التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر

Cyber Treats and the Security of the Digital Society: Algerai Case Study

لمياء زواوي ***ZOUAOUI Lamia***

جامعة باتنة 1، الجزائر، lamia.zouaoui@univ-batna.dz

فهيم رملي ***REMLI Fahim***

جامعة البليدة 2، الجزائر، remlifahim@yahoo.fr

تاريخ الإرسال:2023/01/07 **تاريخ القبول:** 2023/02/24 **تاريخ النشر:** 2023/04/01

ملخص:

تتضمن بيئة المعلومات وتكنولوجيا المعلومات والاتصالات العديد من التهديدات التي تمس بأمن المجتمع الرقمي، فقد أدى النقل السريع والعشوائي للبيانات الخاصة بالأفراد والمجتمعات للعالم الافتراضي إلى جعل أمنهم المجتمعي والهوياتي محلّ تهديد دائم، ويعاني في هذا الإطار المجتمع الجزائري من التبعات السلبية للانكشاف الرقمي والاستخدام العشوائي لمنصات التواصل الاجتماعي التي تمس قيمه الأساسية وتغير في الكثير من الأحيان ثوابته الأصلية، كما تخلق أيضا العديد من المشاكل النفسية والهوياتية داخل المجتمع بفعل غياب عنصري الرقابة والردع. تأتي هذه المقالة للبحث في مضامين التهديدات السيبرانية وأمن المجتمع الرقمي في الجزائر، وذلك عبر التطرق إلى المقصود من التهديدات السيبرانية وأشكالها، ثم إلى مخاطر انتهاك الخصوصية الرقمية وتبعاته على أمن المجتمع الرقمي، وكذا مخاطر استخدام الفضاء السيبراني في الترويج للتطرف، والفبركة الرقمية في البيئة السيرانية.

الكلمات المفتاحية: *التهديدات السيبرانية؛ أمن؛ المجتمع الرقمي؛ الجزائر.*

Abstract:

The information and communication technology environment includes many threats to the security of the digital society, as a result of the rapid and random transfer of data of individuals and communities to the virtual world, making their societal security and identities a permanent threat. In this context, we find that Algerian society suffers from the negative consequences of digital exposure, which could affect its basic values and create problems due to the absence of control and deterrence. This article examines cyber threats and the security of the digital society in the Algerian case. Beginning with what is meant by cyber threats and their forms, then the dangers of violating digital privacy, and the dangers of using cyberspace to promote extremism and abuse of digital fabrication.

Keywords: *Cyber Threats; Security; Digital Society; Algeria.*

* **المؤلف المرسل: فهيم رملي**، remlifahim@yahoo.fr

مقدمة:

أدى تعاقب الثورات الصناعية إلى بروز فضاءات جديدة للتفاعل الانساني تتسم بطابع الافتراضية وبنقل العلاقات الاجتماعية، والسياسية، والاقتصادية إلى مستوى جديد صعبُ التحكّمِ والترويض أمنيا، فقد أصبح للأفراد هوية رقمية وحق في الخصوصية المعلوماتية، يمارسون عبره عمليات تواصلية تجمع بين السرية أحيانا والانفتاح أحيانا أخرى، وتحمل في الآن ذاته مخاطر جمة على أمن الفرد والمجتمع. فبتداخل الثقافات التي كثيرا ما تحمل بذور الصراع - بحسب الطرح الهينتنغتوني حول صدام الحضارات- عبر هذا الفضاء المرن تصبح هوية الفرد الثقافية وشخصيته المجتمعية وقيمه الرئيسية محل تهديد دائم، أين تتم محاولة تمييعها وتذويبها ضمن قوالب هوياتية جديدة هدفها بلوغ الهوية المشتركة الفاقدة للخصوصية المحلية -بحسب الطرح الفوكوياميِ حول الثقافة العالمية-، وتتجاوز التهديدات التي تتضمنها بيئة المعلومات تلك التهديدات الصلبة التي كانت تؤرق أمن الدول والجماعات سابقا، فهي تهديدات هلامية تتخذ من الاختراق والبرمجة النفسية للأفراد والشعوب هدفا رئيسيا.

انطلاقا مما ورد أعلاه تتم معالجة الموضوع من خلال طرح الإشكالية التالية: كيف تهدد مخاطر بيئة المعلومات أمن المجتمع الرقمي الجزائري؟. وللإجابة -مؤقتا- على هذه الإشكالية تم وضع الفرضية التالية: كلما افتقدت المجتمعات الحديثة للوعي والمناعة الأمنية على مستوى الفضاء الافتراضي كلما زادت احتمالات تهديد أمن مجتمعها الرقمي، والحالة الجزائرية بطبيعة الحال ليست بمعزل عن هذا الافتراض. ولتناول هذا الموضوع تم تبني خطة مكونة من أربعة عناوين رئيسية؛ يستهدف الأول تحديد وحصر التهديدات المرتبطة بالمجال السيبراني، أما العناوين الأخرى فتحاول ربط تلك التهديدات بمجالاتها المتعلقة بالانتهاكات التي تطال أمن الأفراد من حيث التعدي على خصوصيتهم الرقمية، ثم إبراز صور استغلال الفضاء السيبراني كآلية لتعزيز التهديدات اللاتماثلية ويتم هنا تخصيص العنوان للإرهاب السيبراني، ليتم التطرق إلى أحد أكثر التهديدات الناعمة على مستوى الفضاء السيبراني "الفبركة الرقمية".

1. التهديدات السيبرانية:المفهوم والأشكال:

يعتبر الفضاء السبيراني أحد الفضاءات الحديثة للتفاعل الإنساني التي زادت بروزا بعد التوجه السريع والهائل لاستغلال التطور التكنولوجي في خدمة متطلبات الأفراد والمجتمعات، وبسبب حداثته لم يعرف المصطلح إجماعا حول تعريفه، إذ أن التعاريف المقدمة بشأنه تختلف حسب الجهة المقدمة له، أهدافها وقدرتها على استغلاله. وقد ظهر مصطلح الفضاء السيبرانية لأول مرة سنة 1982 على يد الامريكي مؤلف قصص الخيال العلمي ويليام جيبسون William Gipson الذي اشتق الكلمة Cybernetics، فللتعبير عن فكرة الهلوسة الجماعية التي يشترك فيها مليارات المنشغلين عبر العالم لجأ **جيبسون** للجمع بين مصطلح السيبرنيطيقا Cybernetics وكلمة فضاء Space وسكّ منهما مصطلح الفضاء السيبراني Cyberspace الذي أصبح حقيقة مع انتشار شبكة الانترنت (فرحات 2019، ص.90).

هذا، وتشير المقاربة الإيتيمولوجية لكلمة "cyber"إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم"governor" . وقد تم تعريف الفضاء السيبراني من قبل الوكالة الفرنسية لأمن أنظمة المعلومات Anssi على أنه فضاء للتواصل يعتمد على الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. أما الاتحاد الدولي للاتصالات

فيعرف الفضاء السيبراني على أنه مجال مادي وغير مادي، يتكون وينتج عن عناصر ممثلة في أجهزة الكومبيوتر، وكذا الشبكات، والبرمجيات، وحوسبة المعلومات، ومعطيات النقل والتحكم، إضافة إلى مستخدمي كل هذه العناصر(https://bit.ly/3785qWs). كما عرفه عبد القادر محمد فهمي بأنه جموع شبكات الحاسوب في العالم، وكل ما ترتبط به وتتحكم فيه هذه الشبكات، وهو لا يقتصر على شبكة الانترنت فقط وإنما يشمل العديد من شبكات الحاسوب الأخرى، فالفضاء الالكتروني يشمل كل شبكات الحاسوب التي تدير نشاط الدول ومؤسساتها ومرافقها وكل ما يتعلق ببيئتها الحيوية، و في القطاعات المدنية والعسكرية(فهمي2018، ص.17).

وجدير بالذكر أن مصطلح الفضاء السيبراني هو مصطلح جديد ظهر نتيجة لثورة تكنولوجيا المعلومات والاتصالات، وأصبح بفعل طبيعته الافتراضية - التي يصعب التحكم فيها - محمّلا بالتهديدات الجديدة التي تعكّر أمن الدول والمجتمعات، ومن أبرز هذه التهديدات نجد:

* **الانتهاكات التي تطال سرية البيانات الشخصية وإفشائها:** تتعدد صور الاعتداء على سرية البيانات الشخصية منها مخالفة القائمين على عملية المعالجة للشروط والأساليب القانونية المنصوص عليها داخليا، كعدم منح الترخيص من الجهات المختصة أو إلغائه أو انتهاء مدته، كما تعد في ذات الصدد مسألة الإفشاء غير المشروع للبيانات أحد أهم صور الانتهاكات التي تطال سرية البيانات وأكثرها شيوعا هي تلك المتعلقة بالتعاملات الالكترونية البنكية ومثالها ما ثبت من خلال قضية بنك (جزل تشافت) السويسري التي حاول خلالها عملاء فرنسيون تابعين لإدارة خدمات رقابة التعاملات التجارية والمالية فك شيفرة بيانات شخصية لمواطنين فرنسيين تحمل حسابات لدى البنك وذلك للاستعانة بها في أعمال البحث والتقصي التي تجري بشأن التهرب الضريبي(الذهبي2018، ص.147).

* **إدخال معطيات أو معلومات وهمية والتجسس على الحياة الخاصة للأفراد:** إذ يتمكن المعتدي من خلال سرقة واختلاس البيانات الشخصية للمعتدى عليه من توظيف المعطيات المحصّل عليها في أمور تتعلق بالذمة المالية، وقد تكون الحكومات أيضا مسؤولة على الانتهاكات التي تطال الحق في الخصوصية الرقمية، وهو ما كشف عنه تقرير الجمعية العامة للأمم المتحدة الذي ورد فيه ما يلي "*يبدو أن الحكومات تعتمد بشكل متزايد على برمجيات الاختراق الهجومية من أجل التسلل إلى الأجهزة الرقمية للأفراد، وهذا النوع من الاختراق الحاسوبي يتيح القيام عشوائيا باعتراض وجمع كل أنواع الاتصالات والبيانات، سواء كانت مشفرة أو غير مشفرة، ويتيح أيضا الإطلاع عن بُعد وبشكل سرّي على محتوى الأجهزة الشخصية والبيانات المخزّنة فيها، مما يمكن من إجراء مراقبة آنية للبيانات المتوافرة على هذه الأجهزة والتلاعب بها*"(الاستاذ2013، ص435).

* وفيما يتعلق ببرامج التجسس فإنها عادة ما تكون مخفية داخل ملف ملحق برسالة إلكترونية يحصد سرّا البيانات الموجودة داخل جهاز ما وتخص صاحبه، أو تخص تطبيقات صممها ذلك الجهاز، ثم ينقل تلك البيانات إلى الطرف الآخر، وقد عرّفها موقع "كاسبيرسكي" Kaspersky بأنها برامج يتم تثبيتها من دون موافقة المستخدم سواء أكان ذلك على حاسوب عادي أو تطبيق مضمّن في مستعرض الويب الذي يستخدمه أو تطبيق هاتف محمول مثبت على هاتفه، تعمل على نقل معلومات شخصية وسرية تتعلق بالمستخدم إلى المهاجم. وقد تكون المعلومات تقارير حول عادات استعراض الإنترنت أو عمليات الشراء التي يقوم بها، كما يمكن تعديلها لتسجيل أشياء مثل ضغطات لوحة المفاتيح أو معلومات بطاقة الائتمان أو كلمات المرور أو بيانات اعتماد تسجيل الدخول(https://bit.ly/3kvpYLo).

* **هجمات التصيد Phishing:** التصيّد هو نوع من الهجمات السيبرانية، حيث يُشكل المهاجم كيانًا أو شركة مرموقة من أجل خداع الأشخاص وجمع معلوماتهم الحساسة كبيانات بطاقة الائتمان، وأسماء المستخدمين، وكلمات المرور وما إلى ذلك. ونظرًا لأن التصيد يتضمن التلاعب النفسي ويعتمد على الفشل البشري بدلاً من الأجهزة أو البرامج فإنه يعتبر نوعًا من هجمات الهندسة الاجتماعية. وتستخدم هجمات التصيد رسائل إلكترونية مزيفة تقنع المستخدم بإدخال معلومات حساسة في موقع ويب مزيف، وعادة ما تطلب هذه الرسائل من المستخدم إعادة تعيين كلمة المرور الخاصة به أو تأكيد بيانات بطاقة الائتمان ثم تأخذه إلى موقع ويب مزيف يشبه جدًا الموقع الأصلي.

* التجسس المعلوماتي Information spyware : وذلك عن طريق التنصت والتجسس على أجهزة الحواسيب واعتراض المراسلات الالكترونية، وغالبا ما يتم ذلك عبر تثبيت برامج التجسس المعرفة على أنها برامج مصممة لجمع البيانات من حاسوب أو جهاز آخر وإعادة توجيهها إلى طرف آخر من دون موافقة المستخدم أو معرفته حتى. ويتضمن هذا عادةً جمع بيانات سرية مثل كلمات المرور، ورموز PIN، وأرقام بطاقات الائتمان، ومراقبة ضغطات لوحة المفاتيح، وتعقب عادات الاستعراض، وجمع عناوين البريد الإلكتروني. إضافة إلى كل ذلك، تؤثر هذه الأنشطة في أداء الشبكة وإبطاء النظام، فضلاً عن الإضرار بالعمليات التجارية بوجه عام. وتنقسم برامج التجسس بوجه عام إلى أربع فئات أساسية؛ أحصنة طروادة في المقام الأول، وبرامج الإعلانات المتسللة في المقام الثاني، وملفات تعريف الارتباط للتعقب في المقام الثالث، وبرامج مراقبة النظام في المقام الرابع والأخير (https://bit.ly/3vUd670).

* **الإرهاب المعلوماتي:** ينطلق الإرهاب بجميع أشكاله وشتى صنوفه من دوافع متعددة، ويستهدف غايات معينة، ويتميز الإرهاب الالكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الالكترونية. وقد عرفته **دوروثي دينينغ Dorothy Denningg** على أنه الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمّرًا وتخريبيًّا لتوليد الخوف بحيث يكون مشابهًا للأفعال المادية للإرهاب. أما **جيمس لويسJames Lewiss** فيعرفه على أنه استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة كالطاقة والنقل، والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين. كما ويعرّفُ الإرهاب السيبراني على أنه نقطة التقاء الفضاء الإلكتروني والإرهاب، ويشير إلى الهجمات والتهديدات غير القانونية بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها عندما يتم ذلك لتخويف أو إكراه حكومة أو شعبها لتحقيق أهداف سياسية أو اجتماعية. هذا، ويميز البعض من الباحثين بين نوعين من الإرهاب السيبراني؛ يشير أولهما إلى الإرهاب السيبراني الخالص Pure Cyber Terrorism، والذي يتصل بالهجمات المباشرة على البنيه التحتية للضحية لتحقيق أهداف مختلفة. بينما يُشير الثاني إلى الإرهاب السيبراني الهجين Hybrid Cyber Terrorism، وفيه يستخدم الارهابيون الفضاء السيبراني في مختلف الأنشطة كالدعاية والحرب النفسية، والتخطيط لهجمات إرهابية فعلية، وتجنيد أعضاء جدد، وجمع الأموال، والتبرعات... الخ(لطفي2022، ص.ص.159-160).

* **الفبركة الرقمية Digital Fabrication:** تعتبر الفبركة الرقمية أحد أهم صور التداول العشوائي وغير المراقب للمعلومات ضمن الفضاء السيبراني، وتأتي في شكل نص، أو صورة أو مقطع فيديو، في الحالة الاولى يتم التأليف أو تحريف نص معين لتغيير الحقيقة، وفي الحالة الثانية تتم الفبركة من خلال برامج تعديل الصور

والفيديوهات التي يمكن من خلالها إضافة أو حذف عناصر من الصورة أو الفيديو ، وتنقسم الفبركة الرقمية إلى ثلاثة أنماط رئيسية هي الأخطاء غير المقصودة والتي تنشأ غالبا نتيجة للجهل بالمعلومة الصحيحة، وكذا الأخطاء المقصودة بغرض تحقيق أهداف ومصالح خاصة، وأخيرا المحاولات المرتبطة بنشر خطاب الكراهية والتطرف(العازمي 2021، ص.1220).

2. المخاطر القائمة على انتهاك الخصوصية الرقمية وأثرها على أمن المجتمع الرقمي:

تنشأ مخاطر خصوصية البيانات من الأجهزة التي تكون قادرة ومصممة على التواصل مع بعضها البعض، ونقل البيانات بشكل مستقل إلى طرف ثالث، حيث تؤدي عمليات التواصل هذه وتبادل البيانات التي تبدو غير ضارة لعدم حساسيتها إلى تجميع البيانات وتحليلها، ومن ثم التوصل للكشف والمعرفة الدقيقة للأفراد ما يزيد من إمكانية تتبع المستخدم و تحديد شخصيته و هويته، وتعتبر في هذا الصدد الهواتف الذكية أحد مداخل انتهاك الخصوصية الرقمية للأفراد لسهولة تعرضها لعمليات الاختراق، والتي يقصد بها كل الطرق التي يستخدمها الأشخاص للوصول سرا إلى بيانات الهاتف واستعراض ما يوجد عليه، وهي عادة تستهدف حسابات الخدمة المصرفية عبر الانترنت، البريد الالكتروني (للعمل او الشخصي)APPLE ID أو حساب جوجل، كلمة مرور الهاتف، مواقع التواصل الاجتماعي التي يشترك بها صاحب الهاتف و ما تحوز عليه من معلومات ذات خصوصية عالية(https://bit.ly/3kty6MI).

فالهواتف الذكية أصبحت قادرة على رصد البيانات الوصفية كالمعلومات المسجلة حول المكالمات والرسائل النصية كالتوقيت والمدة التي تكشف في حال تجميعها على تفاصيل شخصية لا يكاد يعلم بها إلا المستخدم، كما تمكن أيضا من تتبع الموقع الجغرافي للمستخدم، وهو ما أظهرته صحيفة **وول ستريت جورنال The Wall Street Journal** عندما أعلنت عن قيام شركتي آبل **Apple** وجوجل **Google** بتصميم أنظمتها للهواتف الذكية، بحيث تنقل إليها باستمرار الموقع الجغرافي لبناء قاعدة بيانات عملاقة تمكن من الاستحواذ على سوق الخدمات القائمة على تحديد المواقع والتي قدرت قيمتها 2.9 مليار دولار (https://on.wsj.com/39xQm5n).

من جهة أخرى فإن الهواتف النقالة إضافة إلى أجهزة الكومبيوتر المتصلة بالانترنت مجهزة بعنوان بروتوكول (ip) خاص يوفّر محدد هوية فريد لكل جهاز، وهو ما يوفر خاصية التتبع لهذه الأجهزة، ومن أشهر الأدوات المبتكرة لتتبع مستخدمي الانترنت ما يعرف باسم ملفات تعريف الارتباط cookies وملفات التجسس web buggs (مندل وآخرون 2012، ص.14). وفي سياق غير بعيد عن ذلك أصبح الحق في الخصوصية الرقمية أكثر عرضة للانتهاك والتعدي بسبب الرواج الكبير التي عرفته مواقع التواصل الاجتماعي المعرفة على أنها مواقع الكترونية تركز على بناء أو إظهار العلاقات الاجتماعية بين الأفراد، إذ تعمل على تسهيل الصداقات الافتراضية وتنميتها عبر إتاحة فرص مشاركة الصور وتبادل الحديث عبر الانترنت، لكنها وفي المقابل لا تنطوي على سياسات صارمة في ما يتعلق بحماية خصوصية المستخدمين، حيث تكون عرضة للانتهاك من قبل أشخاص عاديين، أو من قبل الشركات المالكة للمواقع ذاتها، أو من خلال شركات أخرى تمكنت من اختراق البنية الأمنية الهشة لهذه المواقع.

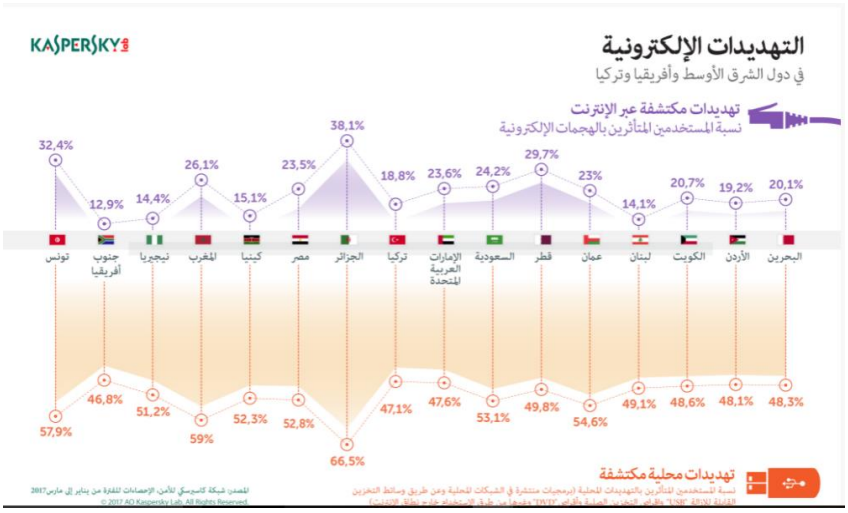
فشركة فايسبوك مثلا، تجمع كل البيانات الخاصة بمستخدميها، والتي تتيح لها معرفة أهم التفاصيل عن المستخدمين، وحياتهم الشخصية، وميولهم، وأبرز ما يبن ذلك تلك الأسئلة التي يطرحها فيسبوك

على مستخدميه ماذا في ذهنك الآن؟ ما الجديد اليوم؟ أو تلك الكوزيات الخاصة التي تقوم بتجميع البيانات الشخصية من خلال الأصدقاء هل تعرف صديقك كما ينبغي؟ وغيرها من الآليات التي تبيّن أن جمع البيانات الشخصية يتعدى الاهتمام بتأمين منصة تبادل أخبار بين الأصدقاء ونقاش حول قضايا معينة إلى سعي دؤوب لفهم ميول المستخدم ورصد تفاصيل حياته اليومية، بحيث يصبح من السهل رسم طيف خاص به وتحديد كيفية استهدافه بالإعلانات أو الأخبار أو الانضمام إلى مجموعات تبحث عن مؤيدين وتابعين(جبور جبور 2018، ص.34).

إن الكلام أعلاه يبين أن شبكات التواصل الاجتماعي ما هي إلا شكل جديد من أشكال التحكم الاجتماعي، بحيث يمكن لأيّ كان مراقبة نشاط وتحركات شخص آخر، وتتم هذه المراقبة عبر مستويين؛ **الأول مرئي** و يقوم به الأصدقاء، أو متتبعو الشخص المعني، **والثاني غير مرئي** وتقوم به البرامج والتطبيقات المتخصصة في رصد وتحليل الاهتمامات، والتي تستخدمها المواقع المختلفة ومحركات البحث، كما قد يتم استغلال البيانات الشخصية المأخوذة خلسة عن مستخدمي مواقع التواصل الاجتماعي في عمليات الهندسة الاجتماعية، وهو ما كشفت عنه فضيحة **كامبريدج أناليتيكا**، حيث قامت شركة بريطانية تعمل في تحليل البيانات تُدعى "كامبريدج أناليتيكا Cambridge Analytica"بتوفير بيانات حول توجّهات الناخبين الأمريكيين من خلال تطبيق يتم الدخول إليه عبر حساب الفيسبوك، وهو ما أدى للحصول على بيانات ما يقرب من 50 مليون شخص من مستخدمي الموقع الاجتماعي الشهير دون علمهم أو موافقتهم(https://bit.ly/3hb3leY).

هذا، وقد استطاعت شركات عدة متخصصة في التجسس من النيل من خصوصية مستخدمي مواقع التواصل الاجتماعي عبر استغلال الثغرات الموجودة بهذه المواقع، ونذكر من هذه الشركات مثلا شركة NSO الشركة الاسرائيلية التي تأسست سنة 2010 من قبل الإسرائيليين الاثنين شاليفهوليو وعمري لافي، وقد عملت هذه الشركة على عمليات تطوير و استخدام برامج القرصنة PEGASUS 3 وسرقة بيانات خاصة انطلاقا من استخدام رقم هاتف المستخدم، وتوضح شركة كاسبرسكي المتخصصة في برامج الحماية من الفيروسات أن بيغاسوس مؤلف من وحدات حيث يقوم أولا بمسح الجهاز المستهدف، ثم يثبت الوحدة الضرورية لقراءة رسائل المستخدم وبريده الالكتروني، والاستماع إلى المكالمات، والتقاط صور للشاشة، وتسجيل نقرات المفاتيح، وسحب سجل متصفح الإنترنت، وجهات الاتصال. كما أن بإمكانه الاستماع إلى ملفات الصوت المشفرة، وقراءة الرسائل المشفرة، بفضل قدراته في تسجيل نقرات المفاتيح وتسجيل الصوت، حيث يسرق الرسائل قبل تشفيرها، والرسائل الواردة بعد فك تشفيرها، وقد تم رصد نشاط هذا البرنامج في عدة دول عربية منها الجزائر، قطر، تونس، المغرب، الأردن ولبنان.

رسم توضيحي للتهديدات الالكترونية في دول الشرق الأوسط وشمال إفريقا التي تندرج الجزائر ضمنها



المصدر: https://bit.ly/3s3YvEJ

وقد تطرق تحقيق لمجلة الجيش الجزائري إلى العديد من الحالات التي تم من خلالها الاحتيال على الأفراد إلكترونيا والتي نجد منها ما يلي:

* **الاحتيال عن طريق البطاقة الذهبية:** تم ارتكاب أكثر من 40 عملية احتيال تحت ستار تطبيق "بريدي موب" الذي أطلقته وزارة البريد والمواصلات السلكية واللاسلكية، حيث تعرض موظفون من مختلف القطاعات الحيوية لعمليات النصب والاحتيال عبر شبكات التواصل الاجتماعي خاصة فايسبوك؛ حيث استخدم مرتكبو هذه الجرائم حسابات الفايسبوك التي تم اختراقها من خلال ربط اتصال مع أصدقاء الفايسبوك من تلك الحسابات نفسها، بغرض إقناع الضحايا أنهم سيستفيدون من منحة مخصصة لوباء كوفيد 19 وذلك دون ترك مجال للضحايا للشك في أن حسابات أصدقائهم قد تم التلاعب بها من قبل أشخاص آخرين.

ويذكر ذات التقرير الوارد أعلاه أحد الحالات المتعرضة للاحتيال، حيث تلقى الضحية رسالة على المسنجر من زميل له يبلغه من خلالها أنه من أجل الاستفادة من هذه المنحة، لابد من التسجيل في قائمة المستفيدين بإدخال المعلومات الشخصية كرقم البطاقة الذهبية، ليقوم الضحية بإرسال رقمه إلى مرتكب عملية الاحتيال معتقدا أنه زميله، حيث تم خصم مبلغ يقدر ب " 60 مليون دينار" من حسابه البريدي الجاري " CCP ".

* **التصيد الاحتيالي عن طريق إعلانات التوظيف:** وذلك من خلال نشر الاعلانات الخاصة بالتوظيف في العديد من مناصب الشغل والاختصاصات على صفحات وهمية في وسائل التواصل الاجتماعي على غرار فايس بوك، وتحمل هذه الصفحات شعارات مطابقة لتلك الخاصة بالمؤسسة الرسمية التي يتم تنفيذ الاحتيال باسمها، وقد قام العديد من زوار هذه المواقع بإرسال كافة بياناتهم الشخصية وحتى جوازات سفرهم الخاصة بغية التواصل مع مسؤولي هذه الصفحات لتزويدهم بمعلومات وافية حول هذه المناصب الوهمية(مجلة الجيش الجزائري 2021، ص.35).

3. مخاطر استخدام الفضاء السيبراني في الترويج للفكر المتطرف:

إن أحد مسببات تلوث البيئة الرقمية يكمن في استغلال الشبكات المعلوماتية في نشر الفكر المتطرف وخطاب الكراهية بين أفراد المجتمع الواحد من خلال إثارة نعرات القومية، العرقية، المذهبية...كما تم استخدام الشبكة العنكبوتية ومختلف وسائل التواصل الاجتماعي في جذب الشباب للحركات الإرهابية من خلال اتباع أسلوب التجنيد الالكتروني الذي يستند إلى النشر الواسع والحذر للأفكار والتصورات الإرهابية من خلال الاستعطاف وكسب التأييد المرتبط بالجوانب الدينية، ولعل قضية ariduka تُعدّ مثالا حيّا حول ذلك؛ حيث تمكّن الإرهابيون التابعون لتنظيم القاعدة من إقناع أحد الشباب البالغين من العمر 21 سنة من الإقدام على عملية إطلاق نار على جنود أمريكين في مطار فرانكفورت، إذ عمل الإرهابيون على استغلال الانترنت ومواقع التواصل الاجتماعي وكذا الألعاب الإلكترونية في الترويج لأفكارهم وعقائدهم والفيديوهات التي توضح كيفية عمل القنابل والتدريبات المختلفة، وهو ما أقر به ذات الشاب عندما صرح بأن تجنيده تم من خلال لعبة world of warcraft (غويتا ووكس2017، ص.19).

وعموما فان دور التكنولوجيا الحديثة في تجنيد الإرهابيين وتنفيذ العمليات الإرهابية يكمن فيما يلي:

- **التجنيد:** تعمل الجماعات الإرهابية على نشر الأفكار المتطرفة والمعتقدات المتشددة على نطاق واسع يمكن من بلوغ مرحلة التجنيد العالمي من خلال استغلال مزايا السعة والوقت التي تمنحها فضاءات التواصل الجديدة، وعلى سبيل المثال تم تجنيد العديد من الأفراد من دول مختلفة للمشاركة إلى جانب التنظيم الإرهابي "داعش" في المنطقة العربية، وهو ما يظهره دليل المقاتلين الإرهابيين الأجانب لمعاهدة التدريب القضائي في بلدان الشرق الأوسط وشمال إفريقيا الصادر عن هيئة الأمم المتحدة، بحيث نجد في عرضه للحالات المختلفة الحالة التالية التي تمكنت من التشبع من الفكر الإرهابي ومتابعة العمليات المختلفة التي ينفذها التنظيم على الأرض من خلال شبكات التواصل الاجتماعي؛ "*في عام 2014، شرعت معلمة تعمل في عمان الأردنية، بالرغبة في دعم تنظيم داعش وبدأت في متابعة أخبار ذلك الكيان الإرهابي عبر الأنترنت (خاصة المواقع الإعلامية ووسائل التواصل الاجتماعي)، فتواصلت مع أحد أعضاء "داعش" عبر الأنترنت وأعربت عن رغبتها في الانضمام إلى التنظيم في سوريا ودعم ما يسمى بجهاد النكاح، وحاولت بعدها تجنيد نساء أخريات للزواج من المقاتلين الجهاديين، وبالفعل تمكنت من تجنيد زميلة سابقة لها وتلقت كلتاهما تعليمات بالسفر إلى تركيا للسياحة قبل أن يتم تهريبهما عبر الحدود إلى سوريا*"(مكتب الأمم المتحدة المعني بالجريمة والمخدرات2021، ص.16).

- **الدعاية والتحريض:** تتخذ الجماعات الارهابية من الشبكات المعلوماتية حيزا لممارسة عملية الدعاية والتحريض للقيام بأعمال إرهابية داخل دول مختلفة، كما تتخذها للتأثير على القُصّرِ ودفعهم للانخراط في عمليات إرهابية تخدم أهداف جماعة معينة، حيث يتم بالاستناد على الألعاب الالكترونية الموصولة بالانترنت والمصممة خصيصا للتأثير على نفسية الفرد وكسب تعاطفه اتجاه الإرهابيين.

- **التمويل:** يمكن للتنظيمات الإرهابية أن تستغل الانترنت لتمويل أعمالهم الإرهابية، وتصنف الطرائق التي يستخدمونها إلى أربع فئات عامة ممثلة في الطلب المباشر، والتجارة الالكترونية، واستغلال أدوات الدفع عبر الانترنت، وأخيرا استغلال المنظمات الخيرية.

- **التدريب:** أصبحت التنظيمات الإرهابية تستخدم الانترنت استخداما متزايدا بوصفه ساحة تدريب بديلة للإرهابيين، وهناك مجموعة متزايدة من الوسائط التي توفر منصات لنشر أدلة عملية في صورة كتيبات

الكترونية، ومقاطع صوت، وفيديوهات، ومعلومات، ونصائح، بحيث يتم استغلالها في نشر موضوعات تدعم العمل الإرهابي ككيفية الانضمام إلى التنظيمات الإرهابية، وكيفية صنع المتفجرات والأسلحة النارية، وكيفية التخطيط للهجمات الإرهابية و تنفيذها، لتصبح بذلك هذه المنصات بمثابة معسكر تدريبي افتراضي، ولعل مجلة "**انسباير**" الالكترونية التابعة لتنظيم القاعدة تعتبر دليلا حيّا حول هذا الطرح؛ إذ تسعى هذه المجلة إلى إتاحة كمية كبيرة من المواد الإيديولوجية الرامية إلى تشجيع الإرهاب بما في ذلك تصريحات منسوبة إلى **أسامة بن لادن** و**أيمن الظواهري** وغيرها من الشخصيات المعروفة من تنظيم القاعدة، كما تتضمن أعداد المجلة تعليمات عملية حول كيفية صنع المتفجرات، وصورا توضيحية تمكن من التجسيد الفعل للنصائح والارشادات المقدمة في سبيل القيام بعمل إرهابي(مكتب الأمم المتحدة المعني بالمخدرات والجريمة2013، ص.08).

وفي المتن تتناول المجلة الالكترونية الطريقة التي يتم من خلالها الحصول على قنبلة سهلة الصنع وغير متاحة للكشف وقادرة على الفتك بالعشرات من الأشخاص، وهو ما يبرز الكيفية التي يتم من خلالها استغلال الانترنت في الترويج للفكر المتطرف وتسهيلها لنشر العمل الإرهابي خاصة في أوساط الشباب الذين لم يكتسبوا مناعة فكرية ضد محاولات التسميم الإيديولوجي الذي تحاول الحركات الإرهابية انتهاجه لحشد أكبر عدد ممكن من الأفراد لصفوفها. فكثيرا ما يتم الاستناد إلى تكنولوجيا المعلومات والاتصال في تنشئة الأفراد وتلقينهم للأفكار والمعتقدات المختلفة، غير أن ذلك أصبح يشكّل تهديدا جوهريا للكثير من المجتمعات التي لم تبلغ بعدُ مرحلة النّضج في العالم الافتراضي؛ حيث لا تزال غير قادرة على بلورة رأي محايد غير خاضع للتجاذبات السياسية والايديولوجية المنتشرة على مستوى البيئة المعلوماتية، ما يجعل مناعتها هشة أمام عمليات الاستغلال الهادفة لتوجيه الأفكار والقناعات نحو زوايا محددة تخدم أهدافا ضيقة.

وفي ذات السياق أعلاه، تعتبر الجزائر من الدول العربية الأقل عددا من حيث المجنّدين في التنظيمات الإرهابية باستخدام الوسائل الحديثة، فبالنسبة للتنظيم الإرهابي "داعش" لم ينضم سوى 170 جزائري، في وقت بلغ عدد التونسيين والمغربيين المنضمين إليه نحو ثلاثة آلاف وألفًا وخمسمائة على التوالي(https://bit.ly/3kL4Hxx)، إلا أن ذلك لا يزيح جميع المخاوف المتعلقة بإمكانية تجنيد أفراد جزائريين ضمن التنظيمات الإرهابية من خلال استخدام تكنولوجيا المعلومات والاتصال، وهو ما يستوجب بالضرورة اتباع سياسة معلوماتية، وأمنية، ورقابية صارمة قادرة على تشتيت محاولات اندساس الخلايا الإرهابية ذات الأفكار المتطرفة داخل المجتمع الجزائري، خاصة خلال الفترات الانتقالية التي تشهد حالات الانقسام والتشتت بين التيارات الإيديولوجية المختلفة كتلك التي سادت أثناء الحراك الشعبي الجزائري، والذي شهد العديد من محاولات التأثير الممنهج على توجهات الجماهير.

4. مخاطر الفبركة الرقمية في البيئة السيبرانية:

يعتبر الفضاء الرقمي أحد الفضاءات الجديدة المتخذة لنشر وتداول المعلومات الكاذبة والشائعات في المجتمعات الحديثة، مسببة بذلك تلوّثا معلوماتيا حادا يؤثر على أفكار الأفراد وتوجهاتهم وحتى مواقفهم تجاه القضايا المجتمعية، الوطنية والدولية. فبسبب غياب عنصُرَيْ الرقابة والردع عبر الفضاءات الجديدة زادت مستويات التداول العشوائي للمعلومات بين أوساط المجتمعات محلية كانت أو دولية، وهو ما عمدت إلى توضيحه مؤسسة الفكر الأمريكية **راند** من خلال تقريرها المعنون ب: رصد وسائل التواصل الاجتماعي" عبر لتحليلات وزارة الدفاع الأمريكية لوسائل التواصل الاجتماعي في المستقبل دعما لعمليات المعلومات"؛ حيث

اعتبرت الدراسة أن وسائل التواصل الاجتماعي أصبحت تشكّل عنصرا رئيسيا وحاسما في عملية تشكيل الرأي العام من خلال التبادل الواسع والسريع للمعلومات ضمنها، فعلى سبيل المثال ينشر مستخدمو "تويتر" وحدهم 500 مليون تغريدة يوميا، كما ينشر المستخدمون الصور ومقاطع الفيديو، وتحديثات بشأن الحالة على وسائل التواصل الاجتماعي، وغالبا ما تشمل ملفاتهم الشخصية تفاصيل شخصية تمثل عمرهم، وجنسهم، وأفراد عائلتهم، ومكان عملهم، وتوفر هذه المنشورات رؤية حول حياة الأفراد اليومية، بالإضافة إلى المواقف والسلوكيات المرتبطة بالشبكات الاجتماعية(مارسيلينو 2017، ص.10).

وعموما يمكن تصنيف الشائعات عبر شبكات التواصل الاجتماعي من حيث أهداف نشرها إلى قسمين؛ **النوع الأول** شائعات موجهة لهدف محدد، ينشرها أصحابها وهم على يقين ودراية تامة بكون هذه الأخبار عارية عن الصحة، وعادة ما يكون لديهم هدف أو غرض محدّد من نشر هذه الأخبار بحسب نوع الخبر والمجال الذي يقع في خانته، وهذا النوع من الشائعات ليس بالضرورة أن يكون تأثيره سلبياً، فقد يأتي إما لغرض تسويقي أو إعلاني، أي أن الشائعة هنا تقوم بوظيفة ما، ويسعى مروجوها إلى تحقيق أهداف معينة من طرف جهات محددة.

أما **النوع الثاني** من الشائعات فهو الذي يفرز تداعيات على الأمن الوطني للدول والمجتمعات، وفي الغالب فإن هذه النوعية من الشائعات تتنوع مصادرها وأهدافها، فقد تكون نتاجَ أشخاصٍ أو جهات خارجية أو شركات كبرى، وفي الغالب فإن دوافع وأهداف هذه النوعية من الشائعات تتمثل في الآتي:

- زعزعة الاستقرار الداخلي للدول والمجتمعات، خاصة إذا استهدفت هذه الشائعات رموز أو قيادات دولة ما، أو تطرقت إلى قضايا ترتبط بالأمن المجتمعي للمواطنين في دولة ما، هنا يظل تأثير الشائعة قائماً ومستمراً لفترة ما، خصوصاً في زمن الاتصال السريع والتواصل عبر الشبكات الاجتماعية والمعلومة الآنية.

- إثارة الفتن والخصومات وتعميق الخلافات القائمة بين فئات المجتمع، والتي تعمل الشائعات على إيجادها محاولة استغلال الظروف والمواسم والمناسبات بغرض النيل من سمعة الشخص المقصود أو المساس بمركزه الاجتماعي أو التعرض لمكانته.

- تهديد الأمن الاقتصادي للدول والشركات الكبرى، من تركيز مروجي الشائعات على المنشآت الاقتصادية والتجمعات العمالية وأسواق البورصة وغيرها من السلع التي تلعب دوراً استراتيجياً في حياة الناس، بقصد خلق كل ما من شأنه إعاقة سير الإنتاج والتنمية الاقتصاد (https://bit.ly/3N5kgwT).

وقد عرفت الجزائر في السنوات الأخيرة العديد من محاولات الفبركة الرقمية الهادفة إلى زعزعة الاستقرار وتشتيت الرأي العام المحلي تجاه القضايا المحورية التي يسعى إلى بلورة رؤية واضحة حولها، وذلك لما تحمله من أهمية سياسية واقتصادية ومجتمعية بالغة على الأمن القومي للدولة، ولعل فترة الحراك الشعبي التي انطلقت بعد مظاهرات 22 فيفري 2019 كانت أكثر الفترات غزارة من حيث التوظيف الممنهج والموجه للفضاء الرقمي في نشر الشائعات والترويج لها افتراضيا، وبغية نشر وتوسيع نطاق الأخبار غير الموثوقة والتي ارتبطت غالبا بأطراف ذات أجندات سياسية متباينة، وقد تم في هذا الإطار الاعتماد على العديد من الأساليب المساعدة كالتزييف العميق، والذباب الالكتروني، والبروباغندا.

ويعتبر الذباب الالكتروني على سبيل المثال أحد الأساليب المستخدمة في ترويج الشائعات ضمن الفضاء الرقمي، ويعرّف على أنه روبوتات أو برامج مصممة على أنها أشخاص حقيقية وظيفتها إدارة حسابات وسائط التواصل الاجتماعي، وتعمل بشكل خاص على إظهار عدد هائل من المنشورات المزيفة (الهاشتاغ) حتى تبدوا حقيقية، وذات مصداقية بسبب التداول الواسع لها في منصات التواصل الاجتماعي (Bennsoula2020, p.199.)، وبما أن السجالات السياسية أصبحت تُدار بطرق افتراضية فقد تم الاعتماد على الذباب الالكتروني خلال فترة الحراك الشعبي كشكل مستحدث للطابور الخامس الذي يعمل على توجيه وحصر الرأي العام ضمن توجهات محددة قد تسبب المزيد من الاحتقان الشعبي وتؤدي إلى قطع سبل التوفيق بين الأطياف المختلفة.

خاتمة:

من خلال البحث تم التوصل إلى مجموعة من الاستنتاجات نوردها على النحو التالي:

- أصبحت التهديدات السيبرانية تشكل نمطا مستحدثا لتهديدات هلامية ناعمة مصاحبة لموجة العولمة، فهي تهديدات متعددة الأوجه تستهدف الدول والأفراد على حد سواء، كما أنها مصممة لتكون محل استخدام فوري وفعال للنيل من قدرة الخصم (دول أو أفراد) وفعاليته وروحه المعنوية خاصة وأن تفعيلها يعتمد على التكنولوجيا الحديثة، ويخضع لاعتبارات تتعدى الاستراتيجيات التقليدية القائمة على المواجهة الميدانية المباشرة، ولا ينفي ذلك إمكانية استخدام التهديدات السيبرانية ضمن الاستراتيجيات طويلة المدى، والمرتبطة ببرمجة المجتمعات وهندسة تفكيرها الجمعي بما يخدم مصالح الجهة المستخدمة والمطورة لها.

- أدى نقل الأفراد والدول لبياناتهم إلى العالم الافتراضي لتعريض أمنهم الرقمي لجملة من التهديدات التي يتعدى تأثيرها حدود هذا العالم ليؤثر على واقعهم المعاش، فبالنسبة للأفراد فإن أي انتهاك يطال سرية بياناتهم يعتبر اعتداءً على حقهم في الخصوصية الرقمية التي تطرح العديد من الاشكالات القانونية والتقنية كتلك المتعلقة بقصور التشريعات المحلية والدولية في هذا الخصوص وصعوبة التحري وحفض الحقوق، خاصة فيما يتعلق بالجرائم المالية المرتبطة بالسطو واختراق الحسابات البنكية وسرقة كلمات المرور...، أما بالنسبة للدول فإن التهديدات السيبرانية تطرح مشاكل جدية متعلقة بعرقلة البنية التحتية والقطاعات الحيوية المرتبطة بالشبكة المعلوماتية.

- بالنسبة للجزائر فان نسب التهديدات السيبرانية في ارتفاع مستمر ويرجع ذلك بالأساس إلى زيادة الربط بالشبكة المعلوماتية، زيادة اندماج الأفراد ضمن الفضاء الافتراضي، وغياب الرقابة على مستوى هذا الفضاء، وعدم مواءمة التشريع المحلي لهذا النوع من الجرائم ذات الصفة التطورية التمويهية، والتي يصعب تتبع أثرها ورصد مصدرها بعد وقوع الجريمة. وقد تبين من خلال ما ورد في ثنايا المقالة أن الجزائر مُعرّضة إلى نمطين اثنين من التهديدات السيبرانية؛ يتعلق **الأول** بالتهديدات المرتبطة بالنيل من سرية البيانات والاعتداء على الحق في الخصوصية الرقمية ضمن الفضاء الرقمي، أما النمط **الثاني** فهو المتعلق بعمليات الفبركة الرقمية والتداول العشوائي للأخبار والمعلومات، أما ما تعلق بالتهديدات المرتبطة بالإرهاب السيبراني فهي أقل مقارنة بالتهديدين السابقين.

قائمة المراجع:

1-الذهبي،خدوجة. (ديسمبر،2018). "حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)"،مجلة الاستاذ الباحث للدراسات القانونية والسياسية،المجلد الأول، العدد الثامن.

2- الاستاذ، سوزان عدنان. (ديسمبر،2013) "انتهاك حرمة الحياة الخاصة عبر الانترنت"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث.

3- العازمي، استقلال دليل محمد ماجد. (جانفي،2021) "مخاطر الفبركة الرقمية في الاعلام الجديد جائحة كورونا عبر وسائل التواصل الاجتماعي " نموذجا "، مجلة البحوث الاعلامية، العدد السابع والخمسون، ج 3.

4-الأمن السيبرانيCyber Security، الموسوعة السياسية، منشور على الموقع : https://bit.ly/3785qWs تم الاطلاع بتاريخ 17 /10 /2020.

5- الأمم المتحدة، الحق في الخصوصية في العصر الرقمي، الدورة 39 لمجلس حقوق الإنسان، ص 8، منشورة على الموقع: https://bit.ly/3kvpYLo تم الاطلاع بتاريخ 2021/05/05.

6- المنظمة العالمية للمستهلك، حملة اليوم العالمي لحقوق المستهلك لعام 2019: منتجات ذكية موثوقة، منشور على الموقع: https://bit.ly/3kty6MI تم الاطلاع بتاريخ 2021/05/07.

7- الشائعات في وسائل التواصل الاجتماعي وتأثيراتها السلبية، مجلة درع الوطن الإماراتية، منشور على: https://bit.ly/3N5kgwT تم الإطلاع بتاريخ 2022./01/12

8- جبور، منى الأشقر. وجبور،محمود. (2018). البيانات الشخصية والقوانين العربية "الهم الأمني وحقوق الأفراد"، لبنان: المركز العربي للبحوث القانونية والقضائية.

9- لطفي، وفاء. (جانفي،2022). "الجهود الدولية في مكافحة جرائم الارهاب السيبراني"،مجلة دراسات، المجلد الثالث والعشرون، العدد الأول.

10- محمد فهمي، عبد القادر . (ديسمبر،2018)."الحروب التقليدية وحروب الفضاء الالكتروني: دراسة مقارنة في المفاهيم وقواعد الاشتباك"، مجلة العلوم القانونية والسياسية، المجلد 16، السنة الثامنة، العدد 2.

11- مندل وآخرون، توبي.(2012). دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، فرنسا: منظمة اليونسكو.

12- مارسيلينو، وليام. (2017). رصد وسائل التواصل الاجتماعي: عبر لتحليلات وزارة الدفاع الامريكية لوسائل التواصل الاجتماعي في المستقبل دعما لعمليات المعلومات، مؤسسة راند.

13- مجلة الجيش الجزائري(تحقيق). (ديسمبر،2021). العدد 701.

14- مكتب الأمم المتحدة المعني بالجريمة والمخدرات. (فيفري،2021).المقاتلون الإرهابيون الأجانب: دليل لمعاهدة التدريب القضائي في بلدان الشرق الأوسط وشمال إفريقيا، فيينا: الأمم المتحدة.

15- مكتب الامم المتحدة المعني بالمخدرات والجريمة. (2013). استخدام الانترنت لأغراض إرهابية، فيينا: مكتب الأمم المتحدة المعني بالمخدرات والجريمة.

15- ما هو التصيد، نقلا عن موقع: https://bit.ly/3vUd670 تم الاطلاع بتاريخ 2020/10/21.

16- نهاد محمود، جدل التوظيف الانتخابي للبيانات الشخصية لمستخدمي الفيسبوك، الاربعاء 21 /2018/03، تم نشره على موقع https://bit.ly/3hb3leY والاطلاع بتاريخ 2021/05/07.

17- عبد الاله بن داودي، دور الدروس المستخلصة من الجزائر في رسم المشهد العراقي، نشر يوم 8 أوت 2018، على الموقع التالي: https://bit.ly/3kL4Hxx تم الاطلاع بتاريخ 2022/01/10 .

18- فرحات، علاء الدين. (ديسمبر،2019). "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الواحد والعشرين"، مجلة العلوم القانونية و السياسية ، المجلد 10، العدد 03.

19- غوبتا، رافي. ووكس،هاغبرو.(2017). وسائل التواصل الاجتماعي وتأثيرها على المجتمع، القاهرة: المجموعة العربية للتدريب والنشر.

20- Angwin, Julia, And Jennifer Valentino-DeVries , Apple ,Google Collect User Data, https://on.wsj.com/39xQm5n looked : 29/04/2021.

21-Bensoula,Noureddine. (Jeune, 2020)."Electronic Flies and Public Opinion", Journal of Sociological and Historical Studies , Vol 11, Issue01.