مجلة الدراسات القانونية والاقتصادية

المواجهة التشريعية لجريمة الارهاب عبر الفضاء الإلكتروني في ظل جائحة كورونا (دراسة مقارنة)

دكتور أحمد السيد عبد الرازق بطور
المدرس المنتدب بكلية الحقوق
جامعة حلوان

الملخص باللغة العربية :

مع ظهور فيروس كورونا تغيرت الأحوال وتبدلت الأمور وأصبح للحياة منظور آخر، فمع أغلب بل وكل المعاملات في صورتها العادية التقليدية إنتقلنا إلى الحياة الألكترونية والمعاملات التقنية في أغلبها، ومع الحياة والحرية بدون قيود الى إنتشار رائحة الموت وفرض الحظر والعزل الصحي، ومن نتاج كل ذلك ظهرت عائلة جديدة من الجرائم السيبرانية في ظل الاستعمال المفرط لوسائل التواصل الاجتماعي وأدوات الفضاء السيبراني فكانت جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا من أخطر جرائم الفضاء السيبراني.

الكلمات الدالة: جائحة كورونا، الارهاب، الفضاء الألكتروني، الفضاء السيبراني، الاجرام الألكتروني، المواجهة التشريعية.

Abstract

With the emergence of the Corona virus appearance, conditions have changed and things have changed, and life has a different perspective with most and even all transactions in their normal traditional form. We have moved to electronic life and technical transactions in most of them and with life and freedom without restrictions, to the spread of death smell and the imposition of bans and sanitary isolation. As a result of all this, a new family of cybercrimes has emerged with excessive use of social media and cyberspace tools. The crime of terrorism via cyberspace during Corona pandemic was one of the most dangerous crimes in cyberspace.

Keywords: Corona pandemic , terrorism , electronic space, cyberspace , cybercrime , legislative confrontation

مقدمة :

(ISSN: 2356 - 9492)

يمر العالم اليوم بأزمة، تسبب بها ظهور فيروس كورونا المستجد، لم يسبق لها مثيل في تاريخنا الحديث من حيث أبعادها وأضرارها التي طالت جميع نواحي الحياة في شتى مجالاتها، والتي تبدو كإعصار هائج يصعب التنبؤ بأثاره المدمرة، وفي هذا الشأن يجد العديد من الباحثين[١] أنفسهم مكتوفي الأيدي نحو التنبؤ بما سوف يكون على أرض الواقع، وكيف سيصبح شكل العالم وأوضاعه ما بعد جائحة كورونا.

وتُعد الثورة التكنولوجية وخاصة ثورة الاتصالات من أهم التطورات –إن لم تكن أهمها– التي يعيشها العالم اليوم[٢]، وفي الوقت الذي تطلعت فيه البشرية الى استغلال هذا المناخ العالمي الجديد لتحقيق مزيد من التقدم والرخاء، فقد استغلت الجماعات الاجرامية المنظمة ما أتاحه العصر الجديد من امكانيات، وما وفره من أساليب ووسائل لاستحداث أنماط جديدة من الجرائم المنظمة العابرة للحدود الوطنية، والتي من أخطرها الاجرام الألكتروني. وبعد ظهور فيروس كورونا المستجد (كوفيد ١٩) –الجائحة العالمية– أضحت أزمة ظهوره تفرض تحدياً عالمياً يتعين على جميع الدول مواجهته من خلال التعامل الافتراضي عن بُعد باستعمال معطيات التقنيات التكنولوجية للتواصل بدءاً بتقنيات المحادثة المرئية، والبريد الألكتروني، مروراً بكافة وسائل التواصل الاجتماعي وصولاً إلى كافة قطاعات المجتمع، وذلك من أجل توفير الاحتياجات الاساسية للمجتمع. وبالتالي أصبحت العديد من التصرفات –ومنها القانونية– إن لم يكن أغلبها تتم عن بُعد، إذ تم الانتقال من العالم التقليدي الى العالم الافتراضي وهو ما يعني أيضاً ظهور أنماط غير تقليدية من الاجرام تستهدف المستشفيات والشركات وغيرها من الوظائف الحيوية في المجتمع كاستخدام هذه التقنيات في اختراق أنظمة المعلومات للدول، وممارسة أعمال االتجسس وغيرها من الأعمال التي تؤثر على الأمن القومي الداخلي وعلى السلم والأمن الدوليين، فظهر ما يُعرف بـ "إرهاب الفضاء الألكتروني" من

١) عبدالله بن خالد بن سعود الكبير آل سعود: إستغلال الأزمات: الجماعات الارهابية، اليمين المتطرف، والجريمة المنظمة في ظل فيروس كورونا، المجلة العربية للدراسات الأمنية، مجلد (٣٦)، العدد (٢)، يوليو ٢٠٢٠، ص ١٥٩ وما بعدها.
٢) أم السعد بن زينب: الجريمة الألكترونية وإجراءات مكافحتها في المجتمع الجزائري، المؤتمر الدولي المحكم: الجريمة والمجتمع، عمان، ٢٠١٧، ص ١٩٣.

خلال إنشاء حسابات خاصة بالارهاب لنشر وترويج الافكار المتطرفة وتمويل حساباتها ونشر الفيروسات واختراق المواقع، كما تقوم بتوظيف هذه التقنيات في بث خطابات الكراهية والترويج للأفكار الهدامة.

أهمية الدراسة:

تبدو أهمية هذه الدراسة في أن الارهاب عبر الفضاء الألكتروني تتمثل خطورته في سهولته بخلاف الارهاب بمدلوله التقليدي، فيمكن القيام بالهجمات الارهابية من المنزل دون بذل أي جهد يُذكر، بالاضافة إلى تعدد أشكاله وتنوع أساليبه وأثاره المدمرة، فعن طريق رابط يرسله (الجاني) إلى شريكه عن طريق الإنترنت تحدث العديد من الأثار المدمرة والتخريب مع صعوبة أو استحالة تتبع ذلك الخطاب أو الرسالة مما يشكل ملاذاً آمناً للارهابيين، وبالتالي بات الارهاب عبر الفضاء الألكتروني يمثل تهديداً واضحاً للأمن القومي للدول ويمثل خطراً يفوق المعقول على الأفراد وآمنهم وحياتهم وهو ما يجعل دراسة هذه الظاهرة من كافة جوانبها أمراً لا بد منه.

منهج الدراسة:

تتناول هذه الدراسة جريمة الارهاب عبر الفضاء الألكتروني من خلال الاعتماد على المنهج الوصفي لبيان مفهوم جريمة "الارهاب عبر الفضاء الألكتروني" وبيان صورها. وقد تم التعرض للنصوص القانونية المتعلقة بالموضوع من خلال المنهج الاستقرائي، بالاضافة إلى تحليل بعض نصوصها من خلال المنهج التحليلي مع بيان آليات مواجهة هذه الجريمة تشريعياً مما أقتضى سلك المنهج المقارن.

إشكالية الدراسة:

تعالج هذه الدراسة مشكلة على درجة كبيرة من الأهمية والخطورة، خاصة في ظل عدم وجود تشريعات جنائية كافية تواجه مثل هذه النوعية من الإجرام المستحدث والمتطور بإستمرار والذي يقوم باستخدام وسائل التكنولوجيا والتقنيات الحديثة كوسيلة لجريمة أو مجالاً لها، حيث تقوم بعض الدول بالإكتفاء باللجوء إلى النصوص التقليدية في قانون العقوبات وتطبيقها عند اللزوم، في حين ذهبت دول أخرى إلى محاولة تطويع وتحديث القوانين الجنائية القائمة لتكون قادرة على الصمود في مواجهة هذا السيل العارم

(ISSN: 2356 - 9492)

من الإجرام، ومن ناحية ثالثة قام البعض الأخر بإفراد قوانين خاصة لمجابهة مثل هذه النوعية من جرائم التقنيات الحديثة.

لذا جاءت هذه الدراسة لتجيب عن تساؤل هام ورئيسي:

- مدى كفاية النصوص التشريعية وفعاليتها في مواجهة جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا ؟

ويتفرع عنه عدد من التساؤلات التالية:

- مفهوم الارهاب عبر الفضاء الألكتروني ؟
- هل تتميز الدعوى الجنائية بخصوص جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا بذاتية معينة ؟
- ما هي صور ومظاهر جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا؟
- أليات مواجهة جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا؟

خطة الدراسة:

تم تقسيم هذه الدراسة إلى مبحثين كالتالي:

المبحث الأول: ماهية الارهاب عبر الفضاء الألكتروني.

المبحث الثاني: أليات مواجهة جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا.

المبحث الأول

ماهية الإرهاب عبر الفضاء الألكتروني

إن مجرد التلفظ بكلمة الارهاب يثير الرعب في النفس ويُسري قشعريرة في الأبدان ويحمل الانسان إلى عالم أخر يفقد فيه كيانه، وإذا كان حديثنا عن الارهاب في صورته التقليدية فما بالك لو انتقلنا إلى العالم الافتراضي حيث الارهاب عبر الفضاء الألكتروني، وما يتميز به من استخدام المواد المعلوماتية والوسائل الألكترونية التي جلبها عصر التقنية المعلوماتية حيث المكان الذي تعمل به أجهزة وبرامج الحاسب وشبكات الأنترنت. وبالتالي كان لا بد علينا أن نوضح مفهوم مصطلح "الارهاب عبر الفضاء

الألكتروني" قبل أن نتعمق ونتوغل في أعماق هذه الجريمة وهو ما سنوضحه في المطلب الأول.

المطلب الأول

مفهوم الإرهاب عبر الفضاء الألكتروني

عرف البعض الارهاب عبر الفضاء الألكتروني بأنه: "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الألكترونية الصادر من الدول أو الجماعات أو الأفراد على الانسان نفسه بغير حق بشتى أنواعه وصور الإفساد في الأرض"[٣].

في حين ذهب البعض الأخر الى أنه "هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة ألكترونياً، توجه من أجل الانتقام أو إبتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة، وبالتالي لكي يُنعت شخصاً ما بأنه إرهابياً على الانترنت وليس فقط مخترقاً، فلا بد وأن تؤدي الهجمات التي يشنها الى عنف ضد الاشخاص أو الممتلكات أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب"[٤] ، وفي اتجاه ثالث وتحت مفهوم الارهاب الألكتروني عرفه البعض أنه هو "استخدام التقنيات الرقمية لإخافة وإخضاع الأخرين، أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية"[٥]، واستخلاصاً لما سبق ومن خلال ما استعرضناه من تعريفات يتضح لنا أن أهم ما يميز الارهاب عبر الفضاء

---

٣) فريدة بن عمروش: الارهاب الألكتروني: دراسة في إشكاليات المفهوم والأبعاد، المجلة الجزائرية للعلوم الاجتماعية والانسانية، مجلد (٨)، العدد (٢)، ديسمبر ٢٠٢٠، ص ٢١٨. للمزيد أيضاً أنظر:
Jordan J. Plotnek, Jil Slay: Cyber Terrorism; A homogenized taxonomy and definition, Review computers & security, Vol. 102, March 2021, 102145, p. 7-8.

٤) الشيماء محمد محمود حسن: دور الدولة في الحد من أثار الارهاب الرقمي في الأسرة المصرية، دراسة تحليلية، مجلة بحوث الشرق الأوسط، العدد (٥٥)، مايو ٢٠٢٠، ص ١٥ وما بعدها.

٥) فهد يوسف الكسابسة: الارهاب الألكتروني عبر الانترنت في التشريع الأردني –دراسة مقارنة، مجلة العلوم القانونية والسياسية، مجلد (٩)، السنة (٥)، العدد (١)، كانون أول ٢٠١٥، ص ١٤٣. وللمزيد أنظر أيضاً:
- Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, Hossein Taji: Cyber terrorism challenges, the need for global response to a multi-jurisdictional crime, computer low & security review, Vol. 29, issue 3, June 2013, p. 207-215.

(ISSN: 2356 - 9492)

الألكتروني هو استخدامه للتقنيات الرقمية والفضاء الإفتراضي حيث توجد الأنظمة الرقمية والشبكة المعلوماتية والأجهزة الحاسوبية والبرامج التخريبية والتدميرية التي تستخدم في بث الرعب والعدوان والاعتداء سواء بطريقة مباشرة أو غير مباشرة على الأفراد أو المؤسسات كالمستشفيات وشركات الكهرباء والمياة والاتصالات والأنظمة المصرفية والعسكرية وغيرها وأياً كان الدافع منها ما يستوجب مسايرته قانونياً.

ومن جماع ما تقدم يمكننا تعريف الارهاب عبر الفضاء الألكتروني بأنه هو كل عمل غير مشروع يتم عن طريق استغلال الوسائل الألكترونية أو النظام المعلوماتي أو شبكة المعلومات الدولية –الانترنت– ويكون موجهاً ضد الأفراد أو الجماعات أو الدول بقصد ارتكاب أعمال تخريبية أو تدميرية أو عدوانية أو ارهابية عن طريق هذه الوسائط مما قد يترتب عليه اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير البيانات أو التلاعب بها وسواء كانت الخسائر مادية أو معنوية. ولما كان ذلك كذلك وبعد ما تم سرده مما سبق فإن هناك تساؤل يفرض نفسه على نطاق البحث خصوصاً بعد ما وضح بيانه من عناصر توضح مدى خطورة هذه الجريمة ومدى ما يترتب عليها من آثار بشعة ألا وهو: هل تبقى الدعوى الجنائية بشأن جريمة الارهاب عبر الفضاء الألكتروني شأنها شأن أي جريمة تطبق نحوها القواعد الإجرائية العادية أم أن هناك خصوصية معينة تجاه هذه الجريمة ؟ هذا ما سنحاول إلقاء الضوء عليه خلال السطور القادمة إن شاء الله.

- **تفرد الدعوى الجنائية بشأن جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا في التشريع المصري والمقارن:**

أوضحت الشرطة الجنائية الدولية (الانتربول) في تقرير لها أن هناك عدد من المواقع الألكترونية تبيع منتجات طبية غير مشروعة وكمامات مقلدة منتشرة على مواقع التواصل الاجتماعي والشبكة العنكبوتية، بالاضافة الى قيام البعض برفع أسعار بعض السلع والمستلزمات على الأشخاص من خلال المتاجر الألكترونية والأسواق المنتشرة على شبكة الانترنت مستغلين مرور العالم بجائحة كورونا.

وبما أن المجتمع الدولي أمام جريمة – الارهاب عبر الفضاء الألكتروني– اجتاحت العالم بسرعة جنونية، فكان لازم ولا بد من تطويع كافة الأحكام والاجراءات لمواجهة سرعة الانتشار، كالتجاوز عن بعض القيود التي تحد من حرية النيابة العامة في تحريك الدعوى الجنائية عن جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا والتي سنوضحها فيما يلي:

١-رفع القيد على إقامة الدعوى الجنائية: ينص القانون المصري رقم ٩٥ لسنة ٢٠٠٣ على أن النيابة العامة غير مقيدة عند مباشرتها التحقيق ورفع الدعوى في الجرائم الارهابية[٦] بقيد الطلب المنصوص عليه في قانون الاجراءات الجنائية. إلا أن المشرع قد عاد وقرر قيد –وقتي– لاقامة الدعوى وذلك كوسيلة للحد من ظاهرة الارهاب وهو ما نص عليه بالقانون رقم ٩٧ لسنة ١٩٩٢ في مادته العاشرة التي تنص على أن "لا تقام الدعوى الجنائية ضد من إنتمى بأي صفة كانت الى إحدى الجمعيات أو الهيئات أو المنظمات .... المنصوص عليها في المادة ٨٦ مكرر عقوبات، أو بادر خلال شهر من تاريخ العمل بهذا القانون بإبلاغ النيابة العامة أو سلطات الأمن .... عن التنظيم وتوقفه عن ممارسة أي نشاط فيه، وكذلك المادة التي تنص على أن "لا تقام الدعوى الجنائية الناشئة عن حيازة أو إحراز أسلحة أو ذخائر أو .... اذا بادر الحائز أو المحرز من تلقاء نفسه بتسليمها الى النيابة العامة أو لسلطات الأمن خلال المدة المشار إليها في الفقرة السابقة، ولا يسري ما تقدم على الحالات التي بدأ فيها التحقيق أو رفعت فيها الدعوى الجنائية"، وبالتالي يتضح أن هذا القيد على حرية النيابة العامة هو قيد وقتي لكونه مقرر لمدة شهر من تاريخ ١٩ يوليو ١٩٩٢ –ومحدد– خاص فقط للمتهمين بالانضمام لاحدى التنظيمات الارهابية غير المشروعة، وبالتالي متى شكل سلوك المتهم جريمة في حد ذاته فلا محل لاعمال ذاك النص وهو ما يسري من باب أولى على جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا وما تحمله من ظروف إستثنائية. وفي نفس الصدد تضمن **القانون رقم ٣ لسنة ٢٠٠٤ بشأن**

٦) رجاء محمد بوهادي: القواعد الاجرائية الاستثنائية لمواجهة جرائم الارهاب، المجلة الليبية العالمية، العدد (٢١)، يونيو ٢٠١٧، ص ١٢ وما بعدها.

(ISSN: 2356 - 9492)

مكافحة الارهاب في قطر بعض الأحكام الإجرائية الخاصة بملاحقة الجرائم الارهابية ومنها ما تنص عليه المادة ١٧ منه على ألا تتقيد النيابة العامة في مباشرتها للتحقيق وتحريك الدعوى في الجرائم الارهابية بقيد الشكوى أو الطلب المنصوص عليها في قانون الإجراءات الجنائية. وبالتالي فإن دل ذلك فإنما يدل على خطورة هذه الجريمة وتشعب أثارها وأمتداده لجوانب عدة في المجتمع ولقطاعات حيوية كالقطاع الصحي والمستشفيات خصوصاً في ظل جائحة كورونا.

إلا أنه على الجانب الأخر ومن خلال التدقيق في بعض التشريعات العربية نجد منها على الرغم من اصاره لقوانين خاصة بمكافحة الارهاب في العصر المعلوماتي إلا أنها خلت من أي نص يتضمن الإشارة إلى عدم التقيد بقيود رفع وتحريك الدعوى الجنائية بشأن جريمة الارهاب سواء صورتها التقليدية أو عبر الفضاء الألكتروني **كقانون رقم ٥٨ لسنة ٢٠٠٦ بشأن حماية المجتمع البحريني**[٧] من الأعمال الارهابية وأيضاً **القانون رقم ٦٠ لسنة ٢٠١٤** بشأن جرائم تقنية المعلومات مما يعد سقطة تستوجب إعادة النظر في هذه التشريعات وتعديلها بما يتوافق مع طبيعة هذه الجرائم الارهابية المرتكبة في الفضاء الرقمي خصوصاً في ظل الوباء العالمي.

٢- عدم تقادم الدعوى الجنائية: إدراكاً من المشرع المصري لمدى خطورة الجريمة الارهابية وأنها تمس وجدان وكيان المجتمع المصري، مما لا يستقيم معه أن يستفيد الجاني من القواعد الاجرائية الخاصة بالتقادم المنصوص عليها في **المادة (١٥) من قانون الاجراءات الجنائية المصري**[٨]، حيث نصت المادة (٥٢) من القانون رقم (٩٤) لسنة ٢٠١٥ بشأن مكافحة الارهاب على أنه "لا تنقضي الدعوة الجنائية في الجرائم الارهابية ..... بمضي المدة". وهو نفس ما سار عليه **المشرع الاماراتي في قانون**

٧) دراسة حول تشريعات مكافحة الارهاب في دول الخليج العربية واليمن، الأمم المتحدة، المكتب المعني بالمخدرات والجريمة، ص ١١١ وما بعدها.

٨) الهاني محمد طايع رسلان: الاحكام الاجرائية الحديثة لمواجهة الجرائم الارهابية في التشريع المصري والاماراتي، مجلة جنوب الوادي للدراسات القانونية، العدد (٢)، ديسمبر ٢٠١٧، ص ٢٠٢. وللمزيد أنظر:

- Giovanni Bottazzi, Gianluigi Me: Responding to cyber crime and cyber terrorism, botnets an insidious threat, 2014, p. 231-257.

الارهاب رقم ٧ لسنة ٢٠١٤ حيث تنص المادة (٥٢) في فقرتها الأولى على أنه "استثناء من نص الفقرة الثانية من المادة (٢٠) من قانون الاجراءات الجزائية، لا تنقضي الدعوى الجزائية بمضي المدة في الجرائم الارهابية". وقام **المشرع الفرنسي بتعديل المادة ١/٧٠٦ من قانون الإجراءات الجنائية** بما يجعل جريمة الارهاب لا تسقط بالتقادم. ومما لا شك فيه أن السياسة الجنائية التي سار عليها المشرع الجنائي المصري والإماراتي والفرنسي تتركز على منطق قانوني سليم يمد مبرره في وجوب ألا يستفيد المتهم في هذه الجريمة التي تتسم بدرجة كبيرة من الخطورة وتروع المجتمع وتهدد أمنه بالقواعد الإجرائية المتعلقة بتقادم الدعوى الجنائية الناشئة عنها، وإذا كان ذلك بخصوص جريمة الارهاب في صورتها التقليدية، فما بالك بها في نسختها عبر الفضاء الإفتراضي التي تشكل أكثر خطورة وأشد جسامة بما يجعل هذه الأحكام تمتد إليها وتنطبق عليها من باب أولى.

وعلى خلاف ذلك نجد أن **المشرع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥** في شأن مكافحة جرائم تقنية المعلومات[٩] قد نص المادة (١٨) منه على أنه "تسقط الدعوى الجزائية المنصوص عليها في هذا القانون بحسب مدة العقوبة ..." وهو ما يعد من وجهة نظرنا المحدودة غفلة تستدعي وجوب التدخل وتعديل هذه المادة لما تمثله جرائم العصر الرقمي على وجه العموم وجريمة الارهاب عبر الفضاء الإفتراضي على وجه الخصوص في صورها المتعددة الواردة في هذا القانون تعد ساخر على حق المجتمع وقطاعاته الحيوية وعلى حق الانسان في حماية صحته والحفاظ عليها من أي ضرر يمس بها خصوصاً في ظل جائحة كورونا كما هو الحال في التعد على البيانات الشخصية للمرضى في المستشفيات وإفشاء أسرارهم المرضية أو في حالة الإتلاف عمداً لمستند ألكتروني يتعلق بالفحوصات الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية أو سهل للغير مثل ذلك أو مكنه منه وذلك من خلال العالم الإفتراضي.

٩) قانون رقم ٦٣ لسنة ٢٠١٥، في شأن مكافحة جرائم تقنية المعلومات .

(ISSN: 2356 - 9492)

٣- عدم سقوط العقوبة المحكوم بها بمضي المدة: لما كانت جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا يترتب عليها من أثر سيء في النفوس لما تسببه من ذعر وعدم استقرار ونشر للفتنة واستغلال لأسوء الظروف في ظل وباء عالمي فقد استثناها المشرع المصري من الاحكام بشأن سقوط العقوبة وهو ما نصت عليه المادة (٥٢) من **القانون المصري رقم (٩٤) لسنة ٢٠١٥** بشأن مكافحة الارهاب التي تنص على أنه "..... ولا تسقط العقوبة المحكوم بها بمضي المدة". وقد قام **المشرع الليبي في المادة (٢٦) من قانون رقم (٣) لسنة ٢٠١٤** بإلغاء حق تقادم العقوبة المحكوم بها في الدعوى الجنائية من جرائم الارهاب[١٠]. وفي اتجاه مغاير لذلك ذهب **المشرع التونسي في المادة (٦١) من القانون رقم ٧٥ لسنة ٢٠٠٣** بشأن مكافحة الارهاب ومنع غسل الأموال إلى النص على أنه "تسقط العقوبة المحكوم بها في الجرائم الارهابية، ...." وهو ما نراه قد جانب الصواب نظراً لطبيعة هذا النوع من الإجرام في ضوء ما يتمتع[١١] به من ذاتية معينة.

وفي نهاية هذا المطلب وبعد أن تعرفنا على مفهوم الارهاب عبر الفضاء الألكتروني نجد أن هناك حاجة ملحة تفرض نفسها على نطاق البحث وهي كيف يمكن التعرف على هذه الجريمة ؟ وهل تقع في صورة واحدة أم يمكن أن يكون لها أكثر من هيئة ؟ هذا ما سوف نحاول التعرف عليه إن شاء الله في المطلب القادم.

المطلب الثاني

مظاهر جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا

١- الاحتيال أو التصيد عبر الفضاء الألكتروني: فمن المعروف أن نتيجة لظروف حظر التجول في ظل جائحة كورونا، فقد أصبحت منصات ومواقع التواصل الاجتماعي ملتقى للتسوق مما يتطلب ادخال البيانات الشخصية[١٢] لروادها مع أرقام

١٠) رجاء محمود بوهادي: مرجع سابق، ٢٠١٧، ص ١٤ وما بعدها.
١١) قانون رقم ٧٥ لسنة ٢٠٠٣ لمكافحة الارهاب ومنع غسل الأموال.
١٢) معاذ سليمان راشد محمد الملا: جرائم تقنية المعلومات وجائحة فيروس كورونا بين الواقع والمأمول: دراسة تأصيلية، مجلة كلية القانون الكويتية العالمية، مجلد (٩)، العدد (٣٤)، يونيو ٢٠٢١، ص ٣٢ وما بعدها.

وبيانات بطاقاتهم الائتمانية مما يجعلهم فريسة سهلة المنال للمتخصصين في النصب والاحتيال الألكتروني، هذا بالإضافة إلى أن أغلب المراسلات تمر عن طريق البريد الألكتروني في ظل توقف معظم مكاتب البريد عن الدوام الكامل مما ساعد على إنتشار الهجمات الألكترونية والاحتيال والتصيد الألكتروني ونشر البرامج الخبيثة واستغلالها أسوء استغلال خصوصاً مع إجراء أغلب المعاملات سواء على النطاق الحكومي أو العام والخاص عن بُعد كالمؤتمرات والندوات والاجتماعات أياً كان نوعها. وهو ما نص عليه **المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨** تحت مسمى جرائم الاحتيال في المادة (٢٣) وتنص على أن "كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق الى أرقام أو بيانات بطاقات البنوك أو غيرها من أدوات الدفع الألكترونية "..... فإن قصد ... الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائة ألف جنية ....، وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف جنية ....، اذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير". وهو ما قرره **المشرع الكويتي**[١٣] في إطار **المادة الأولى من القانون رقم ٦٣ لسنة ٢٠١٥** بشأن مكافحة جرائم تقنية المعلومات.

٢-تدمير المواقع والبيانات عبر الفضاء الألكتروني: وذلك من خلال اختراق شبكات الانترنت[١٤] لتحقيق أهداف غير مشروعة وعدوانية ذو طابع جنائي أو سياسي، وأيضاً الدخول عن بُعد لنظام التحكم في علاج المستشفيات خلال جائحة كورونا وذلك بهدف قتل المريض، وهو ما نص عليه **المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨** في المادة (٢٠) في جريمة الاعتداء على الأنظمة

١٣) معاذ سليمان راشد محمد الملا: مرجع سابق، ٢٠٢١، ص ٤٣ وما بعدها.
١٤) جمال علي خليل الدهشان: الارهاب في العصر الرقمي الارهاب الألكتروني: صوره ومخاطره وأليات مواجهته، المجلة الدولية للبحوث في العلوم التربوية، مجلد (١)، العدد (٣)، يوليو ٢٠١٨، ص ١٠١ وما بعدها.

(ISSN: 2356 - 9492)

المعلوماتية، وهو أيضاً ما نص عليه **المشرع الاماراتي**[١٥] **بنص المادة السادسة في فقرتها الثانية من قانون مكافحة الجرائم الارهابية لسنة ٢٠١٤.** وبالتالي فمن المتصور إختراق الشبكة العنكبوتية، تقصد تدمير المواقع الألكترونية والنظم المعلوماتية وإلحاق أضرار واسعة المدى بالبنية التحتية المعلوماتية وتدميرها مع القيام بهجوم ألكتروني إرهابي على المواقع الخاصة والقطاعات الحيوية للمجتمع والسيطرة عليها بحيث يؤدي ذلك إلى العبث بها وبمحتوياتها، بل وقد يصل الأمر إلى تدميرها في أحياناً كثيرة من خلال الاتصال بنقطة إتصال رئيسية أو فرعية عن طريق الولوج الآلي Server–PC وهو ما يتطلب بالفعل شخص ذو ثقافة تقنية على أعلى مستوى أو مجموعة نظم مترابطة شبكياً يكون لها القدرة على المعرفة والإلمام بالثغرات التقنية في التطبيقات بما يمكن من الولوج واختراقها وتدميرها والحاق الأذى بالبيانات المتاحة عليها أو استغلالها على نحو سيء.

٣- الترويج للأفكار والمعتقدات الداعية الى ارتكاب أعمال إرهابية عبر الفضاء الألكتروني: عندما بدأت جائحة كورونا في الظهور والانتشار أصدر تنظيم داعش في صحيفة "النبأ" في مارس ٢٠٢٠ مجموعة توجيهات لاتباعه توضح كيفية التعامل مع الأوبئة بشكل عام، وكيفية الاستغلال الأمثل لها وذلك تحت عنوان "أسوء كوابيس الصليبيين" حيث اعتبر التنظيم ان هذه الجائحة هي عذاب من الله على أمم من خلقه. وهو ما واجهه المشرع المصري وحسناً ما فعل عندما نص على تلك الأفعال وتجريمها في المادة (٢٩) من **قانون مكافحة الارهاب رقم ٩٤ لسنة ٢٠١٥** حيث تقول: "يعاقب بالسجن المشدد .... كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو المعلومات الدولية أو غيرها بغرض الترويج للأفكار أو المعتقدات الداعية الى ارتكاب أعمال ارهابية ....". وعلى ذلك وبناء على ما تقدم فإنه يمكن استخدام الواقع الإفتراضي

١٥) محمد كاسب خليفة المسافري: الارهاب الألكتروني وسبل مواجهته، المجلة المغربية للأدارة المحلية والتنمية، العدد (١٥٠، ١٥١)، ابريل ٢٠٢٠، ص ٣٨٤ وما بعدها. وللمزيد أيضاً أنظر:
- Bertrand Venard: Cyber security behavior under covid-19 influence, International conference on cyber situational awareness, Dublin, Irland, A. 16, June 2021, p. 9.

من خلال اختراق أحد المواقع الموجودة بالفعل والخاصة بإحدى الجهات سواء كانت على المستوى الفردي أو الجماعي ونشر الأفكار الهدامة والدعوة إليها من أجل إحداث بلبلة وفتنة خصوصاً في ظل استغلال الأحداث الجارية من انتشار وباء عالمي يجتاح العالم، وقد يتم ذلك أيضاً عن طريق إنشاء أحد المواقع خصيصاً لذلك، إضافة إلى أنهم قد يستخدموا هذه المواقع في مهاجمة المنظمات الارهابية الأخرى وفي توجيه رسائل لمؤيديهم، وهو ما حدث في الكويت مع حدث يبلغ من العمر سبعة عشر سنة في منطقة الفنطاس حيث استهدف عشرات الضباط الأمريكيين المقيمين في برجين سكنيين بناء على توجيه عبر أحد المواقع على الشبكة العنكبوتية.

٤- غسل الأموال عبر الفضاء الألكتروني: إن جائحة كورونا جعلت معظم المعاملات ألكترونية مما شكل تربة خصبة للارهابيين لكي تنمو فيها بذور عمليات غسل الأموال لتمويل العمليات الارهابية عبر الفضاء الألكتروني وهو ما جرمه **المشرع المصري في المادة (٢٠) من قانون مكافحة الارهاب رقم ٩٤ لسنة ٢٠١٥** فتنص "يعاقب بالسجن المشدد.... كل من: ١) أخفى أو تعامل في أشياء استعملت أو أُعدت للاستعمال في جريمة ارهابية، أو الاموال الأخرى التي تحصلت منها...."، وأيضاً المادة (٣) من ذات القانون التي تنص "يُقصد بتمويل الارهاب كل جمع أو تلقي ..... أو توفير أموال أو أصول .... لأي نشاط ارهابي،.... أياً كان مصدره وبأي وسيلة كانت بما فيها الشكل الرقمي أو الألكتروني"، وأيضاً واجه تلك الجريمة ونص عليها **المشرع الأردني**[١٦] **في المادتان (٦، ٧) من قانون جرائم نظم المعلومات لسنة ٢٠١٠ ،** وكذلك قانون مكافحة غسل الاموال وتمويل الارهاب وتعديلاته رقم (٢٦) لسنة ٢٠٠٧. وبناء على ذلك فمن خلال الحصول على بيانات البطاقات الإتمانية والمعلومات والتفاصيل الخاصة بالمعاملات المالية والمصرفية الألكترونية التي تتم عبر الإنترنت يتم الحصول على الأموال وتنفيذ عمليات البيع والشراء الوهمية سواء للنفس أو للغير بقصد محو أي صفة غير مشروعة لهذه الأموال واستخدامها في تنفيذ عملياتهم الارهابية.

١٦) فهد يوسف سالم الكساسبة: مرجع سابق، ٢٠١٥، ص ١٥٠ وما بعدها.

(ISSN: 2356 - 9492)

٥- **التزوير عبر الفضاء الألكتروني:** خلال فترة الحظر أثناء جائحة كورونا قد يحصل البعض على تصاريح للخروج من الجهة المسئولة سواء كانت وزارة الداخلية أو غيرها وذلك من خلال الموقع الألكتروني، وقد يقوم صاحب الشأن بتزوير التصريح من أساسه أو بالذهاب الى مكان أخر غير المصرح له به بقصد ارتكاب غرض غير مشروع ، وهنا نجد أن **المشرع المصري قد نص على تجريم ذلك في قانون التوقيع الألكتروني رقم ١٥ لسنة ٢٠٠٤، وذلك في المادة (٢٣) فقرة (ب)** التي تنص على أنه "مع عدم الاخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون أخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة ألاف جنية ولا تجاوز مائة ألف جنية أو بإحدى هاتين العقوبتين كل من: (أ) .... (ب) أتلف أو عيب توقيعاً أو وسيطاً أو محرر ألكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق أخر. وقد جرم **المشرع الكويتي**[١٧] **ذلك في البند الثاني من المادة (٣) من القانون رقم ٦٣ لسنة ٢٠١٥** بشأن مكافحة جرائم تقنية المعلومات، وأيضاً في **البندين (ج)، (د) من المادة (٣٧) من قانون المعاملات الألكترونية رقم (٢٠) لسنة ٢٠١٤.** ومن هذا المنطلق فإن القيام بإدخال المعلومات إلى الفضاء السيبراني واستخدامها على نحو مغاير للحقيقة أو على الجانب الأخر إن تم إدخال بيانات غير صحيحة على خلاف الحقيقة بقصد الوصول لغرض غير مشروع كالحصول على تصريح بالمرور واستعماله على نحو في غير ما أصدر له يُعد تزويراً ألكترونياً يقع تحت طائلة العقاب.

٦- **التجسس عبر الفضاء الألكتروني:** فمن خلال برامج معينة وعن طريق الفضاء السيبراني أو شبكة الإنترنت يتم الوصول إلى المعلومات والبيانات السرية المتعلقة والخاصة بالهيئات والمؤسسات الحكومية أو الخاصة أو هيئات القطاع العام سواء كانت معلومات عسكرية أو اقتصادية أو صحية أو سياسية بهدف استخدامها لتحقيق أهداف ارهابية، وقد يتم ذلك أيضاً عن طريق تثبيت كود التجسس الألكتروني

١٧) معاذ سليمان راشد الملا: مرجع سابق، ٢٠٢١، ص ٤٦ وما بعدها.

داخل أحد أنظمة الكمبيوتر وذلك خلسة عن طريق أحد الأشخاص العاملين داخل تلك المؤسسة أو المصلحة من خلال استغلال موقعه أو وظيفته، وبناء عليه يستخدم الارهابيون هذه المعلومات لزيادة فعالية هجوم مستقبلي، كما يمكن من خلال هذه المعلومات وعن طريق أحد البرامج الخبيثة التحكم الألكتروني في أحد المرافق الأساسية وإصدار تعليمات ضارة أو غير صحيحة تتسبب في تحقيق نتائج خطيرة. وقد يتم اقتحام المواقع الألكترونية[١٨] للمستشفيات من أجل الحصول على بعض بيانات المرضى وذلك خلال فترات العزل الصحي أثناء جائحة كورونا أو اختراق المواقع الخاصة للجهات القائمة على انتاج اللقاح لمعرفة التفاصيل الدقيقة وهو ما نص **المشرع المصري على تجريمة في المادة (٢٩) من قانون مكافحة الارهاب رقم ٩٤ لسنة ٢٠١٥، وأيضاً قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ في المادة (١٤).**

وفي نهاية هذا المطلب وبعد أن استعرضنا بعض نماذج وصور لهذه الجريمة محور حديثنا لم يعد لدينا أدنى شك على مدى خطورتها، وأن أسلوب مكافحتها لم يكن بالأمر الهين نظراً لأن القائمين عليها غالباً ما يكونوا على مستوى عال من الدقة والتنظيم، بالإضافة إلى أنهم ذو ثقافة تقنية عالية متربعين على قمة الهرم التكنولوجي وهو ما يعني أن مواجهتها يجب أن تكون بنفس المستوى لإرتكابها إن لم يكن أعلى مع القابلية للتطور باستمرار مجاراة لأي تطور إجرامي في هذا الشأن. فهل تحقق ذلك ؟ هذا ما سوف نتعرف عليه في السطور القادمة.

المبحث الثاني

آليات مواجهة جريمة الارهاب عبر الفضاء الألكتروني في ظل جائحة كورونا

مما لا شك فيه أن ارتفاع نسبة جرائم تقنية المعلومات على وجه العموم وجريمة الارهاب عبر الفضاء الألكتروني على وجه الخصوص خلال فترة تفشي جائحة كورونا

١٨) وهيبة شريف: أساليب الجريمة الألكترونية: مسار الانتقال من الارهاب التقليدي الى الارهاب الألكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي، مجلد (٨)، العدد (١)، ديسمبر ٢٠١٨، ص ٦٩. وللمزيد أيضاً أنظر: Harjinder Singh Lallie, Xavier Bellekens: Cyber security in the age Covid-19: A timeline and analysis of cyber-crime and cyber attacks during the pandemic, Computer & Security Review, Vol. 105, June 2021, p. 1-5.

(ISSN: 2356 - 9492)

كان بسبب الاعتماد على النظام المعلوماتي وشبكة المعلومات الدولية لإنهاء العديد من التعاملات خلال هذه الأزمة وخصوصاً أثناء فترات حظر التجول وكذلك العزل الصحي، مما يتطلب إصدار تشريعات قوية قادرة على مواجهة مثل هذا النوع من الاجرام، بالاضافة الى أنه يجب تعاون الدول وتكاتفها مع بعضها البعض لمواجهة هذه الأزمة والمرور منها وهو ما سوف نتحدث عنه في المطلب الأول والثاني ان شاء الله.

المطلب الأول

آليات الصعيد الوطني والمقارن

أولاً: التشريع المصري: في واقع الأمر أصدر المشرع المصري حزمة من التشريعات تمثل ترسانة قانونية على مستوى عال لمواجهة هذا النوع من الاجرام الذي يتميز بطبيعة خاصة[١٩] كونه عابر للحدود يعتمد على الكمبيوتر والانترنت قادراً على اختراق قواعد البيانات والبنية التحتية بالاضافة إلى صعوبة تعقب مرتكبي هذه النوعية من الجرائم.

١) الدستور المصري: نصت **المادة ٣١** منه على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون". ومن هذا المنطلق وبناء على توجيهات المشرع الدستوري بما يتوائم مع مقتضيات مكافحة الجرائم ذات التقنية المعلوماتية لحماية شبكات وأنظمة وتقنيات المعلومات والفضاء السيبراني بوجه عام من أي شكل من أشكال التعدد التقني المعلوماتي خصوصاً في ظل عدم قدرة النصوص التقليدية المنصوص عليها في قانون العقوبات على مواجهة أغلب النماذج المستحدثة من هذه النوعية من الجرائم ذات التقنية العالية العابرة للحدود وهو ما حدث بالفعل بإصدار المشرع **لقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ وقانون رقم ١٧ لسنة ٢٠٢٠** بشأن مكافحة غسل الأموال وتمويل الارهاب مع تضمينها نصوص

١٩) ياسمين أحمد اسماعيل صالح: الارهاب الألكتروني في ظل أزمة فيروس كورونا: الانماط – التداعيات، مجلة السياسة والاقتصاد، مجلد (١٠)، العدد (٩)، يناير ٢٠٢١، ص ٧٣. وللمزيد أنظر أيضاً سليم محمد سليم حسين: السياسة الجنائية في مواجهة الارهاب الألكتروني، دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، مجلد (٦١)، العدد (٢)، ٢٠١٩، ص ٩٥ وما بعدها.

إستثنائية تمثل خروجاً على القواعد العامة الموضوعية لتكون قادرة على مواجهة هذه النوعية الفريدة من الإجرام الألكتروني.

٢) قانون مكافحة الارهاب رقم ٩٤ لسنة ٢٠١٥ المعدل بالقانون رقم ١٥ لسنة ٢٠٢٠: تنص المادة (٢٩) منه على أن "يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين كل من أنشأ أو استخدم موقعاً على شبكة الاتصال أو شبكة المعلومات الدولية أو غيرها بغرض الترويج للافكار أو المعتقدات الداعية الى ارتكاب أعمال ارهابية ....."، وهي إحدى صور جريمة الارهاب عبر الفضاء الألكتروني وهو ما استغلته الجماعات الارهابية خلال جائحة كورونا للدعوة الى أعمال ارهابية. وتأسيساً على ذاك وفقاً لما تنص عليه هذه المادة فإن السلوك الإجرامي في جريمة الارهاب ذو الفضاء الألكتروني يتكون من عنصرين: الأول – إنشاء موقع أو استخدامه على شبكة الاتصالات أو الشبكة العنكبوتية أو غيرها. الثاني – أن يكون هذا الإنشاء أو الاستخدام من أجل تحقيق أحد الأغراض الآتية: ١- الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال ارهابية، ٢- بث تسجيل ما بهدف تضليل السلطات الأمنية والتأثير عليها وتشويشها بشأن جريمة ارهابية، ٣- تبادل الرسائل وإصدار التوجيهات والتكليفات بين أعضاء الجماعة الارهابية أو أحد المنتمين إليها سواء داخلياً أو خارجياً بإعتبار شبكة الإنترنت وسيلة جيدة للإتصال بين الجماعات الارهابية المتطرفة فهي تساعدهم على التواصل والتنسيق فيما بينهم مهما بعدت المسافات وكذلك تمكنهم من إصدار الأمر والتعليمات من موقعهم دون الحاجة لإمتلاك حاسب آلي وذلك من خلال أجهزة الهاتف المحمول وهو ما حدا ببعض الدول إلى قطع خدمة "بلاك بيري" لخوفها من استغلالها في الأعمال الارهابية عن بُعد.

٣) قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨: تنص **المادة (١٤)** منه على جريمة الدخول غير المشروع حيث تقول: "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائة ألف جنية، أو باحدى هاتين العقوبتين، كل من دخل عمداً أو دخل بخطأ غير عمدي وبقي بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه"، كما في حالة

(ISSN: 2356 - 9492)

اختراق نظام تصاريح الخروج في فترات الحظر خلال جائحة كورونا. وبناء على ذلك فقد جرم المشرع جريمة الدخول غير المشروع سواء لموقع أو حساب أو نظام معلوماتي حرصاً منه على حماية البيانات الشخصية أياً كان شكل التعدي أو صورته طالما مكث فيها بدون وجه حق فترة من الزمن وسواء تم هذا الدخول عمداً أو على سبيل الخطأ وهو ما لم نؤيده من جانبنا فكيف يساوي المشرع بين الحالتين مع أن الفارق كبير وواسع المدى وهو ما كان يجب عليه تداركه بتغليظ العقوبة في حالة العمد وجعلها أقل في حالة الخطأ. وأيضاً نصت **المادة (١٨)** على جريمة الاعتداء على البريد الألكتروني حيث قالت: "يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائة ألف جنية، .... ، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً ألكترونياً أو موقعاً أو حساباً خاصاً بأحد الناس". لقد أصبح البريد الألكتروني من أكثر الوسائل استخداماً في مختلف القطاعات لما يتميز به من سهولة وسرعة لايصال الرسائل، إلا أنه من زاوية أخرى يُعد من أعلى الاستخدامات للارهابيين في التواصل فيما بينهم وتبادل المعلومات وتناقلها والتخطيط لها، كما يقوموا باستغلاله على نحو سيء في نشر أفكارهم والترويج لها من خلال الرسائل الألكترونية، إضافة إلى قيام البعض من خلال مستواهم التقني العالي بإختراق البريد الألكتروني الخاص بالأخرين والاطلاع عليه وهتك أسرارهم وبياناتهم وأدق تفاصيلهم والاطلاع عليها والاستفادة منها في أعمالهم الغير مشروعة، كما أنه من خلال الضغط على زر معين واحد يمكن إيصال رسالة لكل أنصارهم ومؤيديهم في أنحاء العالم في ثانية واحدة في ذات الوقت دون أي تكلفة تُذكر. وقد تم اختراق البريد الألكتروني[٢٠] الخاص بالعاملين في مراكز إنتاج اللقاح أو المستشفيات خلال جائحة كورونا.

٤) قانون التوقيع الألكتروني: تنص المادة (٢٣) فقرة (ب) على عقاب – الحبس والغرامة – كل من أتلف أو عيب توقيعاً أو وسيطاً أو محرراً ألكترونياً أو زور شيئاً من

٢٠) بدره هويبل: الارهاب في الفضاء الألكتروني، رسالة دكتوراة، ٢٠١٢، جامعة عمان العربية، ص ١١٨. وللمزيد أنظر أيضاً: وليد سمير فهيم المعداوي: مكافحة جرائم تقنية المعلومات والارهاب الألكتروني وفقاً لأحدث التشريعات المصرية، مجلة الفكر الشرطي، مجلد (٢٩)، العدد (١١٤)، يوليو ٢٠٢٠، ص ٢١٠ وما بعدها.

ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق أخر كما في حالة تقليد أو تعييب التوقيع على تصريح الخروج في حظر التجوال خلال جائحة كورونا، وكذلك اتلاف أو تعييب أو تزوير بطاقات الحصول على مصل كورونا.

٥) قانون رقم ١٧ لسنة ٢٠٢٠ المعدل لقانون رقم ٨٠ لسنة ٢٠٠٢: بشأن مكافحة غسل الاموال وتمويل الارهاب. في واقع الأمر أصبحت عملية غسيل الأموال من أكثر العمليات شيوعاً عبر الواقع الإفتراضي، فمن خلال الحصول من قبل الارهابيين على معلومات بطاقات الائتمان أو البيانات التي يتم استخدامها في تنفيذ العمليات المصرفية أو المالية عبر الفضاء الألكتروني يتم الاستيلاء على أموال الأخرين سواء لأنفسهم أو لغيرهم، إضافة إلى القيام بعمليات البيع والشراء الوهمية إخفاء لهوية هذه الأموال واستخدامها في تمويل عملياتهم الارهابية.

ثانياً: التشريع السعودي: أصدرت المملكة العربية السعودية عدداً من القرارات والأنظمة الخاصة بحماية النظام المعلوماتي ومكافحة الجرائم المعلوماتية والتي تهدف إلى الحد من الاجرام الألكتروني بما في ذلك الارهاب عبر الفضاء الألكتروني من خلال تضييق الخناق على الاستخدام الغير مشروع للحاسب الآلي والانترنت بما يسهم في حماية الأمن والنظام العام والحفاظ على تنمية الاقتصاد القومي، ومنها ما يلي:

١) قرار مجلس الوزراء[٢١] رقم (١٦٣) في ١٤١٧/١٠/٢٤ هـ الذي ينص على اصدار الضوابط المنظمة لاستخدام شبكة الانترنت والاشتراك فيها ومن ذلك الامتناع عن الوصول أو محاولة الوصول الى أي من أنظمة الحاسبات الألية الموصولة بشبكة الانترنت[٢٢] أو إلى أي معلومة خاصة أو مصادر معلومة دون الحصول على موافقة المالكين، وكذلك الامتناع عن إرسال أو استقبال معلومة مشفرة إلا بعد الحصول على الترخيص اللازم والامتناع عن الدخول الى حسابات الأخرين أو محاولة استخدامها بدون تصريح أو الاطلاع على الرقم السري للمستخدم. ومن مراجعة هذا القرار يتضح لنا أنه

٢١) ابراهيم سليمان الحربي: الارهاب المعلوماتي وتمويله في ضوء النظام السعودي، مجلة مصر المعاصرة، مجلد (١١٠)، العدد (٥٣٤)، ابريل ٢٠١٩، ص ٢٨٤ وما بعدها.
٢٢) حسن فضيل خليف المناصير: جريمة الدخول غير المشروع الى النظام المعلوماتي والتعدي على محتوياته – دراسة مقارنة، رسالة ماجستير، جامعة حرش، ٢٠١٦، ص ٤٠ وما بعدها.

(ISSN: 2356 - 9492)

يوضح ويبين مدى سعي المملكة العربية السعودية ومبادرتها المحمودة لتنظيم التعاملات عبر الفضاء الألكتروني وضبطها على نحو يساعد على مكافحة الارهاب الألكتروني.

٢) نظام مكافحة جرائم الارهاب وتمويله الصادر بالمرسوم الملكي رقم م/٢١ بتاريخ ١٤٣٩/٢/١٢ هـ، وهو ما قد نصت المادة الأولى منه على تعريف الجريمة الارهابية وجريمة تمويل الارهاب، وقد شدد هذا النظام على معاقبة المتهمين ممن تثبت إدانتهم بالسجن وذلك في المادة الخامسة والثلاثين حيث تقول: "يعاقب بالسجن مدة لا تزيد على خمس وعشرين سنة ولا تقل عن ثماني سنوات، كل من حرض آخر على الانظمام إلى أي كيان ارهابي، أو المشاركة في أنشطته، أو جنده، أو ساهم في تمويل أي من ذلك، فإن كان قد عمل على منعه من الانسحاب من الكيان، أو استغل لهذا الغرض ما يكون له عليه من ولاية أو سلطة أو مسئولية أو أي صفة تعليمية أو تدريبية أو توجيهية أو اجتماعية أو ارشادية أو اعلامية، فلا تقل عقوبة السجن عن خمس عشرة سنة". وهذا إن دل على شيء فإنما يدل على حرص المشرع السعودي على تغليظ العقوبة على التحريض على الانظمام لكيان ارهابي أو المشاركة أو التجنيد أو المساهمة في التمويل، وكذلك عقاب من استغل ولايته أو سلطته أو مسئوليته أياً كانت صورتها أو هيئتها بما يعكس السعي الدائم للمملكة لمكافحة الارهاب أياً كانت طبيعته.

٣) نظام مكافحة غسل الأموال الصادر بالمرسوم الملكي رقم م/٣١ بتاريخ ١٤٣٣/٥/١١ هـ .

٤) قواعد مكافحة غسل الأموال وتمويل الارهاب الصادر عن مجلس هيئة السوق المالية في سبيل مواجهة العمليات الارهابية بموجب القرار رقم (١ – ٣٩ – ٨ – ٢٠٠٨ م).

ثالثاً: التشريع الماليزي: تُعد ماليزيا من أولى الدول في جنوب شرق أسيا التي سنت تشريعات الفضاء السيبراني للتعامل مع الارهاب السيبراني والتي من أهمها:

١) قانون جرائم الكمبيوتر ١٩٩٧[٢٣]: لمكافحة الجرائم الألكترونية حيث يجرم عمل القراصنة ونشر الفيروسات والاتصال الغير مشروع للوصول إلى أجهزة الحاسب الآلي.

٢) قانون التوقيع الرقمي: دخل حيز التنفيذ في أكتوبر ١٩٩٨ وهو يضمن أمن القضايا القانونية المتعلقة بالمعاملات الألكترونية ويحقق ويفي بمتطلبات السرية وسلامة المعلومات.

٣) قانون الاتصالات والوسائط المتعددة لعام ١٩٩٨ المعدل في ٢٠٠٦، وتم النص فيه على إنشاء لجنة الاتصالات والوسائط المتعددة الماليزية مع صلاحيات الاشراف على الاتصالات والأنشطة المتعددة الوسائط وتنظيمها.

٤) قانون حماية البيانات الشخصية لعام ٢٠١٠[٢٤] : وهو يضمن عدم إساءة استخدام أي بيانات شخصية يتم جمعها، كما يشترط الحصول على موافقة الأفراد قبل جمع بياناتهم الشخصية أو مشاركتها، ووضع عقوبة جنائية تصل إلى لـ ٥٠٠٠٠٠٠ رينغيت ماليزي والسجن ثلاث سنوات أو احداهما اذا تم مخالفة شروط تسجيل البيانات.

المطلب الثاني

آليات الصعيد الدولي

إن ظاهرة الارهاب عبر الفضاء الألكتروني تتفاقم يوماً بعد يوم[٢٥]، حيث المعاملات الألكترونية والاعتماد على التكنولوجيا والتحول الرقمي أمراً أصبح واقعاً خصوصاً في ظل الوباء –فيروس كورونا– الذي يجتاح العالم، مما شكل بيئة خصبة لانتشار الأعمال الارهابية الرقمية باستخدام الفيروسات لاتلاف المعلومات والبيانات سواء على المستوى الوطني أو الدولي وذلك عن طريق القرصنة المعلوماتية أو عن طريق استغلال شبكات ومنصات وسائل التواصل الاجتماعي مما يشكل قدراً بالغاً على

٢٣) وفاء لطفي: الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجاً، مجلة كلية الاقتصاد والعلوم السياسية، مجلد (٢٣)، العدد (١)، يناير ٢٠٢٢، ص ١٦٥ وما بعدها.

24) Tharshini N.K., Hassan Z., Mas'ud F.H.: Cyber crime threat landscape – a mid movement control order in Malaysia, International Journal of Business and Security, Vol. 22, issue 3, Dec. 2021, p. 1589-1601.

٢٥) محمد محمود أحمد الرمادي: الابعاد الاجتماعية للارهاب الألكتروني: دراسة ميدانية، مجلة كلية الأدب، مصر، العدد (٣٧)، أكتوبر ٢٠١٩، ص ١١.

(ISSN: 2356 - 9492)

الاقتصاد وعلى التجارة ومعاملاتها الألكترونية، ولذلك كان لا بد أن يكون هناك تكاتف دولي واسع المستوى لكي يتم مواجهة هذا الاعصار العالمي.

أولاً: المستوى الاقليمي:

١) المؤتمرات والندوات:

- ندوة الدليل الرقمي[٢٦] الصادرة عن المنظمة العربية للتنمية الادارية التابعة لجامعة الدول العربية، والتي أصدرت العديد من التوصيات المتعلقة بالجوانب الاجرائية والتدريبية في مجال مكافحة جرائم تكنولوجيا المعلومات.
- المؤتمر الدولي[٢٧] لتجريم الارهاب الألكتروني عام ٢٠١٧ الذي نظمته دولة الامارات العربية بهدف تعزيز وترسيخ قيم التعاون بين الدول للتصدي لهذه النوعية من الاجرام المعلوماتي.

٢) الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية ٢٠١٠: والتي تنص في مادتها رقم (٢١) على جريمة الاستعمال غير المشروع لتقنية أنظمة المعلومات والتي من ضمن صورها: (أ) الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات، (ب) تعطيل أو تحريف تشغيل أحد نظم المعلومات، (ج) ادخال بيانات بطرق غير مشروعة.

٣) الاتفاقية العربية لمكافحة غسل الأموال وتمويل الارهاب ٢٠١٠: والتي نصت في مادتها الأولى وعرفت الأموال: كل ذي قيمة مالية من عقار أو منقول ..... أياً كان شكلها بما فيها الألكترونية والرقمية، كما نصت في الباب الثالث منها في المادة التاسعة على تجريم غسل الأموال أياً كان مصدرها، وفي المادة العاشرة على تجريم تمويل الارهاب، كما نصت في الباب الخامس تحت عنوان التعاون القانوني والقضائي على المساعدة القانونية المتبادلة وعلى الإنابة القضائية[٢٨].

---

٢٦) ناصر محمد البكر الزعابي، راشد بن رشيد بن ابراهيم: تداعيات جرائم الارهاب الألكتروني على استقرار الدول وأمنها، مجلة الفكر الشرطي، المجلد (٢٨)، العدد (١١٠)، يوليو ٢٠١٩، ص ٤٠.

٢٧) ياسمين أحمد اسماعيل صالح: مرجع سابق، ٢٠٢١، ص ٧٤.

٢٨) عمر سالم: الإنابة القضائية الدولية في المسائل الجنائية "دراسة مقارنة"، بدون سنة نشر، ص ٤٥ وما بعدها.

٤) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠: والتي انضمت لها جمهورية مصر العربية في ٢٠١٤ ، وقد نصت مادتها السادسة على جريمة الدخول غير المشروع وعرفتها الفقرة (أ) بأنها الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار وهو ما قد يحدث خلال جائحة كورونا عند الدخول لموقع أحد المستشفيات أو مراكز انتاج اللقاح بقصد الوصول للبيانات وتدميرها أو بقصد الحصول على أسرارها. وقد نصت المادة الخامسة عشرة على الجرائم المتعلقة بالارهاب والمرتكبة بواسطة تقنية المعلومات وهو ما قد يحدث خلال فترة كورونا من استخدام مواقع التواصل الاجتماعي لنشر الشائعات واثارة الفتن والدعوة الى المزيد من الاعمال الارهابية.

ثانياً المستوى الدولي:

١) دور الشرطة الجنائية الدولية (الانتربول) في مكافحة جرائم الارهاب عبر الفضاء الألكتروني: لا شك أن جريمة الارهاب عبر الفضاء الألكتروني تمثل قدراً كبيراً من الجسامة بوصفها جريمة ماسة بالقيم التي يؤمن بها المجتمع الدولي، وقد لعب الانتربول دوراً محورياً هاماً في شأن مكافحتها، ففي عام ٢٠١٧ [٢٩] تم افتتاح أعمال جمعية الشرطة الجنائية لمناقشة مشكلات الارهاب عبر الفضاء الألكتروني وأكدت على أهمية تبادل المعلومات بين أجهزتها واعتمادها على مستخدمي شبكة المعلومات الدولية للحصول على المعلومات الخاصة بالمتهمين.

٢) مجلس الأمن: اشار مجلس الأمن في قراره رقم (١٩٦٣)[٣٠] لسنة ٢٠١٠ الى "ازدياد استخدام الارهابيين للتكنولوجيا الجديدة للمعلومات والاتصالات وبخاصة الانترنت لأغراض التجنيد، وكذا التحريض على دعم الاعمال الارهابية"، وأكد على ضرورة التعاون الدولي بين بلدان العالم لمواجهة هذا النوع من الاجرام خصوصاً بعد ازدياد استغلالهم لوسائل التواصل الاجتماعي.

٢٩) هادي طلال هادي: المواجهة القانونية الأمنية لجرائم الارهاب الألكتروني، مجلة الأمن العراقية، العدد (٤٥)، الجزء (٢)، ٢٠١٩، ص ٢٩٠ وما بعدها.
٣٠) خالد محمد نور عبدالحميد الطباخ: المواجهة القانونية للارهاب الألكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، المجلد (٣)، العدد (١)، ٢٠١٧، ص ٣٢.

(ISSN: 2356 - 9492)

٣) اتفاقية بودابست للتصدي للجرائم الألكترونية ٢٠٠١ [٣١]: وهي تُعد أول معاهدة دولية تهدف لمواجهة الجرائم الألكترونية من خلال اتباع سياسة جنائية مشتركة لحماية المجتمع من هذا النوع من الجرائم، لاسيما من خلال اعتماد التشريعات المناسبة وتنسيق القوانين الوطنية، وتحسين تقنيات التحقيق، وزيادة التعاون الدولي والمساعدة المتبادلة.

٤) الاتفاقية الدولية لقمع تمويل الارهاب لسنة ١٩٩٩ : نصت المادة (١٢) على أن تتبادل الدول الأطراف أكبر قدر من المساعدة القانونية فيما يتعلق بأي تحقيقات أو اجراءات جنائية أو .... مما يُعد توجيهاً للتعاون بين الدول في مجال المساعدة القانونية خصوصاً في ظل الاجرام الألكتروني الذي يتصف بصعوبة اثباته وشدة ذكاء المجرم الألكتروني، وفي اطار مكافحة الجريمة بوجه عام والجريمة الألكترونية على وجه الخصوص تنص المادة (١٨) على أن تتعاون الدول الاطراف في منع الجرائم المعنية بإتخاذ كافة التدابير الممكنة.

٥) اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ٢٠٠٠[٣٢]: والتي تنص في مادتها رقم (٢١) على نقل الاجراءات الجنائية بما يساعد على إقامة العدل، وفي مادتها رقم (٢٩) فقرة (ح) تشير الى الطرق المستخدمة في مكافحة الجريمة المنظمة التي تُرتكب باستخدام الحواسيب أو شبكات الاتصال السلكية واللاسلكية أو غير ذلك من أشكال التكنولوجيا الحديثة.

الخاتمـة

تناولت الدراسة ظاهرة من إطار فريد ذو طابع خاص ألا وهي جريمة الارهاب عبر الفضاءء الألكتروني وما يضفي عليها طابع أكثر خصوصية هو ارتكابها ومظاهرها في ظل وباء –جائحة كورونا– مما جعل منها جريمة من أخطر جرائم العصر، وبالتالي

٣١) محمد محمود أحمد الرمادي: مرجع سابق، ٢٠١٩، ص ١٢.

32) Rose Cecily: The creation of review, Mechanism for the UN convention against transnational organized crime and its protocols, American Journal International Law, Vol. 114, issue 8, Jan. 2021, p. 51-67.

كان ولا بد علينا التعرف لبيان مفهومها الذي اتضح لنا أنه لم يستقر رأي عليه، بالاضافة الى النماذج المختلفة التي حاولنا أن نتعرض لبعض صورها قدر المستطاع، وصولاً في النهاية الى استعراض آليات مواجهتها تشريعياً على المستوى الوطني والدولي. وقد خلصنا في نهاية هذه الدراسة إلى عدد من النتائج والتوصيات.

أولاً: النتائج:

١) إن الارهاب عبر الفضاء الألكتروني ما هو إلا إمتداد للارهاب في صورته التقليدية، وصورة له مع مقام الأول –الألكتروني– على الاستفادة من شبكة المعلومات والتقدم التقني في تحقيق جريمة وتسخير كل الأدوات الألكترونية والواقع الإفتراضي لتحقيق أهدافه أياً كانت صورتها سواء كانت ضد الأفراد أو المؤسسات أو الدول وسواء كانت الخسائر مادية أو معنوية وهو ما حدث بالفعل خلال جائحة كورونا.

٢) مما لا شك فيه أن هناك علاقة وطيدة بين الارهاب والفضاء الألكتروني والجرائم المعلوماتية فالأول يُعد أحد صور الأخيرة والثاني –الفضاء الألكتروني– يقوم بلعب ثلاثة أدوار بحيث يختلف دوره حسب كل سيناريو، فقد يكون وسيلة ارتكاب الجريمة وقد يكون هدفها، أما الدور الأخير فهو قد يكون بيئة ارتكاب الجريمة.

٣) من خلال استعراض بعض صور ومظاهر –الاحتيال أو التصعيد عبر الفضاء الألكتروني وتدمير المواقع والبيانات والترويج للأفكار والمعتقدات الداعية إلى ارتكاب أعمال ارهابية عبر الفضاء الألكتروني وغسل الأموال والتزوير والتجسس عبر الفضاء الألكتروني–، هذه الجريمة يتضح لنا أن أمر إثباتها ليس بالهين وذلك لسهولة ارتكابها ومحو أثارها في ثوان معدودة، إضافة إلى أنها لا تقع إلا في صورة عمدية ولا يتصور وقوعها عن طريق الخطأ أو عدم التحرز أو عدم الاحتياط.

٤) نظراً لطبيعة هذه الجريمة وكونها ذات طبيعة خاصة سواء بالنظر لخطورة مرتكبيها كونهم ذو قدرة هائلة على الاستفادة من معطيات الذكاء الاصطناعي والتقدم التقني أو سواء بالنظر لخطورة أثارها وضخامة خسائرها فقد لجأت العديد من التشريعات إلى تفريد الدعوى الجنائية بشأنها بقدر من الخصوصية، كما هو الحال في التشريع المصري عندما نص على عدم تقيد النيابة العامة عند مباشرتها التحقيق ورفع الدعوى

(ISSN: 2356 - 9492)

في الجرائم الارهابية بقيد الطلب المنصوص عليه في قانون الاجراءات الجنائية، وكما هو الحال أيضاً عندما ذهب المشرع الإماراتي إلى النص على أنه لا تنقص الدعوى الجزائية بمضي المدة في الجرائم الارهابية في قانون الارهاب رقم ٧ لسنة ٢٠١٤.

٥) إذا كان هناك عدد لا بأس به من التشريعات سواء على المستوى الوطني أو الدولي التي تم سنها لمواجهة مثل هذا النوع من الاجرام السيبراني إلا أنها غير مفعلة على أرض الواقع في الفضاء السيبراني، وهو ما حدث بالفعل خلال جائحة كورونا التي أفرزت صوراً مختلفة من هذه الجريمة خلال تلك الفترة.

ثانياً: التوصيات:

١) أهمية نشر الوعي بمدى خطورة هذا النوع من الاجرام السيبراني تدريجياً خلال المراحل التعليمية المختلفة حسب مدى الوعي والادراك مع ضرورة تخصيص مادة تعليمية لجميع الكليات على مختلف تخصصاتها وتكون عالية المستوى للتوعية بهذا النوع من الاجرام الألكتروني.

٢) التأكيد على إنشاء قسم بكلية الذكاء الاصطناعي لتخريج كوادر يتم الحاقها بالأقسام المتعلقة بمكافحة الاجرام المعلوماتي بوزارة الداخلية ومصلحة الخبراء بوزارة العدل.

٣) أهمية تفعيل التعاون الدولي وتبادل الخبرات المنصوص عليه في التشريعات الداخلية والاتفاقيات الاقليمية والدولية سواء على مستوى الخبراء أو ضباط مكافحة الجرائم السيبرانية أو القضاة حتى يتم الاستفادة من الدول الرائدة في هذا الشأن.

٤) ضرورة معالجة الجوانب الاجرائية وتحديثها باستمرار لمكافحة مثل هذه النوعية من الجرائم عبر الفضاء الألكتروني مع أهمية النص على مجموعة من القواعد الاستثنائية لمواجهة هذه الجريمة –تظل قائمة لحين احداث أثارها.

٥) مع عصر التحول الرقمي يجب أن تقوم الدولة بتوعية جميع العاملين بالجهاز الاداري بكيفية التعامل مع الفضاء السيبراني وتفادي الوقوع في الاخطاء المعلوماتية وحماية البيانات الشخصية خصوصاً في مثل هذه الأزمة العالمية من جائحة كورونا.

٦) تفعيل تطبيق تشريعات مكافحة جرائم الارهاب عبر الفضاء الألكتروني وجرائم الفضاء السيبراني لكي تطبق على أرض الواقع وحتى لا يحدث فجوة بين النظرية والتطبيق، وهو ما حدث بالفعل خلال أول أزمة –جائحة كورونا– مع ضرورة تحديثها باستمرار لكي تزامن ما يستجد من جرائم سيبرانية.

٧) أهمية تخصيص إدارات خاصة لمكافحة جرائم الارهاب عبر الفضاء الألكتروني بصورها المختلفة مع تزويدها بكوادر مدربين على أعلى مستوى وتطعيمها بالمتميزين من أصحاب الخبرة في هذا الشأن مع التأكيد على أهمية إنشاء نيابة متخصصة للتحقيق في جرائم الارهاب عبر الفضاء الألكتروني واختيار أعضائها بدقة ممن لهم القدرة على التعامل مع مثل هذه النوعية من الجرائم مع عقد الدورات التدريبية لهم باستمرار وتزويدهم بالخبرة اللازمة.

المراجع

أولاً: المراجع العربية:

- ابراهيم سليمان الحربي: الارهاب المعلوماتي وتمويله في ضوء النظام السعودي، مجلة مصر المعاصرة، مجلد (١١٠)، العدد (٥٣٤)، ابريل ٢٠١٩.
- الشيماء محمد محمود: دور الدولة في الحد من أثار الارهاب الرقمي في الأسرة المصرية، دراسة تحليلية، مجلة بحوث الشرق الأوسط، العدد (٥٥)، مايو ٢٠٢٠.
- الهاني محمد طايع رسلان: الاحكام الاجرائية الحديثة لمواجهة الجرائم الارهابية في التشريع المصري والاماراتي، مجلة جنوب الوادي للدراسات القانونية، العدد (٢)، ديسمبر ٢٠١٧.
- أم السعد بن زينب: الجريمة الألكترونية وإجراءات مكافحتها في المجتمع الجزائري، المؤتمر الدولي المحكم: الجريمة والمجتمع، عمان، ٢٠١٧.
- بدره هويبل: الارهاب في الفضاء الألكتروني، رسالة دكتوراة، جامعة عمان العربية، ٢٠١٢.
- حسن فضيل خليف المناصير: جريمة الدخول غير المشروع الى النظام المعلوماتي والتعدي على محتوياته – دراسة مقارنة، رسالة ماجستير، جامعة حرش، ٢٠١٦.

(ISSN: 2356 - 9492)

- جمال علي خليل الدهشان: الارهاب في العصر الرقمي الارهاب الألكتروني: صوره ومخاطره وأليات مواجهته، المجلة الدولية للبحوث في العلوم التربوية، مجلد (١)، العدد (٣)، يوليو ٢٠١٨.
- خالد محمد نور عبدالحميد الطباخ: المواجهة القانونية للارهاب الألكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، المجلد (٣)، العدد (١)، ٢٠١٧.
- دراسة حول تشريعات مكافحة الارهاب في دول الخليج العربية واليمن، الأمم المتحدة، المكتب المعني بالمخدرات والجريمة.
- فريدة بن عمروش: الارهاب الألكتروني: دراسة في إشكاليات المفهوم والأبعاد، المجلة الجزائرية للعلوم الاجتماعية والانسانية، مجلد (٨)، العدد (٢)، ديسمبر ٢٠٢٠.
- فهد يوسف الكسابسة: الارهاب الألكتروني عبر الانترنت في التشريع الأردني – دراسة مقارنة، مجلة العلوم القانونية والسياسية، مجلد (٩)، السنة (٥)، العدد (١)، كانون أول ٢٠١٥.
- رجاء محمد بوهادي: القواعد الاجرائية الاستثنائية لمواجهة جرائم الارهاب، المجلة الليبية العالمية، العدد (٢١)، يونيو ٢٠١٧.
- سليم محمد سليم حسين: السياسة الجنائية في مواجهة الارهاب الألكتروني، دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، مجلد (٦١)، العدد (٢)، ٢٠١٩.
- عبدالله بن خالد بن سعود الكبير آل سعود: إستغلال الأزمات: الجماعات الارهابية، اليمين المتطرف، والجريمة المنظمة في ظل فيروس كورونا، المجلة العربية للدراسات الأمنية، مجلد (٣٦)، العدد (٢)، يوليو ٢٠٢٠.
- عمر سالم: الإنابة القضائية الدولية في المسائل الجنائية "دراسة مقارنة"، بدون سنة نشر.
- ناصر محمد البكر الزعابي، راشد بن رشيد بن ابراهيم: تداعيات جرائم الارهاب الألكتروني على استقرار الدول وأمنها، مجلة الفكر الشرطي، المجلد (٢٨)، العدد (١١٠)، يوليو ٢٠١٩.

- محمد كاسب خليفة المسافري: الارهاب الألكتروني وسبل مواجهته، المجلة المغربية للأدارة المحلية والتنمية، العدد (١٥٠، ١٥١)، ابريل ٢٠٢٠.
- محمد محمود أحمد الرحاوي: الابعاد الاجتماعية للارهاب الألكتروني: دراسة ميدانية، مجلة كلية الأدب، مصر، العدد (٣٧)، أكتوبر ٢٠١٩.
- معاذ سليمان راشد محمد الملا: جرائم تقنية المعلومات وجائحة فيروس كورونا بين الواقع والمأول: دراسة تأصيلية، مجلة كلية القانون الكويتية العالمية، مجلد (٩)، العدد (٣٤)، يونيو ٢٠٢١.
- وفاء لطفي: الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجاً، مجلة كلية الاقتصاد والعلوم السياسية، مجلد (٢٣)، العدد (١)، يناير ٢٠٢٢.
- وليد سمير فهيم المعداوي: مكافحة جرائم تقنية المعلومات والارهاب الألكتروني وفقاً لأحدث التشريعات المصرية، مجلة الفكر الشرطي، مجلد (٢٩)، العدد (١١٤)، يوليو ٢٠٢٠.
- وهيبة شريف: أساليب الجريمة الألترونية: مسار الانتقال من الارهاب التقليدي الى الارهاب الألكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي، مجلد (٨)، العدد (١)، ديسمبر ٢٠١٨.
- هادي طلال هادي: المواجهة القانونية الأمنية لجرائم الارهاب الألكتروني، مجلة الأمن العراقية، العدد (٤٥)، الجزء (٢)، ٢٠١٩.
- ياسمين أحمد اسماعيل صالح: الارهاب الألكتروني في ظل أزمة فيروس كورونا: الانماط – التداعيات، مجلة السياسة والاقتصاد، مجلد (١٠)، العدد (٩)، يناير ٢٠٢١.

ثانياً: المراجع الأجنبية:

- Bertrand Venard: Cyber security behavior under covid-19 influence, International conference on cyber situational awareness, Dublin, Irland, A. 16, June 2021.

(ISSN: 2356 - 9492)

- Giovanni Bottazzi, Gianluigi Me: Responding to cyber crime and cyber terrorism, botnets an insidious threat, 2014.

- Harjinder Singh Lallie, Xavier Bellekens: Cyber security in the age Covid-19: A timeline and analysis of cyber-crime and cyber attacks during the pandemic, Computer & Security Review, Vol. 105, June 2021.

- Jordan J. Plotnek, Jil Slay: Cyber Terrorism; A homogenized taxonomy and definition, Review computers & security, Vol. 102, March 2021.

- Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, Hossein Taji: Cyber terrorism challenges, the need for global response to a multi-jurisdictional crime, computer low & security review, Vol. 29, issue 3, June 2013.

- Rose Cecily: The creation of review, Mechanism for the UN convention against transnational organized crime and its protocols, American Journal International Law, Vol. 114, issue 8, Jan. 2021.

- Tharshini N.K., Hassan Z., Mas'ud F.H.: Cyber crime threat landscape – a mid movement control order in Malaysia, International Journal of Business and Security, Vol. 22, issue 3, Dec. 2021.