اتجاهات المشرع العقابي الإماراتي في تعديلات قانون مكافحة جرائم تقنية المعلومات Attitude of UAE Penal legislator in Light of the Amendments to the Law on Combating Cybercrimes

Article · October 2019

DOI: 10.12816/0054860

CITATIONS

0

1 author:

Muaath Almulla

Police Academy of kuwait & Kuwait International Law School (KILAW)

6 PUBLICATIONS **0** CITATIONS

SEE PROFILE

اتجاهات المشرع العقابي الإماراتي في تعديلات المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات

العقيد الدكتور. مهاذ سليمان راشد الملا[1]

أستاذ القانون الجزائي المساعد بأكاديمية سعد العبد الله للعلوم الأمنية كلية الشرطة - الكويت

DOI: 10.12816/0054860

مستخلص

موضوع الدراسة: لم تكن مواجهة جرائم تقنية المعلومات يسيرة على دول العالم، ذلك أن الواقع التقني وضعنا أمام نموذج إجرامي مرن ومتجدد ساهم حتى في تطوير النموذج التقليدي للجريمة، فلم يكن أمام دول العالم سوى السعي الحثيث نحو تحصين مقوماتها الأساسية من خلال تطوير أدواتها التشريعية لضمان مواجهة فعالة لصنوف الإجرام عبر أدوات تقنية المعلومات وشبكات الاتصالات. وتعتبر دولة الإمارات العربية من الدول العربية التي رسمت سياسة واضحة منذ بداية الألفية لمواجهة هذه النوعية من الجرائم، فضلاً عما يتمتع به المشرع من مرونة منحته القدرة على المواجهة بإجراء تعديلات على الأحكام والقواعد القانونية.

أهداف الدراسة: نهدف في دراستنا الوقوف على جهود المشرع الإماراتي للحد من الآثار المدمرة لجرائم تقنية المعلومات وقراءة اتجاهاته من خلال التعديلات التي أجراها ومدى استيعابه لتطورات الحاصلة في البيئة الإلكترونية.

منهجية الدراسة: استعنا في هذه الدراسة بالمنهج التحليلي حيث استعرضنا نصوص التعديلات التي أجراها المشرع العقابي الإماراتي على المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

نتائج الدراسة: توصلت الدراسة إلى العديد من النتائج التي تضعنا أمام سعي المشرع إلى تحقيق التوازن بين حرية استخدام أجهزة تقنية المعلومات من قبل المستخدمين وضمان التزامهم بالقوانين المعمول بها بتشديد العقاب على انتهاكها.

مفردات البحث:

المشرع العقابي الإماراتي، تعديلات، جرائم تقنية المعلومات، العنوان البروتوكولي، الأبعاد تدابير، الإرهاب الإلكتروني، البيانات الشخصية.

1- **دكتور مهاذ سليمان راشد محمد الملا ضابط بوزارة الداخلية برتبة عقيد حقوقي، وأستاذ مساعد بأكاديمية سعد العبد الله للعلوم الأمنية – كلية القانون الكويتية العالمية، له العديد من الدراسات المنشورة وغير المنشورة، كما شارك في العديد من الفعاليات الأكاديمية والمجتمعية.**

Attitudes of UAE Penal Legislator in the light of the Amendments of Federal Decree -Law No. (5) of 2012 on Combatting Cybercrimes

Colonel Dr. Muaz Suleiman Al Mulla [1]

Assist Professor of Penal Code – Saad Al Abdullah Academy for Security Sciences
State of Kuwait.

DOI: 10.12816/0054860

Abstract

Countering cybercrimes is an arduous task given the flexibility and renewability of such crimes which went beyond the confines of traditional crime. In order to respond effectively to such crimes, countries had to seek tirelessly to enhance their counter legislative tools. United Arab Emirates is among the Arab countries that managed to develop a clear -cut policy since the beginning of the 2000s, blazing a trail in countering cybercrimes. It managed to counter such crimes by dint of its flexible legislations: UAE introduced amendments to legal provisions and rules. This study sheds light on amendments set out in Federal Decree -Law No. (5) of 2012 on Combatting Cybercrimes, in a bid to highlight the efforts made by UAE legislator to curb the devastating effects of cybercrimes, and to explore to what extent legislator took into account developments on both cyber and virtual spheres.

Keywords:

UAE Legislator – Cybercrimes – IP Address – Deportation – Counter- Terrorism Measures – Personal Information.

1- Dr. Muaz is a jurist Colonel at Ministry of Interior, and an assistant professor at Saad Al Abdullah Academy for Security Sciences – Kuwait International Law School. He published numerous studies, and took part in a host of academic and community events.

مقدمة:

أدركت دول العالم تماماً الأبعاد الخطيرة لأدوات تقنية المعلومات وشبكات الاتصالات على مصالحها ومقوماتها الأساسية، فعلى الرغم من مآثرها المميزة والجميلة في تطوير الحياة البشرية العلمية والعملية؛ إلا أنها كانت بالمقابل تعمق من جوانبها السلبية وعلى النحو الذي يجعلنا وبحق نعيش في حالة من الفوضى إلكترونية –إن جاز وصفنا– وكانت من أبرز سماتها اتساع دائرتي الانحراف والجريمة.

إزاء ذلك؛ واجهت دول العالم هذه الفوضى بتطوير أدواتها التشريعية التي وإن اختلفت سياستها في آلية المواجهة[1] واختلفت أيضاً في المسميات التي أطلقت على جرائمها[2]، إلا

1- أغلب تشريعات دول العالم اعتمدت على تخصيص قوانين تُعنى بمكافحة جرائم تقنية المعلومات، وتعتبر مملكة السويد أول الدول التي سنت تشريعاً يتعلق بمواجهة هذه النوعية من الجرائم وهو قانون حماية البيانات الصادر سنة 1973، وتلتها الولايات المتحدة الأمريكية بإصدار قانون حماية أنظمة الحاسوب الآلي سنة 1976، ثم تبعها قانون الحريات المعلوماتية الفرنسي 1978، ثم التشريع الإنجليزي في قانون مكافحة التزوير والتزييف سنة 1981 ثم تلتها كندا وهولندا وغيرها.

وعلى مستوى الدول العربية فقد كانت سلطنة عمان أول الدول التي عدلت أحكام قانون الجزاء رقم 7 لسنة 1974 وذلك بموجب المرسوم السلطاني رقم 2001/72، وكانت دولة الإمارات العربية المتحدة أول دولة تصدر تشريعاً خاصاً بجرائم تقنية المعلومات وهو المرسوم بقانون اتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات المُلْغى، ثم تلتها المملكة العربية السعودية في المرسوم الملكي رقم 17 لسنة 1428 هجرية كثاني دولة عربية واجهت هذه النوعية من الجرائم.

2- تفاوتت الأمم في إطلاق مصطلح ومفهوم موحد لهذه النوعية من الجرائم، فنجد بعض التشريعات تطلق عليها مصطلح الجرائم المعلوماتية وتشريعات أخرى تطلق عليها جرائم الحاسوب الآلي والإنترنت ومنهم من اكتفى بإطلاق مصطلح جرائم الإنترنت وتشريعات أخرى تبنت المفهوم الذي نراه صحيحاً إلى حد قريب وهو جرائم تقنية المعلومات وهو المصطلح الذي تبناه المشرع الإماراتي أو الجرائم الإلكترونية كالمشرع الأردني وإلى غير ذلك من مصطلحات أو مسميات عديدة تفاوتت ولم تجد حتى الآن سبيلاً لتوحيدها، ومردّ ذلك بطبيعة الحال اختلاف الفقهاء حول تحديد المصطلح والمفهوم المناسبين لها. وللمزيد من التفاصيل راجع د. محمد الهيتي، جرائم الحاسوب، الطبعة الأولى–2006، دار المناهج، عمان، ص72 وما بعدها. ود. أيمن عبدالله فكري، جرائم نظم المعلومات، 2007، دار الجامعة الجديدة، الإسكندرية، ص73. وفي الفقه الإنجليزي راجع:

أنها تتفق جميعها على ضرورة الحد من آثارها ومعالجة تداعياتها الخطيرة على مجتمعاتها من خلال الاستفادة من تجارب الدول التي واجهت هذه النوعية من الجرائم وعملت على تحصين مقوماتها وإيجاد الحلول المناسبة لضمان مواجهة فعالة، ولا يتأتى ذلك إلا من خلال فتح قنوات التعاون الدولي فيما بينها.

وتبدو أهمية الدراسة في أنها تبحث مسلك المشرع الإماراتي في مواجهة جرائم تقنية المعلومات، حيث حرص على تطوير تشريعاته الاتحادية والمحلية باستمرار لاسيما منذ بداية الألفية حيث الطفرة الاقتصادية الهائلة التي شهدتها دولة الإمارات آنذاك، وقد صدر المرسوم بقانون اتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات الذي ألغي بموجب المادة 50 من المرسوم بقانون اتحادي الجديد رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات[1].

والجدير ذكره أن هذه الصحوة سبقتها مساهمة دولة الإمارات في الإطار العربي حيث قدمت مشروعاً أُطلق عليه تسمية "قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها"[2].

وتيسيراً للعلم بمستحدثات المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الجديد، فإننا سوف نشرع ببيان التعديلات التي أجراها المشرع منذ صدور هذا المرسوم بقانون، للوقوف على مدى استيعابه للتطورات الحديثة في المحيطين

Jonathan Clough, Principles of Cybercrime, S-Edition, 2015, Cambridge University Press, United Kingdom, P 9-11.

1- صدر القانون الملغي في 30 يناير 2006. انظر الجريدة الرسمية لدولة الإمارات العربية المتحدة، العدد رقم540- السنة 42، بتاريخ 26 أغسطس 2012 . وقد ألغي المرسوم بقانون القديم بموجب المادة 50 من المرسوم بقانون الجديد.

2- اعتمد مجلس وزراء العدل العرب في دورته التاسعة عشرة هذا المشروع بقانون بموجب القرار رقم 495- د19 – 8 أكتوبر 2003، وتم اعتماده أيضاً من قبل مجلس وزراء الداخلية العرب في دورته الحادية والعشرين في القرار رقم 417 – د 2004/21. راجع الرابط الإلكتروني لموقع جامعة الدول العربية:

https://carjj.org/

الإلكتروني والافتراضي، وهو ما يملي علينا اتباع المنهج التحليلي حيث سنناقش التعديلات التي تناولها المشرع ونبحث في كل تعديل على حدة مدى جدواها لمواجهة هذه النوعية من الجرائم، كما أننا سوف نبحث ما تناوله المشرع لضمان مواجهة هذه الجرائم. فقسمنا الورقة البحثية إلى مبحثين اثنين وهما على النحو التالي:

المبحث الأول: التعديل في المرسوم بقانون اتحادي رقم 12 لسنة 2016.

المبحث الثاني: التعديل في المرسوم بقانون اتحادي رقم 2 لسنة 2018.

المبحث الأول
التعديل في المرسوم بقانون اتحادي رقم 12 لسنة 2016

صدر المرسوم بقانون اتحادي رقم 12 لسنة 2016 لتعديل حكم المادة (9) من المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات[1]، وهو أول تعديل على هذا القانون منذ صدوره. وفي هذا المبحث سنتحدث عن ثلاثة موضوعات نسعى من خلالها الإحاطة الكاملة بما جاء في هذا التعديل. فقمنا بتقسيم المبحث إلى ثلاثة مطالب الأول نبين فيه النص محل التعديل واستجلاء الغاية منه، والثاني نتحدث فيه عن الطبيعة القانونية للعنوان البروتوكولي، أما الثالث فسوف نخصصه لعرض البنيان القانوني للموضوع محل الاعتداء.

المطلب الأول - النص محل التعديل وتحديد غاية المشرع من هذا التعديل:

نصت المادة الأولى من هذا التعديل على أنه" **يستبدل بنص المادة (9) من المرسوم بقانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات النص الآتي: 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**

1- صدر هذا التعديل بتاريخ 23 مايو 2016 راجع الموقع الإلكتروني لوزارة العدل على الرابط التالي:
http://ejustice.gov.ae/

باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها"[1].

وبمطالعة هذا النص نجد أن المشرع قد عمد إلى تعديل حكم المادة 9 من خلال استبدال أمرين اثنين: **الأول** يتعلق بالعقوبة المقررة للجريمة حيث كانت قبل تعديلها تعد من قبيل جرائم الجنح المعاقب عليها بالحبس، ولم يحدد المشرع مدتها، ويعني ذلك أن القاضي سيعمل وفق ما تقرره القواعد العامة بشأن تحديد عقوبة الحبس، وقد تقرر في المادة 69 من قانون العقوبات الاتحادي الصادر سنة 1987 على أن عقوبة الحبس تكون بين الحد الأدنى وهو شهر واحد والحد الأقصى ثلاث سنوات ما لم ينص القانون على خلاف ذلك. أما بالنسبة لعقوبة الغرامة فقد كانت قبل التعديل تقرر أيضاً حدين الأدنى هو مائة وخمسون ألف درهم والأقصى هو لا تجاوز خمسمائة ألف درهم، والغرامة وفقاً لذلك لا تخضع للقواعد العامة المقررة في المادة 71 عقوبات حيث تقرر أن الحد الأدنى بالنسبة لعقوبة الغرامة المالية هو ألف درهم بينما الحد الأقصى لا أن يزيد على مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح[2].

أما بالنسبة للأمر **الثاني** 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،

1- تنص المادة 9 قبل التعديل على أنه "**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**".

2- عدلت المادة 71 من قانون العقوبات الاتحادي بموجب المرسوم بقانون اتحادي رقم 7 لسنة 2016 بشأن تعديل بعض أحكام قانون العقوبات رقم 3 لسنة 1987.

http://ejustice.gov.ae/

إلا أنه لم يرد لفظ الإنترنت ضمن ألفاظ وتعريفات المادة الأولى، بينما اللفظ الجديد والأدق مدرج ضمن هذه المادة منذ صدور المرسوم بقانون محل البحث.

فقد عرف المشرع الشبكة المعلوماتية وهي التي استعان بها التعديل الجديد، وكانت مدرجة في المادة الأولى على أنها" **ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات**".

فهذا التعريف يشير إلى الأداة التي تربط بين الوسائل والبرامج لتبادل المعلومات وهي ذاتها شبكة الإنترنت. وما فعله المشرع في هذا الشأن هو إعادة ضبط الألفاظ المستخدمة في القانون بحيث تكون متوافقة مع ما جاء من ألفاظ ومفاهيم في نص المادة الأولى هذا من ناحية، وأن المشرع أراد إزاحة الغموض واللبس الذي قد يدفع الجمهور المخاطب أصلاً بقواعد هذا القانون إلى أن يطرح سؤالاً جوهرياً وهو" لماذا لم يدرج المشرع لفظ الإنترنت في المادة الأولى ؟"

وتبدو غاية المشرع من وراء هذا التعديل على الرغم من عدم قيامه بتفسيره أو إيضاحه له في مذكرة خاصة ملحقة في المرسوم بالقانون الخاص بالتعديل، إلا أننا نستشعر غايته من واقع زيادة حالات التحايل عبر الشبكة المعلوماتية وما يمثل ذلك– بطبيعة الحال– من مخاطر تهدد المجتمع من ناحية وتهدد دعائم الاقتصاد الرقمي من ناحية أخرى، ذلك أن مثل هذه العمليات ستفقد ثقة المتعاملين في إجراء تعاملاتهم عبر القنوات الرقمية وهو ما يتعارض مع التوجه الاقتصادي والخدماتي في دولة الإمارات العربية المتحدة التي باتت معظم التعاملات فيها حكومية (الحكومة الإلكترونية) كانت أم غير حكومية تجرى إلكترونياً. فقد كشفت شركة نورتن التابعة لشركة سيمانتك في تقريرها الصادر عام 2017 حول مخاطر استخدام شبكات واي فاي العامة أن 95% من المستخدمين في دولة الإمارات العربية المتحدة تصرفوا بطريقة خطرة لهذه الشبكات، وكان عدد الضحايا وفق ما رصده التقرير هو 3.72 مليون مستخدم مع خسائر بقيمة 3.86 مليون درهم، كان من بينها نسبته متضررين بسبب التحايل على

المستخدمين عبر العنوان البروتوكولي[1]. إلى جانب ذلك، يعتبر أسلوب التحايل على العنوان البروتوكولي من الأساليب الفنية الذكية والخطيرة التي لا يشعر فيها المجني عليه أثناء إجراء تعاملاته عبر شبكة الإنترنت أو عبر حسابه في شبكات التواصل الاجتماعي، ويبدو أن هذا الأمر هو ما دفع المشرع الإماراتي إلى تخصيص مادة في إطار المرسوم بقانون رقم 5 لسنة 2012 بحيث يميزها عن جريمة الاحتيال الإلكتروني المنصوص عليها في المادة 11 من المرسوم بقانون رقم 5 لسنة 2012[2]، وهي جريمة تتبع بطبيعتها الأساليب العادية إلا أن ما يميزها عن الاحتيال التقليدي، أن أدوات تقنية المعلومات تلعب دوراً رئيساً 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 11.

المطلب الثاني - الطبيعة القانونية للعنوان البروتوكولي:

عرف المشرع الإماراتي العنوان البروتوكولي في إطار المادة الأولى بأنه "**معرف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات، ويتم استخدامه لأغراض الاتصال**". ولم يتناول المشرع هذا المفهوم سابقاً في المرسوم بقانون المُلْغى، كما لم يتناوله في التشريعات الإلكترونية الأخرى، ولكن أُدرج منذ صدور المرسوم بقانون الجديد، أي أنه ليس مفهوماً حديثاً على الجمهور بل كان مدرجاً قبل التعديل رقم 12 لسنة 2016.

1- راجع الروابط الإلكترونية التالية:

https://aitnews.com/2017/08/28/نورتن-تكشف-عن-أحدث-تقاريرها-حول-مخاطر-ا

https://www.menaherald.com/tech/information-technology/372-مليون-مستخدم-ضحايا-الجريمة-الإلكترونية-في-الإمارات-عام-2017-مع-خسائر

2- تنص المادة 11 على 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**".

والعنوان البروتوكولي مصطلح باللغة العربية لمصطلح وهو ترجمة لمصطلح عُرف باللغة الإنجليزية بلفظ (IP-address) أو (PII)[1]، وهو عبارة عن رقم تعريفي بالجهاز المتصل بالشبكة المعلوماتية سواء كان الجهاز المتصل هاتفاً محمولاً أو حاسوباً آليًا أو غير ذلك من أدوات يمكن من خلالها الاتصال بشبكة الإنترنت، فكل جهاز يتم منحه عنواناً يتكون من 32 رقماً يمكن من خلاله تحديد مكانه، فعندما يلج كل مستخدم إلى شبكة الإنترنت فإنه يدخل عنواناً معروفاً قابلاً للقراءة ليتحول بعد ذلك إلى أرقامٍ هي عنوان الجهاز المتصل[2].

وهذا العنوان على الرغم من طبيعته التقنية المتطورة وارتباطه أيضاً ببروتوكولات أخرى عديدة عند الاتصال بشبكة الإنترنت، إلا أن له أهمية كبيرة جداً في الجانب التجاري والإعلاني كونه يمثل قيمة في عالم التجارة الإلكترونية أو بالأصح التجارة بقواعد بيانات المستخدمين[3]، كما أن له أهمية في الجانب القانوني لضمان حقوق وحريات المتعاملين عبر شبكة الإنترنت فضلاً عن إمكانية تتبع الجناة في الجرائم الجنائية. وقد اختلف الفقه الأوروبي حول الطبيعة القانونية للعنوان البروتوكولي فالبعض يرى بأنه بيان شخصي للمستخدم يمكن بموجبه تحديد هويته وذلك من خلال مطالبة مزود خدمة الإنترنت بالإفصاح عنه، والبعض الآخر يرفض الاعتراف به كبيان شخصي استناداً إلى أن العنوان التعريفي يحدد الجهاز وليس الأشخاص، فالجهاز قد يكون بيد أطفال أو يكون في أماكن عامة كمقاهي الإنترنت على سبيل المثال أو المكتبات العامة أو غيرها من أماكن عامة أخرى قد يصعب فيها تحديد

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

2- راجع د. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، مجلة الحقوق، جامعة الكويت، العدد رقم 3 لسنة 35، سبتمبر 2011، الكويت، ص396. وحول ذلك راجع أيضاً:

Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haïdara. Droit des activiéts numériques, 1Edition, 2014, Dalloz, Paris, P743.

3- د. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى- 2016، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، ص339.

الشخص المستخدم، هذا فضلاً عن أن العنوان البروتوكولي تارة يكون عنواناً ثابتاً وتارة أخرى يكون متحركاً، وقد تبع ذلك اختلاف القضاء الأوروبي الذي تفاوتت أحكامه بشأن ذلك[1].

إلا أن محكمة العدل الأوروبية قد حسمت هذا الخلاف في الحكم رقم 2006/275 الصادر بتاريخ 29 نوفمبر 2008، بشأن الرد على ما أثارته محكمة أسبانية بشأن الاستفسار عن طبيعة العنوان البروتوكولي، وذلك للفصل في دعوى اشتهرت بمسمى Promusicae أو "بروموسيكا" حيث نشأ نزاعٌ بين طرفين هما جمعية خاصة لإدارة حقوق النشر ومزود خدمة الوصول يتعلق بانتهاك حق المؤلف عبر شبكة الإنترنت، وقد أكدت المحكمة في حيثياتها أن العنوان البروتوكولي هو من قبيل البيانات الشخصية الذي يتطابق مفهومه مع ما جاء في المادة الثانية من التوجيه المُلْغى رقم 95/46 بشأن حماية البيانات الشخصية ونقلها[2]. من أجل ذلك اعترف المشرع الأوروبي بالعنوان البروتوكولي كأحد نماذج البيانات الشخصية لمستخدمي شبكات الاتصالات، حيث قام بإدراجه تحت مسمى الرقم التعريفي في إطار المادة الثانية من التوجيه رقم 2002/58 بشأن معالجة البيانات الشخصية وحماية الخصوصية المعدلة بالأمر التوجيهي رقم2006/24، فعرفها بأنها" الرقم المخصص للأشخاص الذين يشتركون أو يسجلون للوصول إلى خدمات شبكة الإنترنت أو خدمة الاتصال عبرها"[3].

1- راجع د. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتوتير، الطبعة الأولى- 2013، دار النهضة العربية، القاهرة، ص100. ود. محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، طبعة أولى-2016، دار النهضة العربية، القاهرة، ص41. وفي الفقه الفرنسي راجع:

Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haïdara. Op, cit, p745.

2- ARRÊT DE LA COUR (grande chambre), Dans l'affaire C-275/06, 29 janvier 2008.

http://curia.europa.eu/juris/document/

http://fr.jurispedia.org/index.php/Statut_juridique_de_l%27adresse_IP_(fr)#cite_note-22

3- للمزيد من التفاصيل راجع اللائحة على الرابط الإلكترونية التالي:

وإذا كان هذا الاعتراف قد جاء على سند ما ورد في تعريف البيانات الشخصية في التوجيه المَلْغي رقم 95/46 بشأن حماية البيانات الشخصية ونقلها، فقد جاء التأكيد على هذا الاعتراف أيضاً وبشكل واضح وصريح، حيث حدد المشرع نماذج للبيانات الشخصية بشكل واسع وردت على سبيل المثال كان من بينها العنوان البروتوكولي أو الرقم التعريفي عبر الإنترنت في اللائحة الجديدة رقم 2016/679 الخاصة بحماية البيانات الشخصية ونقلها، وذلك في إطار البند الأول من المادة الرابعة حيث عرفت البيانات الشخصية بأنها" **معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد (موضوع البيانات)، والشخص يمكن تحديده بشكل مباشر أو غير مباشر من خلال الرجوع وبشكل خاص إلى الاسم أو رقم معرف أو بيانات الموقع أو معرف عبر الإنترنت أو إلى عامل أو أكثر من العوامل المحددة لهويته الفيزيائية، الفسيولوجية، الهوية الجينية، أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية للشخص الطبيعي**"[1]. وهذا التعريف يقتصر– كما هو واضح– على بيانات الشخص الطبيعي دون بيانات الشخص الاعتباري. وإذا كنا قد بينا سابقاً أن المشرع الإماراتي قد انفرد في إدراج تعريف خاص للعنوان البروتوكولي، ولكن لم يحدد في مفرداته الطبيعة القانونية لهذا العنوان حيث اكتفى ببيان طبيعتها التقنية بمعنى أن المشرع اقتصر على إيضاح آلية الربط بين الوسيلة والشبكة المعلوماتية ولم يتطرق للمستخدم. **وهو ما يدعونا إلى طرح التساؤل عن مدى اعتباره من قبيل البيانات الشخصية في التشريع الإماراتي ؟**

باستقراء نصوص المرسوم بقانون رقم 5 لسنة 2012، وجدنا أن المشرع الإماراتي يعترف ضمنياً بالعنوان البروتوكولي كبيان شخصي للمستخدم وذلك استناداً لما ورد في البند الثالث من المادة 2 التي تناولت تجريم الدخول غير المشروع إلى الموقع الإلكتروني أو النظام المعلوماتي أو شبكة المعلومات أو وسيلة تقنية المعلومات، وقد شدد المشرع العقاب على من يتلاعب بالمحتوى المعلوماتي بأي صورة من الصور التي حددها النص في الفقرة 2 وهي

---

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024

1- للمزيد من التفاصيل حول اللائحة الأوروبية الجديدة راجع:

IT Governance Privacy Team, EU GENERAL DATA PROTECTION REGULATION (GDPR), 2Edition- 2017, IT Governance Publishing, P10.

(الإلغاء، الحذف، التدمير، الإتلاف أو التغيير) أو نسخها أو إفشائها أو نشرها أو إعادة نشرها وكانت هذه البيانات شخصية[1]. فضلاً عن ذلك تناول المشرع العديد من النصوص التي تدلل على الطابع الشخصي للبيانات بشكل غير مباشر، ومنها على سبيل المثال ما ورد في المادة 7 حيث تناولت مسائل الاعتداء على البيانات أو المعلومات المتعلقة بالفحوصات الطبية للشخص الطبيعي، وما ورد في المادة 11 التي تناولت تجريم الاستيلاء دون وجه حق على مال أو منفعة أو سند أو توقيع باتباع طرق احتيالية أو باتخاذ اسم كاذب أو انتحال شخصية وإلى غير ذلك من نصوص جرمت الاعتداء على المعلومات أو البيانات ذات الطابع الشخصي.

ولما كان العنوان الإلكتروني عبارة عن بيان تعريفي لكل شخص يستخدم جهازاً إلكترونيا يستطيع من خلاله الاتصال بشبكة الإنترنت، فإنه يمكن أن يكون بمثابة بيان شخصي له أو هويته الرقمية كما يصفها بعض الفقهاء[2]، طالما أمكن تحديده بموجب هذا العنوان. وبالتالي يمكن أن يكون هذا العنوان موضوعاً لاعتداءات كثيرة.

*** تشريعات إمارة دبي تتوافق مع المعايير الأوروبية بشأن حماية البيانات الشخصية**

تتجه دولة الإمارات العربية المتحدة إلى إعداد مشروع خاص لتنظيم حماية البيانات الشخصية للمستخدمين من مخاطر التهديدات الإلكترونية في بيئة الاتصالات[3]، وذلك على النحو الذي يتوافق مع معايير أحكام اللائحة الأوروبية رقم 2016/679 بشأن حماية البيانات الشخصية ونقلها، وهذا المسعى يتلاءم مع توجه الدولة في تعزيز الجانب الرقمي والذكاء

1- نص البند الثالث من المادة الثانية على أنه " ... **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 2 من هذه المادة شخصية**".

2- للمزيد من التفاصيل راجع د. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، المرجع السابق، ص 99 وما بعدها.

3- مقال في صحيفة الاتحاد ، بعنوان/ حماية البيانات الشخصية، نشر بتاريخ 27 يوليو 2018. راجع الرابط: https://www.alittihad.ae/wejhatarticle/99484/حماية-البيانات-الشخصية

الاصطناعي. والسؤال هنا هل يحتاج المشرع فعلاً إلى تشريعات جديدة فضلاً عما هو معمول به لضمان حماية البيانات الشخصية؟.

باعتقادنا أن المشرع الإماراتي ليس بحاجة إلى تشريعات جديدة بقدر حاجته إلى إعادة ترتيب المدونة التشريعية التي تكاد تغطي جوانب عديدة في البيئة الإلكترونية سواء كانت تلك التشريعات محلية أو اتحادية، ففي إمارة دبي على وجه التحديد هناك بعض التشريعات التي تتوافق مع المعايير الأوروبية فيما يتعلق بالبيئة الإلكترونية إذ يمكن للمشرع الاستفادة منها كالقانون رقم 1 لسنة 2007 بشأن حماية البيانات والذي يطلق عليه (**DIFC DATA PROTATION LAW**)، وأيضاً القانون رقم 26 لسنة 2015 بشأن تنظيم ونشر بيانات المتعاملين التي تتشابه إلى حد قريب مع الآلية المتبعة في قانون حماية الحريات المعلوماتية الفرنسي رقم 17 لسنة 1978، هذا فضلاً عن قيام المشرع في إمارة دبي بإصدار قانون رقم 2 لسنة 2016 الخاص بإنشاء مؤسسة بيانات دبي.

لذلك نهيب بالمشرع الاتحادي الاستفادة قدر الإمكان من تجربة المشرع المحلي لمواجهة التعاملات الإلكترونية ومخاطرها، كما ندعو المشرع إلى تبني لائحة تسميات ومفاهيم موحدة بحيث تتوافق مع كافة القوانين الاتحادية والمحلية المتصلة بالجوانب الإلكترونية، لتصبح المرجع الوحيد في دولة الإمارات فضلاً عن أنها تسهل للقضاء والجمهور المخاطب بتلك القوانين القدرة على فهم واستيعاب تلك المصطلحات ومفاهيمها بسهولة.

المطلب الثالث - البنيان القانوني لجريمة التحايل على العنوان البروتوكولي:

في ضوء ما سبق؛ وجدنا أن العنوان البروتوكولي عبارة عن بيان يعرف جهاز المستخدم في البيئة الإلكترونية والافتراضية، ويستطيع مزود خدمة الإنترنت (ISP)[1] أن يستدل بموجب هذا العنوان على بيانات محددة لصاحب هذا العنوان أو على الأقل إمكانية تحديده، لأن العنوان البروتوكولي قد يكون بياناً لأكثر من شخص[2].

1- (ISP) اختصاراً لعبارة Internet Serves Provider

2- راجع د. مروة زين العابدين صالح، المرجع السابق، ص99. وراجع في الفقه الإنجليزي لدى:

وفي هذه الجريمة يستهدف الجاني بطريقة فنية خداع العنوان البروتوكولي لتحقيق مشروعه الإجرامي، وفي هذا الجانب نتفق في ما ذهب إليه أحد الفقهاء من أن جريمة التحايل على العنوان الإلكتروني جريمة إلكترونية بحته، وأن المشرع ميز بينها وبين جريمة الاحتيال الإلكتروني المنصوص عليها في المادة 11، فالجاني باتباع هذا الأسلوب يتم عن ذكاء يستحق معه تشديد العقاب[1]، وهذا بالفعل ما أراده المشرع الإماراتي في هذا التعديل.

تتطلب جريمة التحايل على العنوان البروتوكولي توافر ركنين مادي وآخر معنوي، أما الركن المادي، فنلاحظ أن المشرع حدد شكل التجريم بأن قيده في قيام الجاني بارتكاب سلوك التحايل على العنوان البروتوكولي، وكلمة التحايل في اللغة تعني تحايلَ، تحايُلاً، فهو مُتحايِل، والمفعول مُتحايَل عليه. وفي الاصطلاح تعني تحايل على الرَّجل/ تحايل على الشَّيءِ، سلك معه مسلك الحذق ليبلغ منه مأربَه[2]. والحذاقة مفهوم يشير بدوره إلى قدرة الجاني على إتقان الشيء أو إلمامه أو مهارته في ارتكاب سلوك التحايل عبر أدوات تقنية المعلومات، وبالتالي يخرج من نطاق التجريم إذا كان سلوك التحايل على موضوع آخر غير العنوان البروتوكولي، فإذا كان التحايل على النظام الإلكتروني أو على إحدى وسائل تقنية المعلومات فإن المادة واجبة التطبيق هي المادة 11. كذلك نلاحظ أن المشرع حدد طرق التحايل إما عن طريق استخدام عنوان وهمي أي عنوان تعريفي لا يعود لشخصية حقيقية بل شخصية مستعارة، فالبعض يلجأ إلى استخدام برامج معينة كاستخدام تقنية RDP أو برنامج PD Proxy أو تقنية TOR VPN لتشفير اتصالاته بغية إخفاء أو تغيير عنوانهم التعريفي أو بالأحرى يتلاعبون بإخفائه في الشبكة، وهو ما يسمح للبعض من ارتكاب جرائم مختلفة عبر شبكة الإنترنت ويصعب في ذات الوقت تحديد هويتهم لدى جهات التحقيق. ومن بين القضايا التي

Andrew Murray, Information Technology Law- The Law and Society, 3rd edition- 2016, Oxford University Press, United Kingdom, P23.

1- راجع أ. د. إمام حسنين عطا الله، جرائم تقنية المعلومات في التشريعات والصكوك العربية، طبعة أولى- 2017، مركز الدراسات والبحوث، جامعة نايف للعلوم الأمنية، الرياض، ص276 وما بعدها.

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

أثارت جدلاً واسعاً في دولة الإمارات ما أشيع عن تجريم استخدام شبكة VPN والأصل أن هذه الشبكة أو التقنية مشروعة وأن مسألة التجريم تنحصر في حالات سوء استخدامها[1] وهذا ما قصده المشرع من إطلاق لفظ التحايل على هذا السلوك. ويتحقق السلوك الإجرامي أيضاً بذات الأسلوب ولكن من خلال استخدام عنوان تعريفي يعود لشخص آخر، كاستخدام موقع Iplogger على سبيل المثال الذي يمكن المستخدم من تحديد هوية الشخص ومن ثم نسخ عنوانه، وهذا الأسلوب يشكل في حقيقته اختراقاً لنظام الشخص الآخر. 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، وليس ذلك فحسب بل إلى جانب إمكانية استغلال المخترقين حسابات تعود لأشخاص آخرين في هذه المواقع أو الشبكات بسبب ثغراتها الأمنية، يستطيع المستخدم العادي أيضاً إنشاء حساب وهمي دون تحديد بياناته الشخصية[2]. كذلك نلاحظ أن المشرع توسع في طرق التحايل على العنوان البروتوكولي بدلالة العبارة التي أوردها في النص" **أو بأي وسيلة أخرى**"، مستدركاً ما قد يظهر في المستقبل من أدوات جديدة تمكن المستخدمين من إخفاء هويتهم. إلى جانب ذلك؛ اشترط المشرع لقيام الجريمة أن يكون التحايل إما بقصد ارتكاب جريمة جنائية بصرف النظر عما إذا كانت منصوص عليها في هذا القانون أو في أي قانون آخر، أو كان بقصد إخفاء آثارها، كمحو أو إخفاء المحتوى المعلوماتي من صور أو محادثات أو نصوص أو غير ذلك من مواد معلوماتية، وينصرف مفهوم الإخفاء أو التستر على جناة آخرين لهم علاقة بالجريمة.

وبالنسبة للركن المعنوي؛ فالواضح أن جريمة التحايل على العنوان البروتوكولي من الجرائم العمدية، ولا يمكن تصور وقوعها على خلاف ذلك، لأن لفظ التحايل يشير بحد ذاته إلى تعمد الجاني إلى ارتكاب السلوك محل التجريم، ومن ثم تأخذ صفة العمد صورة القصد

1- مقال نشر على الموقع الإلكتروني لصحيفة الاقتصادي، راجع الرابط التالي:
https://aliqtisadi.com/804988/الإمارات-تحارب-الجرائم-الالكترونية

2- مقال منشور على مدونة جديد الإنترنت ، راجع الرابط التالي:
http://newinternt.blogspot.com/2015/09/blog-post_19.html

الجنائي العام القائم على عنصرين رئيسين هما العلم والإرادة، فالعلم يعني علم الجاني بأنه يخفي هويته بإحدى الطرق المبينة باستخدام أدوات تقنية المعلومات، وعلمه أيضاً بأن ذلك سيمكنه من ارتكاب جريمته أو إخفاء آثارها للحيلولة دون اكتشاف آثارها أو الكشف عن جناة آخرين. أما الإرادة فتعني اتجاه إرادة الجاني 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.

*** بعض التطبيقات بالمخالفة لنص المادة 9:**

- إرسال رسائل مفبركة منسوبة لهيئة تنظيم الاتصالات الإماراتية تدعو عدداً من مستخدمي أجهزة الهواتف المحمولة إلى دفع مخالفة قيمتها خمسة آلاف درهم[1].
- تعرض عدد من المستخدمين لرسائل احتيال مالي بعد اختراق حسابات الواتساب خاصة بشخصيات تتمتع بمصداقية لدى شريحة من الجمهور واستغلال الجناة جهات الاتصالات في هواتف المجني عليهم[2].

المبحث الثاني
التعديل في المرسوم بقانون اتحادي رقم 2 لسنة 2018

صدر المرسوم بقانون اتحادي رقم 2 لسنة 2018 مشمولاً بتعديل أحكام المواد (26) و (28) و(42) من المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات[3]، ويعتبر التعديل الثاني منذ صدور المرسوم بقانون محل البحث، وقد تبنى

1- مقال منشور على موقع الإمارات اليوم، راجع الرابط الإلكتروني التالي:
https://www.emaratalyoum.com/business/local/2018-01-25-1.1065037

2- مقال منشور على موقع البيان الإلكتروني راجع الرابط التالي:
https://www.albayan.ae/across-the-uae/news-and-reports/2018-10-03-1.3373257

3- صدر هذا التعديل بتاريخ 24 يوليو 2018م راجع الموقع الإلكتروني لوزارة العدل الإماراتية على الرابط التالي:

المشرع في التعديل سياسة تميل تارة إلى الشدة في تقرير العقاب وتارة أخرى تميل نحو الإصلاح وإعادة تأهيل بعض الجناة، فضلاً عن إدخاله بعض السلوكيات المخالفة ضمن النماذج الإجرامية. وقبل الخوض في تفاصيل هذا التعديل أردنا الإشارة إلى أن المشرع الإماراتي قد اعتبر المادتين 26 و28 من قبيل الجرائم الماسة بأمن الدولة بصريح الفقرة الأولى من نص المادة 44 من المرسوم بقانون رقم 5 لسنة 2012[1].

تحقيقاً لذلك، سوف نقسم حديثنا في هذا المبحث إلى ثلاثة مطالب أيضاً، نناقش في كل مطلب مادةً من مواد التعديل على حدة نستوضح فيها رؤية المشرع حولها.

المطلب الأول - تعديل المادة 26 الخاصة بأنشطة الإرهاب الإلكتروني:

تنص المادة 26 بعد تعديلها على أنه" **يعاقب بالسجن مدة لا تقل عن عشر سنوات ولا تزيد على خمسة وعشرين سنة والغرامة التي لا تقل عن مليوني درهم ولا تجاوز أربعة ملايين درهم، كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو لاستقطاب عضوية لها، أو ترويج أو تحبيذ أفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية.**

وتكون العقوبة الحبس مدة لا تزيد على خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم لمن حمل أياً من المواقع المشار إليها في الفقرة الأولى من هذه المادة أو أعاد بثها أو نشرها بأي وسيلةٍ كانت أو تكرر دخوله إليها لمشاهدتها، أو نشر أي محتوى يتضمن التحريض على الكراهية.

---

http://zayedalshamsi.ae/ar/2018/08/30/مرسوم-بقانون-اتحادي-رقم-2-لسنة-2018-بتعديل-ب/

1- نصت الفقرة الأول من المادة 44 على أنه" تعتبر الجرائم الواردة في المواد (4، 24، 26، 28، 29، 30، 38) من هذا المرسوم بقانون من الجرائم الماسة بأمن الدولة...".

وللمحكمة- في غير حالات العود- بدلاً من الحكم بالعقوبة المشار إليها في الفقرة السابقة أن تحكم بإيداع المتهم في إحدى دور المناصحة أو الحكم بوضعه تحت المراقبة الإلكترونية ومنعه من استخدام أياً من وسائل تقنية المعلومات خلال فترة تقدرها المحكمة على ألا تتجاوز الحد الأقصى للعقوبة المقررة ".

وبالنظر إلى هذا النص نلمس أن مواجهة الأنشطة المتعلقة بالإرهاب الإلكتروني لم تكن حديثة العهد، بل كان المشرع يجرمها أيضاً في إطار المرسوم بقانون القديم رقم 2 لسنة 2006، ومع ذلك لم يعرف المقصود بالإرهاب الإلكتروني[1]، ومن أفضل التعريفات الفقهية لهذه الجريمة هو تعريفها بأنها كل فعل يقوم به فرد أو جماعة منظمة باستخدام وسائل تقنية المعلومات أو الشبكة المعلوماتية من شأنه إحداث ضرر أو تعريض مصلحة يحميها القانون لخطر تنفيذاً لمشروع إرهابي[2].

1- عرف المشرع النشاط أو العمل الإرهابي في إطار المادة 2 من المرسوم بقانون اتحادي رقم 1 لسنة 2004 الخاص بمكافحة الجرائم الإرهابية، على أنه" **كل فعل أو امتناع عن فعل يلجأ إليه الجاني، تنفيذاً لمشروع إجرامي فردي أو جماعي، بهدف إيقاع الرعب بين الناس أو ترويعهم، إذا كان من شأن ذلك الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو إيذاء الأشخاص أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر بمن في ذلك ملوك ورؤساء الدول والحكومات والوزراء وأفراد عائلاتهم وأي ممثل أو موظف رسمي لدولة أو لمنظمة دولية ذات صفة حكومية وأفراد أسرهم الذين يعيشون في كنفهم المقررة لهم الحماية وفقاً للقانون الدولي أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الطبيعية للخطر**". وعرف في المادة الأولى من المرسوم بقانون اتحادي رقم 7 لسنة 2014 بشأن الجرائم الإرهابية، العديد من المصطلحات التي لم تكن موجودة ضمن تعريفات المرسوم بقانون اتحادي رقم 1 لسنة 2004 الملغي، حيث عرف المشرع في المرسوم الصادر سنة 2014 عدة مصطلحات وهي الجريمة الإرهابية والغرض الإرهابي والنتيجة الإرهابية والتنظيم الإرهابي والشخص الإرهابي.

2- د. زين العابدين عواد الكردي، جرائم الإرهاب الإلكتروني- دراسة مقارنة، الطبعة الأولى 2018، منشورات الحلبي الحقوقية، بيروت- لبنان، ص84.

وما نلاحظه أن المشرع أبقى على وصف هذه الجريمة كجناية معاقب عليها بالسجن المؤقت المشمولة بعقوبة الغرامة المالية في المرسوم بقانون رقم 2 لسنة 2018، ولكنه رفع سقف العقوبة من السجن مدة خمس سنوات إلى السجن بين حدين الأدنى عشر سنوات والأقصى خمس وعشرون سنة، كما رفع قيمة الغرامة لتكون بين حدين الأدنى مليونا درهم والأقصى أربعة ملايين درهم وذلك عن الجنايات التي تتعلق أو تتصل بأنشطة إرهابية. بجانب ذلك أضاف المشرع فقرتين جديدتين هما الفقرتان الثانية والثالثة، فجاءت الفقرة الثانية تجرم أنشطة جديدة وهي تحميل محتوى معلوماتي من المواقع الإلكترونية المشار إليها في الفقرة الأولى، أو إعادة بثها أو نشرها بأي طريقة كانت، أو تكرر الولوج إليها لمشاهدة ما فيها من محتوى محظور، أو نشر محتوى يتعلق مضمونه بالتحريض على الكراهية، وقد قرر المشرع إنزال عقوبة السجن مدة لا تزيد عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز عن مليون درهم. أما الفقرة الثالثة ونلاحظ فيها أن المشرع منح المحكمة سلطة جوازية في توقيع العقاب على مرتكبي الأنشطة المشار إليها في الفقرة الثانية فقط، شريطة ألا يكون الجاني عائداً لها، فإذا ثبت عودته إليها كانت العقوبة وجوبيه على الجاني. وفي هذا الجانب أضاف المشرع ثلاثة تدابير مستحدثة يجوز للمحكمة أن توقعها على الجاني غير العائد وهي كالتالي:

أ- الإيداع في أحد دور المناصحة وهي دور خاصة بإعادة تأهيل المتطرفين فكرياً للعودة إلى المجتمع أفراداً سويين وذلك من خلال إعداد برامج أو أنشطة متنوعة لتصحيح مسار الفئات الضالة[1].

ب- الإخضاع تحت المراقبة الإلكترونية وهي أحد الأساليب الحديثة لتنفيذ العقوبة السالبة للحرية في المنزل، حيث يقضي المحكوم عليه العقوبة داخل المنزل مقيداً

1- المناصحة تعني تقديم النصيحة أو المشورة لشخص ما لإعلان توبته تجاه مخالفة قام بارتكابها بسبب فكره غير السوي، وهي فكرة وقائية تهدف إلى تصحيح مسار هذا الشخص. للمزيد من التفاصيل راجع اللواء سعيد بت عمر البيشي، ورقة عمل بعنوان/عرض تجربة المملكة العربية السعودية في المناصحة وإعادة التأهيل، مقدمة في الحلقة العلمية بعنوان" مكافحة الإرهاب"، والتي أقيمت في الرياض في الفترة ما بين 15-17 سبتمبر 2011، التقرير الإحصائي لجهود إدارة المناصحة بمركز محمد بن نايف للمناصحة والرعاية. https://repository.nauss.edu.sa/

بسوار إلكتروني في المعصم أو في القدم بحيث تمكن الجهات المختصة من مراقبته عن بعد[1].

ج- التدبير الثالث وهو ملحق بإخضاع المحكوم عليه تحت المراقبة الإلكترونية أن يمنع من استخدام أدوات تقنية المعلومات أثناء الفترة التي تقررها المحكمة شريطة ألا تتجاوز الفترة الحد الأقصى للعقوبة المقررة.

إن غاية المشرع من هذا التعديل واضحة جداً، إذ يرى أن منابر التطرف الفكري بكافة أشكاله والإرهاب الإلكتروني على وجه التحديد آخذه بالتمدد والانتشار عبر بوابة شبكة الإنترنت ومنتدياتها ومواقع التواصل الاجتماعي، وهي بلا شك تشكل منافذ خطيرة على كافة أفراد المجتمع وأطيافه، فالمشرع أراد تعزيز الحماية بشكل أكبر على النحو الذي يحكم السيطرة قدر الإمكان أمام الفئات التي تختبئ وراء ستار التقنيات الحديثة[2]، ذلك أن الجهات المحظورة التي عنى المشرع بتحديدها وهي الجماعات الإرهابية أو أي مجموعة أو جمعية أو منظمة أو

1- هذا التدبير نظمته بعض التشريعات الأوروبية كالتشريع الفرنسي في أحكام المواد من 131-36-9 إلى 131-36-13 من قانون العقوبات، ونظمها إجرائياً في المادة 362 من قانون الإجراءات الجنائية. للمزيد من التفاصيل راجع:

Michèle-Laure Rassat, Droit pénal général, 4éd- 2017, ellipses, Paris, P572.

ويعترف بها التشريع الأمريكي كسلطة جوازية للمحكمة، وقد نظم أحكامها في البنود 6 و13 و14 و19 و22 من المادة 18 تحت مسمى(شروط الاختبار) راجع الموقع الرابط الإلكتروني التالي:

U.S. Code › Title 18 › Part II › Chapter 227 › Subchapter B › § 3563 - Conditions of probation https://www.law.cornell.edu/uscode/text/18/3563

كما يعترف بها التشريع الإنجليزي في القسم رقم 215 (متطلبات المراقبة الإلكترونية) في قانون العدالة الجنائية رقم 2003

Anthea Hucklesby and Ella Holdsworth, Electronic Monitoring in England and Wales, May 2016, University of Leeds, UK, the Criminal Justice Programme of the European Union, p14. http://28uzqb445tcn4c24864ahmel.wpengine.netdna-cdn.com/files/2016/06/EMEU-Electronic-monitoring-in-England-and-Wales.pdf

2- تأتي غاية المشرع مكملة لغايته في التشريعات الأخرى التي تجرم ظاهرة الإرهاب، كالمرسوم بقانون رقم 1 لسنة 2004 بشأن مكافحة الجرائم الإرهابية والقانون الاتحادي رقم 7 لسنة 2014 بشأن الجرائم الإرهابية.

هيئة غير مشروعة قد بدأت تعتمد وبشكل كبير على استقطاب الجمهور والتغرير بهم عبر تلك المنصات لتنفيذ مشروعهم الإرهابي من خلال نشر أو بث محتوى معلوماتي يتضمن سموماً فكرية من شأنها أن **تغذي** العقول اللينة– إن صح التعبير– أو المشاعر الجياشة لدى العديد من الأشخاص والتغرير بهم على النحو الذي يدفعهم للقيام بسلوكيات تتعارض مع قيم الاعتدال والوسطية. فشبكة الإنترنت ومواقعها ومنتدياتها مكنت التنظيمات الإرهابية من نشر فكرها وتجنيد الأعضاء واستقطابهم، حيث استفادت كثيراً من عالمية تبادل البيانات والمعلومات عبرها فقد أصبحت الوسيلة الإعلامية الأولى[1]، فهذه الشبكة تعج بمحتويات ذات طابع عنيف كطرق تصنيع القنابل أو المفرقعات أو عرض الأساليب التي تنفذ بها عمليات الإعدام والقتل سواء عبر الألعاب الإلكترونية أو عبر مقاطع أو صور، أو محتويات من شأنها أن تعزز الكراهية والعنصرية وتبث روح الفرقة والحقد بين أفراد المجتمع، وإلى غير ذلك وسائل تعد منهجاً منحرفاً يدفع الأجيال إلى الانخراط في الجماعات المحظورة أو التواصل مع أعضائها أو تقمص شخصياتهم المريضة.

وقد اشترط المشرع لقيام الجريمة المنصوص عليها في المادة 26 مع افتراض ضرورة ارتكابها بواسطة أدوات تقنية المعلومات أو شبكات المعلوماتية، توافر ركنين أولهما هو الركن المادي والآخر معنوي. أما الركن المادي فيشمل صورتين هما:

أولاً: إنشاء أو إدارة الموقع الإلكتروني أو الإشراف عليه أو نشر معلومات لجماعات إرهابية أو جهات غير مشروعة: ينصرف مفهوم الموقع الإلكتروني إلى الحسابات التي ينشئها المستخدمون عبر مواقع التواصل الاجتماعي بمختلف أنواعها، ونلاحظ في هذا الجانب أن إنشاء مثل هذه المواقع أو الحسابات أو إدارتها أو الإشراف عليها ليست مجرمة بحد ذاتها ما لم تكن هذه الأنشطة قد تمت بمعرفة شخص إرهابي أو جماعات أو تنظيمات إرهابية، وبمعنى آخر إن الكيانات الأخيرة هي من قامت بإنشاء تلك المواقع أو الحسابات الإلكترونية بشكل مباشر ذلك أن الغالب يكون إنشاء تلك المواقع أو الحسابات بواسطة

1- Myriam Quéméner et Yves Charpenel, Op, cit, P126.

أشخاص آخرين لا يرتبطون بشكل مباشر بهذه الكيانات بل يكونون بمثابة واجهة لهم أو ساتراً لأنشطتهم المخالفة للقانون من أجل تحقيق الأغراض التي حددها المشرع وهي تسهيل التواصل بتلك الكيانات أو أحد أعضائها عبر هذه المنافذ من أجل تنفيذ التعليمات الصادرة من قياداتها أو التنسيق بين أعضائها، أو استقطاب أعضاء جدد لها باستهداف أصحاب العقول اللينة واستغلال مشاعرهم، أو الترويج أو التحبيذ لأفكارها أو تمويل أنشطتها، أو تقديم المساعدة الفعلية لها من خلال حملات جمع التبرعات، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو غير ذلك من أنشطة داعمة لتنفيذ الأعمال الإرهابية. ولا يشترط لقيام الجريمة تحقق النتيجة التي تصبو إليها تلك الكيانات، بل تتحقق بمجرد تحقق السلوك، ولا يشترط أيضاً لتحقق الركن المادي ارتكاب الجاني الأفعال كلها جملة واحدة بل يتحقق هذا الركن ولو ارتكب الجاني أحد هذه الأفعال. وقد شدد المشرع العقاب على مرتكبي هذه الأنشطة المجرمة.

ثانياً: تحميل محتوى معلوماتي من المواقع المحظورة أو إعادة بثها أو نشرها أو تكرار الدخول إليها أو نشر محتوى يحرض على الكراهية: وهي مجموعة الأفعال التي أدرجها المشرع في التعديل الجديد، تتمثل في تحميل المحتوى المعلوماتي سواء كان نصيًا أو صورًا أو مقاطع فيديو من المواقع الإلكترونية المحظورة أو إعادة بث أو نشر المحتوى غير المشروع، وقد أُدخل ضمن الأنشطة المحظورة في هذه الفقرة سلوك تكرار الدخول إلى المواقع لمشاهدة المحتوى أو نشر محتوى يتضمن تحريضاً على الكراهية، **وقد** عرف المشرع هذا السلوك في إطار المادة 1 من المرسوم بقانون اتحادي رقم 2 لسنة 2015 بشأن مكافحة التمييز والكراهية، بأنه" **كل قول أو عمل من شأنه إثارة الفتنة أو النعرات أو التمييز بين الأفراد أو الجماعات**". وعلى الرغم من تشابه سلوك التحريض على الكراهية الواردة في هذا المرسوم بقانون مع ما ورد في المادة 24 من المرسوم بقانون رقم 5 لسنة 2012، إلا أن التمييز بينهما يمكن في تحقيق الغرض الإرهابي.

وبالتالي يكون نص المادة 26 من القانون الأخير واجباً للتطبيق متى ارتكب هذا النشاط عبر أدوات تقنية المعلومات لتنفيذ غرض إرهابي، أما إذا ارتكبت النشاط لتنفيذ غرض آخر، فإن المادة واجبة التطبيق هو نص المادة 24. ونلاحظ هنا أن المشرع لم يشترط أن يكون القائم بهذه الأنشطة من الإرهابيين بل من الأشخاص الذين تم استقطابهم أو تحبيذهم للانضمام إلى الجماعات المحظورة وبالأحرى الأشخاص المغرر بهم. وقد قرر المشرع عقوبة أخف من العقوبة المقررة في الفقرة الأولى.

وجرائم المادة 26 من الجرائم العمدية التي تتطلب توافر عنصرين هما العلم والإرادة أما العلم فيعني علم الجاني بأنه ينشئ موقعاً أو ينشر معلومات لجماعة إرهابية، فإذا جهل القائم على إنشاء الموقع أو مديرها أو المشرف عليها سينتفي القصد عنه، وهذا قد يحدث عملاً حينما يتدخل شخص ينتمي إلى هذا التنظيم أو هذه الجماعة إلى موقع لا يرتبط به أو بمالكه سوى أنه تدخل بتعليق أو بإضافة مادة يمكن الاستدلال على انتمائه لها. إلا أن ذلك لا يمنع من مساءلة المسؤول عن هذا الموقع بموجب نص المادة 39 من ذات القانون، متى توافرت شروطها التي أسست قيام مسؤولية هذا الشخص طبيعياً كان أم اعتبارياً، متى علم بطبيعة المحتوى غير المشروع ولم يبادر بإزالته أو منعه خلال مدة محددة يُخطر بها هذا المسؤول بإشعار موجه إليه من قبل الجهة المختصة باتخاذ ما يلزم لإزالة المحتوى غير المشروع.

*** تعقيب الباحث:**

بهذا التعديل أراد المشرع تعزيز فكرة الردع لدى مستخدمي أدوات تقنية المعلومات وحماية المجتمع من آفة التطرف الفكري وقد حرص على ألا يتعارض ذلك مع ضمانات حرية الرأي عن التعبير والفكر، ويظهر لنا الحرص من خلال إقراره تدابير علاجية للمستخدم المنحرف لتصحيح مساره الفكري وتعديل سلوكه فضلاً عن إيقاع العقوبة المقررة عن الأفعال المشار إليها في المادة 26.

ومع ذلك نجد أن المشرع غفل عن الإحاطة الواضحة بشأن سلوك من يقوم بتحميل المحتوى المعلوماتي من المواقع أو المنتديات المحظورة حيث تضعنا صياغة النص أمام

غموض يصعب تفسيره أو أن تفسيره قد يقودنا إلى أمر غير منطقي وهو مسألة تجريم كل من يقوم بتحميل المحتوى غير المشروع من تلك المواقع المحظورة في حين أن هذا المحتوى ممكن أن يصل إلى المستخدم بأي طريقة أخرى غير التحميل كأن يحصل عليها عن طريق الواتساب على سبيل المثال أو عن طريق ذاكرة منفصلة، إذا أراد الجاني أن يتحايل على هذا النص، كذلك من يقوم بتحميل هذا المحتوى أو تكرر ولوجه إلى الموقع المحظور لا يعني بالضرورة استخدام ما تم تحميله في أمر غير مشروع بل قد يكون تحميل هذا المحتوى لأجل نشر التوعية بين الجمهور. كذلك الأمر بالنسبة لتكرار الولوج إلى الموقع إذ لا يعني تكرار الولوج إليه ميل المستخدم نحو تلك الجماعات، وبالتالي قد يكون تكرار الدخول بقصد دراسة سلوكياتهم، هذا إلى جانب أن الولوج إلى تلك المواقع قد يكون من طرف شخص آخر على خلاف المستخدم الأساسي للجهاز الذي ولج من خلاله أول مرة.

لذلك نهيب بالمشرع الإماراتي في هذا الجانب الالتفات إلى المقاصد من وراء السلوكيات الواردة في الفقرة الثانية أي بإضافة عبارة تدل فعلاً على القصد من وراء تحميل هذا المحتوى أو تكرار الولوج إلى الموقع المحظور، فتحايل المستخدم على سبيل المثال على العنوان البروتوكولي من أجل تحميل محتوى غير مشروع أو الوصول إلى الموقع يكفي لقيام القصد الجنائي لديه، متى ثبت أن تحايله كان بقصد ارتكاب جريمة فتحايله على العنوان البروتوكولي قرينة قابلة لإثبات العكس.

المطلب الثاني - تعديل المادة 28 الخاصة بتعريض أمن الدولة للخطر أو المساس بالنظام العام أو الاعتداء على مأموري الضبط القضائي أو المكلفين بتنفيذ القوانين:

نصت المادة 28 بعد تعديلها على أنه" **يعاقب بالسجن المؤقت والغرامة التي لا تجاوز مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال، أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة**

ومصالحها العليا للخطر أو المساس بالنظام العام، أو الاعتداء على مأموري الضبط القضائي أو أي من المكلفين بتنفيذ أحكام القوانين"[1].

وبالنظر إلى هذا النص نجد أن المشرع الإماراتي قد اكتفى بإضافة عبارة جديدة في ذيل النص، حيث اقتصر التعديل على إدخال مأموري الضبط القضائي أو المكلفين بتنفيذ أحكام القوانين ضمن الحماية المقررة في المادة 28، ويعتقد البعض في هذا الجانب أن هذا النص لم يكن ضمن الجرائم المنصوص عليها في المرسوم بقانون رقم 2 لسنة 2006[2]، ولكن من ناحيتنا نرى عكس ذلك حيث سبق للمشرع تناولها في إطار نص المادة 20 من المرسوم القديم. وقد عرف المشرع الإماراتي مأموري الضبط القضائي في إطار المادة 33 من قانون الإجراءات الجزائية رقم 35 لسنة 1992، حيث نصت على أنه" يكون من مأموري الضبط القضائي في دوائر اختصاصهم : **1. أعضاء النيابة العامة. 2. ضباط الشرطة وصف ضباطها وأفرادها. 3. ضباط وصف ضباط وأفراد حرس الحدود والسواحل. 4. ضباط الجوازات. 5. ضباط الموانئ البحرية والجوية من رجال الشرطة والقوات المسلحة. 6. ضباط وصف ضباط الدفاع المدني. 7. مفتشو البلديات. 8. مفتشو وزارة العمل والشؤون الاجتماعية. 9. مفتشو وزارة الصحة. 10. الموظفون المخولون صفة مأموري الضبط القضائي بمقتضى القوانين والمراسيم والقرارات المعمول بها".**

وبهذا النص نجد أن مسألة تحديد مأموري الضبط القضائي تكون وفق ما ورد في حكم هذه المادة، أي وفق ما يقرره قانون الإجراءات الجنائية، وهذا ما يجعلنا نطرح سؤالاً مهماً وهو إذا كان المشرع قد جعل أمر تحديد مأموري الضبط القضائي بموجب قانون الإجراءات الجزائية، فهل يتعارض ذلك مع حكم ما جاء في المادة 49 من المرسوم بقانون محل البحث

1- تنص المادة 28 قبل تعديلها على أنه" **يعاقب بالسجن المؤقت والغرامة التي لا تجاوز مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال، أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام**".

2- راجع أ. د. إمام حسنين عطا الله، المرجع السابق، ص415.

تأسيساً على أن المادة الأخيرة قد منحت أيضاً وزير العدل سلطة تحديد مأموري الضبط لإثبات الجرائم التي تقع بالمخالفة لأحكام هذا المرسوم ؟

الحقيقة أن المادة 34 من قانون الإجراءات الجنائية أجابت على ذلك بوضوح، حيث أجازت لوزير العدل تخويل بعض الموظفين هذه الصفة لمواجهة الجرائم التي تقع في دائرتهم أو تقع ضمن اختصاصهم[1]، وذلك على سند ما ورد في البند العاشر من المادة 33 المشار إليها والتي بينت أن منح هذه الصفة أيضاً يكون بموجب قوانين أو مراسيم أو قرارات معمول بها في الدولة، فنص المشرع صراحة في إطار المادة 49 من هذا المرسوم، 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**".

مما يعني أن المشرع الإماراتي حرص في كل التشريعات المتعلقة في الجوانب التخصصية ومنها الجانب الإلكتروني أن يراعى طبيعة الجرائم المراد إثباتها من ناحية وتخصص من يتمتع بصفة الضبطية القضائية لإثبات مفردات الواقعة وهذا من ناحية أخرى. لذلك نجد تبرير عدم تحديد مهام الضبطية القضائية في هذا المرسوم إلى الطبيعة الجرائم محل الإثبات والطابع التخصصي الذي يؤهله في القيام بإجراءات البحث والتحري وجمع الاستدلالات[2]. فهذه النوعية من الجرائم وما تتسم به من خصائص تميزها عن الجريمة

1- نصت المادة 34 على أنه "**يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص أو السلطة المختصة تخويل بعض الموظفين صفة مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع في دائرة اختصاصهم وتكون متعلقة بأعمال وظائفهم**".

2- تجدر الإشارة إلى أن المشرع تناول ذات الحكم في إطار المادة 27 من المرسوم القديم، حيث نصت على أنه" **يكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل والشؤون الإسلامية والأوقاف صفة مأموري الضبط القضائي في ضبط الجرائم والمخالفات التي تقع بالمخالفة لأحكام هذا القانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم**". ويبدو أن الاختلاف بينها بين النص الجديد ينحصر في أمرين الأول يتعلق بالجهة المانحة للصفة ففي النص القديم يمنح هذه الصفة وزير العدل والشؤون الإسلامية والأوقاف، في حين النص الجديد اقتصر على منح هذه

التقليدية لاسيما في الشق الإجرائي الذي لا زال يشكل الجانب الأضعف في المواجهة مقارنةً بالجانب الموضوعي، ففحص الأدلة التي تمتاز بأنها غير المرئية أو غير مقروءة إلا من خلال وسائط تقنية، ورصد الجناة الذين يستطيعون طمس أدلة الجريمة وإثباتها، وصعوبة ملاحقتهم إذ يستطيعون التخفي خلف الستار التقني، وإلى غير ذلك من صعوبات كثيرة تشكل تحدياً صريحاً على المكلفين بإثباتها وليس ذلك فحسب بل تشكل تحدياً على دول العالم بأسره[1]، لذلك كان التعاون الدولي أحد القنوات التي تسهل من مواجهة جرائم تقنية المعلومات وهو ما لم يتناوله المشرع في هذا المرسوم.

ويبدو فيما نراه قصوراً قد شاب تلك النصوص أن المشرع لم يلزم أيضاً المواطنين والجهات الخاصة كالشركات والمؤسسات بتقديم التسهيلات لمأموري الضبط القضائي أو المكلفين بتنفيذ أحكام القوانين، ذلك أن النص اقتصر على السلطات المحلية فقط، كذلك عدم تناول المشرع في هذا المرسوم المهام الموكلة لمأموري الضبط القضائي أو المكلفين بتنفيذ القوانين. واستناداً لنص المادة 49 لا يجوز لأي موظف من غير الوارد ذكرهم في قرار وزير العدل أن يقوم بإجراء من إجراءات الضبط القضائي في جرائم تقنية المعلومات، لأن ذلك سيترتب عليه بطبيعة الحال بطلان الإجراءات، باستثناء الموظفين ذوي الاختصاص العام وهم أعضاء النيابة العامة وأعضاء الشرطة[2].

ولما كانت غاية المشرع من تجريم نشر أو بث أي معلومات أو ثقافات من شأنها أن تتعارض مع القيم والمبادئ السائدة في الدولة وتخل بنظامها العام، ومن بين هذه المضامين تحصين مأموري الضبط القضائي أو المكلفين بتنفيذ أحكام القوانين، الذين أراد المشرع إضفاء الحماية القانونية عليهم من مختلف الاعتداءات التي قد يتعرضون لها عبر أدوات تقنية

الصفة من وزير العدل، أما الأمر الآخر وهو يتعلق بدور مأمور الضبط ذلك أن النص القديم يقرر دوره في ضبط الجرائم دون إثباتها، على خلاف النص الجديد الذي اقتصر على إثبات الجرائم.

1- حول خصائص هذه الجرائم وتحدياتها راجع د. محمد الهيتي، المرجع السابق، ص221 وما بعدها. ود. أيمن عبدالله فكري، المرجع السابق، ص96. وراجع تلك الخصائص أيضاً لدى: Philippe Rosé, Op, cit, P40.

2- حكم محكمة التمييز – دبي، طعن رقم 2011/39 جزائي.

المعلومات، وذلك باعتبار أن هذه الفئة ممثلين للدولة وممثلين أيضاً للمجتمع في إرساء دعائم العدالة وحماية الأفراد من مخاطر الاعتداء على حقوقهم ومصالحهم.

وبالتالي فإن أي اعتداءً عليهم إنما يشكل اعتداءً صريحاً على أجهزة العدالة في الدولة. وينفرد المشرع الإماراتي في إقرار مثل هذه الحماية في إطار التشريع الإلكتروني مقارنة بالتشريعات الإلكترونية الأخرى في الدول المقارنة، ومما لاشك فيه أن ذلك سيضمن احترام هؤلاء لاسيما مع انفلات الآراء عبر هذه الوسائط هذا من ناحية، وتضمن أيضاً أداء أعمالهم على أكمل وجه وهذا من ناحية أخرى.

وعلى أية حال؛ ينبغي لقيام الجريمة المنصوص عليها في المادة 28 ضرورة توافر ركنين مادي وآخر معنوي، أما الركن المادي ففيه عدد المشرع النماذج المخالفة لتنفيذ السلوك الإجرامي بالأسلوب التقني، وهما صورتان: **الأولى** إنشاء موقع إلكتروني أو إدارة هذا الموقع أو الإشراف عليه، وينصرف مفهوم ذلك أيضاً إلى إنشاء حسابات عبر مواقع التواصل الاجتماعي أو منتديات شبكة الإنترنت.

والصورة **الثانية** هي استخدام الجاني أو الجناة المحتوى المعلوماتي بنشره أو بثه عبر المنصات الواردة في الصورة الأولى باستخدام أدوات تقنية المعلومات بمختلف أنواعها كالحاسب الآلي والهاتف المحمول والتابلت أو غير ذلك من أدوات أخرى يمكن من خلالها نشر أو بث المحتوى المعلوماتي المخالف أياً كان شكله معلومات أو أخبار أو رسوم كرتونية، أو أي صور أخرى بشكل نصي أو مصور أو مقاطع فيديو، وسواء كان موضوعه سياسياً أو اقتصادياً أو ثقافياً أو دينياً أو غير ذلك[1]، من مواد تتضمن بطبيعتها رسالة تحريضية ضد المجتمع والدولة على حد السواء. وتختلف هذه الصورة عن الأولى في أن الثانية تفترض أن الجاني قد لا يكون على علاقة بمن أنشأ الموقع الإلكتروني أو الحساب أو يديره.

1- راجع المفاهيم الواردة لدى د. عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة ((المرسوم بالقانون الاتحادي رقم 5 لسنة 2012))، الكتاب الثاني، الطبعة الأولى– 2016، معهد دبي القضائي، دولة الإمارات العربية المتحدة، ص73 وما بعدها.

وقد اشترط المشرع أن يلجأ الجاني أو الجناة إلى اتخاذ إحدى هاتين الصورتين أو كلاهما معاً لتحريض الجمهور أو دفعهم إلى ارتكاب أفعال من شأنها أن تعرض أمن الدولة الداخلي للخطر ومن أبسط الأمثلة التي نسترشد بها في هذا الجانب ما أحدثته الثورات العربية أو كما قيل ثورات الربيع العربي التي خاطبت مشاعر بعض الشعوب بهدف التغيير ولكنها قادت مستقبل بلدانهم إلى هاوية الحروب والإفلاس والمجاعة والفرقة والهلاك. أو تعريض أمنها الخارجي للخطر كبث أو نشر معلومات تنال من سمعة الدولة وهيبتها أمام المحافل الدولية وهي من الأمثلة التي ينتهجها بعض المجرمين خلف ستار حرية التعبير عن الرأي والفكر.

وقد تتعرض مصالح الدولة العليا للخطر سواء كانت هذه المصالح خارجية كالإضرار على سبيل المثال بعلاقاتها مع دول أخرى، أو تهديد مصالحها الداخلية كالإضرار باقتصادها الوطني، ومما لاشك فيه أن تعريض مصالح الدولة للخطر ينصرف بشكل غير مباشر إلى الإضرار بأهم مقومات الدولة وهو المجتمع. كذلك يدخل في نطاق هذه الجرائم الإخلال بالنظام العام الذي ينصرف مفهومه إلى مجموعة الأسس والمبادئ الاجتماعية والدينية والاقتصادية والثقافية والسياسية وغيرها من أمور يقبلها كل مجتمع ويعمل بموجبها وفق ما يحكمها من قيم وعادات وتقاليد تسود فيه، ويعتبر الخروج عنها بمثابة تعدٍّ أو إخلال بالنظام العام، ويمكن اعتبار ما سبق من قبيل الإخلال بالنظام العام طالما كانت الممارسات عبر أدوات تقنية المعلومات أو الشبكة المعلوماتية تضمنت دعوات الخروج عن الأسس والمبادئ السائدة في المجتمع، فالدعوة لاتباع أفكار دينية متطرفة كعبدة الشيطان مثلاً أو نشر الدعوات التي تتبنى أفكار المثلية الجنسية أو غير ذلك مما يتعارض مع المجتمع الخليجي بصفة عامة والإمارات على وجه الخصوص.

إلى جانب ذلك أضاف المشرع تجريم الاعتداء على مأموري الضبط القضائي أو المكلفين بتنفيذ القوانين في مواجهة دعوات المغردين أو المحرضين التي تتناثر عبر شبكة الإنترنت ومواقع التواصل الاجتماعي منها التشكيك من قدرتهم على المواجهة، كما أنهم أصبحوا هدفاً للاعتداء عليهم بعبارات السخرية أو التطاول، ناهيك عن أنهم أصبحوا أيضاً أهدافاً للعنف عبر الألعاب الإلكترونية والذي سيلقي أثره الخطير على المدى البعيد.

جرائم المادة 28 من قبيل الجرائم العمدية التي تتخذ صورة القصد الجنائي العام، بعنصريه العلم والإرادة، أما العلم ويعني علم الجاني بأن سلوكه المتمثل في إنشاء موقع أو حساب إلكتروني أو إدارته أو الإشراف عليه من أجل نشر محتوى معلوماتي يحرض الجمهور على النحو الذي يعرض أمن الدولة ومصالحها العليا للخطر أو يمس نظامها العام، أو من شأنها أن تمس بمأموري الضبط القضائي أو أي من المكلفين بتنفيذ أحكام القوانين. أما الإرادة فتعني اتجاه إرادة الجاني بعد توافر العلم إلى لتحقيق هذه الأغراض.

المطلب الثالث تعديل المادة 42 الخاصة بشأن توقيع تدبير إبعاد الأجنبي:

نصت المادة 42 بعد تعديلها بموجب أحكام المرسوم بقانون اتحادي رقم 2 لسنة 2018، على أنه" **مع مراعاة حكم الفقرة الثانية من المادة (121) 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**".

يتحدث هذا النص عن تقرير تدبير جنائي بحق الأجانب الذين يرتكبون أحد الجرائم المنصوص عليها في هذا المرسوم بقانون[1]، وقد سبق أن تناولها المشرع كأحد التدابير الجنائية المقررة في قانون العقوبات الاتحادي الصادر سنة 1987، وأهمية هذا التدبير جعلت المشرع يتناولها في العديد من المراسيم بقوانين من بينها في المرسوم بقانون الصادر سنة 2006 المُلْغى[2]، كما قد نقلها أيضاً إلى المرسوم بقانون الحالي، وقد أجرى تعديلاً عليها في

1- الإبعاد لا ينطبق إلا على الأجانب، والأجنبي هو كل شخص لا يتمتع بجنسية الدولة التي يعيش في إقليمها. وقد كفل الدستور الإماراتي الصادر سنة 1971حق الأجنبي الذي يعيش على إقليمها بموجب المادة 40 التي نصت على أنه" **يتمتع الأجانب في الاتحاد بالحقوق والحريات المقررة في المواثيق الدولية المرعية أو المعاهدات والاتفاقيات التي يكون فيها الاتحاد طرفاً فيها، وعليهم الواجبات المقابلة لها**". وإذا كان هذا النص يقرر حقاً للأجنبي فقد أوجبت عليه مقابل ذلك عدة واجبات من بينها احترام قوانين الدولة.

2- تنص المادة 42 قبل التعديل على أنه" **تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها**". وقد

المرسوم بقانون رقم 2 لسنة 2018، حيث أضاف المشرع عبارة يراعي فيها تطبيق حكم الفقرة الثانية من المادة 121 من قانون العقوبات الاتحادي[1]، التي نظمت أحكام هذا التدبير.

وقد أطلق على هذا التدبير مصطلحات عديدة مغايرة لمصطلح الإبعاد، فعلى سبيل المثال نجد المشرع الفرنسي استخدم لفظ المنع أو الحظر من الأراضي الفرنسية، واستخدم المشرع اللبناني لفظ الإخراج والطرد في آن واحد، واستخدم المشرع العماني لفظ الطرد، إلا أن المشرع الإماراتي تبنى اللفظ الذي استخدمته معظم التشريعات العقابية ألا وهو الإبعاد.

ولم يشأ المشرع أن يضع تعريفاً لها، ومرد ذلك ارتباط هذا التدبير بالقانون الدولي الخاص وارتباطه بالقانون الجنائي، ويبدو أن هذا السبب الذي جعل الرؤية الفقهية تختلف وتخلط حولها تعريفها[2].

ومن جانبنا فنحن نميل إلى الاتجاه الفقهي الذي يعرف الإبعاد بالنظر إلى نوعيه الإداري والقضائي، فقد قيل بأن الإبعاد الإداري هو الإبعاد الذي يتم بناء على قرار صادر من السلطة التنفيذية باعتبارها صاحبة سيادة. أما الإبعاد القضائي فيقصد به إلزام الشخص الأجنبي بالخروج من الإقليم الوطني بناء على حكم قضائي صادر ضده بالإدانة لارتكابه

نص المشرع على هذا التدبير أيضاً في المادة 25 من المرسوم بقانون الملغي الصادر 2006، حيث نصت على أنه "**فضلاً عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالحبس وفقاً لأحكام هذا القانون**".

1- تنص المادة 121 عقوبات على أنه" **إذا حكم على أجنبي في جناية بعقوبة مقيدة للحرية أو في الجرائم الواقعة على العرض 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**".

2- راجع د. أحمد عبد الظاهر، إبعاد الأجانب في التشريعات الجنائية العربية، الطبعة الثانية– 2010، دار النهضة العربية، القاهرة، ص46 وما بعدها.

جرائم معينة يقرر لها المشرع الجنائي جزاء الإبعاد وطبيعة الإبعاد في التشريع الإماراتي من قبيل التدابير الاحترازية أو الوقائية ترتبط بخطورة الجاني مرتكب الجريمة[1].

وما يهمنا في هذا السياق هو الحديث عن الإبعاد كتدبير جنائي قرره المشرع الإماراتي في إطار المادة 42 المشار إليها، وتتجلى غايته من ذلك لاسيما في جرائم تقنية المعلومات، إلى ردع كل من استهان 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 المرسوم بقانون، وهو بالتالي شخص غير مرغوب فيه.

وعلى الرغم من قسوة هذا الإجراء كون المشرع أوجب على سلطة القضاء الحكم بهذا التدبير بصرف النظر عما إذا كان الحكم بالإدانة بعقوبة الحبس أو كانت العقوبة غرامة مالية، ذلك أن المرسوم القديم كان يقرر هذا التدبير لعقوبة الحبس فقط دون عقوبة الغرامة. كما أوجب المشرع إيقاع هذا التدبير على جرائم تعد أقل خطورة من جرائم جنائية أخرى وردت في قانون العقوبات كجريمة القتل العمد المنصوص عليها في المادة 28 عقوبات، ويرى البعض أن إيقاع هذا التدبير فضلاً عن تنفيذ المحكوم عليه للعقوبة المقررة أي تنفيذ التدبير بعد تنفيذ العقوبة الموقعة على الأجنبي إنما تشكل إفراطاً في فرض تدبير الإبعاد.

من أجل ذلك أجرى المشرع تعديلاً على حكم هذه المادة بموجب المرسوم بقانون اتحادي رقم 2 لسنة 2016، حيث أضاف عبارة في مقدمة النص تقضي بمراعاة حكم الفقرة الثانية من المادة 121 من قانون العقوبات الاتحادي، التي نصت على أنه"... **ويجوز للمحكمة في مواد الجنح الأخرى أن تأمر في حكمها بإبعاده عن الدولة، أو الحكم بالإبعاد بدلاً من الحكم عليه بالعقوبة المقيدة للحرية**"، مما يعني أن المشرع جعل توقيع تدبير الإبعاد

1- للمزيد من التفاصيل راجع د. محمد عبد الرحيم الناغي، جزاء الإبعاد في النظام القانوني لدولة الإمارات العربية المتحدة، مجلة الفكر الشرطي، العدد رقم 100 يناير 2017، شرطة الشارقة، دولة الإمارات العربية المتحدة، ص223.

جوازياً على المحكمة متى كانت الجرائم المنصوص عليها في المرسوم بقانون رقم 5 لسنة 2012 من قبيل جرائم الجنح المعاقب عليها بعقوبة سالبة للحرية أو الغرامة المالية، وقد استثنى من ذلك الجنح الواقعة على العرض. كما أجاز المشرع بموجب هذا التعديل أن تأمر المحكمة بإبعاد الأجنبي بدلاً من توقيع عقوبة سالبة للحرية في جرائم الجنح.

ويكون هذا التدبير وجوبياً على المحكمة مع مراعاة المادة 121 عقوبات اتحادي في الجرائم الواقعة على العرض سواء كانت جناية أم جنحة، كما يكون وجوبياً في جميع جرائم الجنايات المنصوص عليها في هذا المرسوم، ولا يتم تنفيذه إلا بعد انتهاء تنفيذ العقوبة المحكوم بها. إذاً وفقاً للتعديل الجديد؛ يشترط لتوقيع تدبير الإبعاد القضائي توافر عدة شروط، نوردها على النحو التالي:

1. ارتكاب إحدى جرائم تقنية المعلومات المنصوص عليها في المرسوم بقانون رقم 5 لسنة 2012.
2. صدور حكم من المحكمة المختصة بنظر الدعوى الجنائية في جرائم تقنية المعلومات.
3. يجب أن يكون الحكم صادراً بالإدانة في الجنايات والجنح الواقعة على العرض، أو أي جناية أخرى منصوص عليها في هذا المرسوم بقانون.
4. أن يكون الحكم صادراً بالإدانة في الجنح سواء كانت سالبة للحرية أو غرامة مالية.
5. أن يكون المحكوم عليه أجنبياً يقيم على أرض دولة الإمارات العربية المتحدة، ويسري الإبعاد على عائلة المبعد ما لم يكن أحدهم حاصل على جنسية الدولة.

النتائج والمقترحات:

في ختام هذه الدراسة؛ توصلنا إلى بعض النتائج والمقترحات التي نأمل أن تكون موضع اهتمام لدى الشارع الإماراتي، نوجزهما وفقاً للترتيب الآتي:

أولاً - النتائج:

1. تتميز سياسة المشرع الإماراتي بالمرونة استناداً إلى أمرين اثنين الأول يتعلق بالجانب الزمني حيث ألغى المشرع المرسوم بقانون الصادر سنة 2006، واستبدله

بالمرسوم بقانون الحالي بعد مرور ستة سنوات. أما الأمر الثاني ويتعلق بالجانب الموضوعي حيث استحدث المشرع أحكاماً موضوعيةً جديدةً لم تكن موجودة في المرسوم القديم.

2. أجرى المشرع تعديلين على المرسوم بقانون رقم 5 لسنة 2012، وقد لاحظنا ربطاً غائياً بينهما محورهما هو مواجهة المساس بأمن الدولة، ذلك أن التعديل الأول جاء ليواجه التحايل على العنوان البروتوكولي الذي انفرد المشرع بتجريمه مقارنة بالتشريعات الأخرى، وقد شدد المشرع عقوبتها بأن غير وصفها من جنحة إلى جناية ورفع سقف العقوبة السالبة للحرية والغرامة المالية. وجاء التعديل الثاني بشأن أنشطة إنشاء وإدارة المواقع الإلكترونية أو الإشراف عليها من قبل جماعات إرهابية أو جماعات محرضة. وقد يكون التحايل على العنوان البروتوكولي منفذاً لهما لإتمام تلك الأنشطة الإجرامية.
3. تميل سياسة المشرع من واقع هذين التعديلين إلى الرغبة في تحقيق الموازنة بين تشديد العقاب وبين إقرار تدابير وقائية أو إصلاحية مستحدثة أدرجها في التعديل الثاني وهما المناصحة والمراقبة الإلكترونية، وتتأكد تلك الرغبة في إعادته للنظر في التدبير إبعاد الأجانب حيث راعى في تطبيقها ما ورد في حكم المادة 121 من قانون العقوبات.
4. هناك تشريعات محلية جديرة بأن تكون نموذجاً تشريعاً يُهتدى به عند صياغة لائحة خاصة بحماية البيانات الشخصية، وهو القانون المتعلق بتنظيم التجارة العالمية في دبي رقم 1 لسنة 2007 بشأن حماية البيانات، وأيضاً القانون رقم 26 لسنة 2015 بشأن تنظيم نشر وتبادل البيانات في إمارة دبي.
5. تتعدد المصطلحات والتعريفات المتعلقة بالجانب الإلكتروني في هذا المرسوم والمراسيم بقانونين الأخرى ذات الشأن، وهناك حاجة إلى إعادة النظر في هذا المسلك لاسيما وأن بعض التعريفات لم تدرج ضمن هذه المواد وهو تعريف البيانات الشخصية ومزود الخدمة، فضلاً عن وجود بعض المصطلحات الغامضة كمصطلح "سري" ومصطلح" إساءة".

6. على الرغم من قيام المشرع بإجراء تعديلات موضوعية على أحكام المرسوم بقانون محل البحث، إلا أنه لم يغفل الجانب الإجرائي تماماً منذ المرسوم القديم، وهذا هو الجانب الأهم في مواجهة جرائم تقنية المعلومات بصفة عامة، والجرائم التي تناول المشرع تعديلهما في المرسومين بصفة خاصة.

ثانياً – المقترحات:

1. ضرورة تبني المشرع الإماراتي لائحة موحدة تتضمن كافة المفاهيم المتعلقة في البيئة الإلكترونية، بحيث تكون مرجعاً لكافة التشريعات ذات الشأن، مع الأخذ بعين الاعتبار تضمين مفهوم البيانات الشخصية وآلية معالجتها وتحديد مسؤولية مزودي خدمة الإنترنت.
2. ضرورة الاهتداء بالتشريعات المحلية الخاصة المشار إليها عند تنظيم حماية البيانات الشخصية خصوصاً وأنها نماذج تتطابق مع المعايير الأوروبية.
3. ضرورة الاهتمام بالجانب الإجرائي وذلك وفق ما يتلاءم وسياسة المشرع من الناحية الإجرائية، وفحوى هذا الاهتمام تبني القواعد الواردة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بما في ذلك فكرة التعاون الدولي، فلا جدوى من مواجهة هذه الجرائم دون إحكام الجانب الإجرائي خصوصاً وأنها جرائم تتميز بطبيعة عابرة للحدود الوطنية.

المراجع

أولاً - مراجع باللغة العربية:

1. أحمد عبد الظاهر، إبعاد الأجانب في التشريعات الجنائية العربية، الطبعة الثانية– 2010، دار النهضة العربية، القاهرة.
2. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتوتير، الطبعة الأولى– 2013، دار النهضة العربية، القاهرة.
3. إمام حسنين عطا الله، جرائم تقنية المعلومات في التشريعات والصكوك العربية، طبعة أولى–2017، مركز الدراسات والبحوث، جامعة نايف للعلوم الأمنية، الرياض.

4. أيمن عبدالله فكري، جرائم نظم المعلومات، 2007، دار الجامعة الجديدة، الإسكندرية.
5. زين العابدين عواد الكردي، جرائم الإرهاب الإلكتروني- دراسة مقارنة، الطبعة الأولى 2018، منشورات الحلبي الحقوقية، بيروت- لبنان.
6. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، مجلة الحقوق، جامعة الكويت، العدد رقم 3 لسنة 35، سبتمبر 2011، الكويت.
7. سعيد بت عمر البيشي، ورقة عمل بعنوان/ عرض تجربة المملكة العربية السعودية في المناصحة وإعادة التأهيل، مقدمة في الحلقة العلمية بعنوان" مكافحة الإرهاب"، التي أقيمت في الرياض في الفترة ما بين 15-17 سبتمبر 2011، التقرير الإحصائي لجهود إدارة المناصحة بمركز محمد بن نايف للمناصحة والرعاية.
8. محمد الهيتي، جرائم الحاسوب، الطبعة الأولى-2006، دار المناهج، عمان.
9. محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، طبعة أولى-2016، دار النهضة العربية، القاهرة.
10. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى- 2016، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية.

ثانياً - مراجع باللغة الإنجليزية:

1. Andrew Murray, Information Technology Law- The Law and Society, 3rd edition-2016, Oxford University Press, United Kingdom.
2. Anthea Hucklesby and Ella Holdsworth, Electronic Monitoring in England and Wales, May 2016, University of Leeds, UK, the Criminal Justice Programme of the European Union.
3. IT Governance Privacy Team, EU GENERAL DATA PROTECTION REGULATION (GDPR), 2Edition- 2017, IT Governance Publishing.
4. Jonathan Clough, Principles of Cybercrime, S-Edition, 2015, Cambridge University Press, United Kingdom.

ثالثاً - مراجع باللغة الفرنسية:

1. Luc Grynbaum, Caroline Le Goffic, Lydia Morlet-Haïdara. Droit des activités numériques, 1Edition, 2014, Dalloz, Paris.
2. Michèle-Laure Rassat, Droit pénal général, 4éd- 2017, ellipses, Paris.
3. Myriam Quéméner et Yves Charpenel, Cybercriminalité - Droit pénal appliqué, 2éd-2010, Economica, Paris.

4. Philippe Rosé, La ciminalité informatiqué à l'horizon, Analyse prospective, 2005, IHESI- L'Harmattan, Paris.

رابعاً - مصادر أخرى:

1. الجريدة الرسمية لدولة الإمارات العربية المتحدة، العدد رقم540- السنة 42، بتاريخ 26 أغسطس 2012.
2. الموقع الإلكتروني للأمانة العامة لجامعة الدول العربية.
https://carjj.org/sites/default/files/qnwn_lmrt_lrby_lstrshdy_lmkfh_jrym_tqny_lmlwmt.pdf
3. 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-2-لسنة-2018-بتعديل-ب/
4. مواقع تتعلق بدراسات حول مخاطر الجرائم الإلكترونية في دولة الإمارات.
https://aitnews.com/2017/08/28/نورتن-تكشف-عن-أحدث-تقاريرها-حول-مخاطر-ا/
https://www.menaherald.com/tech/information-technology/372-مليون-مستخدم-ضحايا-الجريمة-الإلكترونية-في-الإمارات-عام-2017-مع-خسائر
5. الموقع الإلكتروني لمحكمة العدل الأوروبية.
ARRÊT DE LA COUR (grande chambre), Dans l'affaire C-275/06,, 29 janvier 2008.
http://curia.europa.eu/juris/document/document.jsf?docid=70107&doclang=fr#Footnote*
http://fr.jurispedia.org/index.php/Statut_juridique_de_l%27adresse_IP_(fr)#cite_note-22
6. الموقع الإلكتروني لصحيفة الاتحاد الإلكترونية مقال بعنوان/ حماية البيانات الشخصية، نشر بتاريخ 27 يونيو 2018.
https://www.alittihad.ae/wejhatarticle/99484/حماية-البيانات-الشخصية
7. الموقع الإلكتروني المعاني.
https://www.almaany.com/ar/dict/ar-ar/تحايل

8. الموقع الإلكتروني الاقتصادي، بعنوان/ الإمارات توضح طبيعة العقوبة المفروضة على مستخدمي VPN، نشر بتاريخ 2 أغسطس 2016.
https://aliqtisadi.com/804988-الإمارات-تحارب-الجرائم-الالكترونية/
9. الموقع الإلكتروني مدونة جديد الإنترنت، مقال بعنوان/ إنشاء الكثير من الحسابات المزيفة على الفيسبوك بطريقة شرعية وبدون بريد إلكتروني.
http://newinternt.blogspot.com/2015/09/blog-post_19.html
10. الموقع الإلكتروني الإمارات اليوم، مقال بعنوان/ "تنظيم الاتصالات" تحقق في رسائل مفبركة حول منع استخدام شبكات VPN.
https://www.emaratalyoum.com/business/local/2018-01-25-1.1065037
11. موقع البيان الإلكتروني، مقال بعنوان/رسائل احتيال مالي تطال المستخدمين بعد اختراق "الواتساب"، نشر بتاريخ 3 أكتوبر 2018.
https://www.albayan.ae/across-the-uae/news-and-reports/2018-10-03-1.3373257
12. الموقع الإلكتروني لجامعة كورنال الأمريكية.
U.S. Code › Title 18 › Part II › Chapter 227 › Subchapter B › § 3563 - Conditions of probation
https://www.law.cornell.edu/uscode/text/18/3563
http://28uzqb445tcn4c24864ahmel.wpengine.netdna-cdn.com/files/2016/06/EMEU-Electronic-monitoring-in-England-and-Wales.pdf