أمن المعلومات ودوره في محاربة التطرف الإلكتروني: تجربة الاتحاد الاوروبي انموذجاً

Information security and its role in combating electronic extremism: the European Union experience as a model

م.د. آلاء أمير يوسف
الجامعة المستنصرية/ كلية الآداب
alaa.a85@uomustansiriyah.edu.iq
م.م. سراب أمير يوسف
الجامعة المستنصرية/ كلية الصيدلة
sarabmomeka@uomustansiriyah.edu.iq
م.م. دلال أمير يوسف
الجامعة المستنصرية/ كلية التربية
dalalameer@uomustansiriyah.edu.iq

المستخلص:

يهدف البحث الى التعرف على مفهوم أمن المعلومات، والتعرف على مفهوم التطرف الإلكتروني، واشكال التطرف الإلكتروني، ومعرفة تجربة الاتحاد الاوروبي في مواجهة التطرف على الانترنت واتبع البحث المنهج الوصفي والمنهج التاريخي، وخرج البحث بمجموعة من النتائج وهي ان استخدام الانترنت بشكل واسع من قبل المؤسسات والدول من خلال اتاحة نظم معلوماتها وقواعد بياناتها يجعلها عرضه للاختراق الإلكتروني من قبل الجماعات الارهابية او المؤسسات والدول المتنافسة مما يوجب على الدول والمؤسسات بذل جهود حثيثة ومستمرة لتوفير حماية أمنية قوية لنظمها ومعلوماتها على الانترنت، اما اهم التوصيات التي خرج بها البحث هي الافادة من تجربة الاتحاد الاوروبي في مساعيه في محاربة التطرف الإلكتروني سواء على مستوى اقامة الوحدات والمنصات الإلكترونية لمراقبة المحتوى المتطرف وحذفه، او سن قوانين لحماية الافراد على الانترنت مما له علاقة بمعلوماتهم الشخصية وخصوصيتهم.

الكلمات المفتاحية: أمن المعلومات، تكنولوجيا المعلومات، التطرف الإلكتروني، الارهاب الإلكتروني، الاتحاد الاوروبي.

Abstract:

The research aims to identify the concept of information security, learn about the concept of electronic extremism, the forms of electronic extremism, and know the experience of the European Union in confronting extremism on the Internet. The research followed the descriptive approach and the historical approach, and the research came out with a set of results, namely that the use of the Internet widely by institutions and countries By making their information systems and databases available, they make them vulnerable to electronic penetration by terrorist groups or competing institutions and states, which requires

states and institutions to make diligent and continuous efforts to provide strong security protection for their systems and information on the Internet, The most important recommendations that came out of the research are to benefit from the experience of the European Union in its efforts to combat electronic extremism, whether at the level of establishing electronic units and platforms to monitor and delete extremist content, or enacting laws to protect individuals on the Internet with regard to their personal information and privacy.

Keywords: information security, information technology, electronic extremism, electronic terrorism, the European Union.

مشكلة البحث: برزت مشكلة البحث في التساؤلات الاتية:

1. ما هو المقصود بمفهوم أمن المعلومات؟
2. ما هو المقصود بالتطرف الإلكتروني؟
3. ماهي اشكال التطرف الإلكتروني على شبكة الانترنت؟
4. كيف واجه الاتحاد الاوروبي مشكلة التطرف الإلكتروني على شبكة الانترنت؟

وهدف البحث الى التعرف على مفهوم أمن المعلومات، والتعرف على مفهوم التطرف الإلكتروني، واشكال التطرف الإلكتروني، ومعرفة تجربة الاتحاد الاوروبي في مواجهة التطرف على شبكة الانترنت.

اما فرضيات البحث الرئيسية هي:

1. كلما زادت خطورة التطرف الإلكتروني الذي يهدد أمن الدول كلما زادت الدول في اتخاذ اجراءات لمكافحتها ويبرز ذلك في تجربة الاتحاد الاوروبي.
2. هناك استجابة كبيرة للاتحاد الاوروبي لمواجهة التطرف الإلكتروني لحماية الأمن القومي للاتحاد وذلك من خلال اقامة المراكز الأمنية والتعاون الدولي وسن القوانين.

اما منهج البحث اعتمد البحث المنهج الوصفي لدراسة ابعاد البحث فيما يخص أمن المعلومات والمنهج التاريخي للتعرف على تجربة الاتحاد الاوروبي في مكافحة التطرف الإلكتروني، حيث تناول البحث ثلاث محاور اساسية وهي:

1. المحور الاول تناول أمن المعلومات وذلك من خلال ابعاد عدة وهي المفهوم والمكونات والاهمية ومخاطر أمن المعلومات والتصدي لها.
2. المحور الثاني تناول التطرف الإلكتروني وذلك من خلال ابعاد عدة وهي المفهوم واشكال التطرف الإلكتروني ويشمل الارهاب الإلكتروني والجريمة الإلكترونية.
3. المحور الثاث تناول تجربة الاتحاد الاوروبي لمواجهة التطرف الإلكتروني.

اما الدراسات السابقة فقد وجدت دراسة شعيب قاسمي وفؤاد بلغيث بعنوان[1] (الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية: دراسة حالة الجزائر) تناولت هذه الدراسة الاستراتيجية الدولية لمكافحة الجريمة السيبرانية انطلاقاً من دراسة حالة الجزائر حيث هدفت الى معرفة الجريمة السيبرانية التي ظهرت جراء التطور الهائل في عالم التكنولوجيا والمعلومات فهذه الجرائم اصبحت تشكل خطراً كبيراً على الأمن القومي، وتناولت الاستراتيجيات التي اتبعتها الدول لمواجهة هذه التهديدات الجديدة، خاصة الدول الكبرى مثل الولايات المتحدة الامريكية وروسيا، بالاضافة الى الدول العربية، ومن بينها الجزائر التي وضعت العديد من الاستراتيجيات تمثلت في اليات قانونية وتقنية، وانشاء العديد من المراكز الأمنية لمكافحة هذه الجرائم، بالاضافة الى التنسيق الاقليمي في اطار ثنائي او جماعي للتصدي لهذه الجرائم السيبرانية.

ودراسة فاطمة بنت محمد بن سابق القحطاني[2] (استراتيجيات الأمن السيبراني وتطبيقها بالتخطيط الاستراتيجي لمواجهة الإرهاب الإلكتروني في جامعة الأميرة نورة بنت عبدالرحمن: تصور مقترح) هدف البحث إلى تقديم تصور مقترح لتطبيق استراتيجيات نظام الأمن السيبراني بالتخطيط الاستراتيجي لمواجهة الإرهاب الإلكتروني في جامعة الأميرة نورة بنت عبد الرحمن في إدارة الأمن السيبراني، ومعرفة أسباب الإرهاب الإلكتروني، وأبرز استراتيجيات الأمن السيبراني في الجامعات، وتحديد متطلّبات تطبيق نظام الأمن السيبراني في الجامعات السعودية في ضوء رؤية المملكة 2030 والاستراتيجية الوطنية للأمن السيبراني. واستخدم البحث المنهج الوصفي بأسلوبه الوثائقي. وتوصَّلتْ النتائج إلى أهمية تطبيق استراتيجيات نظام الأمن السيبراني في الجامعات وذلك من خلال توجيه القيادات الجامعية إلى التخطيط الاستراتيجي في ضوء توجُّهات برامج رؤية المملكة 2030 والاستراتيجية الوطنية للأمن السيبراني، لتوفير بيئة إلكترونية أمنة، ولتطبيق أساليب حماية أنظمة تقنية المعلومات الحديثة، ولدعم الإجراءات الاحترازية، ولتصميم بروتوكولات التحقق وأنظمة تشفير البيانات، ولنشر التوعية بمخاطر الإرهاب الإلكتروني والتهديدات السيبرانية في الجامعات وأوصى البحث بأهمية تنسيق وتكامل الجامعات مع الهيئة الوطنية للأمن السيبراني لإعداد برامج تعليمية وتدريبية تنمّي المهارات وتنشر الوعي لدى أفراد المجتمع السعودي للوصول إلى فضاء سيبراني سعودي أمن.

---

(1) شعيب قاسمي، وفؤاد بلغيث. الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية: دراسة حالة الجزائر (رسالة ماجستير)، تبسة، جامعة العربي التبسي– تبسة، كلية الحقوق والعلوم السياسية، 2020.

(2) فاطمة بنت محمد بن سابق القحطاني (استراتيجيات الأمن السيبراني وتطبيقها بالتخطيط الاستراتيجي لمواجهة الإرهاب الإلكتروني في جامعة الأميرة نورة بنت عبدالرحمن: تصور مقترح) بحث مقدم في المؤتمر الدولي لمكافحة الإرهاب الإلكتروني – بالجامعة الإسلامية في المدينة المنورة المملكة العربية السعودية –خلال الفترة (14-15) -5-2022.

المحور الاول: أمن المعلومات

تزأمناً مع الثورة التكنولوجية والرقمية التي اقتحمت مختلف انماط الحياة الانسانية ظهر نوع جديد من التهديدات المتمثلة بالتطرف الإلكتروني، والتي وجب على الدول التعامل معها ومحاولة مجابهتها، والذي زاد من تعقيد هذه النوع من التهديدات هو ذلك الترابط الذي فرضه التعامل الكثيف في الفضاء الشبكي وحجم الخدمات المتوفرة فيه، اضافة الى الوضع الذي خلقه التطور التكنولوجي على مستوى البناءات الداخلية في الدولة بين السياسة والاقتصاد وقطاع التجارة والمال والثقافة وبالتالي فان اي هجوم على اي قطاع من القطاعات من شأنه احداث الضرر على أمن الدول، وبالتالي اصبحت الدول مجبرة على الاهتمام بالفضاء الإلكتروني كونه اضحى ساحة جديدة للتفاعلات الدولية.

اولاً: مفهوم أمن المعلومات:

يُعرف امن المعلومات بأنه "حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المؤسسة نفسها والافراد العاملين فيها واجهزة الحواسيب التي تستخدمها ووسائط حفظ المعلومات التي تضم بيانات المؤسسة وعبر مراحل تكوين المعلومات المتعددة (المعالجة – النقل – التخزين)". ويُعرف ايضاً بانه "حماية المعلومات من انتهاك سريتها أو تدميرها أو استنساخها او تلفها من أشخاص غير مخول لهم سواء كان بشكل متعمد او غير متعمد"[1]. وتم تناول تعريفه من عدة نواحي وهي:

اكاديمياً	وهو يبحث في نظريات واستراتيجيات من اجل تأمين الحماية للمعلومات ضد المخاطر التي تواجهها ومن انشطة الاعتداء عليها.
تقنياً	وهي الادوات والوسائل والاجراءات اللازم توافرها لضمان حماية المعلومات ضد الاخطار المتعددة سواء كانت داخلية او خارجية.
قانونياً	وتهتم بالتدابير والدراسات اللازمة من اجل ضمان سلامة وسرية محتويات المعلومات وتوافرها والتصدي لانشطة الاعتداء أو استغلالها في تنفيذ جرائم المعلومات[2].

ثانياً: مكونات امن المعلومات:

1. سرية المعلومات (Confidentiality of Information): ويشمل جميع التدابير اللازمة لمنع إطلاع الاشخاص غير المصرح لهم على المعلومات الحساسة او السرية، ومن

(1) معجم الحاسبات، الطبعة الموسعة، القاهرة : مجمع اللغة العربية، 1995.

(2) شعيب قاسمي، وفؤاد بلغيث. الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية: دراسة حالة الجزائر، (رسالة ماجستير)، الجزائر، جامعة العربي التبسي – تبسة، 2020، ص 24-25.

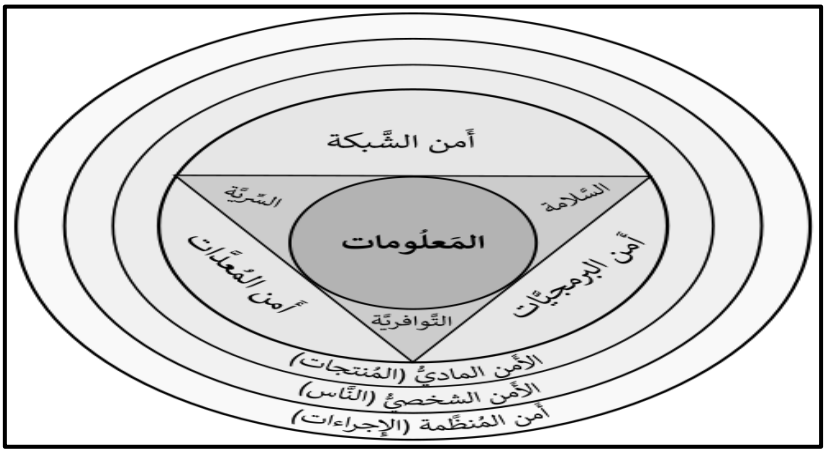
امثلة المعلومات التي يحرص على سريتها هي المعلومات الشخصية والمعلومات العسكرية والمعلومات المالية[1].

2. تكاملية المعلومات (Integrity of Information): ويقصد بها ضمان سلامة المعلومات من تغييرها او تدميرها من قبل جهات غير مخولة[2].

3. توفر المعلومات (Availability of Information): وتعني التاكد من استمرار عمل نظام المعلومات واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمستخدم المعلومات وتوافرها عند الحاجة اليها، والتأكد من ان مستخدمي تلك المعلومات لن يتعرضوا الى منع استخدامهم لها بطريقة غير مشروعة[3].

ويوضح الشكل في ادناه المكونات الثلاث لأمن المعلومات، حيث يتكون من مثلث تتكامل اضلاعه وهي السرية، والتكامل (السلامة)، والتوافرية للمعلومات، ايضاً نلاحظ انواع أمن المعلومات وهي (أمن الشبكة، وأمن البرمجيات، وأمن المعدات، والأمن المادي والأمن الشخصي وأمن المنظمة).

شكل (1) يوضح طبقات ومبادئ أمن المعلومات



المصدر: طبقات أمن المعلومات حسب وكالة الاستخبارات المركزية، الإصدار الثاني، 2022، متاح على الرابط https://commons.wikimedia.org/wiki/File:CIAJMK1209-ar.svg

(1)خالد بن سليمان الغثبر، ومحمد بن عبدالله القحطاني. أمن المعلومات بلغة ميسرة .- الرياض: مركز التميز لأمن المعلومات، 2009، ص 23.

(2) رضا ابراهيم صالح، واحمد عبد السلام ابو موسي. دراسة اثر غدارة أمن المعلومات على نجاح برنامج امن نظم المعلومات المحاسبية: دراسة ميدانية على الشركات المصرية، مجلة الدراسات التجارية المعاصرة، مج6،ع10، 2020، ص119.

(3) امل عبد محمد علي. نظام امن المعلومات في منظمات الاعمال مع نموذج مقترح لمواجهة تهديدات النظام، المجلة العراقية للعلوم الادارية، مج6، ع23، 2009، ص258.

ثالثاً: اهمية امن المعلومات:

تبرز اهمية امن المعلومات كالآتي[1]:

1. جميع قطاعات الدول الامنية والاقتصادية والعسكرية تستند على دقة المعلومات.
2. حاجة الدول الى اجراءات امنية قابلة على صد المخاطر التي يحتمل ظهورها اثناء تعاملها مع جهات اخرى.
3. زيادة الحاجة الماسة لوجود بيئة الكترونية امنة لخدمة القطاع العام والخاص.
4. النمو المتزايد في استخدام التطبيقات الالكترونية وما تتطلبه من بيئة امنة.
5. اتاح تطور تقنيات المعلومات وازدهارها فرصا للاجرام الالكتروني.
6. زيادة الحاجة الى حماية البنى التحتية للشبكة المعلوماتية لضمان استمرارية الاعمال التجارية.

رابعاً: مخاطر أمن المعلومات:

1. المخاطر الداخلية: يعتبر الموظفين داخل المؤسسات هم المصدر الأساسي للمخاطر الداخلية التي تواجهها نظم المعلومات وذلك كون الموظفين على معرفة وعلم بنظم المعلومات أكثر من غيرهم، ومعرفتهم لنقاط الضعف والقوة والقصور للنظم، وقدرتهم على الوصول اليها والتعامل معها واستخدامهم صلاحيات الدخول المخولة لهم، اذن يعتبر الموظفين غير الأمناء خطر يهدد امن البيانات والمعلومات وامكانية تغييرها او تحريفها او تدميرها [2].
2. المخاطر الخارجية: ويمثلها اشخاص لا ينتمون للمؤسسة ولا تربطهم علاقة بها مثل القراصنة والمنافسين الذين يسعوون الى اختراق الضوابط الأمنية والرقابية للنظم للحصول على معلومات المؤسسة السرية، أو عوامل الطبيعة مثل الزلازل والبراكين والحرائق وتؤدي الى فقدان كلي او جزئي للنظم داخل المؤسسة[3].
3. مخاطر الفقد او التلف: وهي المخاطر التي من شأنها تغيير محتويات الملفات وحذفها واحداث خلل فيها، والحاق الضرر بحاسوب اخر، او السيطرة عليه، او سرقة بيانات مهمة وهذه

(1) سلمى عبد الرحمن الدوسري، وجبريل حسن محمد العريشي.
https://www.pnu.edu.sa/ar/Faculties/SocialWork/Documents/Information%20Security.pdf تم الدخول بتاريخ 2024/1/30.

(2) احمد عبد السلام ابو موسى. اهمية مخاطر نظم المعلومات المحاسبية الالكترونية: دراسة تطبيقية على المنشآت السعودية، مجلة كلية التجارة للبحوث العلمية، ع2، 2004 ص3.

(3) سلطان ابراهيم، نظم المعلومات الادارية مدخل النظم .– الاسكندرية: الدار الجامعية للطبع والنشر والتوزيع، 2000، ص 393.

المخاطر تعود الى اسباب عدة اهمها الاهمال، وسوء الاستخدام، او الاعطال المفاجئة في النظام او اصابة الملفات بفايروسات الحاسوب[1].

خامساً: طرق التصدي لمخاطر أمن المعلومات:

هناك العديد من الطرق التي يمكن استخدامها للتصدي من مخاطر أمن المعلومات ومن اهم الطرق هي:

1. استخدام برامج مكافحة الفيروسات والتجسس وتحديثها دورياً.
2. التاكد من تشفير المعلومات المهمة والقيام بعملية اتلاف المعلومات المهمة بطريقة صحيحة وأمنة بحيث لا يمكن استعادتها مرة ثانية.
3. انشاء العديد من الحسابات الشخصية بشكل منفصل وبصلاحيات متعددة وتجنب الوصول الى حساب مدير النظام.
4. تحميل البرامج والملفات من مواقع موثوقة ودقيقة.
5. استخدام كلمة مرور قوية لدخول النظام.
6. تبليغ الجهات الأمنية في حال تكرار الرسائل المشبوهة.
7. الاحتفاظ بوسائط تخزين البيانات وتشمل الاقراص وغيرها في خزائن امنية مخصصة لها، وحفظ نسخ احتياطية للبيانات بشكل دوري.
8. وضع الجدران النارية Firewall والشبكات الافتراضية الخاصة virtual networks private.
9. تعطيل خاصية البلوتوث ان وجدت عند عدم استخدامها[2].

المحور الثاني: التطرف الإلكتروني:

اولاً: مفهوم التطرف الإلكتروني:

عُرف التطرف بانه الشدة او الافراط في شيء او في موقف معين وهو الذهاب الى اقصى الاتجاهات، والتطرف بالتالي هو تجاوز الاعتدال، واذا ما اتصل التطرف بالعنف واصبحت الية التعبير عنه استخدام الافعال الاجرامية المفزعة والمهددة لأمنهم اصبح ذلك مظهرا من مظاهر الارهاب، لان التطرف هنا قد ولد الخوف والرعب وهذه هي اقصى حالات اليأس والاحباط،

(1) أمن المعلومات: ماهيتها وعناصرها واستراتيجيتها متاح على الرابط https://www.damascusuniversity.edu.sy تم الدخول بتاريخ 2024/2/28.

(2) انوار هادي طه الدباغ. تاثير امن المعلومات في التعليم الرقمي: دراسة استطلاعية في بعض تشكيلات الجامعة التقنية الشمالية (المعهد التقني/ الموصل ونينوى)، مجلة تكريت للعلوم الادارية والاقتصادية، مج18، ع59، ص117.

ويكمن التطرف ايضاً في الغلو السياسي، او الديني، او الفكري، ويصبح عندها اسلوب خطير ومدمر للافراد ولكيانات الدول[1].

ثانياً: اشكال التطرف الإلكتروني:

تناولنا اشكال التطرف الإلكتروني متمثلا بكل من:

1. الارهاب الإلكتروني ويشمل المفهوم والخصائص والاسباب.
2. الجريمة الإلكترونية ويشمل المفهوم والخصائص.

1. الارهاب الإلكتروني:

إن ما يتميز به الارهاب الإلكتروني عن الارهاب التقليدي هو الطريقة في استخدام موارد المعلومات والوسائل الالكترونية التي اوجدتها عصر تكنولوجيا المعلومات، فالانظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الارهابيين[2]. حيث يعرف الارهاب التقليدي بانه اي عمل يهدف الى ترويع فرد او او جماعة او دولة بغية تحقيق اهداف لا تجيزها القوانين المحلية او الدولية، وتقوم به عصابات غير منظمة لتحقيق مآرب خاصة بها[3].

اما الارهاب الإلكتروني يعتبر نوع جديد من انواع القوة الناعمة الجديدة حيث لم تعد القوة قاصرة على القوة الصلبة سواء العسكرية او الاقتصادية والتي كانت محتكرة من قبل الدول وليس كل الدول وانما الدول الكبرى فقط، حيث ادى ظهور القوة الافتراضية الى انهاء احتكار القوة التقليدية فاصبح كل من لدية معرفة تكنولوجية ولدية القدرة على استخدامها يمتلك القوة والقدرة على التأثير في النظام العالمي. ويعتبر العصر الحالي هو عصر الفضاء الإلكتروني بامتياز فقد اصبح العمود الفقري لمعظم التفاعلات اليومية واتجهت معظم الدول والحكومات الى تبني نماذج الحكومات الذكية وتعدى الامر الى بناء المدن الذكية[4].

الارهاب الإلكتروني نتج من التزاوج بين ظاهرة الارهاب والثورة التكنولوجية والمعلوماتية والاتصالية وشاع استخدامه عبر الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدام الحواسيب الالية والانترنت تحديدا في ادارة معظم الانشطة الحياتية حيث بات الفضاء الإلكتروني

(1) خليفة الشاوش. الإرهاب والعلاقات العربية – الغربية .– عمان: دار جرير للنشر والتوزيع، 2008، ص 256.

(2) مصطفى يوسف كافي، وماهر عودة الشمايلة، ومحمود عزت اللحام. الاعلام والإرهاب الإلكتروني .– عمان: دار الاعصار العلمي للنشر والتوزيع، 2015، ص 147.

(3) رمزي أحمد عبد الحي، التربية وظاهرة الإرهاب، دراسة في الأصول الثقافية للتربية .– القاهرة: مكتبة الأنجلو المصرية، 2008 ، ص 51.

(4) جمال علي الدهشان. المجلة الدولية للبحوث في العلوم التربوية، مج1، ع3، 2018، ص 92.

يشكل بيئة استراتيجية جديدة لنمو وبروز اشكال جديدة من الصراع ولظهور فاعلين جدد على الساحة الدولية.

الارهاب الإلكتروني هو نفسه الارهاب التقليدي الا انه يستخدم تكنولوجيا المعلومات والاتصالات كمصدر للهجمات، وسنحدد أوجه التشابه والاختلاف بين النوعين وفق مايلي[1]:

جدول (1) يوضح الفرق بين الارهاب التقليدي والارهاب الإلكتروني

الارهاب التقليدي والارهاب الإلكتروني	
اوجه التشابه	**اوجه الاختلاف**
يتداخل الارهاب التقليدي والارهاب الإلكتروني باعتبارهما من الاعمال غير المشروعة التي جرمتها التشريعات والاتفاقيات الدولية.	الوسيلة المستخدمة في ارتكاب الجريمتين مختلفة فالوسيلة المستخدمة في ارتكاب جريمة الارهاب التقليدي تختلف عن نظيرتها الواقعة عبر الانترنت ، فأما الاولى فيلجأ الارهابيون إلى استعمال الوسائل التقليدية العادية في تنفيذ عملياتهم الارهابية كاستخدام السلاح أو القنابل على عكس الارهاب الإلكتروني اذ يعتمد على التقنية الرقمية العالية من حاسبات وانترنت.
تتفقان من حيث الغاية التي يسعيان إليها وهي نشر الرعب والخوف وابتزاز الدول ومحاولة السيطرة على نظامها الداخلي وتمويل الانشطة من خلال الاستيلاء على ممتلكات الناس والسعي لتجنيد أعضاء جدد للانخراط إلى صفوف الجماعات الارهابية.	المكان الذي ترتكب منه وفيه الجريمتين: فالارهاب التقليدي يرتكب في مكان مادي ملموس ومرئي اي تسهل فيه معاينة مسرح الجريمة، مثل وضع إرهابي لمتفجرات أو تفجير نفسه أو خطف طائرة، أما الارهاب عبر الانترنت فيرتكب في العالم الافتراضي الانترنت، فهنا يصعب اكتشاف مدبرها ومنفذها.
كلتا الجريمتان ترتكبان لأجل المساس بالنظام العام وتعريض سلامة المجتمع للخطر وعلى اختلاف الدوافع السياسية الاقتصادية والاجتماعية والشخصية.	يختلف الارهاب التقليدي عن الارهاب الإلكتروني بأن الاول يسهل كشف آثاره من قبل أجهزة الأمن على عكس الثاني الذي يصعب التيقن بها لنقص خبرة أجهزة الشرطة في التعامل مع العالم السيبرياني.
	محل الجريمتين: يقع الاعتداء والعنف في الارهاب التقليدي على الاشخاص سواء كانوا طبيعيين أو معنويين كالدول أو الممتلكات الخاصة أو العامة، ولكن الشأن يختلف في الارهاب عبر الانترنت فهو يعتمد على وسائل ناعمة لا تحدث أضرارا مادية كونه مرتبط بالانترنت الذي يقع في البيئة الافتراضية من اختراق للمواقع الإلكترونية و تدميرها عن طريق نشر الفيروسات واستخدام برامج للتجسس على الدول وتخريب البيانات ومحوها وغيره من الانشطة التخريبية.
	يختلف الارهاب الإلكتروني عن الارهاب التقليدي من

(1) توات عبد الحكيم. جريمة الإرهاب الإلكتروني (رسالة ماجستير)، تبسة، جامعة العربي التبسي – تبسة، كلية الحقوق والعلوم السياسية، 2022، ص ص 22-23.

	حيث أن الاول لا يلجأ إلى العنف والقوة للوصول إلى أهدافه على عكس الارهاب التقليدي الذي يستعملها في تحقيق أغراضه وهو الفارق الجوهري بين الجريمتين.

خصائص الارهاب الإلكتروني: وظفت الجماعات الارهابية كل خصائص التكنولوجيا الحديثة للتعدي والتجاوز على مصالح الاخرين وانتهاك حقوقهم، ومن ابرز تلك الخصائص ما يلي[1]:

الخصائص	الوصف
1.العالمية.	عالمية الجرائم الارهابية، فهي لا تقتصر على بلد او فئة او محافظة وانما اصبحت ترتكب في اغلب مناطق العالم.
2. ينفذه اكثر من شخص.	اذ يمكن ان ينفذه العديد من الاشخاص وفي وقت واحد دون ان تؤثر بمكان العمليات الارهابية.
3. يحتاج الى اشخاص اذكياء.	يحتاج الارهاب الالكتروني الى اشخاص في قمة الذكاء وخاصة في مجال التكنولوجيا والاتصالات.
4. سهولة ارتكابها.	اذ ترتكب العمليات الارهابية بسهولة من اي شخص يمتلك مهارة استخدام تكنولوجيا المعلومات.
5. السرعة القصوى في انتشار اخبارها.	اذ تنتشر الاخبار بسرعة كبيرة ويمكن لأي شخص مرتبط بالانترنت في العالم من الاطلاع على الاخبار المنشورة.
6. جرائم خفية.	حيث لا تترك اي اثر يمكن اكتشافه وصعوبة تحديد الارهابي فضلا عن صعوبة الاحتفاظ بالدليل ان وجد.
7. تعدد انواعه واشكاله.	7. تعدد انواع واشكال الارهاب الإلكتروني الذي يستخدم من خلال التقنيات الحديثة.

اسباب الارهاب الإلكتروني ودوافعه:

أولاً: الدوافع الشخصية :

الدوافع الشخصية التي تؤدي الى الارهاب متعددة، وتبرز فيما يلي:

- رغبة الشخص في حب الشهرة والظهور ولا يمتلك المؤهلات الكافية لها فيقوم بالبحث عما يؤهله باطلا وان كان بالتدمير والتخريب والعدوان.
- فقدان الشخص لأهميتة ودوره في اسرته ومجتمعه وفشله في حياته الأسرية الذي يؤدي الى اكتسابه الصفات السيئة ومنها ضعف الشعور بالانتماء والولاء الى الوطن.
- غضب الشخص على مجتمعه نتيجة الظلم وضياع الحقوق[1].

(1) حسن تركي عمير، وسلام جاسم عبدالله. الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية – عدد خاص، 2013، ص 339-340.

ثانياً: الدوافع السياسية: من الدوافع المحفزة للإرهاب الدافع السياسي اذ تعد السياسات التي تتبعها بعض الدول غير عادلة اتجاه المواطنين وممارسة الكبت السياسي والتهميش المستمر لدور المواطنين، وإنتهاك حقوقهم، وعدم تلبية متطلبات التوازن الإجتماعي، هذه الاسباب تعطي دافعاً قوياً لممارسة الإرهاب بهدف التخلص من هذه الاوضاع، وتؤدي غياب العدالة الإجتماعية، وانعدام المساواة في توزيع الثروات الوطنية والتفاوت في توزيع الخدمات والمرافق الأساسية والاستيلاء على الأموال العامة، وانعدام التنمية المستدامة واهمال الرعاية أو التقصير في أمورهم كلها أسباب تعد دافعاً قوياً لممارسة الإرهاب[2].

ثالثاً: الإسباب الدينية:

يعد الدافع الديني من الدوافع المحفزة للأرهاب فعدم فهم الشريعة والجهل بالدين، اضافة الى تلقي الخطابات الدينية من غير المتخصصين يؤدي الى فهم الامور على غير حقيقتها وكذلك الغلو في الدين والتعصب الديني والطائفي والمذهبي يؤدي الى الارهاب[3].

2: الجريمة الإلكترونية:

الجرائم الإلكترونية وايضاً تعرف بالجرائم المعلوماتية وهي جرائم عالمية وذلك لتعلقها بنظم المعالجة الآلية للبيانات والمعلومات، وهي ابتكارات جديدة في مجال التكنولوجيا والتقنيات تسعى كل الدول الى حمايتها مما دفعها في السنوات الاخيرة على بذل الجهود للتعاون من اجل مكافحة هذا النمط الاجرامي على المستوى الأقليمي والعالمي. فالجريمة الإلكترونية "هي كل فعل او نشاط يتم بطريقة غير مشروعة ويشمل كل نشاط مخالف للقوانين الوضعية والعرفية المتعارف عليها والمعمول بها عبر دول العالم المختلفة واستخدمت فيه وسائط تقنية علمية ليصبح الفعل جريمة الكترونية، فالجريمة الالكترونية هي سلوكيات غير مصرحة ومشروعة واخلاقية لها علاقة بنقل البيانات ومعالجتها الياً"[4]

(1) متاح على الرابط https://repository.najah.edu/ تم الدخول الى الرابط بتاريخ 2024/2/13.

(2) مصطفى سعد حمد مخلف. جريمة الارهاب عبر الوسائل الإلكترونية: دراسة مقارنة بين التشريعين العراقي والاردني (رسالة ماجستير)، عمان، جامعة الشرق الاوسط، 2017، ص 33.

(3) شريف عبد الحميد حسن رمضان. الإرهاب الدولي – اسبابه وطرق مكافحته في القانون الدولي والفقه الاسلامي – دراسة مقارنة، مجلة كلية الشريعة والقانون بطنطا، ع31، 2016، ص 1147.

(4) علي جاسم محمد التميمي. الإرهاب الإلكتروني واثره على المجتمع، المجلة السياسية والدولية، ع 33-34، 2016، ص 491.

خصائص الجريمة الإلكترونية:

تبرز خصائص الجريمة الالكترونية من خلال الجدول الآتي:

الخصائص	الوصف
1. عابرة الحدود.	اذ تعتبر القدرات التي تتمتع بها الحاسبات الالية من حيث انتقال وتبادل كميات هائلة من المعلومات بين نظم تفصلها الاف الاميال والذي اسفر الى نتيجة مفادها ان العديد من الاماكن في دول العالم المختلفة ممكن ان تتأثر بجرائم المعلومات[1].
2. جريمة ناعمة.	الجريمة الإلكترونية جريمة ناعمة لا تتطلب قدرات عنيفة لارتكابها كتبادل اطلاق النار او سفك دماء ولا يوجد شعور لدى المجرم المعلوماتي بعدم اخلاقية ما يقوم به او مساسه بمصالح او قيم يحرص المجتمع على حمايتها ولا يعتبر ما يقوم به يدخل في عداد الجرائم.
3. تحدث اثناء المعالجة الالية للبيانات.	يشترط لقيام جرائم المعلومات التعامل مع بيانات مجهزة ومجمعة داخل نظم المعلومات من اجل معالجتها بشكل الكتروني بحيث تمكن المستخدمين من امكانيات كتابتها عبر العمليات المتسلسلة والتي تتيح امكانية التصحيح او التعديل او المحو او التخزين او الاسترجاع او الطباعة وهي عمليات وثيقة الصلة بتنفيذ جرائم المعلومات وهذا يتطلب اتقان وفهم القائم بها خلال تنفيذها وخاصة في جرائم التقليد والتزوير[2].
4. ترتكب في جميع مراحل تشغيل نظم المعالجة الآلية للبيانات.	في مرحلة الادخال تتم ترجمة المعلومات الى لغة تفهمها الحاسبة، اذ من الممكن ادخال معلومات غير دقيقة، او التعمد في عدم ادخال الوثائق والمعلومات الأساسية المطلوبة، وترتكب اكثر جرائم المعلومات في مرحلة الادخال. اما جرائم مرحلة المعالجة فيكون من خلال عمل تعديلات على برامج الحاسبات الالية عن طريق التلاعب في برامج نظم المعلومات من خلال اضافة تعليمات غير مخول بها او تشغيل برامج جديدة تلغي جزئياً او كلياً عمل البرامجيات الاصلية، وتتطلب هذه الجرائم معرفة فنية عميقة لدى الفاعل بتلك التقنيات في هذه المرحلة ويكون اكتشافها صعباً للغاية، اما مرحلة المخرجات يتم التلاعب في النتائج التي يخرجها نظام المعلومات (الحاسبات الالية) تتعلق ببيانات صحيحة مدخلة ومعالجة بشكل صحيح[3].
5. تستخدم تكنولوجيا معلومات متقدمة.	ترتكب جرائم المعلومات في نطاق تكنولوجيا معلومات متقدمة يتزايد استخدامها بشكل مستمر في ادارة مختلف المعاملات المالية والاقتصادية اذ تهدد هذه الجرائم المراكز الادارية والحسابية وتنقل الاموال والاستثمارات سواء في

(1) كوثر حازم سلطان. موقف القانون والقضاء من الجريمة الإلكترونية (السيبرانية): دراسة مقارنة، مجلة كلية التربية الاساسية، مج22، ع96، 2016، ص 973.

(2) عادل يوسف عبد النبي الشكري. الجريمة المعلوماتية وازمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، مج1، ع7، 2008، ص 115.

(3)الشحات، حاتم عبد الرحمن منصور. الاجرام المعلوماتي .- القاهرة: دار النهضة العربية، 2003، ص 37.

	المؤسسات الخاصة والعامة، وتهدد المعلومات الشخصية المخزونة داخل الحواسيب للمصارف وشركات التامين والمستشفيات ومراكز الشرطة، وتهدد سرية الحياة الخاصة او الحرية السياسية، اضافة الى الخطورة المتعلقة بمعلومات إدارة الدولة والحكومة في ميادين والامن والدفاع والمشروعات النووية وصناعة الاسلحة الحديثة[1].

3. تجربة الاتحاد الاوروبي في محاربة التطرف الإلكتروني:

كان للاتحاد الاوروبي منذ بداية تأسيسه جهود حثيثة لمكافحة الارهاب والجريمة على ارض الواقع اذ تناولت معاهدة الاتحاد الاوروبي او ما تعرف بمعاهدة ماستريخت التي وقعت عام 1991 في ماستريخت ركيزة جديدة وهي (العدل والشؤون الداخلية) والتي تعنى بالتعاون فيما يخص تنقل الاشخاص عبر الحدود ومكافحة الجريمة العابرة للحدود، فنصت المعاهدة على الإرهاب والمخدرات والاحتيال وأشكال الجرائم الخطرة الاخرى، اضافة الى إجراءات مراقبة الحدود الخارجية والهجرة واللجوء والتنقل داخل الحدود الداخلية من قبل المواطنين في الدول غير الأعضاء في الاتحاد وهذا يشمل تعاون كل من السلطات القضائية والشرطية والإدارية والجمركية للدول الاعضاء. وبذلت نشاط كبير للتصدي للجرائم ضد الاطفال، والاتجار بالأشخاص، والفساد، وتزييف وغسل الأموال، والجريمة الالكترونية[2].

واهم الجهود التي قام بها الاتحاد الاوروبي لمواجهة التطرف الإلكتروني من خلال قيامها بعدة اجراءات منها:

اولاً: المركز الاوروبي لمكافحة الإرهاب (European Counter Terrorism Centre (ECTC):

تأسس المركز الأوروبي لمكافحة الإرهاب (ECTC) في اعقاب سلسلة الهجمات الارهابية التي هزت اوروبا في عام 2015، وادت هذه الهجمات الى تعزيز التعاون بين الدول الأعضاء في الاتحاد الاوروبي والشركاء وكان من نتائجه انشاء مركز متخصص لمكافحة الارهاب في يوروبول في يناير/كانون الثاني 2016، وتبرز اهمية هذا المركز كالآتي:

1. يعد مركز للعمليات والخبرة يعكس الحاجة المتزايدة للاتحاد الاوروبي لتعزيز استجابته للارهاب وضمان الاستجابة الفعالة لهذه التحديات.

(1) الشوا، محمد سامي. ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، 2003، ص 67-68.

(2) جون بيندر، وسايمون اشروود، ترجمة خالد غريب علي. الاتحاد الأوروبي: مقدمة قصيرة جدا .- القاهرة: مؤسسة هنداوي للتعليم والثقافة، 2015، ص 100.

2. يمثل المركز الأوروبي لمكافحة الإرهاب حجر الزاوية للتعاون على مستوى الاتحاد الاوروبي في الجهود الوطنية لمكافحة الإرهاب.

3. يعد أول مركز من نوعه يتم إنشاؤه كجزء من السياسة الامنية للاتحاد الاوروبي لمكافحة الارهاب.

وتهدف تجربة وخبرة ECTC في جميع مجالات الظواهر الارهابية الى ما يلي:

1. توفير استجابة شاملة للتهديدات المتغيرة باستمرار للإرهاب في الاتحاد الاوروبي.
2. توسيع دعم الدول الاعضاء والشركاء من غير الاعضاء من اجل التعامل مع الارهاب والتطرف.
3. التعامل مع الإرهاب ذي الدوافع الدينية.
4. تعزيز قدرات سلطات مكافحة الإرهاب.
5. انشاء وتطوير ادوات لتلبية الاحتياجات الناشئة لمكافحة الارهاب.
6. تسهيل الاتصال بين السلطات المختصة في الدول الاعضاء في الاتحاد الاوروبي من خلال منصات يوروبول لمكافحة الارهاب، وهي مساهمة لا تقدر بثمن في مكافحة الارهاب[1].

ثانياً: المنصات الاوروبية لمراقبة المحتوى المتطرف على الانترنت:

اعتمدت لائحة الاتحاد الأوروبي لمراقبة المحتوى المتطرف على الانترنت في (28 أبريل 2021)، ودخلت حيز التنفيذ (7 يونيو 2021) الذي يتناول نشر المحتويات المتطرفة عبر الإنترنت، الهدف الاساسي من التشريع هو الإزالة السريعة للمحتويات المتطرفة على الإنترنت، وانشاء اداة مشتركة واحدة لجميع الدول الاعضاء، ولهذا الغرض ستطبق القواعد على مقدمي خدمات الاستضافة الذين يقدمون خدمات داخل الاتحاد الأوروبي، سواء كانت مؤسستهم الرئيسة في الدول الأعضاء أم لا، تلزم هذه القواعد منصات التواصل وشركات الانترنت بحذف أي محتوى ذو طابع إرهابي خلال مدة ساعة واحدة فقط من نشره وتشمل: مضامين النشر في الإنترنت، التسجيلات الصوتية أو مقاطع الفيديو التي تحرض على ارتكاب جرائم إرهابية أو توفر تسهيلات لارتكاب جرائم إرهابية، ويندرج داخل هذا الإطار الطرق التعليمية لصنع متفجرات وأسلحة نارية، لأغراض إرهابية، وصفت هذه القواعد بالتاريخية، حيث تساهم في منع انتشار

(1) European Counter Terrorism Centre (ECTC), A central hub of expertise working to provide an effective response to terrorism, Access on https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc تم الدخول بتاريخ 2024/2/28.

المحتويات الإرهابية على الانترنت، وتعد خطوة هامة لتأمين رد اوروبي فاعل على الارهاب والتطرف[1]. وابرز الوحدات والمنصات الأوروبية لمراقبة المحتويات على الانترنت هي:

1. منتدى الإنترنت العالمي لمكافحة الإرهاب (Global Internet Forum to Counter Terrorism (GIFCT:

يعد من المنظمات غير الحكومية تم تصميمها لردع المتطرفين من استغلال المنصات الالكترونية، تم تأسس المنتدى عام 2017 من قبل عدة شركات اهمها: (Facebook – Microsoft –Twitter – YouTube) من اجل تطوير البحوث ذات الصلة وتعزيز التعاون الفني بين الشركات الأعضاء، وتبادل المعرفة مع منصات الكترونية اصغر ثم توسعت عضوية (GIFCT) الى ما هو ابعد من الشركات المؤسسة لتضم ما يزيد عن عشرين منصة متنوعة تلتزم بجهود مشتركة من اجل مكافحة الانتشار للمحتويات الإرهابية والمتطرفة العنيفة على الإنترنت[2]. واهم الاهداف التي يسعى المنتدى لتحقيقها هي:

1. تمكين الشركات التكنولوجية بشكل جماعي ومستقل وذلك من خلال والادوات والعمليات لغرض منع المتطرفين من سوء استخدام برامجها والرد عليها.
2. تمكين المشاركة لاصحاب المصالح المتعددين امام إساءة استخدام الانترنت من قبل المتطرفين وتشجيعهم على الوفاء بالالتزامات الرئيسة والمتوافقة مع مهام المنتدى.
3. تفعيل الحوار المدني عبر الانترنت.
4. تعزيز الفهم الواسع للعمليات الإرهابية والمتطرفة العنيفة وتطورها، بما في ذلك التقاطع بين الأنشطة عبر الإنترنت وخارجها.

2. ملف تحليل النشاط الإرهابي (AWF):

إن (AWF) هي الاداة القانونية الوحيدة الموجودة على المستوى الاوروبي تستخدم لتخزين ومعالجة وتحليل المعلومات الواقعية في وقت واحد (البيانات الصلبة) ويشمل ذلك الذكاء أو (البيانات الناعمة) ويشمل ذلك البيانات الشخصية ذات الطبيعة الحساسة، فإن عدد فئات البيانات التي يسمح بتخزينها ومعالجتها هو أوسع ما يكون داخل (AWF) لمكافحة الإرهاب، اذ يتم جمع المعلومات ومطابقتها وتحليلها في بيئات آمنة للغاية من قبل فرق متخصصة تضم محللين وخبراء في مكافحة الإرهاب، أكثر من (100) متخصص في لاهاي يستخدم قاعدة

(1) المركز الاوروبي لدراسات مكافحة الإرهاب والاستخبارات. محاربة التطرف والإرهاب في اوربا – قوانين واجراءات، متاح على الرابط https://www.europarabct.com/ تم الدخول بتاريخ 2024/2/13.

(2) Global Internet Forum to Counter Terrorism (GIFCT), Access on https://gifct.org/about/.

تم الدخول بتاريخ 2024/2/28.

بيانات (AWF) لمساعدة المحققين في جميع أنحاء الاتحاد على فهم ومعالجة الجريمة وجماعات الجريمة المنظمة بشكل أفضل.

ثالثاً: دور الاتحاد الأوروبي في حذف المحتوى المتطرف على الإنترنت:

وقعت الدول الاوروبية اتفاقيات مع محركات الانترنت، لغرض حذف المحتويات المتطرفة ضمن سلسلة جهود بذلتها أوروبا لمواجهة التطرف الديني، وذلك في أعقاب الهجمات الإرهابية التي نفذها متطرفون في عدد من الدول الأوروبية خلال الأعوام الماضية.

1. شراكة أوروبا مع محركات الإنترنت لحذف المحتوى المتطرف:

توصل الاتحاد الأوروبي في (23 أبريل 2022)، مع الدول الأعضاء إلى اتفاق جديد، اذ تم الاتفاق على قانون جديد يمنع المحتويات الإلكترونية الضارة، في أكبر إعادة تنظيم لقانون الاتحاد الأوروبي بهذا الخصوص خلال نحو (20) عاماً، واتفق مفاوضون من البرلمان الأوروبي والدول الـ (28) الأعضاء في الاتحاد الأوروبي، على قوانين جديدة تجبر شركات مثل الفيسبوك، وتويتر، وجوجل، والأمازون، على تنظيم المحتويات الإلكترونية الضارة بشكل أكبر، مثل خطابات الكراهية، والمعلومات المضللة، وإزالة المحتويات غير القانونية، والتعاون مع السلطات، ويتعلق الجانب المظلم للإنترنت أيضاً بمنصات البيع التي تجتاحها منتجات مزيفة أو غير مستوفية للمواصفات، والتي يمكن أن تكون خطيرة، مثل ألعاب الأطفال التي لا تفي بمعايير السلامة. ونصت القواعد الجديدة على[1]:

1.إزالة أي محتوى غير قانوني من قبل المنصات الاجتماعية وحسب القوانين الاوروبية والوطنية بمجرد احاطتها بوجوده على منصاتها.

2. الزام المنصات الاجتماعية على ايقاف حسابات المستخدمين الذين ينتهكون القانون بشكل متكرر.

2. برنامج تعقب تمويل الإرهاب TFTP:

تم انشاء برنامج تعقيب تمويل الإرهاب (TFTP) من قبل وزارة الخزانة الأمريكية بعد وقت قصير من الهجمات الإرهابية في 11 سبتمبر 2001، وأنتج فريق عمل البرنامج معلومات استخباراتية مهمة، ساعدت كل من الولايات المتحدة ودول الاتحاد الأوروبي في الحرب ضد الإرهاب، والكشف عن المؤامرات الإرهابية وتعقب مرتكبيها، ويضمن البرنامج الاتفاق بين الاتحاد الأوروبي والولايات المتحدة بشأن تبادل المعلومات المالية، وحماية خصوصية مواطني الاتحاد الأوروبي، ويمنح سلطات إنفاذ القانون في الولايات المتحدة والاتحاد الأوروبي أداة قوية

(1) محاربة التطرف – دور الاتحاد الأوروبي في حذف المحتوى المتطرف على الإنترنيت متاح على الرابط https://www.europarabct.com تم الدخول بتاريخ 2024/2/14.

في مكافحة الإرهاب، ونصت اتفاقية (TFTP) التي دخلت حيز التنفيذ في 1 أغسطس 2010، على الضمانات المناسبة لاستيعاب المخاوف المشروعة بشأن الأمن والخصوصية واحترام الحقوق الأساسية، تحمي الاتفاقية حقوق حماية البيانات المتعلقة بالشفافية وحقوق الوصول والتصحيح ومحو البيانات غير الدقيقة[1].

رابعاً: القوانين والتشريعات لحماية البيانات:

1. القانون العام لحماية البيانات (GDPR) General Data Protection Regulation

واجهت الانتهاكات الأمنية المتزايدة، والتطورات التكنولوجية السريعة، والعولمة على مدى السنوات العشرين الماضية تحديات جديدة لحماية البيانات الشخصية. في محاولة لمعالجة هذا الوضع، وضع الاتحاد الأوروبي القانون العام لحماية البيانات (GDPR) الذي ينطبق مباشرة على القانون في جميع الدول الأعضاء، طبق قانون حماية البيانات الأوروبية اعتبارًا من 25 مايو 2018 في جميع الدول الأعضاء لمواءمة قوانين خصوصية البيانات في جميع أنحاء أوروبا. يهدف هذا القانون الى تحقيق الاهداف الاتية:

1. وضع القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والقواعد المتعلقة بحرية حركة البيانات الشخصية.
2. حماية الحقوق والحريات الاساسية للأشخاص الطبيعيين، ولا سيما حقهم في حماية بياناتهم الشخصية.
3. منع تقييد أو حظر حرية حركة البيانات الشخصية داخل الاتحاد لاسباب تتعلق بحماية الأشخاص الطبيعيين بما يتعلق بمعالجة بياناتهم الشخصية[2].

سيستفيد المستخدم من هذا القانون من عدة نواح، اهمها أن بياناته الشخصية لم تعد سلعة رخيصة تستخدم في أي شيء على الإنترنت، ويمكنه المطالبة بحذفها من خوادم الشركات التي يتعامل معها وعليها أن تقوم بذلك في فترة قصيرة هذا من جهة، ومن جهة أخرى سيكون على معرفة عن كل البيانات التي تجمع عنه وبهذا يمنع البيانات الخاصة والمهنية التي لا يريد مشاركتها مع الآخرين. وستنطبق مجموعة واحدة من القواعد علي جميع أعضاء الاتحاد الاوروبي وهذا سيخلق قاعدة كبيرة جدا على مستوى العالم للحماية.

القانون يمنح حق الوصول للبيانات والمعلومات الشخصية وحق معرفة كيفية معالجة هذه البيانات، وهو ما بدأت الشركات توفره مثل فيس بوك وجوجل وغيرها، ويضمن القانون الجديد

(1) محاربة التطرف – دور الاتحاد الأوروبي في حذف المحتوى المتطرف على الإنترنيت متاح على الرابط https://www.europarabct.com

(2) https://gdpr-info.eu/

اعلام المستخدمين خلال أقل من 72 ساعة بعد اختراق أي خدمة من الخدمات التي يستخدمونها. اذ أن الاختراقات التي تحصل عادة ما تؤدي إلى تسريب البيانات وسوء استخدامها لأغراض عدة أو بيعها في السوق السوداء، مع القانون الجديد سيتم إشعار المتضررين بالاختراق، وتوفير النصائح والتوصيات من قبل الشركات التي من شأنها مساعدة المستخدمين وحمايتهم من تداعيات الاختراق[1].

رابعاً: النتائج:

اظهرت نتائج البحث ما يأتي:

1. استخدام الانترنت بشكل واسع من قبل المؤسسات والدول من خلال اتاحة نظم معلوماتها وقواعد بياناتها يجعلها عرضه للاختراق الإلكتروني من قبل الجماعات الارهابية او المؤسسات والدول المتنافسة مما يوجب على الدول والمؤسسات بذل جهود حثيثة ومستمرة لتوفير حماية أمنية قوية لنظمها ومعلوماتها على الانترنت.
2. ان مساعي الاتحاد الاوروبي واضحة في مجال توفير الحماية الأمنية من الارهاب وخاصة الارهاب الإلكتروني والجريمة الإلكترونية.
3. للاتحاد الاوروبي دور بارز لمراقبة المحتوى المتطرف، من خلال وحدات ومنصات لمراقبة المحتوى المتطرف من اجل محاربة التطرف الإلكتروني اهمها منتدى الإنترنت العالمي لمكافحة الإرهاب(GIFC) وملف تحليل النشاط الإرهابي(AWF).
4. للاتحاد الاوروبي دور بارز في حذف المحتوى المتطرف على الانترنيت، من خلال شراكة أوروبا مع محركات الإنترنت لحذف المحتوى المتطرف، وبرنامج تعقب تمويل الإرهاب TFTP.
5. للاتحاد الاوروبي دور بارز في سن القوانين والتشريعات اهمها القانون العام لحماية البيانات الشخصية (GDPR).

خامساً: التوصيات:

1. نشر الوعي بشأن أمن المعلومات والتطرف الإلكتروني باشكاله المتعددة والمخاطر التي ينجم عنها من خلال اقامة العديد من المؤتمرات والمحاضرات والورش والندوات.
2. الافادة من تجربة الاتحاد الاوروبي في مساعيه في محاربة التطرف الإلكتروني سواء على مستوى اقامة الوحدات والمنصات الإلكترونية لمراقبة المحتوى المتطرف وحذفه، او سن قوانين لحماية الافراد على الانترنت مما له علاقة بمعلوماتهم الشخصية وخصوصيتهم.

(1) عبد القادر ورسمه غالب. ملامح قانون الاتحاد الاوروبي لحماية البيانات متاح على الرابط https://www.omandaily.com/ تم الدخول بتاريخ 2024/2/14.

3. ضرورة حرص الحكومات وخاصة الحكومة العراقية على اتخاذ تدابير أمنية لحفظ أمن البلد وسكانه من الهجمات الإلكترونية والتطرف الإلكتروني والجرائم الإلكترونية من خلال وضع رؤية واضحة ورسم استراتيجيات أمن المعلومات والأمن السيبراني وتطبيقها على كافة مؤسسات الدولة لحماية انظمتها وقواعدها على الانترنت.

4. ضرورة اجراء دراسات اخرى تتعلق بأمن المعلومات والتي من شانها ان تسلط الضوء على تحديات العالم الرقمي ومخاطره والوقاية منها.

سادساً: المصـــــــــــــــادر :

1. المصادر العربية:

1. احمد عبد السلام ابو موسى. اهمية مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المنشآت السعودية، مجلة كلية التجارة للبحوث العلمية، ع2، 2004.
2. امل عبد محمد علي. نظام أمن المعلومات في منظمات الاعمال مع نموذج مقترح لمواجهة تهديدات النظام، المجلة العراقية للعلوم الادارية، مج6، ع23، 2009، ص ص 256-275.
3. التميمي، علي جاسم محمد. الارهاب الإلكتروني واثره على المجتمع، المجلة السياسية والدولية، ع 33-34، 2016، ص 491. ص ص 475-504.
4. توات عبد الحكيم. جريمة الارهاب الإلكتروني (رسالة ماجستير)، تبسة، جامعة العربي التبسي – تبسة، كلية الحقوق والعلوم السياسية، 2022، ص ص 22-23.
5. جون بيندر، وسايمون أشروود، ترجمة خالد غريب علي. الاتحاد الأوروبي: مقدمة قصرية جدا .– القاهرة: مؤسسة هنداوي للتعليم والثقافة، 2015.
6. حسن تركي عمير، وسلام جاسم عبدالله. الارهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية – عدد خاص، 2013، ص 339-340.
7. الدباغ، انوار هادي طه. تأثير أمن المعلومات في التعليم الرقمي: دراسة استطلاعية في بعض تشكيلات الجامعة التقنية الشمالية (المعهد التقني/ الموصل ونينوى)، مجلة تكريت للعلوم الادارية والاقتصادية، مج18، ع59، ص ص 112-126.
8. الدهشان، جمال علي. المجلة الدولية للبحوث في العلوم التربوية، مج1، ع3، 2018، ص ص 84-121
9. رضا ابراهيم صالح، واحمد عبد السلام ابو موسي. دراسة اثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية، مجلة الدراسات التجارية المعاصرة، مج6،ع10، 2020، ص ص 105- 142.
10. رمزي أحمد عبد الحي، التربية وظاهرة الإرهاب، دراسة في الأصول الثقافية للتربية .– القاهرة: مكتبة الأنجلو المصرية، 2008.
11. سلطان ابراهيم، نظم المعلومات الادارية مدخل النظم .– الاسكندرية: الدار الجامعية للطبع والنشر والتوزيع، 2000.

12. الشاوش، خليفة. الارهاب والعلاقات العربية – الغربية .– عمان: دار جرير للنشر والتوزيع، 2008.
13. الشحات، حاتم عبد الرحمن منصور. الاجرام المعلوماتي .– القاهرة: دار النهضة العربية، 2003.
14. شريف عبد الحميد حسن رمضان. الارهاب الدولي – اسبابه وطرق مكافحته في القانون الدولي والفقه الاسلامي – دراسة مقارنة، مجلة كلية الشريعة والقانون بطنطا، ع31، 2016، ص 1147.
15. شعيب قاسمي، وفؤاد بلغيث. الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية: دراسة حالة الجزائر (رسالة ماجستير)، تبسة، جامعة العربي التبسي– تبسة، كلية الحقوق والعلوم السياسية، 2020.
16. الشكري، عادل يوسف عبد النبي. الجريمة المعلوماتية وازمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، مج1، ع7، 2008، ص ص 111–132.
17. الغثبر، خالد بن سليمان، ومحمد بن عبدالله القحطاني. أمن المعلومات بلغة ميسرة .– الرياض: مركز التميز لأمن المعلومات، 2009.
18. القحطاني، فاطمة بنت محمد بن سابق. استراتيجيات الأمن السيبراني وتطبيقها بالتخطيط الاستراتيجي لمواجهة الإرهاب الإلكتروني في جامعة الأميرة نورة بنت عبدالرحمن: تصور مقترح، بحث مُقدم في المؤتمر الدولي لمكافحة الإرهاب الإلكتروني – بالجامعة الإسلامية في المدينة المنورة المملكة العربية السعودية –خلال الفترة (14–15) –5–2022.
19. كوثر حازم سلطان. موقف القانون والقضاء من الجريمة الإلكترونية (السيبرانية): دراسة مقارنة، مجلة كلية التربية الاساسية، مج22، ع96، 2016، ص ص 969–998.
20. محمد سامي الشوا. ثورة المعلومات وانعكاساتها على قانون العقوبات .– القاهرة: مطابع الهيئة المصرية العامة للكتاب، 2003.
21. مصطفى سعد حمد مخلف. جريمة الارهاب عبر الوسائل الإلكترونية: دراسة مقارنة بين التشريعين العراقي والاردني (رسالة ماجستير)، عمان، جامعة الشرق الاوسط، 2017.
22. مصطفى يوسف كافي، وماهر عودة الشمايلة، ومحمود عزت اللحام. الاعلام والارهاب الإلكتروني .– عمان: دار الاعصار العلمي للنشر والتوزيع، 2015.
23. معجم الحاسبات، الطبعة الموسعة .– القاهرة: مجمع اللغة العربية، 1995.

2. المصادر الإلكترونية:

24. الدوسري، سلمى عبد الرحمن، وجبريل حسن محمد العريشي. دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع، ص 10 متاح على الرابط https://www.pnu.edu.sa/ar/Faculties/SocialWork/Documents/Information%20Security.pdf تم الدخول بتاريخ 2024/1/30.

25. عبد القادر ورسمه غالب. ملامح قانون الاتحاد الاوروبي لحماية البيانات متاح على الرابط https://www.omandaily.com/ تم الدخول بتاريخ 2024/2/14.
26. https://repository.najah.edu/ تم الدخول الى الرابط بتاريخ 2024/2/13.
27. طبقات أمن المعلومات حسب وكالة الاستخبارات المركزية، الإصدار الثاني، 2022، متاح على الرابط https://commons.wikimedia.org/wiki/File:CIAJMK1209-ar.svg
28. محاربة التطرف – دور الاتحاد الأوروبي في حذف المحتوى المتطرف على الإنترنيت متاح على الرابط https://www.europarabct.com تم الدخول بتاريخ 2024/2/14.
29. المركز الاوروبي لدراسات مكافحة الارهاب والاستخبارات. محاربة التطرف والارهاب في اوربا – قوانين واجراءات، متاح على الرابط https://www.europarabct.com/ تم الدخول بتاريخ 2024/2/13.
30. أمن المعلومات: ماهيتها وعناصرها واستراتيجيتها، متاح على الرابط https://www.damascusuniversity.edu.sy تم الدخول بتاريخ 2024/2/28.
31. European Counter Terrorism Centre (ECTC), A central hub of expertise working to provide an effective response to terrorism, Access on https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc تم الدخول بتاريخ 2024/2/28.
32. Global Internet Forum to Counter Terrorism (GIFCT), Access on https://gifct.org/about/ . تم الدخول بتاريخ 2024/2/28