

أثر العامل التكنولوجي في تعزيز الأمن – دولة الإمارات إنموذجاً

م.م. محمد حسين علي الراوي (جامعة بغداد / كلية العلوم السياسية)

الإيميل الرسمي : mohammad.hucol@copolicy.uobaghdad.edu.iq

تاريخ الاستلام : 2023/8/13 تاريخ القبول : 2023/8/23، تاريخ النشر 2024/4/30

المخلص :

أخذ العالم بالتطور من الناحية التقنية والتكنولوجية بصورة كبيرة ومتسارعة في الآونة الأخيرة، ما أدى الى حدوث تغيرات كبيرة في شتى مجالات الحياة منها ما هو ايجابي واخر سلبي حسب مستوى التأثير، وهناك يقين لدى الكثير من مستخدمي التكنولوجيا بأنهم لا يستطيعوا العيش بدون استخدامهم للوسائل التقنية الحديثة، فقد أصبح فيض المعلومات الذي يواجه الأمم والشعوب النبض لجهود التنمية والتحديث لكافة مجالات الحياة الإجتماعية والإقتصادية والثقافية بما فيها الأمنية، وهذا الامر يدعو الى رقابة وتقنين تلك التكنولوجيا بما يسهم في تحقيق أمن الاستخدام المعلوماتي والحفاظ على خصوصية افراد المجتمع، فالحكومات بعدما كانت مُتلقية لتأثيرات الثورة الرقمية في النظام الإجتماعي، أصبحت مُستخدمة لتلك التقنيات في رسم السياسات العامة لاسيما الأمنية منها، فالمعلومة لها دور كبير في نتاج وتقدم وامن الشعوب .

الكلمات الإفتتاحية : التكنولوجيا ، الأمن ، العصر الرقمي ، الإرهاب ، المواطن

**The impact of the technological factor in support security –
the UAE as a model**

Assistant teacher, Mohammad Hussein Ali

University of Baghdad / College of Political Sciences

Abstract:

المقدمة :

تُعدّ المعلومات في عصرنا الحالي كنز عظيم في ظل وجود التكنولوجيا الحديثة التي ساهمت بصورة فعّالة في تخزين، ومعالجة، ونبث المعلومات، حيث أن إمتلاك التكنولوجيا يُشكل قوة لصاحبها، لذلك نجد أن تلك المعلومات بالإمكان الإعتداء عليها، أو تخريبها، أو التجسس عليها، وهذا يتّحتم توفير الحماية اللازمة بالشكل الذي يتناسب مع أهمية تلك المعلومات، فمع هذا التطور الكبير في التكنولوجيا أصبحت الحروب ليس بالضرورة أن تكون بتحرك جيوش وقطعات عسكرية، فقد يتسبب فايروس إلكتروني بأضرار جسيمة يَبقى تأثيرها لفترة طويلة، فحرب المعلومات من أكثر المصطلحات التي أثارَت جدل واسع من حيث المعنى، فهناك من يُفسرها بإستخدام الأسلحة، بينما حقيقة الأمر لا يتعلق بالمجال العسكري فقط وإنما يشمل كافة المجالات السياسية والثقافية والإقتصادية حيث تستخدم حرب المعلومات في تعطيل وتدمير معلومات الخصم وعملياته المبنية على نُظم المعلومات وكذلك على مستوى الأشخاص والشركات وغيرها.

أهمية الدراسة : تستمدّ الدراسة أهميتها من تطور أدوات العصر الرقمي، فحرب المعلومات من أكثر المصطلحات التي أثارَت جدلاً واسعاً من حيث المعنى، فهناك من يُفسرها بإستخدام الأسلحة ذات التقنية العالية في تجهيز الجيوش، بينما حقيقة الأمر لا تتعلق بالمجال العسكري فقط، وإنما يشمل كافة المجالات السياسية، والثقافية ، والإقتصادية .

اشكالية البحث : إستناداً لرؤية الباحث الشخصية بما توفر له من دراسات ومصادر ذات صلة بموضوع الدراسة والتي تنطلق من إشكالية تحاول الإجابة على سؤال مفاده (هل تسهم التكنولوجيا وتقنياتها في تعزيز الأمن ؟)، أي محاولة وضع صورة شاملة لطبيعة التعامل مع أدوات العصر الرقمي وبيان سلبياتها وإيجابياتها وكيفية التعامل معها.

فرضية الدراسة : فرضية الدراسة مفادها أن مع هذا التطور الكبير في التكنولوجيا أصبحت الحروب، أو الأعمال الإرهابية ليس بالضرورة أن تكون بتحرك جيوش وقطعات عسكرية، فقد يتسبب فايروس إلكتروني، أو إختراق ومصادرة المواقع، أو الحسابات الشخصية بأضرار جسيمة يَبقى تأثيرها لمدة طويلة .

هيكلية البحث : سيتم تقسم هذا البحث إلى ثلاثة مطالب :

المطلب الأول : الأمن الإلكتروني .

المطلب الثاني : الإرهاب الرقمي .

المطلب الثالث : المسؤولية الجنائية في العالم الرقمي .

المطلب الأول : الأمن الإلكتروني

يتمحور الأمن الإلكتروني حول ضمان أمن المعلومات من خلال وجود الوسائل والأدوات والحماية اللازمة لضمان سلامة وتأمين المعلومات والمواقع الإلكترونية، إذ تُعد المعلومة نتاج لتشغيل البيانات التي تُساهم بوضع قواعد إتخاذ القرارات، فهناك علاقة وثيقة بين المعرفة والمعلومة التي تُضيف للإنسان الخبرة عبر التجارب والدراسات من خلال البيئة التي يعيش فيها .

إن إتساع مفهوم الأمن تحت مؤثرات التقدم التقني في مجال الثورة الرقمية، أضاف أبعاد

جديدة ومفاهيم أخرى مقارنة مع بروز الفضاء الإلكتروني كساحة الصراعات .⁽¹⁾

يُعرّف الأمن الإلكتروني بأنه منع الإساءة في الإستخدام للمعلومات الإلكترونية أو خزنها أو تسريبها بالطريقة التي تُلحق الضرر بالجهة المألِكة لها، فهو الوسائل والطرق المُعتمدة

للسيطرة على مصادر المعلومات وحمايتها من التلّف، والسّرقة ، والتّزوي⁽²⁾

مفهوم الأمن الإلكتروني، أو وفق منظور دولة الإمارات العربية المتحدة ببساطة هو

حماية وتأمين شبكة المعلومات، والإتصالات، والنظم المعلوماتية التي تُستخدم أي وسيلة

إلكترونية من الوسائل المُتعددة⁽³⁾

لقد كانت ثورة المعلومات وظهور الأنترنت إيداناً ببزوغ عصر جديد خلق بيئة الفضاء

السيبراني الذي أصبح يؤثر في النظام الدولي، لاسيما مع بروز شكل جديد من القوة

المتعلقة بالمجال الرقمي التي انتشرت بين عدد كبير من الفاعلين على المستوى الدولي،

ما جعل الفضاء السيبراني مجال جديد للصراع⁽⁴⁾

تُعد الهجمات الإلكترونية من إحدى أنواع الحروب الحديثة، التي تختلف فيها عملية

الهُجوم عن شكل الحروب التقليدية، حيثُ تَميّز بإستخدام أسلحة إلكترونية سهلة التأثير

والقدرة على الأهداف التي تعمل بالتقنيات الرقمية الحديثة كالبنى التحتية ، والمؤسسات

، الإقتصادية ، والمالية، والسياسية وغيرها، فخطورة الحرب الإلكترونية تبرز في كونها حرباً لا تحتاج إلى أسلحة، أو جنود، بل كل ما تحتاج إليه هو شبكة معلومات متطورة تستهدف الخصوم في حرب نفسية تُدار بكفاءة وإقتدار⁽⁵⁾

إذ عملت دول الخليج ، ومن ضمنها السعودية ، والإمارات على اتخاذ احتياطات وتدابير أمنية شديدة مع تنامي ظاهرة التطرف و الإرهاب بكافة أشكاله، لمنع وصول المتطرفين الى أراضيها، لاسيما مع تصاعد العمليات الإرهابية في العراق بعد عام 2003، واستخدمت أحدث التقنيات في ذلك الأمر⁽⁶⁾

لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة طردية مع إمكانية تعرض المصالح الاستراتيجية ذات الطبيعة السيبرانية إلى أخطار الكترونية وإعادة التفكير بمفهوم الأمن القومي الذي يعني بحماية قيم المجتمع الأساسية⁽⁷⁾

أخذت تلك الحروب صور عدة جمعت بين ضربات إستباقية تُهدف لمواجهة أي تهديدات مُحتملة وحروب بالوساطة، كبيع إحدى منظمات الأعمال العسكرية خدماتها الأمنية والمعلوماتية إلى بعض الجهات، مما يؤدي لإندلاع حرب إفتراضية الراح فيها من يملك المعرفة الرقمية والتقنيات الحديثة .

للحروب الإلكترونية طابع خاص في الفضاء الإلكتروني يعتمد على مدى التطور التكنولوجي وإمتلاك الفايروسات والهاكرز في الهجمات الإلكترونية، فهناك معارك مُنافسة بين شركات برامج الحماية الإلكترونية وصُناع الفايروسات المعلوماتية، فالحرب الإلكترونية سابقاً كانت تقتصر بالتشويش

على أنظمة الرادار والإتصال، بينما في العصر الحالي إتسعت إلى شبكات الإتصال، والمعلومات ، والإختراق لمُختلف أنظمة الدولة⁽⁸⁾

يُمكن أن نُطلق على هذا بالحرب الإلكترونية الباردة، التي أصبحت تُمثل تهديدات أمنية كبيرة على إستقرار الدول في العالم وأسواقه الإقتصادية وبُناه التحتية .

يمثل الخطاب السياسي الناضج وإدارة المؤسسات بصورة صحيحة ومهنية تهتم باحتياجات المجتمع ، ومعالجة ظاهرة البطالة ، ومحاربة الفساد مع وجود حرية للتعبير عن الرأي ،

كل ذلك من شأنه أن يُسهم في الإستقرار الأمني والحد من العمليات الإرهابية بكافة أشكالها (9)

حيث أصبح الفضاء الإلكتروني مؤخراً من ضمن أولويات الدول في سياساتها الداخلية، والخارجية، و الأمن القومي لديها، فقد دفعت التهديدات المستمرة لأمن شبكة المعلومات العديد من الدول إلى التسلح بالمعرفة والتكنولوجيا من أجل حماية الأمن والنظام العام في الدولة .

المطلب الثاني : الإرهاب الرقمي

أسهمت التكنولوجيا الحديثة إلى تعقيد الجانب الأمني في الحياة نوعاً ما، فقد بات هذا الأمر يُشكل تهديد مُتزايد يوماً بعد يوم مع صعوبة السيطرة عليه بمرور الوقت، لتأثيره الكبير وسرعة إنتشاره ، فالتزاوج بين الإرهاب والتكنولوجيا أدى إلى ظهور هذا النوع من الإرهاب الجديد .

تشغل قضية الإرهاب اليوم العالم أجمع بسبب ما تخلفه من آثار على المجتمعات والأفراد والمؤسسات، حيث تعددت اشكاله وتنوعت دوافعه، فضلا عن ممارسات بعض الدول التي تشجع عليه خدمة لمصالحها(10)

نتيجة للتطور التكنولوجي في مجال الإنترنت أخذ الإرهاب بُعداً جديداً يختلف عن النمط المُتعارف عليه، فبدأ الإرهابيون بتوظيف هذه التقنية في ارتكاب الجرائم عبر الفضاء المعلوماتي الذي يُمثل الملاذ الآمن لهم وإمكانية التواصل والتدريب فيما بينهم بسرية تامة

إذ أثرت شبكات تكنولوجيا الإتصال بشكل كبير في عملية تحول الإرهاب إلى تهديد عالمي، حيث مثل الإرهاب الجديد تطور الظاهرة الإرهابية في العصر الحديث، فبعد أن كانت عبارة عن موجات ذات طابع قومي متطرف إجتاحت أوروبا في أواخر القرن التاسع عشر، وكذلك ذات طابع أيديولوجي أثناء الحرب الباردة وإحدى أدوات الصراع بين الشرق والغرب، إتممت الجماعات الإرهابية الجديدة بالنمط العابر للجنسيات تجمعهم قضية دينية، أو قومية مبنية على أسباب ودوافع مُحددة هدفهم إيقاع أكبر أثر مُمكن على الآخرين(11)

عقب أحداث الحادي عشر من سبتمبر عام 2001، شهد الإرهاب تحول جذري كبير في أدواته وآلياته، حيث باتت التكنولوجيا من الوسائل الداعمة للعمل الإرهابي والمساهمة في زيادة ديناميكية وسهولة إنتشاره وتعاظم أثره، على إعتبار أن التكنولوجيا هي مجموعة المعارف والأساليب المتاحة اللازمة للتنمية في كل عصر من العصور، أما تكنولوجيا الإرهاب فتشتمل على جانبٍ (مادي) يتمثل بالمواد، والأدوات، والتجهيزات، والوسائل التي يستخدمها الإرهابي، وجانبٍ آخر (عقلي) يتمثل بالخبرة، والمعرفة، وإسلوب التعامل في البيئة المحيطة (12)

وهذا التطور في مفهوم الإرهاب وآلياته هو ما دفع العديد من الدول إلى توقيع الإتفاقيات لمكافحة الإجرام والتطرف عبر الإنترنت، فضلاً عن قيام بعض الدول بمراقبة الإتصالات الهاتفية، والرسائل النصية، والكثير من الأنشطة التي تُمارس على الشبكة المعلوماتية بما فيها مواقع التواصل الإجتماعي، ما يتحتم علينا دراسة هذا النوع من الإرهاب من أكثر من جانبٍ.

أولاً : أسباب الإرهاب الرقمي و دوافعه :

قد تتشابه دوافع الإرهاب الإلكتروني وأهدافه بإعتبار أن السبب الذي دفع إلى ارتكاب الجريمة يمثل الغاية التي يتوخاها الإرهابيون من جرائمهم وأفعالهم، فباديء الأمر يجب الوقوف على الأسباب التي تقضي إلى الإرهاب الرقمي لمعرفة العلاقة التي تربط التكنولوجيا بأهم وأخطر الجرائم التي تُرتكب بحق البشرية و كالاتي :

1. أسباب تتعلق بالفرد تدفعه بشكل مباشر إلى ارتكاب الجريمة وقد تختلف من شخص

لآخر وهي (13)

أ. أسباب شخصية ونفسية : فهناك من العوامل والأمراض النفسية ما يدفع الفرد إلى الإنتقام لإحداث تغييرات جذرية والتضحية بنفسه وبأرواح الآخرين سواءً أفراد السلطة، أو أفراد عاديين، والعامل النفسي هو المُعبر عن مدى تأثير العمل على المُنفذ في نفوس الأفراد وما يدفعه لذلك الشعور باليأس والإحباط، و الشعور بالنقص والأهمية الذاتية والمركز الأسري، الإغتراب والعزلة، و فقدان الشعور بالإنتماء للوطن والولاء له.

ب. أسباب فكرية : تتمثل بتدخل الدين في سياق العلاقات الوطنية الدولية، وإتخاذه كوسيلة في حلقات الصراع السياسي، فضلاً عن الفهم الخاطيء للشرائع السماوية ، ومبادئها، وأحكامها وسوء تفسيرها، والإجتهاد الشخصي في قضايا الدين دون الرجوع إلى العلماء والمختصين، وكذلك التطرف، و العلو في الفكر الذي يمثل أمر بالغ الخطورة قد يؤدي إلى تكفير الآخر وإستباحة كل ما لديه .

ج. أسباب إجتماعية وإقتصادية : يُمكن أن نراها في التفكك الأسري والإجتماعي مما يؤدي إلى الإنحراف والإجرام، وكذلك فقدان الهوية المجتمعية والعقيدة الصحيحة للمجتمع وفقدان العدل، وقد يلجأ الإرهابيون لنشاطات بُغية إشباع الحاجات المادية ، فالإقتصاد عامل أساس في خلق الإستقرار النفسي لتحقيق رضا الإنسان، وإستقراره الإجتماعي .

2. الأسباب المتعلقة بالدولة : وتأخذ شكلين على النحو الاتي (14)

أ. الدور المباشر للدولة في الإرهاب : فقد تكون الدولة سبباً مباشراً من أسباب الإرهاب والعنف في ظل غياب الحريات العامة والتعبير عن الرأي بالطرق السلمية، وكذلك عبر ممارسة الدولة لسياسات التمييز والفصل العنصري من خلال عمليات الإبادة الجماعية ضد جماعة عرقية معينة يجعل تلك الأقلية تُطالب بالإستقلال والإنفصال عن الدولة مما يدفع تلك الأقليات إلى العنف والإرهاب لتحقيق أهدافها .

ب. الدور غير المباشر للدولة في الإرهاب : تلعب العوامل السياسية، والإجتماعية ، والإقتصادية، والثقافية التي تُعد نتاج السياسة التي تنتهجها الدولة دوراً لا يُستهانُ به في تهيئة بيئة مناسبة للإرهاب تتمثل بإنعدام الحرية السياسية وتعبير الجماعات عن أفكارها، فضلاً عن غياب الدور الفعال للأحزاب السياسية وعدم إهتمامها بالتربية السياسية للمجتمع لاسيما فئة الشباب ناهيك عن إنعدام الثقة في النظام السياسي في الدولة مما يؤدي الى العزوف عن المشاركة السياسية .

3. الأسباب التقنية : هناك بعض الأمور الفنية والتقنية عندما تتواجد تكون بمثابة دافع ومحفز أكبر للقيام بهجمات الإرهاب الإلكتروني ومنها⁽¹⁵⁾

أ. ضعف بنية الشبكات المعلوماتية وإمكانية إختراقها بسبب وجود ثغرات أمنية يسهل الولوج من خلالها وممارسة النشاطات الإرهابية .

ب. غياب الحدود الجغرافية في الشبكة المعلوماتية إلى جانب عدم وضوح الهوية الرقمية للمستخدم يُعد فرصة مناسبة للإرهابيين من أجل ممارسة نشاطاتهم الإرهابية .

جـ. غياب الرقابة والسيطرة على الشبكة المعلوماتية يسهم بشكل كبير في انتشار جرائم الإرهاب الرقمي وتبادل محتواه بسهولة ويسر .

تتطلب المنافسة في المجال الإقتصادي والنشاطات التجارية والإستثمارية، إجراءات موازية في مجال الأمن والتسلح من أجل حماية تلك النشاطات الإقتصادية من أي هجومي إرهابي عسكري ، أو إختراق لمواقع المؤسسات الإقتصادية في الدولة⁽¹⁶⁾

كنتيجة لتلك الأسباب فإن الإرهاب الرقمي يهدف إلى ترويع الأمنين، ونشر، الرعب، والإخلال بالنظام العام وتعريض المجتمع للخطر والنيل من الأمن النفسي للأفراد، فضلاً عن إثارة الرأي العام لتحقيق أغراض سياسية .

ثانياً : **خطر الإرهاب الرقمي وآثاره** : هناك العديد من المزايا والإستخدامات للتكنولوجيا المتطورة والأجهزة التقنية الحديثة، ولكن في الوقت نفسه لها الكثير من المخاطر والمساويء، حيث ظهر ما يُسمى بعنف عصر المعلومات، أو كما يُطلق عليه البعض بالإرهاب الرقمي، الذي تكمن خطورته في سهولة إستخدام الأدوات التقنية التي تكون شديدة التأثير والخطورة .

لقد أصبح الإرهاب الرقمي هاجس مخيف للعالم الذي بات عرضة للهجمات الإرهابية عبر شبكة الإنترنت، عن طريق ممارسة تلك النشاطات الإجرامية من أي مكان في العالم، وهذا ما يشكل خطر حقيقي يتفاقم مع مرور الوقت كون التقنيات الحديثة بمفردها غير قادرة على حماية الناس من العمليات الإرهابية الألكترونية ، والتي غالباً ما تُسبب الأضرار الكبيرة والجسيمة للأفراد ، والدول، والمنظمات من الناحية المادية والنفسية⁽¹⁷⁾

يزداد خطر الإرهاب الرقمي في البلدان والدول المتقدمة التي تمتلك النفوذ والسيطرة وتُدار بُنيتهما التحتية، بالتقنيات الحديثة، والحواسيب، وشبكة الإنترنت، وهذا ما يجعلها هدف سهل المنال، فبدل إستخدام المتفجرات بإمكان الجماعات الإرهابية من خلال لوحة

مفاتيح الحاسوب تدمير البنى التحتية وإحداث أضرار ودمار يفوق ما تُخلفه الأسلحة والمتفجرات (18)

فالهجمات الإرهابية الألكترونية بإمكانها إفقاد السيطرة على الإتصالات وأنظمة القيادة، أو إخراج التحكم بالأسلحة الدفاعية للدولة والهدف من هذه الهجمات هو من أجل السيطرة وإيصال رسائل القوة من قبل تلك الجماعات والتنظيمات الإجرامية ضد الدول والمجتمعات التي تقوم بإستهدافها .

حيث قامت العديد من التنظيمات الإرهابية مثل تنظيم القاعدة و داعش، بإستخدام شبكة الإنترنت لتحقيق أهدافها سواءً كانت دعائية ، أو عسكرية ،فضلاً عن إستغلال تلك الشبكة كوسيلة إعلامية لها توصل رسائلها من خلالها، ويُمكن لمس المخاطر التي تتعلق بالإرهاب الرقمي في أوجه عدة منها(19)

1. مخاطر تتعلق بالفكر الإرهابي و نشر ثقافة العنف : حيث أن ظهور شبكة الإنترنت كأداة إعلامية ذات وسائل متنوعة وسهلة الإستخدام، و بكلفة بسيطة تُساعد على التخفي وفيالوقت نفسه تصل إلى الشرائح المُستهدفة في كُل مكان قد شجع التنظيمات المُتطرفة إلى نشاطها نحو العالم الافتراضي، وهذا ما أكدهُ تصريح الرجل الأول في تنظيم القاعدة الإرهابي أيمن الظواهري، عندما أشار قبل سنوات عدة بأن الحرب إعلامية ليقينه بأن المواجهة الميدانية خاسرة لتلك التنظيمات وأودت بحياة الكثير من نُخبها وأعضائها المُتخصصون في المجالات التقنية .

2. المخاطر المتعلقة بإشاعة الفوضى وزعزعة الإستقرار السياسي : حيث تقوم التنظيمات الإرهابية عبر شبكة الإنترنت بإستغلال النوافذ الإعلامية في نشر المقاطع الفيديوية والبيانات التحريضية ، أو الدعائية، ولا شك أن لكل هذا من شأنه أن يؤثر ولو بشكلٍ نسبي بصورة سلبية على مُعدل الثقة في الحكومات والأنظمة في نفوس مواطنيها، فإننتشار مثل هذه الأعمال الإرهابية عبر شبكة المعلومات وما يرتبطُ بها من إشاعة الفوضى من شأنه أن يؤدي إلى فقدان الشعور بالأمن و زعزعة الإستقرار السياسي .

3. المخاطر المُتعلقة بإثارة النعرات الطائفية والعنصرية : هناك من يُقلل من شأن الدور الذي يلعبهُ الإعلام الجديدي عندما تستغلهُ الجماعات الإرهابية في إثارة النعرات الطائفية،

والقلبية، ولكن الحقيقة أن هذا الأمر على قدر كبير من الخطورة، فأدبيات التنظيمات التي تُمارس الإرهاب الرقمي تجد أن اللعب على وتر الطائفية، وإثارة الفتن هو أبرز، الرسائل المباشرة، أو غير المباشرة التي تهدف تلك التنظيمات إلى الوصول إليها .

4. المخاطر المتعلقة بالجريمة الجنائية الرقمية : تُمارس الكيانات والتنظيمات الإرهاب الإلكتروني، حيث تمتلك الكثير من التقنيين والفنيين المتخصصين في التعامل مع بنية المعلومات في شبكة الإنترنت، وتتحرك تلك التنظيمات في هذا الجانب بالتحديد بدوافع أيديولوجية، أو سياسية، وذلك ما يدفعها لإرتكاب الهجمات الإلكترونية بغرض اختراق الحسابات الرسمية والعسكرية للدول التي تستهدفها، أو تسريب معلومات تتعلق بالأمن القومي، وغيرها من صور الجرائم الرقمية .

يتبلور جوهر الإرهاب الرقمي حول فكرة توظيف التكنولوجيا الحديثة لأغراض متطرفة، تستخدم في العنف والتهديد لتحقيق أهداف سياسية، وكذلك ما يمكن أن يحدثه العنف من تأثير نفسي على الجهة المستهدفة، وإجبارها على تغيير سلوكها، وتغيير مواقفها تجاه قضايا معينة .

ثالثاً : تأثير الإرهاب الرقمي على فئة الشباب :هناك العديد من المزايا والإيجابيات للتكنولوجيا والإعلام الجديد بإمكان الإنسان بصفة عامة، والشباب بصفة خاصة الاستفادة منها، ولكن لا تخلو من السلبيات التي تظهر عند استخدامها من قبل المتطرفين.

تختلف وسائل الإرهاب الإلكتروني عن الوسائل المعروفة لدى الإرهابيين بشكل عام التي تكون ذات طابع تقليدي فبالإمكان أن يُستهدف الشباب بخطر الإرهاب الإلكتروني عبر أكثر من طريق وإتجاه، فقد يكون البريد الإلكتروني هو الوسيلة التي يستهدف بها الإرهاب للتأثير على فئة الشباب عبر رسائل، أو إعلانات، أو أياً من المغريات الأخرى، أو عن طريق شبكات التواصل التي تعج بمختلف التيارات الفكرية المتطرفة وأعضاء التنظيمات الإرهابية⁽²⁰⁾

إن خطورة تأثير الإرهاب الرقمي تكمن في الوسائل المستخدمة التي تُعد وسائل راجحة لدى فئة الشباب، فالأجهزة التكنولوجية الحديثة التي يستخدمها الإرهابيون في نشر

رَسَائِلُهُمْ وَأَفْكَارُهُمْ هِيَ فِي حَقِيقَةِ الْأَمْرِ وَسَائِلِ يَحْرُصُ الشَّبَابُ عَلَى إِسْتِخْدَامِهَا يَوْمِيًّا لِمَا لَهَا مِنْ خَصَائِصٍ وَطَبِيعَةٍ مُوَاطِبَتِهَا لِعَصْرِ الْمَعْلُومَاتِ .

يَسْتَهْدَفُ الْإِرْهَابُ الرَّقْمِيَّ بِالذَّرْجَةِ الْأُولَى الْجَانِبِ النَّفْسِيِّ لِلشُّعُوبِ وَالدُّوَلِ الْمُسْتَهْدَفَةِ عَبْرَ رَسَائِلِهِ، فَقَدْ يَكُونُ هَذَا التَّأثيرُ فِي صُورَةِ بَثِّ رَسَائِلِ مُتتَالِيَةٍ يَكُونُ مُحتَوَاهَا ذَا تَأثيرٍ عَلَى الشُّعُورِ بِالْأَمْنِ النَّفْسِيِّ وَالطَّمَأْنِينَةِ لَدَى الشَّبَابِ، فَقَضَايَا الْإِرْهَابِ فِي عَالَمِ التَّكْنُولُوجِيَا، وَمَا تَنَظَّمُهُ مِنْ أَعْمَالِ تَخْرِيْبٍ وَعُنفٍ تَجْعَلُ أَفْرَادَ الْمُجْتَمَعِ فِي حَالَةٍ مِنَ الْقَلْقِ وَعَدَمِ الْإِسْتِقْرَارِ، مِمَّا يَجْعَلُهُمْ يَعْيشُونَ دَاخِلَ مُجْتَمَعٍ قَدْ لَا يَشْعُرُونَ تَجَاهَهُ بِالْوَلَاءِ (21)

إِذْ يَتَضَمَّنُ الْإِرْهَابُ الرَّقْمِيَّ رَسَائِلَ قَدْ تُؤدِّي إِلَى رَعزَعَةِ الثِّقَةِ الدَّاخِلِيَّةِ لَدَى الشَّبَابِ فِي بِلَادِهِمْ وَفِي قِيَادَاتِهِمُ السِّيَاسِيَّةِ، فَالتَّأثيرُ الْأَخْطَرُ عَلَى فِئَةِ الشَّبَابِ يَكْمُنُ فِي أُسَالِيْبِ الْإِقْنَاعِ، أَوْ مَا يُسَمَّى بِالْآثَرِ الْعَكْسِيِّ، فَقَدْ يُوْدِي التَّعْرُضُ الْمُتَكَرِّرُ لِتِلْكَ الْمُحتَوِيَّاتِ إِلَى شُعُورٍ بِالْتَعَاطُفِ وَالْإِعْجَابِ بِفِكْرَةِ الْقُوَّةِ وَالسِّيَطْرَةِ وَإِخْضَاعِ الدُّوَلِ وَالْقُوَى الْكُبْرَى، وَعَلَيْهِ سَيَكُونُ هَذَا الْأَمْرُ دَافِعًا لِلْإِنْضِمَامِ لِتِلْكَ التَّنْظِيمَاتِ .

رَابِعًا : مَكَاْفِحَةُ الْإِرْهَابِ الرَّقْمِيَّ : مِنْ غَيْرِ الْمُمْكِنِ لِأَيِّ مُجْتَمَعٍ فِي هَذَا الْعَصْرِ أَنْ يَعْيشَ بَمَعزَلٍ عَنِ التَّكْنُولُوجِيَا التَّقْنِيَّةِ الْمُتَسَارِعَةِ، وَالآثَارِ الْأَمْنِيَّةِ، وَالْإِجْتِمَاعِيَّةِ، وَالْإِقْتِسَادِيَّةِ الَّتِي تَنْجُمُ عَنْهَا، فَفِي ظِلِّ التَّرَابِطِ الْوَثِيقِ بَيْنَ دَوْلِ الْعَالَمِ عَبْرَ تَقْنِيَّاتِ الْإِتْصَالَاتِ وَالتَّطْبِيقَاتِ الَّتِي سَمَحَتْ بِإِنْسِيَابِ السِّلْعِ وَالْأَفْكَارِ وَالْمَعْلُومَاتِ بَيْنَ الْمُسْتَعْمِلِينَ، بَاتَ مِنَ الصَّرُورِيِّ لِكُلِّ بِلَادٍ حِمَايَةَ أَفْرَادِهِ وَمُؤَسَّسَاتِهِ مِنْ سَلْبِيَّاتِ هَذَا التَّنْطُورِ .

عَلَى الرَّغْمِ خَطُورَةُ قَضِيَّةِ الْإِرْهَابِ الرَّقْمِيَّ، إِلَّا أَنَّ هُنَاكَ قَلَّةٌ إِهْتَمَّ بِهَذَا الْمَوْضُوعِ عَلَى مُسْتَوَى الدُّوَلِ الْعَرَبِيَّةِ مِنْ حَيْثُ التَّحْلِيلِ لِتِلْكَ الظَّاهِرَةِ، حَيْثُ أَصْبَحَتْ قَضِيَّةٌ دَوْلِيَّةٌ بِسَبَبِ دُخُولِ التَّكْنُولُوجِيَا، فَالْإِرْهَابُ يَرْتَبِطُ بِعَوَامِلٍ سِيَاسِيَّةٍ، وَتَقْافِيَّةٍ، وَإِجْتِمَاعِيَّةٍ نَتِيجَةُ النُّطُورَاتِ السَّرِيعَةِ فِي الْعَصْرِ الْحَدِيثِ، فَقَدْ تَصَاعَدَتِ الْعَمَلِيَّاتُ الْإِرْهَابِيَّةُ وَكَانَ أَكْثَرُهَا تَأثيرًا أَحْدَاثَ الْحَادِي عَشْرٍ مِنْ سِبْتَمْبَرِ عَامِ 2001، وَهَذَا التَّارِيخُ مِثْلُ تَحْوَلِ بَارزِ وَكَبِيرٍ فِي تَارِيخِ الْإِرْهَابِ، وَالتَّنْطُرِ، وَطَرِيقَةِ التَّخْطِيطِ وَالتَّنْفِيزِ لِتِلْكَ الْعَمَلِيَّاتِ (22)

إن مكافحة الإرهاب الرقمي ومعالجة آثاره لا بُد أن تخضع لمعايير عدة ، فالتعاطي مع تلك الظاهرة بوسائلٍ تقليدية لم يعد يُحقق الأهداف المنشودة وتتمثل أبرز وسائل مكافحة هذا الإرهاب بما يأتي :

1. الجانب التقني : بالإمكان الإستفادة من التكنولوجيا الحديثة وتوظيفها بأسلوبٍ علمي من أجل تعقب الإرهابيين، عن طريق تتبع البيانات وتبادل المعلومات التي تكشف عن مُرتكبي تلك الجرائم عبر إيجاد نظامٍ أمني مُتكامل⁽²³⁾

تُوفّر التكنولوجيا الحديثة الكثير من المُميزات لمُرتكبي الإرهاب، ولكن بالإمكان مُراقبتها وتقييد البعض من وظائفها كإرسال البريد الإلكتروني بحزمةٍ كبيرةٍ للكثير من المُتلقيين، والتي قد تكون بمثابة الضوء الأخضر لبدء العمليات الإرهابية .
من متطلبات الدولة الحديثة القائمة على القانون، تحقيق سياسات أمنية شاملة وفق التقنيات الحديثة ونشاطات الأجهزة الأمنية المتناسقة، إذ يسهم ذلك في إتخاذ قرارات ناجحة تكفل الإستقرار الأمني ومواجهة التهديدات الإرهابية⁽²⁴⁾

تلعبُ المُراقبة والقيود إلى تجنب حدوث الخروقات الأمنية أهمية كبيرة لدرء مخاطر هذا النوع من الإرهاب، فالمُراقبة للمواقع ذات النشاطات المشبوهة يكونُ بتصريحٍ قضائي، ولا يُمثل في الوقت نفسه أي مساسٍ بالحريات العامة.

مُكافحة هذا النوع من الإرهاب تتطلّب تعاون وتسيق كبيرين على مُستوى الحكومات والمؤسسات الأمنية، وتوحيد جهودها، وفرض رقابة صارمة على نشر محتوى شبكة الإنترنت الذي يكون ذا صلةٍ بالإرهاب الرقمي، ناهيك عن حماية المواقع الإلكترونية لمؤسسات الدولة من الإختراق .

2. الجانب التوعوي : تُسهم التوعية في خلق بيئةٍ صالحة تدعو إلى التعايش السلمي بين المكونات والمُجتمعات المُختلفة، وكذلك مواكبة النشر العلمي في المجالات العسكرية والأمنية تمثل أهمية كبيرة من حيث تطوير وسائل مكافحة الإرهاب الإلكتروني عن طريق إنشاء إدارات خاصة تعمل وفق تكنولوجيا حديثة تُسهم في مجال التوعية الأمنية لتحقيق أمن المُواطن وغرس مفاهيم بناءة في عقول الشَّباب⁽²⁵⁾

تتطلب مكافحة الإرهاب الرقمي في ظل التكنولوجيا الحديثة بناء قوة إقتصادية، وصناعية، وعلمية في الوقت نفسه من أجل بناء قوة عسكرية قادرة على مواجهة، وبجانب ذلك التأكيد على إصلاح الفكر والعقيدة لدى فئة الشباب لحمايتهم من التيارات المتطرفة وتمكينهم من رؤية الأمور على حقيقتها والرد على حُجج التنظيمات الإرهابية التي تتخذ من العقيدة والدين ذريعة لها لتنفيذ أعمالها الإجرامية .

3. الجانب الإعلامي : قد تلعب وسائل الإعلام دور سلبياً في الدعاية والترويج للإرهاب، ولكن بالإمكان المساهمة في مكافحة الإرهاب الإلكتروني عبر تبني منشورات ومحتويات تهدف الى القضاء على هذا النوع من الإرهاب، إذ ينصب دور الإعلام بالدرجة الأساس على الجانب الإنساني للمواطنين والأفراد، وفي هذا السياق يُركز الإعلام على ضحايا الإرهاب، وأعدادهم، وفتاتهم، لاسيما من النساء والأطفال من أجل رسالة إعلامية فعالة ومؤثرة في نفوس الجماهير⁽²⁶⁾

هناك رسائل ومحتويات إيجابية يُمكن للإعلام أن يساهم فيها للتقليل من شأن المنظمات الإرهابية عن طريق عدم التوسع في نشر البيانات والمقاطع والتهديدات الصادرة عن تلك المنظمات، كي لا تترك تلك الممارسات آثار سلبية في نفوس المواطنين .

المطلب الثالث : المسؤولية الجنائية في العالم الرقمي

هناك قواعد و قوانين تسود أي تنظيم إجتماعي على مر العصور، يلزم أفراد المجتمعات باتباعها في حياتهم اليومية، ولا شك أن هذا الأمر يسري أيضاً في عصرنا الحالي في ظل إنتشار التقنيات والتكنولوجيا الحديثة، فالمسؤولية الجنائية ليست فقط في الواقع الذي نعيشه وما يحدث فيه من جرائم وإعتداءات، وإنما أيضاً يمتد إلى الواقع الافتراضي في العالم الرقمي وما يدور فيه من جرائم إلكترونية تُفرض بالضرر على أفراد المجتمع .

إنّ إلحاق المسؤولية الجنائية على مُستخدم شبكات التّواصل، لا يُمكن إلاّ بالتأكد من ربط حسابه في تلك المواقع بالفاعل الحقيقي فيما تمّ نشره في حساب المُستخدم، مما يلحق فاعله المسؤولية الجنائية، وفي هذه الحالة لا يُمكن الإعتماد عليه بشكل كامل، إلاّ

إذا كان الحساب مُوثق لدى مواقع التّواصل الاجتماعي، أو في حالة قيام الشّخص بالإشارة إلى حسابِه علناً أمام أي وسيلة إعلامية تقليدية⁽²⁷⁾

في حالة إعتراض المُستخدم على تحمّل المسؤولية كالإدعاء بأن حسابِه تعرّض للإختراق، وأن ما تمّ نشره لم يصدر عنه، ففي هذه الحالة يُمكن لمُحققي الجرائم الإلكترونيّة معرفة صدقه عن طريق عنوان شبكة الإنترنت لما هو صادر منه بالفعل أم من غيره، إذ تمثّل أفعال المُستخدمين داخل الفضاء الرقمي مسؤولية قانونية لما يصدرُ عنهم، ولكل جريمة منهم، أو إنتهاك عقوبة خاصة به .

أولاً : صور جرائم مواقع التواصل الاجتماعي

يَعتمدُ تصميم مواقع التّواصل الاجتماعيّة على طريقة التّفاعل بين المُستخدمين، فمُصممو تلك البرامج أضافوا لها بعض التّفاعلات مع الآخرين، وهو ما ساهم في تحقيق قاعدة شعبية كبيرة من المُستخدمين لتلك البرامج حتى أصبحت هي الإستخدام الأكبر في شبكة الإنترنت، وهذا ما أدى إلى نشوء صور جديدة من الجرائم سنتناول الأكثر تأثيراً على حياة المواطن .

1. جريمة الدخول غير المشروع للحسابات : هو دخول غير مُصرح به عن طريق إنتهاك الإجراءات الأمنية، ويُطلق على من يقوم بهذا العمل بالقرصنة، أو (الهاكرز)، وقد يُعبر عن هذه الجريمة بمُصطلح (الإختراق) عبر برامج لكسر الحماية الخاصة ببرامج المُستخدمين، أو قد يتمّ الدخول بدون إختراق بإستخدام كلمة السر الحقيقيّة لشخص لا يمتلك صلاحية الدخول للحساب⁽²⁸⁾

يُعدّ الدخول غير المشروع بخد ذاته جريمة، كونه يُمثّل مرحلة أساسية لإرتكاب مُختلف الجرائم الإلكترونيّة الأخرى، فالمعلومات التي قد يقع عليها هذا العمل تكون ذات أهمية كبيرة، أو حتى أن كان الهدف من هذا العمل هو مجرد إثبات للذات، فعملية الإختراق المعلوماتي من قبل هؤلاء الأشخاص لا بُد أن يُقابله العقاب حتى يُصبح هناك رادع لكل من يُحاول الإعتداء على الأنظمة المعلوماتية⁽²⁹⁾

الهدف من الإختراق قد يكون لأسباب عدة، منها سرقة أو إزالة معلومات مُعينة، أو بقصد إبراز القُدرات التِقنية، أو لإثبات وجود ثغرات أمنية في برامج التّواصل، وقد يكون بدافع الإنتقام والحق الضرر بالآخرين .

2. جريمة التشهير : يُعد التشهير إحدى وسائل الإنتقام إذا لم يُحقق الشخص الذي قام بهذه العملية على ما أُراده بالوسائل الطبيعية، حيث أن عملية التشهير على مواقع التّواصل لها وقع كبير على المَجني عليه من الناحية النفسية والصحية⁽³⁰⁾

من الطّبيعي إن هناك أسباب ودوافع لكل جريمة، حيث أن عملية التشهير في مواقع التّواصل إنتشرت بصورة كبيرة في الآونة الأخيرة بسبب خلافات وخصومة بين المُستخدمين، وقد يكون التشهير سببه الجهل ، والتعصب ، وكذلك بسبب التنافس بين شركات تجارية وأفراد .

لقد جاءت الشريعة الإسلامية بتحريم التشهير والنهي عنه فقد قال تعالى (إن الذين يحبون أن تشيع الفاحشة في الذين آمنوا لهم عذابٌ أليم في الدنيا والآخرة والله يعلم وأنتم لا تعلمون)، أي إصاق تهم وأقاويل لم يَقم الآخريين بفعلها⁽³¹⁾

فبلا شك ان جريمة التشهير تتنافى مع ما جاء به ديننا الحنيف الذي نهى عن القذف ، والسب ، والطعن ، ونهى كذلك عن صرف الأموال من أجل إلحاق الأذى بالآخرين عن طريق تأسيس المواقع من أجل التشهير وفضح من يختلفون معه لأسباب شخصية .

3. جريمة إنتهاك الخصوصية : مع إنتشار شبكة الإنترنت وبرمجيات تسجيل ورصد المعلومات عن الآخرى، أصبح من اللازم حماية الخصوصية كحق مكفول قانونياً وأخلاقياً، فالهدف هو صيانة حياة الفرد الخاصة بمنحه حق الاعتراض على من يتدخل بخصوصياته أو النقصي عنها⁽³²⁾

تمثل الحياة الخاصة حق مشروع من حقوق الذات والأسرة من حيث الحفاظ على معلوماتهم الشخصية وأسرارهم وعدم إستخدامها دون موافقتهم.

مما يُولي الأهمية لتجريم هذا الفعل هو إنتشار مواقع التّواصل وتوّعها حيث تُقدم وسائل جذب وإستخدام لها، فالإمكانات الفائقة في جمع المعلومات عن المُستخدمين في

بنوك المعلومات هي في الوقت الحاضر أخطر أنواع إنتهاك الخصوصية وحرمة الحياة الفردية لاسيما في برامج التّواصل الإجتماعي⁽³³⁾

لعلّ سبب هذا الخطر هو الإقبال الشّدِيد وراء تلك المّواقِع الإجتماعية مِن قِبَل الأفراد مَعَ قِلّة التّثاقفة في مَجَال أمن المّعلّومات، وإدراج كُُلِّ ما يَتعلّق بِهِم مِن بَياناتٍ ومّعلّوماتٍ خاصّة ، وعامة مما يَجْعَل المُستخدِم هَدَفًا سَهلاً لِلجُنَاة سِوَا كانوا أَفراداً ، أو جَماعات .

تُعدّ مّواقِع التّواصل الإجتماعي وسيلة للإعتداء والمّساس بخصّوصية الأفراد مِن قِبَل ضِعاف النفوس، حيثُ أن حِسَابات المُستخدِمين تَحْتوي على كَمِّ هائلٍ مِن المّعلّومات المّخزونة وهنا مَكَامِن الخطر الذي يَنجُمُ مِن الإِستخدام غير المّشروع والخطيء لهذه المّعلّومات، وهذا يَعني إن خصوصية المّعلّومات هي محور الإرتكاز لِحمّاية الحياة الخاصّة في ظِلِّ العالَم الرّقمي⁽³⁴⁾

على الرّغم مِن التّطوّر الكَبير في التّكنولوجيا الذي يَظنّه الأفراد إنه سَهّل مِن حَيَاتِهِم، إلّا أن حَيَاتِهِم الخاصّة أَصبحت مُنتهكة ومُكبلة مِن قِبَل أَصحاب البرامِج الإجتماعية .

4. جريمة إنتحال الشخصية : الغرض من هذه الجريمة هو التّدليس الذي يَقع على الأشْخاص في الخطأ وبقائهم ضِمْن الدائرة نَفْسها الدائرة لَحْمَلِهِم على تَسليم الأموال التي في حَيَازَتِهِم للفاعِلين، وَيكون هذا الفِعْل بالكِتابة، أو الإِشارة، أو الإِتصال، إذ إنّ إنتحال الشّخصية مِن ضِمْن صُور تَزوير المّعلّومات التي تُعرف بِجَعْل الوَقائِع المُزيفة في صورةٍ وقائِعٍ حقيقيّة⁽³⁵⁾

تُعدّ هذه الجريمة مِن صُور الإحتيال والإِستيلاء على المّعلّومات الشّخصية للمُستخدِمين وإِيهام الأخرين، والكذب عَلَيْهِم بدافعِ مادي وتوليد الإِعتقاد لدى المّجني عليه بِتَصديق هذه الأكاذيب بِما يَدفعه للتّسليم إلى ما يُراد مِنه طواعية.

ولمُرتكِبِ جَرِيمة إنتحال الشّخصية غايات وأهداف عدة ، فقد يكون هدفهُ التّشهير، أو المّساس بالخصوصية، وقد يكون لَهْدَفٍ أَشدّ أهمية وهو الإِستيلاء على الأموال، لذلك نَرى قيام الكَثير مِن المُستخدِمين بالتّنبِيهِ بِعَدَم وجود أَكثَر مِن حِسَاب وِذِكِر الإِسم الرّسمي لِلجِهات التي يَتعامل مَعها .

5. جريمة النشر الإباحي : إن القيام بهذه الجريمة هو فعل سيء مهما كان الهدف أو الغرض من ذلك، فهو أمر مرفوض من المجتمع بكل صورته لاسيما في الدول الإسلامية، فكل من ينشر الإباحية هدفه العام هو شيوع الرذيلة، وقد يرافقه غايات أخرى مثل الاستغلال، والإبتزاز الجنسي، والإيقاع بالقاصرات، أو قد يكون الهدف من ذلك المكسب المادي عن طريق هذه الجريمة والترويج لها، أو عرض نفسه جنسياً، أما حقيقة، أو تحايلاً⁽³⁶⁾

إن الهدف من وراء هذه الجريمة قد يكون على صور عدة، فقد يتمثل بإفساد المجتمع نفسياً، ودينياً، وسلوكياً، أو يكون بإرسال فيروسات لإحترق الأجهزة، ويرجع العديد من جرائم الإغتصاب إلى ذلك الكم الهائل من المواد الإباحية المنتشرة في كثير من المواقع على شبكة الإنترنت .

6. جريمة إنشاء حساب للأعمال الإرهابية : تهدف الجماعات الإرهابية إلى تنفيذ مخططاتها عن طريق إشاعة الترويع والخوف بين الناس، فمعظم أهدافهم تتمثل في معارضتهم للنظام الحاكم ورموزه، أو إغتيال من يختلف معهم بالفكر والرؤى، وكذلك قد تهدف تلك الأعمال الإجرامية إلى عزل تلك الدول عن محيطها الخارجي عن طريق تحجيم حركة السياحة، وإستهداف الوافدين من الجنسيات الأخرى، وغيرها من الأهداف⁽³⁷⁾

من خلال مواقع التواصل الإجتماعي يُمكن للإرهابيين بث أفكارهم المتطرفة بمختلف صورها الدينية، والسياسية والغنصيرية، وعليه السيطرة على عاطفة و وجدان فئة الشباب، وإستغلال إندفاعهم وطموحهم وقلة خبرتهم في الحياة من أجل إفساد تفكيرهم وعقائدهم وفي نفس الوقت إستغلال معاناتهم و أوضاعهم المادية من أجل تحقيق أجندة خاصة تتعارض مع مصلحة الوطن والإستقرار المجتمعي⁽³⁸⁾

هناك حقيقة علينا الاعتراف بها وهي أن الإرهابيين بالأمس كانوا بأشد الحاجة إلى التسلح ببندقية، أما اليوم فالإرهابيون من خلال الأجهزة المحمولة، وشبكة الإنترنت أصبحت أدواتهم الرئيسية والفاعلة في نشاطهم الإرهابي الدولي .

خَدَمَت سَبْكَةُ الْإِنْتَرْنَتِ الْخَلَايَا الْإِرْهَابِيَّةَ بِشَكْلِ كَبِيرٍ مِنْ حَيْثُ تَضَخِيمِ الصُّورَةِ فِي أذْهَانِ الْمُتَلَقِّينَ عَنِ حَجْمِ تِلْكَ الْخَلَايَا وَتَأْتِيرِهَا رَغْمَ إِمْتِلَاقِهَا لِعَدَدٍ قَلِيلٍ مِنَ الْأَفْرَادِ الَّذِينَ لَدَيْهِمْ خِبْرَاتٌ فِي مَجَالِ الْحَاسُوبِ وَالْبَرَامِجِ الْمُتَنَوِّعَةِ لِلْإِعْلَامِ لِبَثِّ الرِّسَائِلِ الَّتِي تَخْدُمُ أَهْدَافَهُمْ، وَلَشَّنْ حَرْبٍ نَفْسِيَّةٍ ضِدَّ الْأَعْدَاءِ، وَكَذَلِكَ الدِّعَايَةِ وَالتَّرْوِيجِ لِأَهْدَافِهِمْ بَعِيداً عَنِ الْوَسَائِلِ التَّقْلِيدِيَّةِ كَالصَّحْفِ، وَ التَّلْفِزِيُونِ (39)

أَسْهَمَتْ سَبْكَةُ الْإِنْتَرْنَتِ فِي تَنْظِيمِ وَتَرَابُطِ الْجَمَاعَاتِ الْإِرْهَابِيَّةِ، وَتَبَادُلِ الْأَفْكَارِ، وَالْمُقْتَرِحَاتِ، وَالْمَعْلُومَاتِ بِشَكْلِ كَبِيرٍ، وَكَذَلِكَ مَعْلُومَاتِ مِيدَانِيَّةِ حَوْلِ إِصَابَةِ الْأَهْدَافِ، نَاهِيكَ عَنِ التَّنْسِيقِ وَالتَّخْطِيطِ لِلْأَعْمَالِ الْإِرْهَابِيَّةِ فِيمَا بَيْنَهُمْ بَعْضُ النَّظَرِ عَنِ أَمَاكِنِ تَوَاجُدِهِمْ .

ثَانِيَا : الْأَمْنُ النَّفْسِيُّ : يُعَدُّ مِنْ أَهْمِ الْحَاجَاتِ الْإِنْسَانِيَّةِ لِإِنْبَاءِ الشَّخْصِيَّةِ، حَيْثُ يَمْتَدُّ مِنَ الطُّفُولَةِ وَحَتَّى الشَّيْخُوخَةِ عِبْرَ الْمَرَاكِلِ الْمُخْتَلِفَةِ مِنَ الْعُمُرِ، وَلَكِنْ أَمْنُ الْإِنْسَانِ يُصْبِحُ مُهْدَدًا عِنْدَ تَعَرُّضِهِ إِلَى ضَغُوطٍ إِجْتِمَاعِيَّةٍ وَنَفْسِيَّةٍ لَا يَسْتَطِيعُ مُقَاوَمَتَهَا فِي مَرَحَلَةٍ مِنَ مَرَاكِلِ عُمرِهِ .

نَتِيجَةُ التَّنَطُّورِ الْمَعْلُومَاتِيِّ وَثَوْرَةِ التَّكْنُولُوجِيَا وَالْإِتِّصَالِ حَدَثَتْ تَغْيِيرَاتٌ سَرِيعَةٌ وَكَبِيرَةٌ فِي الْعَالَمِ خِلَالَ الْعَقْدِ الْأَخِيرِ، حَتَّى أَصْبَحَ الْأَمْرُ وَكَأَنَّنا نَعِيشُ فِي قَرْيَةٍ صَغِيرَةٍ، حَيْثُ صَاحَبَتْ هَذَا التَّنَطُّورُ تَحَوُّلَاتٍ إِجْطِمَاعِيَّةٍ، وَكَذَلِكَ كَانَ سَبَباً فِي إِنْعَكَاسِ الْكَثِيرِ مِنَ السَّلْبِيَّاتِ عَلَى الْحَيَاةِ الْبَشَرِيَّةِ لِأَسِيْمَا فِي بُلْدَانِ عَالَمِ الْجَنُوبِ الَّتِي بَدَأَ فِيهَا التَّغْيِيرُ بِشَكْلِ مُفَاجِئٍ وَسَرِيعٍ، وَقَدْ نَجَّمَ عَنِ ذَلِكَ الْكَثِيرِ مِنَ الْمَشْكَلَاتِ النَّفْسِيَّةِ الَّتِي مِنْ أَهْمِ مَظَاهِرِهَا الْقَلْقُ وَالْإِكْتِنَابُ، وَصِرَاعَاتُ الْفَرْدِ مَعَ الْآخَرِينَ، نَاهِيكَ عَنِ مُصَاحَبَةِ ذَلِكَ إِنْعَادَامِ أَمْنِ الْأَفْرَادِ النَّفْسِيِّ (40)

بِسَبَبِ الْحُرُوبِ، وَالْكَوَارِثِ الطَّبِيعِيَّةِ، وَالْأَحْدَاثِ الْإِرْهَابِيَّةِ الَّتِي تَسُودُ الْعَالَمَ، الْيَوْمَ فَضْلاً عَنِ الْأَوْبَةِ وَالْأَمْرَاضِ الْإِنْتِقَالِيَّةِ الْجَدِيدَةِ، كُلُّ ذَلِكَ يَجْعَلُ الْإِنْسَانَ فِي حَالَةٍ مِنَ الْقَلْقِ وَالْخَوْفِ مِمَّا يُجَدِّدُ الْحَاجَةَ إِلَى الْأَمْنِ النَّفْسِيِّ .

يُعَدُّ مَفْهُومُ الْأَمْنِ النَّفْسِيِّ مِنَ الْمَفَاهِيمِ الْمُعْقَدَةِ بِالنَّظَرِ لِتَأْتِيرِهِ بِمُتَغْيِرَاتِ تَكْنُولُوجِيَّةِ، وَإِجْتِمَاعِيَّةِ، وَإِقْتِسَادِيَّةِ، فَالْإِحْسَاسُ بِالْأَمْنِ مُرْتَبِطٌ بِإِسْلُوبِ حَيَاةِ الْفَرْدِ وَمَدَى إِشْبَاعِهِ

لحاجاته وهذا الأمر فيه تباين من شخصٍ لآخر، فقد يرى شخص أن الإرهاب يمثل تهديد مباشر لآمنه النفسي، في حين هناك شخص آخر قد لا تمثل الحوادث الإرهابية له سوى أمر عابر أو حادث عرضي، فهذا الشعور يخضع لإعتبارات نفسية واجتماعية تتعلق بالصحة النفسية للفرد، والتي بالتأكيد تؤثر على مستوى الأمن النفسي للفرد⁽⁴¹⁾

يُمثل مفهوم الأمن النفسي مفهوماً شاملاً ركزت عليه دراسات علم النفس والصحة النفسية، ويُعد العالم الأمريكي "أبراهام ماسلو Maslow" أول من تحدث عن مفهوم الأمن النفسي وعده محور أساس من محاور الصحة النفسية لمقدرة الفرد على مواجهة الإحباطات التي يتعرض لها، إذ قسم ماسلو دوافع سلوك الإنسان وجعلها تنظيم بشكل هرم قاعدته الأساسية هي الحاجات الفسيولوجية، تليها مباشرة الحاجة إلى الأمن، ثم الحاجات الأخرى التي تتعلق بالحُب والتقدير وتحقيق الذات⁽⁴²⁾

الطمأنينة النفسية للأفراد تكون عبر إشباع الحاجات الأساسية، ولعل الحاجة إلى الأمن النفسي تأتي من الثقة في النفس والانتماء إلى جماعة آمنة، وهنا الحاجة للأمن تعني البيئة الاجتماعية بيئة صديقة تُولد شعور لدى الفرد بإحترامه من قبل الآخرين .

من أهم الدوافع النفسية في المجتمع هي الحاجة إلى الأمن، وهي التي تحرك سلوك الإنسان نحو غاياته، فإذا ما أخفق الإنسان في تحقيق الأمن سيؤدي ذلك عجزه عن التحرك نحو تحقيق الذات .

إذ يرى علماء عدة من بينهم ماري مين (Mary Main)، إن الأمن النفسي من أهم حاجات الإنسان النفسية وكذلك من أهم دوافع السلوك اليومي، كما أن الأمن النفسي يُعد من المقومات الأساسية في الحياة لكل فردٍ من المجتمع ، فإذا ما كان هناك تهديد للإنسان هرع إلى ملجأ و ركن آمن ينشُد فيه السكينة⁽⁴³⁾

للأمن النفسي ضرورة وأهمية كبيرة في حياة الأفراد والمجتمعات ومن خلال ما يأتي يمكن أن نتضح تلك الأهمية⁽⁴⁴⁾ 1. الإبداع الفكري والتخطيط السليم في عملية التطور والتنمية لا يمكن أن تتم بدون توفر الأمن والاستقرار لكي يطمئن الإنسان على ثرواته وأستثماراته .

2. غاية العدالة تحقيق الأمن، فغياب العدالة تؤدي لغياب الأمن فواجبات الدولة هي عمران البلاد وأمن العباد.

3. شعور الفرد بالطمأنينة عند تحقق الأمن النفسي ويتمتع كذلك بالرضا والقناعة، فالشعور بالخوف والقلق يجعل الإنسان قريسة للانحراف والفساد .

4. توفر الأمن النفسي للفرد داخل المجتمع والجماعة يولد الشعور بالتقدير والمحبة من قبل الآخرين .

شعور الإنسان بالأمن يُمكنه من ممارسة أعماله اليومية وحياته الطبيعية بكل يسر، فخدمة الأمن هي ضمان حرية الفرد في المجتمع، وإزالة عوامل الخوف كافة، وتخلق في الوقت نفسه ردة ذاتي من خلال تنشئة المواطن بصورة صحيحة في ظل التشريعات النافذة وقوة القانون .

يذكر ماسلو أن تحقيق الأمن النفسي يتم من خلال إشباع الحاجات الأساسية، كالانتماء، والقبول، والاحترام، وتحقيق الذات، فالإنسان الآمن نفسياً هو الذي يشعر بإشباع حاجاته ومقومات حياته الأساسية بصورة غير معرضة للخطر .

يحتاج الأمن النفسي إلى أساليب هامة من أجل الوصول إلى الهدف العام وهو تحقيق درجة من الطمأنينة والرفاهية للفرد، حيث يلجأ الإنسان لتحقيق الأمن النفسي عبر أنشطة يستخدمها الجهاز العصبي لخفض الضغط، والتوتر، والإجهاد، وتحقيق الذات، والشعور بالأمان (45)

تعد الحاجة للأمن النفسي من الحاجات الأساسية التي لا يمكن الاستغناء عنها، وعلى الفرد السعي من أجل تحقيقها، إذ هناك العديد من الأساليب والوسائل التي يتحقق الأمن النفسي للفرد من خلالها وتتمثل بالآتي (46)

1. تنمية القدرات المعرفية للفرد كي يتجنب مآثر العنف والتهديد الداخلي والخارجي لحياته الشخصية .

2. تطوير الذات عبر كسب المهارات والخبرات الجديدة لمواجهة صعوبات ومستجدات الحياة .

3. الوعي التام بعدم بلوغ الكمال يجعل الفرد يفهم طبيعته وإمكانياته وقدراته واستغلال تلك القدرات بصورة مناسبة والسعي إلى سد ما لديه من نقص عبر التعاون مع الآخرين.

4. اعتماد الفرد على وسائل الإعلام لمعرفة الوقائع المختلفة، وأهمية هذا الإسلوب تظهر وقت الحروب ما يجعل الأفراد الذين يعرفون ما يجري حولهم أكثر صلابة في مواجهة الأزمات .

5. أهم ما يدعم شعور الفرد بالأمن هو الثقة بالنفس، فأحد أسباب فقدان الشعور بالطمأنينة والاضطرابات النفسية هو فقدان الثقة بالنفس، وكذلك فقدان الثقة بالآخرين وعليه فقدان التواصل مع المجتمع .

ثالثاً : الإطار القانوني لعقوبة الجرائم الإلكترونية في دولة الإمارات العربية المتحدة :

تعد تجربة دولة الإمارات العربية المتحدة من التجارب الرائدة في معالجة مسألة الجرائم الإلكترونية عبر القانون الاتحادي رقم (2) لسنة 2006، وكذلك القانون رقم (34) لسنة 2021، إذ ذكر المشرع الإماراتي الجرائم التي من الممكن وقوعها والعقوبات المترتبة عليها خلال استخدام تقنيات المعلومات وأدوات التواصل الرقمي، وعدد هذه الجرائم بحدود (74) جريمة، سيتم تناول أبرزها كما يأتي (47)

1. جريمة إختراق المواقع الإلكترونية: تكون عقوبتها الحبس والغرامة أو أحدهما نتيجة تدمير المعلومات، أو إنتهاك الشخصية، وكذلك على مستوى المواقع الإلكترونية للمؤسسات الحكومية، وغير الحكومية وتتراوح عقوبتها ما بين السجن من 6 أشهر إلى 7 سنوات، أو الغرامة من مئة ألف درهم الى مليون وخمسمئة ألف درهم وبالإمكان الحكم بالعقوبتين معاً أو أحدهما .

2. جريمة تزوير المستندات المعترف بها معلوماتياً كمستندات الحكومة الاتحادية والمحلية والمؤسسات أو الهيئات العامة، وتكون عقوبتها الحبس، أو الغرامة، أو كلاهما، وتتراوح الغرامة من مئة وخمسون ألف درهم إلى سبعمائة وخمسون ألف درهم .

3. جريمة الإحتيال على الشبكة المعلوماتية وتتم عبر استخدام عنوان وهمي بهدف ارتكاب جريمة أو الحيلولة دون إكتشافها، وتكون عقوبتها السجن المؤقت والغرامة التي تتراوح من خمسمائة ألف درهم إلى مليوني درهم أو إحدى العقوبتين .

4. جَرِيمة الإعتداء على مَعْلومات وبيانات حكومية عَن طريق الإستحواذ، أو الإلتلاف، أو التَّسريب، أو النسخ، أو النُّشر بغيرِ تَصريح، وتكون عقوبتها السِّجن ما بين (7 - 10) سنوات، والغرامة ما بين خمسمائة ألف درهم إلى خمسة ملايين درهم .
5. جَرِيمة الحصول على رموز وشَفراتٍ الغير بدون تَصريح، حيث كُـل من إستحوذ بغيرِ تَصريحٍ مِن صاحبِ الشَّأن على شَفرةٍ، أو رَقم سري، أو كلمةٍ مرور خاصة بموقع إلكتروني، فعقوبتها الحَبس بمدّةٍ لا تزيد عن ستة أشهر، وبغرامةٍ تتراوحُ بين خَمسون ألف درهم إلى خَمسمائة ألف درهم .
6. جَرِيمة إنشاء البريد والمواقع والحسابات الألكترونية الزائفة، عبر إصطناع مَواقع وحسابات وهمية وإنسابها زوراً لشخصٍ، أو مؤسسة حكومية ، فتكون العقوبة بالحسب من (2 - 5) سنوات، والغرامة من خَمسون ألف درهم إلى مليوني درهم . أو بإحدى هاتين العقوبتين .
7. الإعتداء على وَسائِل الدَفْع الألكترونية، فكل من نَسَخ، أو قَلَد، أو زَوَّر بِطاقة إئتمانية، أو أي وسيلةٍ مِن وَسائِل الدَفْع الألكتروني، بقَصْد الحصول على أموالٍ لِنَفْسِهِ أو لِغَيْرِهِ، تكون العقوبة بالحسب والغرامة من مَأتي ألف درهم إلى مليوني درهم، أو بإحدى هاتين العقوبتين.
8. جَرِيمة العَبَث بالأدلة الرَقمية، كُـل مَسْؤول عَن إدارة حساب، أو بَريد إلكتروني، أو موقع على شَبكة الإنترنت أخفى، أو عَبَث بأدلةٍ رَقمية بقَصْد إعاقة عَمَل جِهات التَّحقيق أو التَّحري، فتكون العقوبة بالحسب لمدّةٍ لا تَقَل عن ستة أشهر، والغرامة بمَبْلَغ لا يَقل عن مَأتي ألف درهم أو بإحدى هاتين العقوبتين .
9. جَرِيمة التَّرويج للجَماعات الإرهابية، فكل من أنشأ، أو أدار مَوقِع إلكتروني، أو نَشَر مَعْلومات، أو أشرف عَلِيهِ، و رَوَّج لها على شَبكة الإنترنت لجماعةٍ إرهابية بقَصْد تَسهيل الإِتصال بقادَتها، أو أعضائها، أو لإسقاطِ أعضاء جُدد، فعقوبة ذلك هي السِّجن لمدّةٍ تتراوح بين (10 - 25) سنة، والغرامة بين مليوني درهم إلى أربعة ملايين درهم.
10. جَرِيمة إثارة الفتن والإضرار بالوحدة الوطنية، كُـل من أنشأ مَوقِع إلكتروني يتضمَّن إثارة الفتن، والكراهية، أو الطائفية، أو العنصرية، أو التَّرويج لها بأي وسيلةٍ مِن وَسائِل

تقنيات المعلومات من أجل إلحاق الضرر بالسلم المجتمعي، أو الإخلال بالنظام، أو الآداب العامة، فعقوبة ذلك هي السجن المؤقت والغرامة مابين مئتي ألف درهم إلى مليون درهم .

11. جريمة السخرية والإضرار بسمعة الدولة، عن طريق نشر معلومات، أو بيانات، أو أخبار، أو صور على مواقع إلكترونية بقصد الإستهزاء والضرر بسمعة وهيبة الدولة، أو مؤسساتها، أو قادتها، أو أي من الرموز الوطنية، فعقوبتها هي الحبس لمدة لا تزيد عن خمس سنوات، وبغرامة لا تزيد على خمسمائة ألف درهم .

12. جريمة الكسب غير المشروع، كل من ارتكب عمداً باستخدام الشبكة المعلوماتية تحويل الأموال غير المشروعة، أو إخفاء وتمويه حقيقة الأموال، أو حركتها، أو ملكيتها، يُعاقب بالحبس مدة لا تزيد عن عشر سنوات، وبغرامة تتراوح بين مئة ألف درهم إلى خمسة ملايين درهم .

13. جريمة المتاجرة بالمخدرات والمؤثرات العقلية، فمن أنشأ، أو أدار موقع إلكتروني للمتاجرة، أو الترويج للمخدرات وتسهيل التعامل بها، فيُعاقب بالسجن المؤقت والغرامة التي تتراوح بين خمسمائة ألف درهم إلى مليون درهم، أو بإحدى العقوبتين .

14. جريمة التحريض على الفجور والدعارة، فكل من أغوى، أو حرّض شخص آخر على ارتكاب الفجور، أو الدعارة، أو ساعد في ذلك عبر شبكة المعلومات، أو إحدى الوسائل التقنية، فيُعاقب بالسجن المؤقت لمدة لا تقل عن خمس سنوات، والغرامة مابين مئتان وخمسون ألف درهم إلى مليون درهم .

15. جريمة نشر المواد الإباحية والمساس بالآداب العامة، كل من أنشأ، أو أشرف على موقع إلكتروني، أو نشر فيه عبر شبكة المعلوماتية مواد إباحية من شأنه المساس بالآداب العامة، يُعاقب بالحبس لمدة لا تقل عن سنة واحدة، والغرامة ما بين مئتان وخمسون ألف درهم، إلى خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، وإذا كان المحتوى مخصص للأطفال، فالعقوبة تكون على أشدها على مستوى الحبس والغرامة معاً .

16. جريمة الابتزاز والتهديد الإلكتروني، فمن هدد أو ابتز شخصاً آخر لدفعه على القيام بفعل، أو الإمتناع عنه باستخدام شبكة المعلومات أو الوسائل التقنية، فتكون العقوبة هي

الحبس لمدة لا تزيد عن سنتين، وبغرامة تتراوح بين مئتان وخمسون ألف درهم إلى خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، وتكون عقوبة السجن لمدة لا تزيد عن عشر سنوات إذا كان التهديد بإرتكاب جريمة، أو بإسناد أمور خادشة للشرف .

17. جريمة السب والقذف، فكل من سب أشخاص آخرين، أو أسند إليه أمر من شأنه أن يجعله محلاً للعقاب، أو الإزدراء من قبل الآخرين، يُعاقب بالحبس والغرامة ما بين مئتان وخمسون ألف درهم إلى خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، وإذا وقعت الجريمة بحق موظف الخدمة العامة بسبب أدائه لعمله عد ذلك ظرفاً مُشدد للجريمة .

تُعد التجربة الإماراتية حتى الآن من أفضل تجارب الدول العربية والأكثر تقدماً في مجال تصديها للجريمة المعلوماتية، لما يتمتع به التشريع الإماراتي من أفقٍ واسعٍ في نطاق التجريم، مما يُغطي أكبر نسبة مُمكنة من الإعتداءات التي تقع ضمن المجال الرقمي .

الخاتمة:

يَعيشُ العالمُ في هذا العصر الثورة الصناعية الرابعة، أو كما يُطلقُ عليها الثورة التكنولوجية التي تَعتمدُ على أنظمة الإنتاج الإلكتروني السريع التي هدفها ربط دولي بين الإنتاج المادي والإفتراضي مما يُتيحُ المزيد من المعلومات والمعرفة، فالعَرْضُ من الثورة الرقمية تحقيق رفاهية المجتمع الإنساني من خلال الإستخدام في الأغراض السلمية وهذا يتوقف على رغبة النظام السياسي في أي دولة، وكذلك أستخدمت تلك التكنولوجيا بشكلٍ سلبي من قبل بعض الدول والجماعات بشكلٍ أُلحق الضرر بالمُجتمعات البشرية، وترك أثراً كبيراً بسبب إستغلال التكنولوجيا في أعمال التطرف والإرهاب .

المصادر : القرآن الكريم

القوانين :

1. القانون الاماراتي الإتحادي رقم (3) لسنة 2012 .
2. قانون الجرائم الإلكترونية الإماراتي رقم (2) لسنة 2006، و قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34) لسنة 2021 .

الهوامش :

1. اسراء شريف كعود، التأثيرات السيبرانية في الأمن القومي للدول الفاعلة الولايات المتحدة انموذجاً، مجلة العلوم السياسية، جامعة بغداد، العدد 64، 2022، ص5.
2. زكي حسين الوردي و جميل لازم المالكي، المعلومات والمجتمع، دار الوراق للنشر، ط1، الرياض، 2002، ص27.
3. القانون الإتحادي رقم (3) لسنة 2012، المادة الأولى التي تنص على إنشاء الهيئة الوطنية للأمن الإلكتروني
4. سهام حسن علي الشمري، مظهرات الامن السيبراني والممارسة الاعلامية وعلاقتها بصناعة الحرب النفسية الافتراضية، مجلة دراسات دولية، جامعة بغداد، العدد 83، 2020، ص148.
5. بيتر سينجر، دور التكنولوجيا في الحرب، مركز الإمارات للدراسات والبحوث الإستراتيجية، ابو ظبي، 2010، ص314.
6. Hayder Abed kadhim, University of Bagdad, The Saudi Foreign Policy towards Iraq after 2014, social science journal, Res Militaris, vol.12, n°3, November issue 2022, p.1602.
7. اسعد طارش عبد الرضا، الامن السيبراني ودوره في انتشار ظاهرة الارهاب في العراق بعد عام 2003، مجلة دراسات دولية، جامعة بغداد، العدد 80، 2020، ص158.
8. أشرف سعيد أحمد، تكنولوجيا المعلومات وحروب الجيل السادس، ط1، حقوق النشر محفوظة لدى المؤلف، 2019، ص85.
9. Muntasser Majeed Hameed, University of Bagdad, Political structure and the administration of political system in Iraq (post-ISIS), Cues tío nes Po lí ti cas Vol. 37, N° 65 (julio-diciembre) 2020, 345-361 IEPDP-Facultad de Ciencias Jurídicas y Políticas – LUZ, p.357.

10. حمدان رمضان محمد، الارهاب السياسي دراسة تحليلية اجتماعية، مجلة الآداب، جامعة بغداد، المجلد 1، العدد 137، 2021، ص 533.
11. حسام الفايز، الإرهاب الإلكتروني والثورة الرقمية، مؤسسة طيبة للنشر والتوزيع، ط1، القاهرة، 2019، ص 70 .
- 12. Ruwantissa Abeyratne, “ cyber terrorism and aviation-national and international responses journal of transportation security, vol.4, issue.4, December 2011 p.337.**
13. حسنين المحمدي بوادي، ارهاب الإنترنت الخطر القادم، دار الفكر الجامعي، ط1، القاهرة، 2006، ص 17.
14. كوركيس يوسف داود، الجريمة المنظمة، دار الثقافة والنشر والتوزيع، عمان، 2007، ص 63- 64.
15. رأفت أحمد، للإسلام وظاهرة الإرهاب، دار المعارف، ط1، القاهرة، 2016، ص 157 .
16. عبد القادر زهير النقوري، المفهوم القانوني لمفهوم الإرهاب الداخلي والدولي، منشورات حلبي القانونية، ط1، بيروت، 2008، ص 52.
- 17. Saad Obaid Alwan, University of Baghdad, Economic and security competition between the United States and Russia in Africa, Journal of Positive School Psychology, 2022, Vol. 6, No. 7,p.466.**
18. جمال يوسف بدير، اتجاهات حديثة في إدارة المعرفة والمعلومات، دار كنوز المعرفة للنشر والتوزيع، الاردن، 2010، ص 166.
19. هشام عمر احمد، جرائم الحاسوب والإنترنت، دار الحكمة للطباعة والنشر والتوزيع، القاهرة، ط1، 2013، ص 44.
20. حسام فايز، الإرهاب الإلكتروني والثورة الرقمية، مصدر سبق ذكره، ص 101 - ص 102.

21. هشام بشير، الارهاب الالكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي، المركز العربي للبحوث والدراسات، مجلة افاق سياسية، العدد6، القاهرة، 2014، ص80.
22. المصدر نفسه، ص151 .
23. عبد القادر الشخلي، طبيعة الإرهاب الإلكتروني، المؤتمر الاسلامي العالمي لمكافحة الارهاب، المملكة العربية السعودية، رابطة العالم الاسلامي، 22 - 25 شباط 2015، ص16.
24. حسنين بوادي المحمدي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر الجامعي، الإسكندرية، 2004، ص8 .
- 25. Hayer abed Kathem, University of Baghdad, The Impact Of The Security And Military Institution On Achieving Iraqi National Security After 2014, Journal of Positive School Psychology, Vol. 6, No. 5, , 2022, p.3398.**
26. عبد القادر الشخلي، طبيعة الإرهاب الإلكتروني، مصدر سبق ذكره، ص21 .
27. عبد الحفيظ عبد الرحيم محبوب، واقع جيوسياسي جديد في الشرق الاوسط يغذيه الصراع والارهاب، دار ناشري، الرياض، 2015، ص175.
28. عملية التوثيق في مواقع التواصل الاجتماعي مثل الفيس بوك، تويتر، انستغرام، هي وضع علامة صح زرقاء بجانب إسم المستخدم للدلالة على ان الحساب غير مزيف ليكسب ثقة الآخرين (الباحث) .
29. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دراسة في الظاهرة الإجرامية المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2008، ص81.
30. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2008، ط1، ص156.

31. عبد الله فهد الشريف، جريمة التشهير بالآخرين عبر الإنترنت وعقوبتها شرعاً، ورقة مقدمة في الجلسة الخامسة من الندوة الرابعة المقامة في كلية الملك فهد الامنية بعنوان : الجريمة المعاصرة رؤية فقهية بتاريخ 2005/9/27 .
32. القرآن الكريم، سورة النور، الآية 19.
33. محمد محمود مكاوي، الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، ط1، مصر، 2010، ص235.
34. فاروق محمد الأباصيري، عقد الإشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة، ط1، الإسكندرية، 2002، ص51.
35. محمود احمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص70.
36. عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2004، ص215.
37. مضر بدران وآخرون، مقاومة جرائم الدعارة على الإنترنت، دار زهران للنشر، ط1، عمان، 2003، ص21.
38. الأخوان منير و ممدوح محمد الجهني، جرائم الإنترنت والحاسب الآلي و وسائل مكافحتها، دار الفكر العربي، الإسكندرية، 2004، ص110.
39. عبد الفتاح حجازي، الجريمة في عصر العولمة، دراسة الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، ط1، دار الفكر الجامعي، الإسكندرية، 2008، ص213.
40. يوسف أحمد الرمج، الإرهاب الإلكتروني وشبكات التواصل، صحيفة الجزيرة، الرياض، العدد الصادر بتاريخ، 2013/8/16.
- 41. Waters E1, cummings EM, “A secure base from which to explore close relationships”, child development, vol.71, no.1,USA, Feb 2000, p.164.**

42. أحمد عبد الفتاح الزكي، إستراتيجية تربوية لمواجهة التحديات الداخلية للأمن القومي : دراسة مستقبلية، اطروحة دكتوراه غير منشورة، جامعة المنصورة، كلية التربية، 2003، ص86.

* ماسلو **Maslow** : عالم نفس أمريكي من اصل روسي، أشتهر بنظريته تدرج الحاجات أو سُلم الحاجات، حاصل على شهادة البكلوريوس والماجستير في علم النفس وشهادة الدكتوراه في الفلسفة العامة .

43. Bruce Schneier, “ The psychology of security”, In serge vaudenay (ed.), progress in cryptology Africacrypt, berlin: springer – verlag berlin heidelberg, 2008, p.50.

<https://www.schneier.com/wp-content/uploads/2015/08/paper-psychology-of-security.pdf>
15-3-2023.

44. Londervill. Susan & Main. Mary, “ security of attachment, compliance, and maternal training methods in the second year of life”, developmental psychology, vol.7, 1981, p.290.

45. اياد محمد نادي، الشعور بالأمن النفسي وتأثره ببعض المتغيرات لدى طلبة جامعة النجاح الوطنية، رسالة ماجستير غير منشورة، جامعة النجاح، كلية الدراسات العليا، فلسطين، 2005، ص17.

46. Maurice J. Elias & Steven E. Tobias, ” Raising emotionally intelligent teenagers : parenting with love, laughter, and limits”, new York: harmony, 2000, p.47.

47. حامد زهران، علم النفس الإجتماعي، عالم الكتب للنشر والطباعة، ط6، القاهرة، 2003، ص86 .

48. قانون الجرائم الألكترونية الإماراتي رقم (2) لسنة 2006، و قانون مكافحة الشائعات والجرائم الألكترونية رقم (34) لسنة 2021 .

المصادر الأجنبية

1. Hayder Abed kadhim, University of Bagdad, The Saudi Foreign Policy towards Iraq after 2014, social science journal, Res Militaris, vol.12, n°3, November issue 2022, p.1602.
2. Muntasser Majeed Hameed, University of Bagdad, Political structure and the administration of political system in Iraq (post-ISIS), Cues tio nes Po lí ti cas Vol. 37, N° 65 (julio-diciembre) 2020, 345-361 IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ, p.357.
3. Ruwantissa Abeyratne, “ cyber terrorism and aviation-national and international responses”, journal of transportation security, vol.4, issue.4, December 2011.
4. Saad Obaid Alwan, University of Baghdad, Economic and security competition between the United States and Russia in Africa, Journal of Positive School Psychology, 2022, Vol. 6, No.
5. Hayer abed Kathem, University of Baghdad, The Impact Of The Security And Military Institution On Achieving Iraqi National Security After 2014, Journal of Positive School Psychology, Vol. 6, No. 5, , 2022.
6. Waters E1, cummings EM, “A secure base from which to explore close relationships”, child development, vol.71, no.1, USA, Feb 2000, p.164.
7. Bruce Schneier, “ The psychology of security”, In serge vaudenay (ed.), progress in cryptology Africacrypt, berlin:

springer – verlag berlin heidelberg, 2008, p.50.

[https://www.schneier.com/wp-](https://www.schneier.com/wp-content/uploads/2015/08/paper-psychology-of-security.pdf)

[content/uploads/2015/08/paper-psychology-of-](https://www.schneier.com/wp-content/uploads/2015/08/paper-psychology-of-security.pdf)

[security.pdf](https://www.schneier.com/wp-content/uploads/2015/08/paper-psychology-of-security.pdf) 15-3-2023.

8. Londervill. Susan & Main. Mary, “ security of attachment, compliance, and maternal training methods in the second year of life”, developmental psychology, vol.7, 1981.
9. Maurice J. Elias & Steven E. Tobias,” Raising emotionally intelligent teenagers : parenting with love, laughter, and limits”, new York: harmony, 2000.