السلطات المحلية بالإمارات تقديم التسهيلات اللازمة للموظفين (صفة الضبط القضائي) الذين يصدر بشأنهم قرار بتمكينهم من القيام بعملهم خصوصاً أعمال الاستدلال والتفتيش.

وقد تناول المشرع الأوروبي هذا الالتزام في عدة مواضع في الاتفاقية الأوروبية، حيث ألزم دول الأعضاء باتخاذ تدابير تشريعية بغية تمكين سلطاتها من القيام بواجباتهم، فقررت إجبار مزود الخدمة على التعاون مع الجهات المختصة، وتمكين السلطات من القيام بواجباتها بالبحث عن البيانات المخزنة في النظام المعلوماتي ومصادرتها (المادة ١٩)، وبجمع بيانات النظام المعلوماتي (المادة٢٠)، واعتراض المحتوى فيما يتعلق بنطاق الجرائم الجسيمة (المادة ٢١).

---

(٤٨) تنص المادة ٤٥ على أنه: «يعد شريكاً بالتسبب في الجريمة:
أولاً: من حرض على ارتكابها فوقعت بناء على هذا التحريض.
ثانياً: من اتفق مع غيره على ارتكابها فوقعت بناء على هذا الاتفاق.
ثالثاً: من أعطى الفاعل سلاحاً أو آلات أو أي شيء آخر استعمله في ارتكاب الجريمة مع علمه بها، أو ساعد الفاعل عمداً بأي طريقة أخرى في الأعمال المجهزة أو المسهلة أو المتممة لارتكاب الجريمة.
وتتوفر مسئولية الشريك سواء أكان اتصاله بالفاعل مباشرة أم بالواسطة».

وقد نظمت الاتفاقية هذه الإجراءات في المادة ١٤ بشأن نطاق تطبيق تلك الأحكام، حيث أجازت الاتفاقية لدول الأعضاء مد نطاق تطبيق هذه العمليات في الجرائم المنصوص عليها في الاتفاقية ما لم تتعارض تلك الإجراءات مع قوانينها الداخلية. وقد أجازت المادة ١٥ من الاتفاقية أن تسعى دول الأعضاء إلى وضع شروطٍ وضمانات لتطبيق هذه الأحكام من قبل السلطات المختصة دون الإخلال بما ورد ببنود اتفاقية مجلس أوروبا لعام ١٩٥٠ بشأن حماية حقوق الإنسان واحترام الغير من صكوك دولية وإقليمية أخرى.

ولم تختلف منهجية المشرع العربي في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث تبنى الأحكام الإجرائية ذاتها التي تمكن السلطات المختصة من القيام بمهامها في التحفظ على البيانات المخزنة، وأيضاً البيانات المتعلقة بتتبع المستخدمين (المادة ٢٣)، وإصدار الأوامر بتسليم المعلومات (المادة ٢٥)، وتفتيش البيانات المخزنة (المادة ٢٦)، وضبط المعلومات (المادة ٢٧)، والجمع الفوري لمعلومات تتبع المستخدمين (المادة ٢٨)، واعتراض المحتوى (المادة ٢٩).

أما بالنسبة للمشرع الإماراتي فقد حرص في بيان المادة ٤٧ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ على امتداد تطبيق أحكام المرسوم على كافة الجرائم التي من خارج حدود الدولة[٤٩]، وأشار في المادة ٤٩ إلى صلاحيات مأموري الضبط القضائي لمواجهة آثارها داخل إقليم الدولة، حيث ألزم المشرع السلطات المحلية بتسهيل مهامهم في البحث دون الإشارة إلى صلاحياتهم خارج حدود الدولة[٥٠]، إلا أن هذه الصلاحيات تجد مكانها في القانون رقم ٣٩ لسنة ٢٠٠٦ بشأن التعاون القضائي الدولي في المسائل الجنائية.

ثانياً: العقوبات المقررة

شدد المشرع على عقوبة جريمة التحايل عبر العنوان البروتوكولي في أول تعديل أجري على أحكام المرسوم بقانون اتحادي رقم ٥ لسنة٢٠١٢بشأن مكافحة جرائم تقنية

(٤٩) تنص المادة ٤٧ على أنه: «مع عدم الإخلال بأحكام الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات، تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة ، إذا كان محلها نظاماً معلوماتياً إلكترونياً أو شبكة معلوماتية أو موقعاً إلكترونياً أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منهما».

(٥٠) تنص المادة ٤٩ على أنه: «يكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل صفة مأموري الضبط القضائي في إثبات الأفعال التي تقع بالمخالفة لأحكام هذا المرسوم بقانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم».

المعلومات[٥١]، حيث قرر المشرع في المرسوم بقانون اتحادي رقم ١٢ لسنة ٢٠١٦ [٥٢] اعتبار هذه الجريمة من قبيل الجنايات بعدما كانت من الجنح[٥٣].

والجدير ذكره في هذا المقام أن هذا التعديل جاء مقتصراً فقط على حكم المادة ٩ دون غيرها؛ مما يضعنا أمام تصور استشعار المشرع خطورة هذه الجريمة.

وقد فرض المشرع الإماراتي على مرتكبي جريمة التحايل على العنوان البروتوكولي عقوبات أصلية وعقوبات تبعية، أما العقوبات الأصلية فتتمثل في عقوبة سالبة للحرية وهي عقوبة السجن المؤقت، وعقوبة مالية وهي عقوبة الغرامة المالية، ونلاحظ أن المشرع قد ترك تحديد مدة عقوبة السجن المؤقت للقواعد العامة التي تقرر أن مدة السجن ما بين ثلاث سنوات كحد أدنى، وخمس عشرة سنة كحد أقصى.

أما بالنسبة لعقوبة الغرامة فقد جعلها المشرع وفقاً للنص بين حدين: حد أدنى لا يقل عن خمسمائة ألف درهم، وحد أقصى لا يتجاوز مليوني درهم أو بإحدى هاتين العقوبتين.

وللقاضي سلطة تقديرية عند توقيع العقاب؛ إذ أجاز له النص إما الجمع بين عقوبة السجن المؤقت والغرامة المالية أو الحكم بإحداها. ولا يخل ذلك- وفق ما تقرره المادة ٤٨ من المرسوم ذاته- بالحكم على الجاني بأي عقوبة أشد ينص عليها في قانون العقوبات، أو أي عقوبة ينص عليها قانون آخر.

فضلاً عن ذلك، أجاز المشرع للمحكمة أن تحكم بعقوبات تكميلية عملاً بنص المادة ٤١ والتي جاء فيها أنه: «مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة».

---

(٥١) تنص المادة ٩ قبل التعديل على أنه: «يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين 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».

(٥٢) صدر هذا التعديل بتاريخ ٢٣ مايو ٢٠١٦ راجع الموقع الإلكتروني لوزارة العدل على الرابط التالي: http://ejustice.gov.ae/downloads/latest_laws2016/unionlaw12_2016_5_2012.pdf

(٥٣) عرف المشرع عقوبة الجناية في المادة ٢٨ عقوبات اتحادي، حيث نصت على أن: «الجناية هي الجريمة المعاقب عليها بإحدى العقوبات الآتية: ١. أية عقوبة من عقوبات الحدود أو القصاص فيما عدا حدي الشرب والقذف. ٢. الإعدام. ٣. السجن المؤبد. ٤. السجن المؤقت».

والواضح أن هذه العقوبات أراد المشرع بها أن تكون بمثابة مانع قد يحول إقرارها دون استعمال أدواتها في ارتكاب الجرائم عبرها بالمستقبل، وهي بحسب الترتيب المصادرة أو محو المحتوى غير المشروع بإتلافها. كما يحكم بإغلاق المحل أو الموقع الإلكتروني، ويندرج ضمن مفهوم الموقع الحسابات عبر مواقع التواصل الاجتماعي سواء أكان هذا الإغلاق كلياً أم جزئياً، وقد وردت هذه العقوبة في المادة ٨٢ من قانون العقوبات الاتحادي[٥٤].

وقد اشترط المشرع عند الحكم بهذه العقوبات عدم الإخلال بحقوق الغير حسني النية، أي عدم المساس بحقوق أشخاص لا يستحقون تلك العقوبة لانقطاع صلتهم بالجريمة، كأن يكون جهاز الحاسوب الآلي أو الهاتف المحمول خاصاً بوالد الابن الذي ارتكبت الجريمة من خلال جهازه، أو كان الجهاز خاصاً بمقهى إنترنت وإلى غير ذلك.

ثالثاً: التدابير الجنائية

فرض المشرع الإماراتي تدابير جنائية على مرتكبي جرائم تقنية المعلومات، والتدابير الجنائية عبارة عن مجموعة من الإجراءات التي تهدف إلى منع وقوع الجريمة مستقبلاً، ومن بين التدابير التي حرص المشرع الإماراتي على تناولها في إطار هذا المرسوم هو تدبير إبعاد الأجنبي عن الدولة[٥٥]، فقد قرر في نص المادة ٤٢ من المرسوم بقانون اتحادي في شأن مكافحة جرائم تقنية المعلومات أنه: «مع مراعاة حكم الفقرة الثانية من المادة (١٢١) من قانون العقوبات، تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون، وذلك بعد تنفيذ العقوبة المحكوم بها»[٥٦].

---

(٥٤) تنص المادة ٨٢ عقوبات على أنه: «تحكم المحكمة عند الحكم بالإدانة بمصادرة الأشياء والأموال المضبوطة التي استعملت فيها أو كان من شأنها أن تستعمل فيها أو كانت محلاً لها أو التي تحصلت من الجريمة . فإذا تعذر ضبط أي من تلك الأشياء أو الأموال، حكمت المحكمة بغرامة تعادل قيمتها ، وذلك كله دون الإخلال بحقوق الغير حسن النية».

(٥٥) لم تختلف سياسة المشرع الإماراتي في تقرير هذا التدبير، بل نقله المشرع من المرسوم بقانون رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات الملغى.

(٥٦) عدلت هذه المادة مؤخراً بموجب المرسوم بقانون رقم ٢ لسنة ٢٠١٨ بشأن تعديل بعض أحكام المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، ويعتبر ثاني تعديل لأحكام هذا القانون. وقد صدر بتاريخ ٢٤ يوليو ٢٠١٨م، راجع الموقع الإلكتروني لوزارة العدل في دولة الإمارات العربية المتحدة على الرابط التالي: http://zayedalshamsi.ae/ar/2018/08/30/ مرسوم-بقانون-اتحادي-رقم-٢-لسنة-٢٠١٨-بتعديل-ب/
تجدر الإشارة إلى أن هذه المادة كانت تقرر قبل التعديل إبعاد الأجنبي إذا ارتكب أي جريمة من الجرائم المنصوص عليها في المرسوم بقانون محل البحث، وتوقيعها يكون وجوبياً على المحكمة سواء أكانت الجريمة المرتكبة من قبيل الجنايات أم الجنح، وسواء أكانت العقوبة سالبة للحرية أم غرامة مالية.

وبهذا النص؛ نجد أن غاية المشرع تتجه نحو ردع الأجانب الذين يستهينون بقوانين الدولة والقيم السائدة في المجتمع الإماراتي، وقد ربط المشرع هذا التدبير بالخطورة الإجرامية لدى الأجنبي الذي يعيش في دولة الإمارات وقد أساء استخدام أدوات تقنية المعلومات أو الشبكة المعلوماتية، وترتب عليها وقوع إحدى الجرائم المنصوص عليها في هذا القانون، وهو بالتالي يعد من قبيل الأشخاص غير المرغوب فيهم في الدولة.

واستناداً إلى ذلك فقد أوجب المشرع على المحكمة مراعاة ما جاء في حكم المادة ١٢١ من قانون العقوبات الاتحادي(٥٧)، بأن ألزمها بإيقاع هذا التدبير إذا كانت الجريمة المرتكبة من قبل الأجنبي تعد من قبيل الجنايات المقيدة للحرية، أما إذا كانت من قبيل جرائم الجنح فإنه يجوز للمحكمة أن تأمر بإبعاده عن الدولة فوراً بدلاً من توقيع عقوبة سالبة للحرية. وقد استثنى المشرع من تطبيق هذا الحكم متى كان الأجنبي زوجاً أو قريباً من الدرجة الأولى لمواطن إماراتي، ولا يسري هذا الاستثناء إذا كانت الجريمة من قبيل الجرائم الماسة بأمن الدولة. تطبيقاً لذلك إذا ارتكب الأجنبي جريمة التحايل على العنوان البروتوكولي المنصوص عليها في المادة ٩ من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، فإن إبعاده يكون وجوبياً تأسيساً على أن وصف الجريمة جناية، ما لم يتحقق الاستثناء الوارد في الفقرة الثانية التي تقيد المحكمة إذا تبين أن للأجنبي رباطاً أسرياً حتى الدرجة الأولى مع مواطن إماراتي، ففي هذه الحالة تمتنع المحكمة عن توقيع هذا التدبير.

وإذا كان التحايل على العنوان البروتوكولي بقصد ارتكاب جريمة أو جرائم ماسة بأمن الدولة من جهة الداخل أو من جهة الخارج باستخدام أدوات تقنية المعلومات أو الشبكة المعلوماتية، فإن القانون الواجب التطبيق هو قانون مكافحة جرائم تقنية المعلومات تحديداً في إطار المواد من ٢٤ وحتى ٣٢، فمتى ما تحققت إحدى هذه الصور بصرف النظر جناية كانت أم جنحة فإن تدبير إبعاده يكون وجوبياً.

---

(٥٧) نصت المادة ١٢١المعدلة بأحكام المرسوم بقانون اتحادي رقم ١٥ لسنة ٢٠٢٠ في شأن تعديل بعض أحكام قانون العقوبات الصادر سنة ١٩٨٧ على أنه: «إذا حكم على الأجنبي في جناية بعقوبة مقيدة للحرية وجب الحكم بإبعاده عن الدولة، ويجوز للمحكمة في مواد الجنح الأخرى أن تأمر في حكمها بإبعاده عن الدولة، أو الحكم بالإبعاد بدلاً من الحكم عليه بالعقوبة المقيدة للحرية.
واستثناء من نص الفقرة السابقة ومن أي نص ورد في أي قانون آخر، لا يجوز الحكم على الأجنبي بالإبعاد إذا كان زوجاً أو قريباً بالنسب من الدرجة الأولى لمواطن، وذلك ما لم يكن الحكم صادراً في جريمة من الجرائم الماسة بأمن الدولة».

خاتمة

في ختام البحث توصلنا إلى بعض النتائج التي نراها مفسرة لفلسفة المشرع العقابي الإماراتي والتي تتجه في مجملها إلى رسم سياسة فعالة لمواجهة الأساليب المستحدثة لجرائم تقنية المعلومات، وقد بنينا توصياتنا على تلك النتائج، نتناول أهمها تباعاً على النحو التالي:

أولاً: النتائج:

١ - العنوان البروتوكولي وفقاً للمفاهيم الحديثة يعد نموذجاً من نماذج البيانات الشخصية.

٢ - يعترف المشرع الإماراتي بمفهوم البيانات الشخصية ولكنه لم يعرفها ضمن المادة الأولى الخاصة بالتعريفات، كما أنه لم يتناولها في التشريعات الإلكترونية الأخرى، إلا أننا وجدنا أن تعريف البيانات الشخصية مدرج ضمن قانون دبي المالي العالمي رقم ١ لسنة ٢٠٠٧ بشأن حماية البيانات.

٣ - التحايل على العنوان البروتوكولي جريمة استحدثها المشرع الإماراتي، وهي من قبيل الجرائم الإيجابية.

٤ - يعد التحايل على العنوان البرتوكولي نافذة لارتكاب جرائم خطيرة عبر شبكتي الإنترنت العميق والإنترنت المظلم.

٥ - إن هذه الجريمة ذات طابع فني بحت لا تتم إلا عبر أدوات تقنية المعلومات أو بالأحرى عبر برامجها، كما أنها لا تتحقق إلا في بيئة الإنترنت، وتتصف بأنها من جرائم الوسيلة.

٦ - لم يهتم المشرع الإماراتي كثيراً بدور مزود خدمة الإنترنت على الرغم من أهميته في مواجهة العديد من الجرائم والتي من بينها جريمة التحايل على العنوان البروتوكولي.

ثانياً: التوصيات:

١ - المشرع الإماراتي بحاجة إلى إدراج مصطلح البيانات الشخصية وتعريفه ضمن المادة الأولى في المرسوم بقانون محل البحث والخاصة بالتعريفات، وضرورة الاعتراف بالعنوان البروتوكولي كأحد عناصر هذه البيانات.

٢ - المشرع الإماراتي بحاجة أيضاً إلى إدراج تعريف لمزود الخدمة في المادة الأولى، ونرى ضرورة تبني ما ذهب إليه المشرعان الأوروبي والعربي بشأن تحديد التزامات مزود خدمة الإنترنت ومسؤوليته القانونية تجاه تلك الالتزامات، وهذا بطبيعة الحال يحتاج إلى غربلة المادة ٣٩ من المرسوم بقانون محل البحث.

٣ - يُستبدل لفظ منع الدخول الوارد في المادة ٣٩ بلفظ آخر وهو الحجب؛ وذلك لشموليته وتوافقه مع المحتوى غير القانوني.

٤ - تبني الآلية الإجرائية الواردة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة سنة ٢٠١٠ في القاهرة، وبناء الاتفاقيات بموجبها.

مراجع البحث

أولاً: مراجع اللغة العربية

- أشرف جابر السيد، الجوانب القانونية لمواقع التواصل الاجتماعي، ٢٠١٣، دار النهضة العربية، القاهرة.
- إمام حسنين عطا الله، جرائم تقنية المعلومات في التشريعات والصكوك العربية، طبعة أولى-٢٠١٧- ١٤٣٩، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض.
- حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها-دراسة مقارنة، طبعة أولى ٢٠١٧، مكتبة بدران الحقوقية، لبنان.
- تشيلسي أيه لويس، التخفي: نظرة متعمقة في شبكة تور (شبكة تخفي) وآثارها على أمن الحاسوب وحرية الرأي والتعبير في العصر الرقمي، مجلة معهد دبي القضائية، العدد (٥)، السنة (٣)، فبراير ٢٠١٥، دولة الإمارات العربية المتحدة.
- علاء التميمي عبده، التنظيم القانوني للعنوان البروتوكولي الموقع الإلكتروني كأحد عناصر الملكية الصناعية ٢٠١٧، دار النهضة العربية، القاهرة.
- حمد أمين الرومي، ، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣.
- محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، الطبعة الأولى ٢٠١٦، دار النهضة العربية، القاهرة.
- محمود محمود مصطفى، شرح قانون العقوبات، طبعة ١٠، القسم العام، دار النهضة العربية، القاهرة، ١٩٨٣.
- مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى ٢٠١٦، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية.
- منال البلقاسي، شبكات وأمن المعلومات، طبعة أولى ٢٠١٩، دار التعليم الجامعي، الإسكندرية.

- وليد بن صالح، الإنترنت المظلم والعملات الافتراضية: التحديات الجديدة للقانون الجنائي، بحث منشور في المؤتمر السنوي الخامس الدولي بعنوان/ التحديات المعاصرة للضمانات القانونية في عالم متغير، ٩-١٠ مايو ٢٠١٩، الجزء الثاني، مجلة كلية القانون الكويتية العالمية، الكويت.

ثانياً: مراجع باللغة الإنجليزية

- Andrew Murray, Information Technology Law- The Law and Society, 3rd edition-2016, Oxford University Press, United Kingdom.
- Chris Reed, Computer Law, 7edition-2011, OXFORD UNIVERSITY, UK.
- Donn B. Parker. Fighting Computer Crime, a New Framework for Protecting Information, John Wiley & Son, New York, NY, USA ©1998.
- Klaus Von Lampe, Organized Crime, Analyzing illegal Activities, Criminal Structures and Extra-legal Governance, 2016, Sage.
- Michael Chertoff and Tobby Simon: The Impact of the Dark Web on Internet Governance and Cyber Security, Paper Series: No. 6 February 2015.
- Mohsin Qadir, "What is Spoofing?" An Average Internet User's Guide, March 31, 2018. PUREVPN.
- https://www.purevpn.com/blog/what-is-ip-spoofing-scty/
- https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402/
- Peter Carey, Data Protection- A Practical Guide to UK and EU Law, 5ed-2018, OXFORD UNIVERSITY PRESS, UK.

ثالثاً: مراجع باللغة الفرنسية

- Alain Bensoussan, Règlement européen sur la protection des données: Textes, commentaires et orientations pratiques, Édition : 2e

edition 2018, Bruylant,

- Fabrice Mattatia, Internet et les réseaux sociaux : que dit la loi ? 3e edition-2015, Eyrolles, Paris.
- Guillaume Desgens-Pasanau, La protection des donnees personnelles, 2edition-2016, LexisNexis, Paris.
- Ludovic Pailler, Les réseaux sociaux sur internet et le droit au respect de la vie privée, 2012, Larcier, Belgique.
- Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haidara. Droit des activites numeriques, 1Edition, 2014, Dalloz, Paris.

رابعاً: مصادر أخرى

- الموقع الإلكتروني لقناة سكاي نيوز العربية

https://www.skynewsarabia.com/technology/848802-عدد-الأجهزة-المتصلة-بالإنترنت-يفوق- سكان-الأرض

- الموقع الإلكتروني لمؤسسة لآيكان

http://archive.icann.org/tr/arabic.html

- الموقع الإلكتروني لصحيفة الاتحاد الإماراتية

https://www.alittihad.ae/wejhatarticle/99484/حماية-البيانات-الشخصية

- الموقع الإلكتروني للمركز الثقافي الأوروبي

https://rm.coe.int/16800cce5b

- الموقع الإلكتروني لمحكمة العدل الأوروبية

http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN#Footnote

- الموقع الإلكتروني مركز دبي المالي العالمي

http://www.difc.ae/download_file/49/196

- موقع المعاني الإلكتروني

https://www.almaany.com/ar/dict/ar-ar/ تحايل

- الموقع الإلكتروني الإمارات اليوم

https://www.emaratalyoum.com/business/local/2018-01-25-1.1065037

- الموقع الإلكتروني الاقتصادي

https://aliqtisadi.com/804988-الإمارات-تحارب-الجرائم-الإلكترونية/

- الموقع الإلكتروني لمدونة جديد الإنترنت

http://newinternt.blogspot.com/2015/09/blog-post_19.html

- الموقع الإلكتروني لوزارة العدل في دولة الإمارات العربية المتحدة

http://ejustice.gov.ae/downloads/latest_laws2016/unionlaw12_2016_5_2012.pdf

http://zayedalshamsi.ae/ar/2018/08/30/مرسوم-بقانون-اتحادي-رقم-٢-لسنة-٢٠١٨-بتعديل-ب/

- الموقع الإلكتروني لصحيفة البيان الإماراتية

https://www.albayan.ae/across-the-uae/news-and-reports/2018-05-24-1.3273214

The Crime of Spoofing the Protocol Address (IP) analytical study in the UAE penal legislation

Dr. Muaath Suleiman Al-Mulla

Abstract:

The UAE penal legislator is the only one to criminalize spoofing the protocol address in the framework of Federal Decree-Law No. 5 of 2012 regarding combating information technology crimes and its amendments, which is a philosophy that tends to control user behavior while using the Internet, especially since this behavior is a window for crossing into the deep and dark internet where There are criminal activities in all of their forms, including organized crime. In this research, we try to study the position of the Emirati penal legislator and show his philosophy in criminalizing this behavior and his desire to achieve effective protection for Internet users. On the protocol address down to some findings and recommendations.

Search vocabulary: Fraud - the protocol address - the dark and deep internet - crime - the UAE legislator.