

انتحال الهوية الرقمية Digital identity theft

سويسي فتيحة

قاضية باحثة بمركز البحوث القانونية والقضائية

البريد الإلكتروني: souici.justice@gmail.com

تاريخ النشر: 2025/06/28.	تاريخ القبول: 2025/06/27	تاريخ الارسال: 2025/06/23
--------------------------	--------------------------	---------------------------

الملخص:
أدى التطور المتسارع لتكنولوجيات الإعلام والاتصال إلى بروز مفهوم جديد للهوية يسمى بالهوية الرقمية، والتي تعبر عن الوجود الرقمي للشخص في العالم الافتراضي. إلا أن هذه الهوية وعلى غرار الهوية الواقعية قد تتعرض لعملية الانتحال من طرف الغير بتقنيات مختلفة على مستوى شبكة الإنترنت، الأمر الذي أدى لانتشار صورة حديثة من صور الإجرام السيبراني يسمى بجريمة انتحال الهوية الرقمية، والتي تعتبر من أكثر الجرائم ارتكابا في الوقت الراهن، ومن أكبر التحديات التي تواجهها الدول نظرا لمخاطرها المتزايدة. وسنتناول في هذا المقال مختلف التقنيات والأساليب المستخدمة لارتكاب هذه الجريمة والآليات القانونية للوقاية منها ومكافحتها، مع الإشارة إلى عدم تجريم هذا الفعل في التشريع الجزائري. الكلمات المفتاحية: هوية رقمية، مجرم سيبراني، معطيات ذات طابع شخصي، تصيد الكتروني، هندسة اجتماعية، انتحال رقمي.

Abstract:

The rapid development of information and communication technologies has led to the emergence of a new concept of identity called digital identity, which expresses a person's digital presence in the virtual

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

world.

However, this identity, like real-life identity, can be subject to impersonation by third parties using various online techniques. This has led to the spread of a new form of cybercrime called digital identity theft, which is considered one of the most prevalent crimes today and one of the greatest challenges facing countries due to its growing risks.

In this article, we will discuss the various techniques and methods used to commit this crime, as well as the preventative and legal mechanisms to combat it, while noting that this act is not criminalized under Algerian law.

key words: digital identity, cybercriminal, personal data, phishing, social engineering, digital impersonation.

المقدمة:

أدى التطور الهائل في مجال الاتصالات والتكنولوجيات الرقمية المتقدمة إلى ظهور أنواع مستحدثة من الجرائم اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو الجرائم السيبرانية والتي برزت نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها بطرق غير مشروعة، وتعتبر جريمة انتحال الهوية الرقمية من أبرز الجرائم الماسة بحق الأشخاص في الهوية الرقمية¹.

كما انعكس هذا التطور التكنولوجي على نمط حياة الأفراد في المجتمع بشكل فعال، إذ أسفر عن تدفق المعلومات في مختلف المجالات وبالنسبة نقل المجتمع البشري إلى عصر جديد يسمى بـ "مجتمع المعلومات" société de

¹ لمزيد من التفاصيل بخصوص حقوق الإنسان الرقمية les droits de l'homme numériques، راجع يوسف منصورة، "شرعية حجب المواقع الالكترونية بين التشريع الجزائري والمقارن وأثره على حرية التعبير"، دار الخلدونية، دون طبعة، الجزائر، 2022، ص 11.

المجلة الجزائرية للقانون والعدالة

انتقال الهوية الرقمية

l'information¹، والذي يتطور بوتيرة سريعة بفضل الاستخدام المتزايد لتكنولوجيات الإعلام والاتصال قصد الاتجاه نحو رؤية مستقبلية تتضمن مفهوم شامل يتمثل في أن "مجتمع المستقبل هو المجتمع الشامل الرقمي"، La future société du tout numérique².

وبالرغم من أن الإنترنت أصبحت جزءاً أساسياً من حياتنا اليومية على كل المستويات، بل هناك من وصفها " بالتراث الإنساني المشترك"³، باعتبارها ثروة مشتركة للمجتمع البشري، إلا أنها وفي مقابل الإيجابيات الكثيرة التي قدمتها الثورة الرقمية، فإن هذه الأخيرة تنطوي على سلبيات عديدة ومخاطر كانتهاك الخصوصية المعلوماتية، وسرقة بيانات الهوية...إلخ، وذلك نتيجة إساءة استخدام بعض الأشخاص لأنظمة البيانات والمعلومات بإتباع أساليب غير مشروعة، مما كان له تأثير خطير على حقوق الإنسان بصفة عامة وعلى حقوقه الرقمية بصفة خاصة، وهو ما أفضى إلى ظهور الحاجة لوضع قواعد قانونية

¹ - يُعرف مجتمع المعلومات بأنه: " المجتمع الذي يتعامل أفرادُه مع المعلومات بشكل عام وتكنولوجيا المعلومات والاتصال بشكل خاص، في تسيير أمور حياتهم بمختلف قطاعاتها الاقتصادية، الإنمائية، الثقافية، التربوية، الصحية والسياسية"، لامية طالة، "من مجتمع المعلومات إلى مجتمع المعرفة: نحو مقاربة مفاهيمية"، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، المجلد 11، العدد 01، الجزائر، 2021، ص 174.

² - كوثر مازوني، " واقع حقوق الملكية الفكرية في البيئة الرقمية"، دار هومة، الجزائر، 2020، ص 5.

³ . التراث المشترك للإنسانية أو مبدأ التراث المشترك: هو مبدأ من مبادئ القانون الدولي ينص على وجوب حماية مناطق إقليمية محددة وعناصر من التراث المشترك للإنسانية (ثقافية وطبيعية) من استغلال فرادى الدول أو الشركات وإبقائها في أمان للأجيال القادمة. أنظر يوسف منصرة، " التوفيق بين حوكمة الانترنت والأمن السيبراني للدول"، مجلة صوت القانون، جامعة خميس مليانة، العدد 2 لسنة 2023، الجزائر، ص 318.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

ومعايير دولية ملزمة في مجال حماية الحقوق الناجمة عن الهوية الرقمية، عن طريق تجريم الأفعال التي من شأنها الاعتداء على مثل هذه الحقوق، وهو ما بات يعرف بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال¹.

من هذا المنطلق، أثارت مسألة حماية الهوية الرقمية اهتمام المجتمع الدولي في السنوات الأخيرة، وقد تُرجم هذا الاهتمام بتكاثف الجهود الدولية بإبرام اتفاقيات دولية تنص على منع الانتهاكات الحاصلة في مجال حماية الهوية الرقمية والحقوق المترتبة عنها على الأنترنت، وتأكيدا للاهتمام بهذا المجال باشرت العديد من الدول إلى وضع تشريعات تتعلق بالهوية الرقمية تضمن حقوق الأفراد والمؤسسات، كما استدعى الأمر السعي لتحقيق الموازنة بين استخدام التكنولوجيا المتطورة وبين حماية الحق في الحياة الخاصة.

تكمن أهمية هذه الدراسة، في كونها تتعلق بجانب من جوانب تواجد الفرد في الفضاء الافتراضي إذ تأتي في وقت يزداد فيه الاهتمام بحماية الهوية الرقمية، وأصبحت ضرورة ملحة لنشر ما يسمى بثقافة الهوية الرقمية. فالحماية القانونية للهوية الرقمية تعتبر من أبرز مواضيع عصر المعلوماتية إثارة للجدل القانوني بسبب الانتشار السريع للإنترنت الذي أدى إلى ظهور الحاجة إلى وضع حلول للاعتداءات الواقعة عليها. كما يتم تسليط الضوء على جريمة انتحال الهوية الرقمية والأساليب والتقنيات المستخدمة، وتبيان مختلف الأحكام القانونية المطبقة على مرتكبي هذا النوع من الجرائم المستحدثة. ومن هذا المنطلق فإن مسألة حماية الهوية الرقمية على شبكة الأنترنت تثير الإشكالية التالية:

¹ - لمزيد من التفاصيل راجع:

Frédéric DECHAMPS, Caroline LAMBILOT, " Cybercriminalité état des lieux ";Anthémis ;2016 ;p110 .

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

ما مدى مساهمة المشرع الجزائري للتطورات التكنولوجية السريعة في مجال حماية الهوية الرقمية من الاعتداءات الماسمة بها؟
لمعالجة هذه الإشكالية، تم تقسيم الدراسة إلى مبحثين، يتناول المبحث الأول الإطار المفاهيمي للهوية الرقمية، في حين تم تخصيص المبحث الثاني لجريمة انتحال الهوية الرقمية وآليات مكافحتها.

المبحث الأول: الإطار المفاهيمي للهوية الرقمية

أدى التطور التكنولوجي الحاصل في مجال المعلومات إلى تطور مفهوم الهوية من وضعيتها التقليدية (في العالم المادي)¹، إلى وضعيتها الحديثة (في العالم اللامادي) وهو الأمر الذي نشأ عنه بروز صورة مستحدثة للهوية أفرزتها البيئة الرقمية وظهور ما يسمى بـ " الهوية الرقمية "، هذه الأخيرة أصبحت اليوم تحتل مكانة هامة في الفضاء الرقمي، ولتحديد إطارها المفاهيمي فإنه يتعين التطرق لمختلف التعاريف وتحديد مكونات الهوية الرقمية (المطلب الأول)، ثم الوقوف على مفهوم انتحال الهوية الرقمية كإحدى صور التعدي على حقوق الشخصية (المطلب الثاني).

¹ - جاء في قرار للمحكمة العليا بأنه يُقصد بهوية الإنسان الخصائص والمعلومات التي تسمح بتعريفه وتمييزه عن غيره وحتى لا يقع الخلط بين الناس فتنشأ صعوبات في متابعة الإجراءات أو تنفيذ الأحكام ألزم المشرع الجهات القضائية التأكد من هوية الأطراف. لتفاصيل أكثر، أنظر جيلالي بغدادي، الاجتهاد القضائي في المواد الجزائية، ج 3، الديوان الوطني للأشغال التربوية، الجزائر، 1996، ص 418.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

المطلب الأول: مفهوم الهوية الرقمية

في الواقع، يَصْغُب وضع تعريف دقيق وشامل للهوية الرقمية إذ تتوسع التعاريف بخصوصها باستمرار ومن الصعوبة وصفها بدقة¹، وأحيانا يتم استخدامها بالتبادل مع مصطلحات أخرى مشابهة. وتبعا لذلك، سنتناول تعريف الهوية الرقمية (الفرع الأول)، تمييزها عن بعض المصطلحات المشابهة (الفرع الثاني)، مكوناتها (الفرع الثالث).

الفرع الأول: تعريف الهوية الرقمية

تعددت التعريفات التي أعطيت للهوية الرقمية، فقد عرّفها الفقيه Olivier ITEANU بالقول: "تعتبر نموذج أو شكل خاص للهوية، ومن المحتمل أن تكون بمثابة مفتاح لفهم المجتمع المعلوماتي"²، كما تم تعريفها أيضا بأنها "مجموعة المعلومات الموضوعية أو الذاتية المرتبطة بشخص ما، والتي تمت رقمنتها بواسطة عملية معلوماتية، بغض النظر عن مؤدي المعالجة، وعملية التجميع، ووجهة البيانات فالهوية الرقمية هي عملية إسقاط الهوية الواقعية للشخص على دعامة رقمية سواء كانت شاملة أو مجزأة"³.

¹ - المدلول اللغوي لمصطلح الهوية حسبما ورد في معجم الوسيط: "هي حقيقة الشيء أو الشخص الذي تميزه عن غيره"، أنظر الويزة حدة، خلفاوي شمس ضيات، الهوية الرقمية في العالم الافتراضي دراسة في الفرص ومخاطر الاستخدام، مجلة رقمنة للدراسات الإعلامية والاتصالية، جامعة الجزائر3، المجلد 02، العدد 03، ديسمبر 2022، ص 38.

² - Olivier ITEANU, L'identité numérique en question, édition EYROLLES, France, 2008, p3.

³ - «L'identité numérique est l'ensemble des informations objectives ou subjectives relatives à une personne, numérisées par un procédé informatique, quels que soient l'auteur du traitement, le procédé de collecte, et la destination de la donnée. L'identité numérique est une projection de l'identité de la personne humaine sur un

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

وفي نفس السياق، أكد جانب من الفقه على هذا المعنى بالقول أن "الهوية الرقمية ليست سوى إسقاط بشكل أو بآخر، للهوية الشخصية"¹. وبالرغم من صعوبة تعريف هذا المصطلح من الناحية القانونية، حاولت بعض التشريعات العربية وضع تعريف له على غرار المشرع الليبي الذي عرّف الهوية الرقمية بأنها "تمثيل رقمي لمعلومات الفرد داخل المجتمع على شبكة المعلومات الدولية بالصيغة التي اعتمدها هذا الفرد والمتوقعة من قبل الآخرين، وقد يكون للفرد أو للجهة هويات رقمية متعددة في المجتمعات الالكترونية المتعددة"².

إلا أن الملاحظ من خلال هذا التعريف أنه حَصَرَ مجال تطبيق الهوية الرقمية على الفرد دون سواه في حين أن هذه الأخيرة تطبق على الشخص

support informatique ; qu'elle soit exhaustive ou parcellaire » ; « L'identité numérique: une projection de l'identité réelle sur les supports numériques, échappant assez majoritairement à la personne ». Nicolas CHAMBARDON, "L'identité numérique de la personne humaine: Contribution à l'étude du droit fondamental à la protection des données à caractère personnel"; thèse doctorat , université de LYON , école doctorale de droit, présenté et soutenue le 27/09/2018, p26, p521.

¹- إبراهيم عطية محمود المهدي، "الحق في الهوية الرقمية في ضوء حماية البيانات الشخصية والخصوصية المعلوماتية دراسة وصفية تحليلية مقارنة"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة دمياط، العدد 84، مصر، جوان 2023، ص 543.

²- المادة الأولى، الفقرة الثامنة من القانون رقم 5 لسنة 2022، بشأن مكافحة الجرائم الالكترونية، منشور في الجريدة الرسمية الليبية لسنة 2023، العدد 1، السنة الأولى، أطلع عليه في موقع: www.Lawsociety.ly على الرابط <https://lawsociety.ly/legislation/> بتاريخ 2024/03/23

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الطبيعي والمعنوي، وكان من المستحسن توظيف مصطلح الشخص لكونه أكثر دقة من حيث المعنى.

من خلال التعاريف السالفة الذكر، يمكن استخلاص أن مفهوم الهوية الرقمية له صلة كبيرة بمفهوم المعطيات الشخصية وحمايتها التقنية، لأنها تعتبر بمثابة رابط تكنولوجي (تقني) ما بين شخصية أو هوية واقعية وشخصية افتراضية، بمعنى آخر أنها تربط بين الشخص وممارساته أو نشاطاته المتعددة على مستوى شبكة الانترنت، أي بمثابة محاكاة للهوية داخل النظام الرقمي، هذا من جهة¹.

ومن جهة أخرى، فإن الهوية الرقمية لها علاقة وطيدة بالخصوصية، باعتبار أن المفهوم يرتبطان بالبيانات الشخصية للفرد ومنع الكشف عن خصوصيته للجميع أي مراعاة ضرورة احترام الخصوصية في جانبها الرقمي وحمايتها من كافة الانتهاكات.

والملاحظ كذلك، أن مجمل التعاريف تتفق على أن الهوية الرقمية هي انعكاس للبيانات الشخصية والمعلومات التي يصرح بها المستخدم إضافة إلى جملة الممارسات والنشاطات التي يقوم بها داخل الفضاء الرقمي.

وفي هذا الصدد، ونظرا لمكانة الهوية الرقمية وأهميتها البالغة على الإنترنت وصفها البعض بأنها بمثابة "ADN الحمض الريبي الرقمي لمستخدم

¹ - شفيقة حداد، أسماء بلاغماس، "الهوية الرقمية و الأمن الهوياتي الجزائري في ظل تحديات المجتمع الشبكي، المجلة الجزائرية للأمن والتنمية، جامعة الحاج لخضر باتنة، المجلد 10، عدد 02، الجزائر، ص 211.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الأنترنت"، لأن العناصر المشكلة للهوية الرقمية تعتبر بمثابة جينات وبالتالي تُكوّن ADN الرقمي للفرد¹.

نستخلص مما سبق أنه ليس من السهل وضع تعريف دقيق لمفهوم الهوية الرقمية نظرا للتغيرات التي يشهدها العصر الرقمي باستمرار ولكن يمكن القول بأن: "الهوية الرقمية هي مجموعة بيانات ومعلومات خاصة بشخص ما، في العالم الرقمي، والتي تسمح بالتعرف عليه عند استخدامه الخدمات والأنظمة والأدوات الرقمية والتي عادة ما تكون في واجهة ملفه الشخصي، فهي تمثيل رقمي حقيقي للشخص تتضمن بيانات واقعية".

الفرع الثاني: الهوية الرقمية للشخص المعنوي

يتمتع الشخص المعنوي بالهوية الرقمية على غرار الشخص الطبيعي، إلا أن تكوين الهوية الرقمية لدى الشخص المعنوي يخضع لجملة من الضوابط التي يتعين على المؤسسة أن تلتزم بها حتى تضع أسسا وبنية تحتية ثابتة لنظام الهوية الرقمية وحتى تكون قادرة على التحكم في مخرجاتها من معلومات وبيانات. ولقد أدى إدخال مختلف التكنولوجيات الحديثة للإعلام والاتصال على مستوى المؤسسات والشركات التجارية سواء في القطاع العام أو الخاص إلى

¹ - Selon Fred Cavazza : «l'identité numérique d'un individu est composée de données formelles (coordonnées, certificats...) et informelles (commentaires, notes, billets, photos ...). Toutes ces brides d'information composent une identité numérique plus globale qui caractérise un individu, sa personnalité son entourage et ses habitudes. Les petits bouts d'identité fonctionnent comme des gènes: ils composent l'ADN numérique d'un individu ».

GeoffreyDorne ; <https://fr.slideshare.net/slideshow/projet-geoffrey/12558113>

اطلع عليه بتاريخ 2023/11/25

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

جعلها أكثر عُرضة للهجمات السيبرانية ومن بينها انتحال الهوية الرقمية للمؤسسات باعتبارها من الأشخاص المعنوية مما يؤدي لإلحاق عدة أضرار لاسيما الأضرار المالية وهذا ما أشارت إليه العديد من الدراسات والإحصائيات. وفي نفس السياق، فإن تعميم استخدام تكنولوجيا المعلومات والاتصالات، ووسائل الدفع الالكترونية، من شأنه مضاعفة إمكانيات تسجيل البيانات وتخزينها مما يشكل تهديدا خطيرا للحريات مما يتعين على المؤسسات اتخاذ كافة التدابير وتعزيز الأمن السيبراني على مستوى أجهزتها. وبالتالي فإن الصفحات التي تقوم الشركات والمؤسسات بإنشاءها على مستوى مواقع التواصل الاجتماعي يمكن كذلك أن تتعرض لاختراقات الكترونية أو انتحال للهوية رقمية كإنشاء صفحة فايسبوك باسم الشركة ونشر محتوى ضار مما يؤدي للأضرار بسمعة الشركة وباسمها التجاري. ومن أمثلة ذلك:

• حالة البنك الأمريكي JPMorgan Chase

في عام 2014، تعرض بنك "جي بي مورغان تشيس" JPMorgan Chase في نيويورك إلى هجوم الكتروني تم على إثرها اختراق بيانات 83 مليون زبون، بما في ذلك الأسماء وعناوين البريد الإلكتروني والعناوين الجغرافية وأرقام الهواتف. وتعتبر أكبر هجمة الكترونية على الإطلاق تعرضت لها أكبر مؤسسة مالية في التاريخ الأمريكي¹.

¹ - علي حميدوش، "الجرائم الاقتصادية الإلكترونية : الدواعي والمآلات والحلول"، مداخلة أُلقيت في إطار أشغال الملتقى الوطني "الأشكال المتعددة للجريمة الاقتصادية والمالية وسبل مواجهتها"، النادي الوطني للجيش ، الجزائر، بتاريخ 23 و24 فيفري 2022.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

● قضية شركة *Hutchinson*

تتمثل وقائعها في قيام الشركة الفرنسية المسماة Hutchinson برفع شكوى ضد احدى العائلات والتي تم تسريحها من الشركة، على إثر قيامها بإنشاء قناة مزيفة باسم الشركة وبشعارها، بإضافة صورة في هيئة شيطان ونشر محتوى ضار على مستوى موقع التواصل الاجتماعي يوتيوب YouTube وإنشاء عدة حسابات وهمية باسم نفس الشركة على مستوى الشبكات الاجتماعية: Vimeo, Twitter, et Google+ ، وقامت محكمة الجناح بباريس بإدانة المتهمه على أساس انتحال الهوية الرقمية للشركة والتشهير بمقتضى أحكام المادة 4-226 من قانون العقوبات الفرنسي وأكدت أن الهوية الرقمية للشخص المعنوي يمكن انتحالها على غرار الشخص الطبيعي لكون الشركة تحوز على بيانات شخصية من شأنها التعرف عليها بصفة مباشرة كرقم التسجيل في السجل التجاري، العلامة التجارية والتي قد تكون مسجلة في المعهد الوطني للملكية الصناعية، رقم التعريف الجبائي، شعار الشركة، كما أن سمعة الشركة قد تعرضت لأضرار¹.

الفرع الثالث: تمييز الهوية الرقمية عن المصطلحات المشابهة

هناك مصطلحات أخرى مشابهة للهوية الرقمية على غرار "المُعَرَّف الرقمي" و "الهوية البيومترية"، مما يثير التساؤل: هل يوجد فرق بين هذه المصطلحات؟

¹ - Tribunal judiciaire de Paris (17e ch.), 11 mars 2022, n° 18-27-1000552, Sté Hutchinson c/ A. K. www.dalloz.fr2024/05/02 اطلع عليه بتاريخ

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

أولاً: تمييز الهوية الرقمية عن المُعرّف الرقمي ID

يوجد تداخل وارتباط بين مصطلحي: الهوية الرقمية والمُعرّف الرقمي أو ما يسمى ID، فغالبا ما يتم استخدام هذا الأخير أي المُعرّف الرقمي كاختصار للهوية الرقمية إذ يُستخدم للمساعدة في تحديد هويتنا الرقمية بمعنى آخر أن طرق تثبيت هوية شخص ما تتم عموما بفضل استعمال سواء IDENTIFIANT - كلمة المرور - الرقم السري وبالتالي هي عناصر من الهوية الرقمية، وأحيانا يتم استخدام مصطلح الهوية الرقمية بالتناوب مع المُعرّف الرقمي أو ما يسمى ID وهو اختصار لكلمة IDENTIFIANT¹.

ثانياً: تمييز الهوية الرقمية عن الهوية البيومترية

تتضمن الهوية البيومترية جميع التقنيات (القياسات الحيوية) التي يمكن من خلالها التعرف على هوية الفرد أو التحقق منه تلقائيا بناء على خصائصه أو معطياته الجسدية أو البيولوجية أو حتى السلوكية: كبصمات الأصابع، التعرف على الصوت وملامح الوجه، قزحية العين، هندسة اليد، والتحليل السلوكي مثل: حركات أصابع اليد على مستوى لوحة مفاتيح جهاز الكمبيوتر، ولقد أكدت اللجنة الوطنية للمعلوماتية والحريات بفرنسا في دراسة لها، أن استخدام التقنيات البيومترية الالكترونية على مستوى الهوية لا يعني بالضرورة أنها تحتوي على هوية رقمية، وعلى العكس من ذلك، لا تتطلب الهوية الرقمية بالضرورة استخدام التقنيات البيومترية².

¹ -www.meltingmots.com

اطلع عليه بتاريخ 2024/03/01 <https://meltingmots.com/abbreviations/identifiant/210>

² - L'utilisation de techniques biométriques au sein d'un titre d'identité n'implique pas forcément qu'il contienne une identité numérique. Inversement une identité numérique ne nécessite pas forcément

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الفرع الرابع: مُكوّنات الهوية الرقمية

مما لا شك فيه أن وضعية الهوية في العالم الافتراضي تكون أكثر تعقيدا مقارنة مع تلك المتواجدة في العالم المادي، وطالما أن مفهوم الهوية الرقمية مرتبط بمفهوم المعطيات الشخصية، فإنه لا بد من التأكيد على أنها تعتبر من عناصر الهوية في جانبها الرقمي بل تشكل إحدى ركائزها لكونها تساعد في تحديد الشخص والتعرف عليه¹.

وعموما، تنقسم العناصر المكونة للهوية الرقمية إلى جزأين:

أولاً: السّمات الرقمية

تتمثل في المعطيات الشخصية كأرقام البطاقات البنكية، بيانات اعتماد تسجيل الدخول للحسابات الشخصية، عناوين البريد الإلكتروني، الرمز السري، اسم الدومين DNS، رقم الهاتف رقم بطاقة التأمين الطبية، عنوان بروتوكول الانترنت... الخ².

وتجدر الإشارة إلى أن عنوان بروتوكول الانترنت³ (adresse IP) يعتبر من البيانات ذات الطابع الشخصي¹، إذ أنه يمكن تحديد الشخص والتعرف عليه

L'utilisation de techniques biométriques. L'identité numérique, commission nationale de l'informatique et des libertés, février 2023, pp 5 et 6
https://www.cnil.fr/sites/cnil/files/2023-03/CNIL_Dossier-thematique_Identite%20numerique.pdf (2024/04/30)

¹- لمزيد من التفاصيل، راجع أرزقي سي حاج محند، "حماية المعطيات ذات الطابع الشخصي في القانون الجزائري والمقارن"، منشورات بغداد، الجزائر، 2023، ص ص 17 و 20.

²- GeoffreyDorne, op cit,p8.

راجع أيضا إبراهيم عطية محمود المهدي، المرجع السابق، ص 550.

³- عنوان بروتوكول الإنترنت IP هو عبارة عن عنوان رقمي يُعين كل جهاز حاسوب على التسلسل الشجري لشبكة الإنترنت يتكون هذا العنوان من أربعة أعداد تتراوح بين 0 و 255، تفصل هذه الأعداد ثلاث نقاط. مثال 123.124.213.122، لمزيد من التفاصيل، أنظر محاربة

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

من خلال عنوان بروتوكول الانترنت². وهذا ما أكدته المحكمة الأوروبية بمقتضى قرار مؤرخ في 19 أكتوبر 2016، بالقول: إن عنوان بروتوكول الانترنت الديناميكي المسجل من طرف موثر خدمة وسائط الإنترنت بمناسبة اطلاع شخص على موقع الإنترنت يعد من المعطيات ذات الطابع الشخصي شرط أن يحوز موثر

الجريمة المعلوماتية، ملحق 4 قاموس المصطلحات المستخدمة في جرائم الحاسوب، مركز البحوث القانونية والقضائية، أشغال الملتقى الدولي بالجزائر، بتاريخ 5-6 ماي 2010، مطبعة دار النخلة، الطبعة الأولى، الجزائر، 2012/2011، ص 355.

¹- عرّف المشرع الجزائري المعطيات ذات الطابع الشخصي ضمن أحكام المادة 3 الفقرة الأولى من القانون 07-18، المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي، ج ر، عدد 34، وفي نفس السياق عرّفت المادة الثانية من الاتفاقية الأوروبية رقم 108 المؤرخة في 28/01/1981 لمجلس أوروبا المتعلقة بحماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، البيانات الشخصية بأنها: " أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه". كما عرفت اللائحة العامة الأوروبية لحماية البيانات الشخصية RGPD مصطلح الشخص الطبيعي الذي يمكن التعرف عليه بأنه " الشخص الذي يمكن تحديده، بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى احد المعرفات، مثل الإسم، ورقم التعريف، وبيانات الموقع أو المعرف عبر الانترنت أو لعنصر محدد أو أكثر خاص بهويته الجسدية أو الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"، انظر: أرزقي سي حاج محند، المرجع السابق، ص 16.

²- اعتبر القضاء الفرنسي أن عنوان بروتوكول الانترنت هو من البيانات ذات الطابع الشخصي، و أن جمع هذه البيانات وتسجيلها يخضع للقواعد القانونية المنصوص عليها ضمن أحكام القانون رقم 1778 المتعلق بالمعلوماتية والملفات و الحريات، إلا أنه في التشريع الجزائري لم يتم توضيح ما إذا يعتبر عنوان البرتوكول من المعطيات ذات الطابع الشخصي حسب التعريف الوارد في القانون رقم 07/18. لمزيد من التفاصيل انظر: واضح الحاج، التنظيم القانوني لعنوان بروتوكول الانترنت، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، ص 2185.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الخدمة على الوسائل القانونية الكافية للتعرف على هذا الشخص بناءً على المعلومات الإضافية التي بحوزته¹.

وانطلاقاً مما سبق ذكره، تعتبر مسألة حماية المعطيات لشخصية كأساس في حماية الخصوصية وبالتالي، إذا لم تحظى هذه الأخيرة بالحماية الكافية فإنه من السهولة الولوج إلى الإنترنت وسرقة هوية الأشخاص دون علمهم أو موافقتهم ودون الحاجة للإلمام بمعلومات كبيرة².

ثانياً: الأنشطة الرقمية

تعتبر الأنشطة الرقمية كأحد عناصر الهوية الرقمية والمقصود بها مجموع البيانات التقنية التي تستخدم لتحديد وتعقب أنشطة الأفراد على الإنترنت ومثال ذلك: الولوج لمواقع التواصل الاجتماعي والأنشطة الرقمية في الفضاء الرقمي كالإعجابات، التعليقات، المنشورات، نشر الصور والفيديوهات، تاريخ اقتناء المشتريات، استعلامات البحث.. الخ.³

المطلب الثاني: انتحال الهوية الرقمية كصورة مستحدثة للإجرام

السيبراني والتعدي على الحق في الهوية الرقمية

إن إساءة استخدام التكنولوجيات الرقمية الحديثة قد ينجم عنه عدة مخاطر واعتداءات ومن بينها انتحال الهوية الرقمية لكونها على غرار الهوية

¹ - أرزقي سي حاج محند، المرجع السابق، ص 25.

² - منى الأشقر جبور، محمود جبور، "البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد"، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت لبنان، 2018، ص 19.

³ - إبراهيم عطبة محمود المهدي، المرجع السابق، ص 550.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الواقعية في العالم المادي¹ قد تتعرض للانتحال من قبل الغير، وعليه يتم التطرق إلى تعريف جريمة انتحال الهوية الرقمية، ثم المراحل المتبعة لارتكاب الجريمة.

الفرع الأول: تعريف جريمة انتحال الهوية على مستوى شبكة

الأنترنت

وردت عدة تعاريف لانتحال الهوية الرقمية، أهمها: "ذلك السلوك الذي يمارسه الشخص الذي يستعمل أو يستغل عمدا البيانات الشخصية لشخص آخر لأغراض غير مشروعة"².

وأكدت اللجنة الوطنية للمعلوماتية والحريات بفرنسا (CNIL)، أن جريمة انتحال الهوية الرقمية تقوم على استعمال البيانات التي تسمح بالتعرف على الشخص دون موافقته، ومن بين هذه البيانات على سبيل المثال: الاسم واللقب، عنوان البريد الإلكتروني، أو حتى الصور الفوتوغرافية، ثم يتم بعد ذلك استخدام هذه البيانات دون علم الشخص وعلى وجه الخصوص التسجيل في هويته للحصول على قرض، أو اشتراك، لارتكاب أفعال غير مشروعة أو الإساءة للسمعة"³.

² «La pratique par laquelle une personne utilise ou exploite sciemment les informations personnelles d'une autre personne à des fins illégales "Olivier ITEANU, op cit, p 139.

³ -Commission nationale de l'informatique et des libertés , انظر الموقع : www.cnil.fr, الرابط <https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite>

تاريخ الاطلاع: 2024/01/15

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

بمجرد استقراء هذه التعريفات المختلفة، فإنه يتبين أنها غير كافية وأن وضع تعريف دقيق وشامل لانتحال الهوية الرقمية ليس بالأمر السهل نظرا للتطور المستمر لتكنولوجيات الإعلام والاتصال، والتي تعتبر الأداة الأساسية لارتكاب هذا النوع من الجرائم من طرف منتحلي الهوية الرقمية، الأمر الذي ساهم بشكل كبير في تطور التقنيات المستخدمة لارتكاب هذا النوع من الإجرام السيبراني، وعلى هذا الأساس أصبح من الضروري وضع تعريف دولي لهذه الجريمة يشمل جميع العناصر المكونة لمفهوم انتحال الهوية الرقمية.

والجدير بالذكر هنا، أن بعض الدراسات صنفت جريمة سرقة الهوية الرقمية ضمن الجرائم المتصلة بالهوية¹. أما المشرع الفرنسي لم يضع أي تعريف قانوني لانتحال الهوية على مستوى شبكة الأنترنت، وقام بتجريمها بموجب قانون LOPPSI2، وبالتالي أصبحت جريمة مستحدثة ضمن قانون العقوبات ومصنفة في إطار الاستعمال عن طريق الغش لمعطيات ذات طابع شخصي².

وفي نفس السياق، اعتبر Solange GHERNAOUTI أن جريمة انتحال الهوية الرقمية هو شكل من أشكال الجرائم الواقعة على الهوية وعبر عليها بمصطلح Criminalité identitaire، مشيرا إلى أن هذا النوع من الإجرام في تصاعد مستمر وقد يتخذ عدة صور سواء: إنشاء هوية مزيفة على مستوى مواقع التواصل الاجتماعي، أو سرقة بيانات شخصية: رقم التأمين الاجتماعي،

¹- "دراسة شاملة عن الجريمة السيبرانية"، دراسة معدة من قبل الفريق الدولي للخبراء التابعين لمكتب الأمم المتحدة المعني بالمخدرات والجريمة نيويورك، 2013، ص142، انظر

<https://www.unodc.org/documents/organized->

[crime/cybercrime/Cybercrime_Study_Arabic.pdf](https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Arabic.pdf)، تم الاطلاع عليه بتاريخ 2024/04/30.

² - Loi n° 2011-267, du 14 mars 2011, d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure dite (LOPPSI2). <http://www.legifrance.gouv.fr/>

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

رقم جواز السفر، رقم بطاقة التعريف، الرقم التعريفي لبطاقة الطالب، رقم بطاقة الائتمان الالكترونية، رقم الحساب البنكي، الرقم السري لحساب أو بريد الكتروني، الرقم الوطني التعريفي، أو في صورة شراء أملاك أو خدمات باسم الضحية¹، في حين اعتبر البعض الآخر، أن جريمة انتحال الهوية الرقمية تُعدّ من بين جرائم انتهاك خصوصية الهوية الرقمية أو الخصوصية المعلوماتية².

الفرع الثاني: مراحل انتحال الهوية الرقمية

يتطلب ارتكاب جريمة انتحال الهوية الرقمية المرور بمرحلتين أساسيتين:

أولاً: مرحلة الحصول على المعطيات الشخصية للهوية الرقمية وجمعها

ينصب هذا الفعل على استرجاع المعطيات ذات الطابع الشخصي بكافة الطرق غير المشروعة عبر الأنترنت، الأداة الأكثر سهولة لجمع المعطيات الشخصية، إذ يتم تنفيذ الجريمة في وقت وجيز، بدون أي مقابل مالي. وللوصول إلى البيانات الشخصية للمستخدمين يقوم المجرمون السيبرانيون بتنفيذ هجمات عن طريق برامج ضارة تستهدف هذه البيانات، لاسيما على شبكات التواصل الاجتماعي، أو عند ملأ استمارة أو نموذج عبر الانترنيت. ومن بين الحالات التطبيقية حالة شركة مجموعة ياهو **groupe Internet Yahoo** ، بحيث أعلنت هذه الشركة عن تعرضها لهجوم الكتروني خلال سنة 2013، أسفر عن سرقة البيانات الشخصية للمستخدمين من خلال

¹-Solange GHERNAOUTI, la cybercriminalité les nouvelles armes de pouvoir, édition 2018, ITCIS.Algerie , p111.

²- مسعودة طلحة، الهوية الرقمية " مآزق الاستخدام والخصوصية "، مجلة التغير الاجتماعي، جامعة بسكرة، المجلد 04، العدد 01، 2020، ص ص 144.142.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

حساباتهم الإلكترونية والتي بلغت أكثر من 3 مليارات حساب الكتروني، أين تمكن المجرمون السيبرانيون من الوصول إلى بيانات شخصية مهمة للمستخدمين، كعناوين البريد الإلكتروني أو أرقام الهواتف، كلمات المرور، ومن المحتمل أن يتم استخدامها بطريقة مستهدفة لسرقة الهوية الرقمية، ولم يتم اكتشاف الأمر من طرف الشركة إلا خلال سنة 2017¹.

ثانياً: مرحلة استعمال واستغلال المعطيات الشخصية التابعة للغير لارتكاب إساءة أو احتيال

تتمثل هذه المرحلة في استغلال المعطيات ذات الطابع الشخصي للغير والتي تم تحصيلها وجمعها من طرف الجناة لسرقة الهوية إذ تتيح هذه البيانات المسروقة إمكانية تقديم طلبات شراء للسلع نيابة عن الضحية ونشر معلومات كاذبة تهدف إلى الإضرار بسمعة بعض الأشخاص أو ترهيبهم، ونذكر على سبيل المثال: استعمال بطاقات الائتمان البنكية لأغراض غير مشروعة، التصرف في بيانات الهوية وبيعها للغير، فتح حسابات جديدة.

الفرع الثالث: أركان جريمة انتحال الهوية الرقمية

نتعرض إلى الركن الشرعي والمادي والمعنوي والعقوبة المقررة.

أولاً: الركن الشرعي

استناداً إلى مبدأ الشرعية فإنه لا يعاقب الشخص على فعل معين إلا بمقتضى نص قانوني يجرم ذلك الفعل وانتحال الهوية الرقمية هي جريمة معاقب عليها في بعض التشريعات المقارنة على غرار التشريع الفرنسي، إذ تم تجريم فعل انتحال الهوية الرقمية لأول مرة سنة 2011، بمقتضى قانون

نفس المرجع السابق Reinhold Sojer. l'usurpation d'identité sur Internet¹

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

(LOPPSI 2)، والذي بموجبه تم إدراج المادة 1-4-226 ضمن أحكام قانون العقوبات الفرنسي¹.

وقد قامت بعض التشريعات العربية بتجريم فعل انتحال الهوية الرقمية على غرار التشريع الإماراتي بموجب قانون مكافحة جرائم تقنية المعلومات²، أما المشرع الجزائري فلم يقدّم بإدراج أحكام جزائية تُجرّم فعل انتحال الهوية الرقمية على شبكة الإنترنت سواء من خلال قانون العقوبات أو القوانين الخاصة المتعلقة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام، واكتفى بتجريم فعل انتحال الهوية في صورتها التقليدية أي في العالم المادي (انتحال صفة الغير)، وسنّ لها أحكام جزائية بمقتضى المواد 242 إلى 253 مكرر من القسم الثامن المعنون انتحال الوظائف والألقاب أو الأسماء أو إساءة استعمالها من قانون العقوبات.

¹ Loi n° 2011-267, op cit .

يتعين الإشارة إلى أن المشرع الفرنسي أضفى الوصف الجنحي على هذه الجريمة وقَرَّرَ عقوبة سنة حبس و15000 أورو غرامة مالية على مرتكبها إذا قام بانتحال هوية الغير أو استعمال معطيات أو عدة معطيات مهما كانت طبيعتها من شأنها التعريف بالشخص والتي تؤدي إلى الإخلال بالطمأنينة، أو المساس بشرفه أو باعتباره، وتطبق نفس العقوبة إذا ارتكبت الجريمة عن طريق شبكة اتصالات موجهة للعامة على الخط.

² قام المشرع الإماراتي بتجريم بعض الأفعال المتعلقة بانتحال الهوية الرقمية على غرار الاعتداء على البيانات الشخصية وقرر عقوبة الحبس لمدة لا تقل عن 6 أشهر و غرامة لا تقل عن 500.000 درهم ولا تزيد عن 3.000.000 درهم أو بإحدى هاتين العقوبتين (المادة 6) ، كما عاقب على التحايل على عنوان بروتوكول الانترنت بالسجن المؤقت و غرامة لا تقل عن 500.000 درهم ولا تزيد عن 2.000.000 درهم أو بإحدى هاتين العقوبتين (المادة 10) مرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الالكترونية.

ثانياً: الركن المادي

يتمثل الركن المادي لجنحة انتحال الهوية الرقمية في السلوك الإجرامي،
النتيجة والعلاقة السببية بينهما.

ويكمن السلوك الإجرامي في قيام الجاني أو المجرم السيبراني بجمع
وسرقة المعطيات الشخصية، واستعمال واستغلال تلك المعطيات التابعة للغير
لارتكاب إساءة أو احتيال أي لأغراض غير مشروعة، ويُشترط تحقيق نتيجة وهي
الأثر الذي يحدث نتيجة السلوك الإجرامي ولا يشترط أن يكون مادياً بل يمكن
أن يكون معنوياً، كتشويه سمعة الضحية في الفضاء الرقمي، أو ما يسمى
بالسمعة الالكترونية، كما يتعين تحقق العلاقة السببية وهي الصلة التي تربط
بين السلوك والنتيجة، فلا بد أن يكون فعل الجاني قد تسبب في إحداث النتيجة
طبقاً للقواعد العامة¹.

ولمزيد من التوضيح، سنتطرق لمختلف الأساليب والتقنيات المستخدمة
لانتحال الهوية الرقمية على الإنترنت و على مستوى مواقع التواصل الاجتماعي
والمتمثلة في:

1. تقنيات جمع عناصر الهوية الرقمية

هناك عدة تقنيات لجمع عناصر الهوية الرقمية على غرار تقنية التصيد
الاحتيالي، وتقنية استزراع نطاق اسم الدومين، وتقنية محاكاة البريد
الالكتروني.

¹-www.dalloz.fr

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

1.1 تقنية التصيد الاحتيالي الإلكتروني (Phishing)

يعتبر التصيد الاحتيالي من أخطر الهجمات الإلكترونية التي يستخدمها المجرمون السيبرانيون لسرقة البيانات الشخصية والمالية للأفراد والشركات، لاسيما مع استخدام الإنترنت والتقنيات الحديثة في حياتنا بشكل يومي التي أدت إلى تزايد المخاطر الرقمية.

تتضمن هجمات التصيد الاحتيالي استخدام الخدع والأساليب الاحتيالية لإيهام الأفراد بأنهم يتفاعلون مع جهة موثوقة وغير مشبوهة، مثل: البنوك، شركات البريد الإلكتروني، أو حتى مواقع التواصل الاجتماعي.

ويُعرف التصيد الاحتيالي الإلكتروني، على أنه: "محاولة الحصول على المعلومات الخاصة بمستخدمي الأنترنت (معلومات شخصية ككلمة المرور أو مالية كرقم البطاقة المصرفية) عن طريق الرسائل الإلكترونية، أو مواقع الأنترنت وذلك بإيهام الضحية أن مصدرها شركات موثوقة أو مؤسسات مالية وحكومية كالبنوك الإلكترونية"¹.

وأشارت منظمة التعاون الاقتصادي والتنمية (L'OCDE) من خلال تقريرها المنشور سنة 2008 بخصوص سرقة الهوية على الأنترنت، إلى تعريف التصيد الإلكتروني على أنه: "كل اكتساب، أو تحويل، أو حيازة أو استخدام غير مرخص به لمعلومات شخصية سواء تتعلق بشخص طبيعي أو معنوي بغرض استغلالها لأغراض إجرامية، أو ارتكاب أفعال احتيالي أو أية أفعال أخرى"².

¹ - محاربة الجريمة المعلوماتية ، ملحق رقم 4 من قاموس المصطلحات المستخدمة في جرائم الحاسوب، مرجع سابق، ص 363 .

² - Rapport OCDE, Le vol d'identité en ligne

<http://www.oecd.org/dataoecd/3/8/40699509.pdf> chrome-

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

أما اللجنة الوطنية للمعلوماتية والحريات بفرنسا (CNIL) فقد عرفت التصيد الإلكتروني على أنه: " كل استخدام للبيانات التي من شأنها التعريف بالشخص، دون موافقته، قد تتعلق على سبيل المثال: بالاسم واللقب، عنوان البريد الإلكتروني، صور... الخ وهذه البيانات يتم استخدامها من طرف الفاعل من أجل الاستيلاء على حساب بنكي، أو اشتراك أو لأغراض إجرامية أخرى، أو قصد الإساءة لسمعة الشخص"¹.

وجاء في تعريف آخر: "التصيد الإلكتروني يعتبر من بين تقنيات الهندسة الاجتماعية تستعمل من طرف المحتالين من أجل الحصول على معلومات شخصية بغرض انتحال هوية الغير عن طريق إيهام الضحية بأنها تتعامل مع شخص محل ثقة أي موثوق فيه على غرار البنك، الإدارة،... الخ بغرض الابتزاز وانتزاع منه معلومات شخصية، كلمة المرور، أرقام بطاقة الائتمان، تاريخ الميلاد... الخ، وهو شكل من أشكال الهجوم المعلوماتي الذي يستند أساسا على الهندسة الاجتماعية، ويمكن تنفيذ عملية التصيد الإلكتروني عن طريق البريد الإلكتروني، أو مواقع واب مزيفة، أو بأي وسيلة الكترونية أخرى"².

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oecd.org/content/dam/oecd/fr/publications/reports/2012/06/report-on-consumer-protection-in-online-and-mobile-payments_g17a2193/5k948kg5ftq5-fr.pdf2024/02/15 اطلع عليه بتاريخ

¹ - CNIL, Usurpation d'identité en question <http://www.cnil.fr/vos-libertes/vos-droits/details/article/lusurpation-didentite-en-questions/> اطلع عليه بتاريخ 2024/02/03

² - Myriam Quémener, Yves Charpenel. Cybercriminalité droit pénal appliqué, Edition ECONOMICA, France, 2010, p253.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

وفي نفس السياق، اعتبر الخبراء أن التصيد الالكتروني هو شكل من أشكال هجمات الهندسة الاجتماعية أو ما يسمى بـ ¹social engineering وتجدد الإشارة إلى أن حالات التصيد الالكتروني قد ارتفعت خلال فترة تفشي هذا الوباء العالمي كوفيد-19²، إذ بلغت مستويات قياسية حسب آخر الإحصائيات، لاسيما نتائج الإحصائيات المسجلة خلال سنة 2020 إذ ارتفعت محاولات التصيد الالكتروني بنسبة 600 بالمائة منذ نهاية شهر فبراير، و11 بالمائة من مستخدمي الانترنت وقعوا ضحايا لسرقة البيانات الشخصية، وأن الهجمات الالكترونية التي يتم تنفيذها بواسطة رسالة البريد الالكتروني قد بلغت نسبة 75 بالمائة³.

¹ - سيرجيو بيلغاكوف، مداخلة بعنوان "استرداد الأصول من الدول الأجنبية: تجربة روسيا الاتحادية، المشاكل والاتجاهات الحالية"، أشغال الندوة المنظمة من طرف وزارة العدل الجزائرية حول التجربة الروسية في مجال مكافحة الجرائم المعلوماتية ومكافحة الفساد في إطار التعاون مع الفيدرالية الروسية (أعضاء من النيابة العامة الروسية)، إقامة القضاة، الجزائر، 2023/12/27.

تم تعريف الهندسة الاجتماعية social engineering على أنها: «وسيلة تستعمل من أجل التأثير على الأشخاص واستدراجهم لإفشاء معلومات سرية، بدلا من استخدام تقنيات القرصنة المعتادة، وينطبق المصطلح عادة على الدّهاء والخداع بغرض جمع المعلومات والاحتيال، أو الوصول إلى النظام المعلوماتي، في معظم الحالات لا يضع المحتال نفسه وجها لوجه مع الضحية"، أنظر محاربة الجريمة المعلوماتية، ملحق رقم 4 قاموس المصطلحات، المرجع السابق، ص 363.

² - Myriam QUEMENER ; "La cybercriminalité à l'heure de la Covid-19".

<https://cybercircle.com/la-cybercriminalite-a-lheure-de-la-covid-19-par-myriam-quemener-magistrat-docteur-en-droit/>. اطلع عليه بتاريخ 2024/04/30

³ - www.fintechnews.org الرابط <https://www.fintechnews.org/more-than-70-of-online-marketplaces-and-half-52-of-financial-services-organisations-have->

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

وهذا راجع إلى عدة عوامل ومن أهمها زيادة استخدام الأشخاص لشبكة الأنترنت قصد الاستفادة من الخدمات الالكترونية، التعليم الالكتروني، التجارة الالكترونية... الخ نتيجة فرض حالة الحجر الصحي من طرف السلطات بسبب انتشار جائحة كورونا بين مختلف فئات المجتمع، مما دفع بالمجرمين السيبرانيين إلى استغلال الفرصة والظروف المحيطة بتفشي فيروس الوباء العالمي كوفيد 19، لتنفيذ هجماتهم السيبرانية لاسيما التصيد الالكتروني بمختلف تقنياته.

كما أكدت الإحصائيات الصادرة سنة 2020 عن منظمة الانتربول وجود زيادة في الهجمات السيبرانية مع انتشار وباء كوفيد 19، على غرار هجمات الفدية والبرامج الخبيثة بنسبة 36%، المعلومات المزيفة (14 %)، وكذلك زيادة حالات التصيد الالكتروني بنسبة 59%¹. أما الإحصائيات الصادرة سنة 2021 عن مجموعة العمل لمكافحة التصيد الاحتيالي APWG أشارت إلى زيادة في معدلات التصيد الاحتيالي للمواقع الالكترونية خلال الربع الثاني من سنة 2021².

وفي الواقع، تتخذ تقنية التصيد الاحتيالي أثناء تنفيذها صور عديدة ومختلفة، ولكن نذكر الأكثر شيوعا وهي: التصيد الاحتيالي من خلال البريد الالكتروني (أ)، التصيد الاحتيالي من خلال الرسائل النصية (ب)، التصيد الاحتيالي من خلال الاتصالات الصوتية (ج)، والتي يتم تفصيلها كما يلي:

اطلع عليه بتاريخ [increased-adoption-of-id-verification-as-a-result-of-the-pandemic/](https://www.interpol.int/en/News-and-media/Press-releases/2024/03/25/increased-adoption-of-id-verification-as-a-result-of-the-pandemic/)
2024/03/25

¹ - انظر موقع الأنتربول: www.interpol.int تاريخ الاطلاع 2024/01/15 .

² - انظر موقع مجموعة العمل لمكافحة التصيد الاحتيالي APGW: [WWW.APGW.ORG](https://www.apgw.org) تاريخ الاطلاع 2024/01/24 .

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

أ. التصيد الاحتيالي الإلكتروني بواسطة البريد الإلكتروني (Phishing):
يعتبر البريد الإلكتروني¹ اليوم من أهم وسائل الاتصال بين الأشخاص عن طريق شبكة الاتصالات الدولية " الانترنت"، وقد حقق نقلة نوعية في عالم الاتصالات الحديثة واتسع نطاق استخدامه في شتى المجالات وكافة الأجهزة والقطاعات الخاصة والحكومية وأصبح بديلا عن وسائل الاتصال الأخرى كالهاتف. ويتشكل المصطلح ذو الأصل الإنجليزي Phishing نتيجة دمج كلمتين هما: (fishing) معناه الصيد، (phreaking) ويعني قرصنة الخطوط الهاتفية².
وقد تم استحداث هذا المصطلح من طرف القراصنة المعلوماتيون في سنة 1996 والذين قاموا بتحويل حسابات شركة أمريكية مختصة في تقديم

¹ - تم تعريف البريد الإلكتروني E-mail ضمن أحكام المادة الأولى من القانون الفرنسي رقم 575-2004 المؤرخ في 2004/01/22 بشأن الثقة في الاقتصاد الرقمي بأنه " كل رسالة، أيا كان شكلها نصية، أو صوتية، أو مصحوبة بصور أو أصوات، يتم إرسالها عبر شبكة عامة للاتصالات، ويتم تخزينها على أحد خوادم هذه الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها".

وتجدر الإشارة إلى أنه اعتبرت مختلف التشريعات المقارنة، البريد الإلكتروني وأسماء النطاق (الموقع الإلكتروني)، كمصنفات رقمية في شبكة الأنترنت على غرار المشرع الأمريكي من خلال القانون الصادر سنة 1986، والقانون الفرنسي المؤرخ في 2004/06/22، لمزيد من التفاصيل أنظر ليندة رقيق، "القرصنة الإلكترونية لحقوق الملكية الأدبية والفنية"، أشغال الملتقى الوطني الافتراضي حول: الجرائم الماسة بالملكية الفكرية وآليات مكافحتها، دار بيت الأفكار، الطبعة 1، الجزائر، سبتمبر 2022، ص 128.

² - قرصنة خطوط الهاتف أو ما يسمى ب (phreaking): كلمة انجليزية مدمجة في اللغة الفرنسية، وهي تقنية قرصنة تمس أنظمة "تبادل الافرع الأتوماتيكي الخاص " PABX يتمثل هدفها الأساسي في استعارة الأرقام الخضراء من اجل إجراء اتصالات هاتفية لمسافات بعيدة مجانا، أنظر محاربة الجريمة المعلوماتية، ملحق رقم 4 قاموس المصطلحات، المرجع السابق، ص 362.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

خدمات الانترنت تسمى شبكة أمريكا أون لاين (AOL) عن طريق الاحتيال بالاتصال بالضحايا أين تم إيهامهم أنهم موظفين لدى شركة (AOL) للتحقق من كلمات المرور للمستخدمين فتمكنوا من استخدامها لأغراض إجرامية¹.

في هذا الصدد، لتنفيذ تقنية التصيد الالكتروني عن طريق البريد الالكتروني من طرف المجرم المعلوماتي يتعين عليه المرور بالمراحل التالية:

-المرحلة الأولى: تتمثل أساسا في إرسال رسالة عن طريق البريد الالكتروني تتضمن مضمون شبيه جدا للرسائل المرسلة من طرف البنك وذلك بإعادة تشكيل نفس خصائص ذلك البنك: مثل الألوان ،الشعار (logo) ،اللغة ،الرسومات (graphisme) ،...الخ، حتى يتم إيهام المرسل إليه أو الضحية بأنها رسالة مرسلة من طرف بنكه.

-المرحلة الثانية: وهي مرحلة تلقي البريد الالكتروني من طرف الضحية والذي يقوم مباشرة بإرسال معطيائه الشخصية كما طلب منه سواء عن طريق الرد على البريد الالكتروني أو بالنقر مباشرة على الرابط الذي تضمنته تلك الرسالة الوهمية.

-المرحلة الثالثة: تتمثل في استقبال المجرم المعلوماتي أو ما يطلق عليه مصطلح: hameçonneur للمعطيات الشخصية للضحية عن طريق تلك الرسالة أو الموقع الوهمي للبنك، وقيامه مباشرة بجمع واستغلال تلك المعطيات الشخصية لأغراض غير شرعية.

¹-Bahmed et Hassane Boumriga ; la protection de la vie privée dans un système de gestion d'identité ;master ; Universite Abou Bekr Belkaid Tlemcen Algerie ;2012 ;p16
https://www.memoireonline.com/01/14/8693/m_La-protection-de-la-vie-privee-dans-un-systeme-de-gestion-d-identite7.html

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

ومن الناحية التقنية، فإنه لتنفيذ عملية التصيد الالكتروني يتطلب الأمر استعمال البريد غير مرغوب فيه¹ (spam)، أو البرامج الخبيثة (logiciels malveillants)²، واللذان يعتبران كقاعدة أساسية لتنفيذ مختلف الأساليب التقنية التي يستخدمها المجرمون المعلوماتيون لسرقة الهوية الرقمية للغير.

من خلال هذه المراحل، نستخلص أن تقنية التصيد الالكتروني تتمثل أساسا في إرسال رسالة بريد الكتروني E-mail إلى مستخدم عن طريق إعادة إرسالها لمؤسسة أو شركة، وفي هذه الحالة فإن عنوان البريد الالكتروني يمثل هذه المؤسسة أو الشركة أو يعيد تشكيل رمزها أو تسميتها، ويقوم بتوجيه المستخدم على موقع ويب وهمي قصد تضليله، ويطلب من المستخدم إدخال بياناته الشخصية الخاصة، فبمجرد تلقي المستخدم رسالة البريد الالكتروني يتبادر إلى ذهنه أنها صحيحة لكونها تشبه تماما رسائل البريد الالكتروني التي اعتاد التعامل معها والمرسلة من طرف أحد متعامليه كالبنك مثلا، وفي الواقع، إن رسالة الإيمايل غير صحيحة، وتم إرسالها من طرف المجرم السيبراني لغرض قرصنة البيانات الشخصية واستخدامها لأغراض إجرامية غير مشروعة .

ومن أشهر الطرق المتبعة من طرف المجرمين السيبرانيين للاحتيال الرقمي بواسطة البريد الالكتروني عبر تقنية التصيد الالكتروني نذكر على سبيل المثال:

¹ - تعريف البريد غير المرغوب فيه (spam): " البريد المزعج عبارة عن بريد الكتروني غير مرغوب فيه من طرف المرسل إليه قد يتضمن معلومات اشهارية أو محتوى على برامج خبيثة "، انظر محاربة الجريمة المعلوماتية، ملحق رقم 4 قاموس المصطلحات، المرجع السابق، ص 364 .

² - البرامج الخبيثة Malware: " هو دمج لكلمتين "خبيث" Malicious وبرمجية Software يشير هذا المصطلح إلى البرامج المصممة خصيصا لإفساد أو عرقلة الاشتغال العادي لنظام ما مثل: الفيروسات، الديدان، أحصنة طراودة، وكذا جافا سكريبت"، انظر محاربة الجريمة المعلوماتية، ملحق رقم 4 قاموس المصطلحات، المرجع السابق، ص 362.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

-إرسال رسالة مجهولة للبريد الالكتروني التابع للضحية تتضمن روابط مسابقات أو جوائز مغرية كالحصول على مبلغ مالي ضخيم، أو الفوز بعطلة في احد الفنادق الفخمة، أو المشاركة في حملات تبرع وهمية لمساعدة المنكوبين جراء كوارث طبيعية مثلا، وبعد قيام الضحية بالضغط على الرابط المرسل، يُطلب منه إدخال بعض البيانات الشخصية كالاسم، ورقم البطاقة الائتمانية، وفي أغلب الأحيان قد يطلب منه مبلغ زهيد مقابل الاشتراك بالمسابقات مما يؤدي لتعرض البيانات الشخصية للضحية للخطر وفريسة للاحتيال الالكتروني، إذ يمكن للمجرم السيبراني إجراء تحويلات مالية من حساب الضحية بسرعة كبيرة دون أن يعلم هذا الأخير بالأمر في الوقت المناسب.

-إرسال المجرم السيبراني لبريد الالكتروني مزيف يتبين للضحية للوهلة الأولى على أنه مرسل من جهة رسمية، أو زميل، إلا أنها في الواقع محاولة لعملية احتيال رقمي عن طريق التصيد الالكتروني، فمثلا يكون مضمون الرسالة هو طلب تغيير كلمة المرور الخاصة بالضحية على حساب البايبال PayPal وإيهامه بأنه توجد محاولة لاختراق حسابه، ويطلب منها إرسال بيانات شخصية محددة وحساسة ويتبين للضحية للوهلة الأولى أن الرسالة صادرة من الموقع الرسمي نفسه، الأمر الذي يؤدي إلى وجود احتمال كبير لاستجابة الضحية لمحتوى الرسالة الالكترونية وإدخال كلمة مرور جديدة، الأمر الذي يسمح باستخدامها بسهولة من طرف المجرمون السيبرانيون .

- إنشاء تطبيقات مقرصنة من طرف المجرمون السيبرانيون قابلة للتحميل على أجهزة الهواتف الذكية وعند قيام الضحية بتثبيتها على الهاتف النقال والضغط على روابط مجهولة دون معرفة مصدرها، مما يؤدي إلى اختراق واستغلال

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

البيانات الشخصية كالملفات الهامة والصور وسرقة كلمات المرور وأرقام البطاقات الائتمانية والبنكية¹.

وتماشيا مع ما تم ذكره، فبمجرد تفحص دقيق لرسائل التصيد الالكتروني المرسله من طرف المجرم السيبراني يتضح وجود علامات تشير إلى أن الرسالة الالكترونية هي مزيفة من خلال مضمونها، بالمقارنة مع الرسالة الالكترونية المرسله من طرف جهة رسمية وموثوقة، وتتمثل هذه العناصر فيما يلي:

- مقدمة الرسالة لا تحتوي على اسم المستقيل.
- عنوان المرسل غير تابع للشركة الرسمية ويتم إرسال الرسالة الالكترونية كنسخة مخفية.
- في نص الرسالة يطلب من المرسل إليه تحميل المرفقات وهو الأمر الذي يختلف تماما عن رسائل التأكيد الرسمية.
- رسائل التأكيد لا ترسل مع تنبيهات الدخول على الحساب².
- من خلال التمعن في التقنيات السالفة الذكر أو الأشكال المختلفة للتصيد الالكتروني يمكن القول أن التصيد الاحتيالي الالكتروني يعتبر من أسهل الهجمات السيبرانية تنفيذا، وذلك لان المجرم السيبراني لا يحتاج إلى دراية كبيرة

¹ - هيئة الحكومة الرقمية، الاحتيال الرقمي دراسة بحثية، بتاريخ 2023/08/01، رقم الإصدار 1.0 متوفرة على الرابط: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dga.gov.sa/sites/default/file s/2023- pdf. تاريخ الاطلاع 2024/09/19 .

² - لمزيد من التفاصيل حول نموذج لرسالة الكترونية مزيفة مرسله عبر البريد الالكتروني باستخدام تقنية التصيد الالكتروني بواسطة البريد الالكتروني، أنظر موقع مبادرة العطاء الرقمي لنشر الوعي التقني www.attaa.sa

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

بهذا المجال كأن يكون مبرمج أو مخترق محترف. كما أننا نلاحظ أن هذه الهجمات تتشابه في استخدامها استراتيجيات احتيالية تستدرج المستخدمين إلى تقديم معلوماتهم الشخصية مثل: الأسماء، العناوين، رقم الهاتف، رقم الهوية الرقمية الوطنية، بيانات الحسابات المصرفية والبطاقات الائتمانية...إلخ. ولتفادي الوقوع كضحية لهذه التقنية فإنه من بين التوصيات والنصائح المقدمة من طرف اللجنة الوطنية للمعلوماتية والحريات بفرنسا هو ضرورة تأمين البريد الإلكتروني، كما يُنصح بعدم الرد على رسائل البريد المشبوه في صحتها وعدم إرسال المعطيات الشخصية عن طريق البريد الإلكتروني لأنها الوسيلة الأسهل لحفظ وجمع تلك المعطيات وإعادة استغلالها قصد انتحال الهوية الرقمية من طرف الجناة.

ب. التصيد الاحتيالي عبر الرسائل النصية¹ (Smishing):

يقوم المجرمون السيبرانيون بواسطة هذه التقنية بإرسال رسالة نصية قصيرة (sms) إلى هاتف المستخدم قصد إيهامه أنها من البنك تتضمن طلب تحديث بيانات حسابه البنكي مرفقا برابط مزيف قصد استدراج المستخدم إلى النقر على ذلك الرابط لتقديم بياناته الشخصية والمالية .

ج) التصيد الاحتيالي عبر الاتصالات الصوتية² (Vishing):

تستخدم هذه الهجمات الاتصالات الهاتفية الصوتية لإيهام المستخدمين بأنهم يتفاعلون مع جهة موثوقة، مثل البنوك أو شركات الخدمات المالية؛ حيث يتم استخدام تقنيات التلاعب الصوتي والمعلومات المزيفة لإقناع المستخدمين

¹ - أنظر موقع شركة تصميم وتطوير تقنيات حديثة للأمن السيبراني WWW.CEREBRA.SA

اطلع عليه بتاريخ 2024/02/25 .

² المرجع السابق.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

بتقديم معلوماتهم الشخصية والمالية، مثل الرقم السري للحساب المصرفي أو رقم الهوية الوطنية أو رمز التحقق...الخ

2.1 تقنية استزراع نطاق اسم الدومين (pharming):

تُعدّ هذه التقنية من أكثر التقنيات استخداما لانتحال الهوية الرقمية على مستوى الأشخاص المعنوية: المؤسسات والشركات، والتي من خلالها يتم قرصنة نظام اسم الدومين أو ما يسمى باسم النطاق¹ على مستوى شبكة الانترنت التابع للمؤسسات أو الهيئات إذ يقوم المجرم المعلوماتي أو منتحل الهوية الرقمية بقرصنة اسم الدومين الخاص بمؤسسة وإنشاء موقع يشبه الموقع الرسمي لتلك المؤسسة، وبالتالي فإن ضحايا تقنية انتحال اسم الدومين هم في أغلب الأحيان بنوك أو مؤسسات مالية.

من خلال هذه التقنية يقوم القراصنة بوضع برنامج خبيث أو ما يسمى ²code malveillant لكي يتمكنوا من توجيهه أو استدراج الضحايا نحو موقع وهمي بالرغم من أن الضحايا قاموا بإدخال اسم الدومين الصحيح التابع للبنك. وتتخذ هذه التقنية عدة صور إلا أن الصورة الأكثر انتشارا وهي الطريقة الأسهل والأكثر استعمالا يطلق عليها تسمية Fichiers Host أو ما يسمى

¹- تُعرف أسماء النطاق كذلك باسم الموقع الإلكتروني وتعتبر من المصنفات الرقمية لشبكة الانترنت، وهي: " عبارة عن عنوان فريد ومتميز يتكون من عدد من الأحرف الأبجدية أو الأرقام التي يمكن بواسطتها الوصول لأحد المواقع على شبكة الأنترنت وتعتبر أسماء النطاق عنوان الأنترنت تتكون من أجزاء متعددة أكثرها أهمية الجزء الأخير في العنوان وهو المعروف من قبل المستخدمين مثل: gov - com - org - Edu. لتفاصيل أكثر راجع ليندة رقيق، المرجع السابق، ص 128.

²- برنامج خبيث أو ما يسمى code malveillant: " كل برنامج يهدف إلى إحداث ضرر بنظام معلوماتي أو شبكة"، أنظر محاربة الجريمة المعلوماتية، ملحق رقم 4 قاموس المصطلحات، المرجع السابق، ص 357.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

بـPharming Local، وتتطلب هذه التقنية وضع برنامج خبيث على مستوى كمبيوتر الضحية يسمى بحصان الطراودة¹ (cheval de Troie)، وعندما يقوم الضحية بتصفح أي عنوان على مستوى شبكة الانترنت يتم توجيهه نحو موقع وهمي، ومن بين التطبيقات القضائية لتقنية استزراع اسم الدومين، قضية انتحال نطاق اسم الدومين «Louisl.fr» أين قضت محكمة الاستئناف الكبرى في سان مالو Saint-Malo بفرنسا، بالزام احد المترشحين للانتخابات البلدية بدفع تعويض مالي قدره 10000 أورو عن كافة الأضرار اللاحقة بسبب قيامه بعملية تسجيل عنوانين لنطاق اسم الدومان عن طريق الاحتيال بعد أن قام بانتحال اسم منافسه على النحو التالي: «Louisl.com.fr» ; «Louisl.fr»²

3.1 تقنية محاكاة البريد الالكتروني (SPOOFING) :

عرّف OLIVIER ITEANU هذه التقنية على أنها: " عملية قرصنة عنوان بروتوكول الانترنت لجهاز ما عن طريق استخدام برامج خبيثة تتضمن فيروسات أو حصان الطراودة وإدخالها من طرف المجرمون المعلوماتيون في نظام معلومات من أجل سرقة المعطيات ذات الطابع الشخصي". تستهدف هذه التقنية استخدام برنامج خبيث يتضمن فيروسات خطيرة وتوجيهها نحو نظام معلوماتي لسرقة البيانات الشخصية للمستخدمين.

¹ - حصان طراودة Cheval de Troie أو Trojan horse: " هو برنامج ذو مظهر غير مؤذي، يخفي رمزا ماكرا قابلا للتنفيذ، يشنّ أو يساعد في شنّ هجوم، عادة ما يستعمل حصان طراودة في فتح باب خلفي خفي على نظام ما " أنظر محاربة الجريمة المعلوماتية، ملحق رقم 4 قاموس المصطلحات، المرجع السابق، ص 357.

² -Myriam QUÉMÉNER, Yves CHARPENEL, op cit, pp 11 et 35.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

2. انتحال الهوية الرقمية على مستوى مواقع التواصل الاجتماعي

إن تزايد عدد حالات انتحال الهوية الرقمية أصبح لا يقتصر على رسائل البريد الإلكتروني فقط وإنما امتد إلى مواقع التواصل الاجتماعي نظرا لما تشكله من مخاطر رقمية، كما امتدت إلى الأشخاص المعنوية كالمؤسسات والشركات بمختلف أصنافها.

و مما لاشك فيه، أن مواقع التواصل الاجتماعي انتشرت بوتيرة متسارعة في ظل التقدم التكنولوجي في العصر الراهن، إلا أن تطورها الهائل أصبح يشكل اليوم تهديدا للحياة الخاصة للأفراد بسبب تفاقم مخاطر انتحال الهوية الرقمية وسرقة المعطيات الشخصية لاستغلالها لمصالح غير مشروعة، لاسيما أمام سهولة الولوج إلى أي شبكة تواصل اجتماعي إذ انه يكفي فقط إنشاء حساب شخصي بعد ملأ استمارة تتضمن البيانات الشخصية للمستخدم مثل: الاسم، اللقب، تاريخ الميلاد، عنوان بريد الكتروني، صورة... الخ وبعد استكمال إجراءات التسجيل يصبح المستخدم عضوا في تلك الشبكة.

ونتيجة لذلك، يقوم المستخدمون عبر مختلف شبكات التواصل الاجتماعي بنشر بياناتهم الشخصية ومشاركتها أو عرضها مع باقي الأصدقاء أو الأعضاء مثل: الصور، الفيديوهات، المعلومات الشخصية، الآراء السياسية، المعتقدات الدينية، أرقام الحسابات البنكية أو بطاقات الائتمان... الخ دون أخذ أي احتياطات مسبقة وكل هذه المنشورات أصبحت تشكل اليوم تهديدا حقيقيا للمساس بالحياة الخاصة لأن تلك المعلومات والمعطيات ذات الطابع الشخصي يمكن الحصول عليها بسهولة من خلال مواقع شبكات التواصل الاجتماعي.

وتعتبر مسألة حماية الخصوصية المعلوماتية للمستخدم عبر وسائل التواصل الاجتماعي من المسائل المهمة والتي أصبحت محل اهتمام مختلف

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

التشريعات¹، نظرا لأن المخاطر الناجمة عن الاستخدام الواسع لمواقع شبكات التواصل الاجتماعي في تفاقم مستمر من بينها المساس بالسّمة الالكترونية للأشخاص²، إذ أنها أصبحت تثير بعض المخاوف حول أمن وخصوصية البيانات الشخصية التي يدلي بها المستخدمون لاسيما فيما يتعلق بمسألة انتحال الهوية الرقمية وهو الأمر الذي أصبح محل اهتمام الدول، والمنظمات المتخصصة في مكافحة الجرائم السيبرانية، واستنادا لما سبق ذكره فان كل الإحصائيات تشير إلى أن انتحال الهوية عبر مواقع التواصل الاجتماعي في تطور مستمر.

ويعتبر التصيد الالكتروني من أكثر الطرق انتشارا لقرصنة حسابات مواقع الشبكات الاجتماعية بحيث يقوم المجرمون السيبرانيون بإنشاء صفحة تسجيل وهمية في موقع التواصل الاجتماعي أو إنشاء أو استنساخ صفحة الدخول الخاصة بالمستخدمين ومن خلال المظهر الخارجي للصفحة يتبين للوهلة الأولى أنها تمثل صفحة فيسبوك حقيقية.

ثالثا: الركن المعنوي

هي جريمة عمدية تتطلب قيام الجاني بارتكاب الفعل المجرم مع توافر القصد الجنائي بعنصره العلم والإرادة بالإضافة إلى القصد الجنائي الخاص³.

¹ - باسم محمد فاضل، "حماية الخصوصية المعلوماتية عبر البيئة الرقمية"، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2021، ص 163.

² - للإشارة، أدى ظهور الهوية الرقمية إلى بروز مصطلح آخر يسمى بالسّمة الالكترونية E-réputation، لمزيد من التفاصيل أنظر: علي نابقي، "الهوية الرقمية: واقع تكنولوجي وشكل جديد لحضور الفرد المعاصر"، مجلة متون كلية العلوم الاجتماعية والإنسانية، المجلد الثامن، العدد الرابع، جامعة سعيدة، الجزائر، جانفي 2017، ص 535.

³ - نفس المرجع السابق.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

المبحث الثاني: الآليات التقنية الوقائية والتشريعية الردعية
للتصدي لجريمة انتحال الهوية الرقمية.

تثير ظاهرة انتحال الهوية الرقمية على الإنترنت، مخاوف الأشخاص والمؤسسات نظرا لتزايد الحالات المسجلة لاسيما خلال السنوات الأخيرة، وكذلك ظهور عدة صعوبات ومشكلات في مواجهة هذه الصورة المستحدثة من الاعتداءات والتي أصبحت تمثل تحديا كبيرا على المستويين الدولي والوطني قصد التصدي لهذا النوع من الإجرام السيبراني، لذلك أضى من الضروري اتخاذ كافة الاحتياطات والتدابير الوقائية من طرف مستخدمي شبكة الانترنت ويتطلب ذلك ضرورة التدخل عن طريق تطبيق عدة آليات سواء تقنية وقائية (المطلب الأول) ، أو تشريعية ردعية (المطلب الثاني) .

المطلب الأول: الآليات التقنية الوقائية لحماية الحق في الهوية
الرقمية.

لتفادي سرقة البيانات الشخصية وكذلك للتصدي لأي انتهاك محتمل للهوية الرقمية للأشخاص يتعين إتباع جملة من الآليات والأساليب الوقائية على المستوى التقني قصد تجنب الأضرار الناجمة عن أي انتهاك محتمل على الهوية الرقمية عن طريق اتخاذ تدابير الحماية وتعزيز الامن المعلوماتي (الفرع الأول)، وكذا وضع تطبيقات الكترونية (الفرع الثاني).

الفرع الأول: أساليب الوقاية من انتحال الهوية الرقمية بواسطة
تدابير الحماية وتعزيز أنظمة الأمن المعلوماتي.

تُعد أساليب الوقاية إحدى السبل الناجعة للتصدي لمخاطر انتحال الهوية الرقمية باعتبارها بمثابة حماية قبلية يجب اتخاذها من طرف الأشخاص

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

لكونها تساهم في رفع مستوى الوعي لديهم، لاسيما أن بعض التقنيات المستخدمة لارتكاب هذه الجريمة تعتمد أساسا على الهندسة الاجتماعية، والتي يلجأ إليها الجناة باستغلال ثقة الأشخاص بالتحايل الرقمي بهدف الحصول على الأموال أو معلومات سرية أو بيانات شخصية.

أولا: الاحتياطات السلوكية القبلية للوقاية من مخاطر استخدام

الهوية الرقمية

يمكن تفادي الوقوع في فخ المجرمين السيرانيين بإتباع بعض الاحتياطات والأساليب الوقائية فعلى سبيل المثال، يتعين على مستخدمي الانترنت توخي الحذر والفتنة عند القيام بأي معاملة الكترونية كالتحقق من رسائل البريد الالكتروني وعدم نشر أو إرسال البيانات الشخصية لاسيما البيانات الحساسة على شبكة الانترنت أو مواقع التواصل الاجتماعي مثل أرقام بطاقات الدفع البنكية أو كلمة المرور أو كلمة السر، وعدم الرد على رسائل البريد الالكتروني غير المرغوب فيه (spam) الذي قد يحتوي على إشهارات أو برامج خبيثة، وعدم النقر على روابط الكترونية مجهولة المصدر، وكذلك استخدام كلمات سر قوية أو محكمة تشمل أرقاما ورموزا وأحرفا معقدة وتجنب استخدام كلمات السر البسيطة التي لا تحتوي درجة عالية من الحماية. وكذلك ضرورة تغيير كلمات المرور وكلمة السر واستخدم برنامج أمان مناسبًا (مضاد فيروسات، وجدار ناري، وغيرها).

ثانيا: طرق الوقاية على مستوى الأمن المعلوماتي لأجهزة الإعلام

الآلي والأنظمة الالكترونية

يتعين اتباع أساليب وقائية تقنية في مجال الأمن المعلوماتي (السبراني) للأجهزة والأنظمة الالكترونية عن طريق تحديث أنظمة الوقاية من الفيروسات

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

والبرامج الخبيثة على مستوى أجهزة الكمبيوتر والهواتف النقالة الشخصية والأجهزة الذكية، ويتعين أيضا على الأشخاص المعنوية سواء شركات أو مؤسسات اتخاذ نفس الإجراءات الوقائية لكونها عرضة أيضا لانتحال الهوية الرقمية وذلك عن طريق تفعيل أنظمة الأمن المعلوماتي، نظرا لدورها الهام في تأمين بيانات المؤسسات ومستخدميهم، والتأكد من أن حسابات البريد الالكتروني محمية بشكل فعال مع مراعاة التنبيهات الأمنية ضد البرامج الخبيثة قصد تفادي أي ثغرات أمنية، مع وضع برمجيات للتخلص من الرسائل الاحتيالية والمشبوهة ومنع الوصول للمواقع الالكترونية ذات المحتوى المشبوه بتسجيلها مسبقا في " قائمة سوداء "¹.

الفرع الثاني: تعزيز الحماية بواسطة التطبيقات الالكترونية

توجد آليات أخرى تساعد على حماية الأشخاص من انتحال هويتهم الرقمية على الانترنت، تتمثل في استخدام تطبيقات الكترونية ضد مختلف التقنيات المستعملة من طرف المجرمين السبيرانيين السالف ذكرها وهذه التطبيقات الإلكترونية يتمثل دورها في أنها مضادة ومقاومة لهذه التقنيات الاحتيالية أو أي هجوم الكتروني له صلة، ونذكر على سبيل المثال:

- تطبيقات مضادة للتصيد الالكتروني أو ما يسمى ANTI-PHISHING
- تطبيقات مضادة لتقنية استزراع المواقع على الانترنت أو ما يسمى ب

ANTI-PHARMING

¹- وهي نفس التوصيات المقدمة من طرف مختلف الهيئات والمنظمات ذات الصلة على غرار منظمة الإنتربول واللجنة الوطنية للمعلوماتية والحريات بفرنسا في إطار توعية وتحذير الأشخاص من مخاطر انتحال الهوية الرقمية عن طريق تقديم توجيهات ونصائح كأساليب وقائية، لمزيد من التفاصيل أنظر موقع www.interpol.int و www.cnil.fr

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

- تطبيقات مضادة لتقنية محاكاة البريد الإلكتروني ANTI-SPOOFING

المطلب الثاني: الآليات التشريعية الردعية للتصدي لجريمة انتحال الهوية الرقمية.

قصد التطرق للآليات القانونية الردعية للتصدي لجريمة انتحال الهوية الرقمية سيتم الوقوف على أحكام التشريع الجزائري والفرنسي لتقييم مدى مساهمتها لتطور الإجرام السيبراني، وبالمضبط انتحال الهوية الرقمية (الفرع الأول)، ليتم بعدها التطرق إلى الآليات القانونية الدولية (الفرع الثاني).

الفرع الأول: الآليات القانونية الردعية في التشريعين الجزائري والفرنسي :

سننظر من خلال هذا الفرع للتشريع الجزائري (أولا)، ثم التشريع الفرنسي (ثانيا).

أولا: التشريع الجزائري

حاول المشرع الجزائري مسايرة التطورات التكنولوجيات وذلك بتكييف المنظومة القانونية عن طريق سنّ عدة قوانين خاصة في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على غرار قانون 04-09 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وقانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، كما أدخل عدة تعديلات على قانون العقوبات وقانون الإجراءات الجزائية قصد مواكبة التطور السريع للإجرام السيبراني. ولقد اعتمدت الجزائر نظام الهوية الرقمية على غرار باقي البلدان في إطار التحول الرقمي وقصد تسهيل الإجراءات في كافة المجالات، إلا أن الملاحظ قصور التشريع الجزائري في مجال تجريم

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

انتحال الهوية الرقمية وتم الاكتفاء بتجريم فعل انتحال الهوية أو صفة الغير في صورتها التقليدية بموجب أحكام قانون العقوبات بمقتضى المواد 242 الى 253 مكرر.

و أمام هذا الوضع ، في ظل غياب نص قانوني صريح في التشريع الجزائري يُجرّم هذا النوع من الأفعال الغير مشروعة "انتحال الهوية الرقمية" يمكن الاستناد إلى تكييفات قانونية أخرى كبدايل وإسقاطها على وقائع تتعلق بهذا النمط من الإجرام السيبراني تتضمن انتهاك للهوية الرقمية على غرار: جريمة النصب(387 قانون عقوبات)، الدخول أو البقاء بغش في نظام معالجة آلية للمعطيات (394 مكرر قانون عقوبات)، جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة (المادة 59 قانون 07_18) ، جريمة التقليد عبر الانترنت(151 من الأمر 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة)¹.

ونظرا لأهمية الحق في الهوية الرقمية، يستوجب الأمر تدخل المشرع الجزائري بإدراج أحكام تشريعية جزائية جديدة ضمن قانون العقوبات قصد إثراء المنظومة التشريعية وذلك بتجريم ومعاينة فعل انتحال الهوية الرقمية وإضفاء الطابع الجنحي للجريمة وفي هذا الصدد فإن التصور المقترح لإدراج جنحة انتحال الهوية الرقمية ضمن التشريع الجزائري يكون وفقا للصياغة الآتية: " يعاقب بالحبس من... إلى، وبغرامة من... إلى ...أو بإحدى هاتين العقوبتين فقط، كل من يقوم بانتحال الهوية الرقمية للغير أو استعمال معطيات أو عدة معطيات مهما كانت طبيعتها تسمح بتعريف الشخص، وذلك

¹ - أنظر طاهري حسين، المواقع الالكترونية و حقوق الملكية الفكرية المنضمنة فيها ، دار الأولى ، طبعة 2024، الجزائر، 2024، ص 50. راجع أيضا كوثر مازوني ، المرجع السابق ، ص 116.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

باستخدام تكنولوجيات الإعلام والاتصال لغرض غير مشروع، والتي من شأنها أن تؤدي إلى الإخلال بالطمأنينة وسمعة الغير".

ثانياً: التشريع الفرنسي

حرص المشرع الفرنسي على ضمان الحماية القانونية ضد أغلب الاعتداءات الماسة بحقوق أو حريات الأشخاص في البيئة الرقمية، بدءاً من صدور أول قانون بعنوان المعلوماتية، الملفات، والحريات والذي نص من خلال أحكامه أن الهدف من المعلوماتية هو خدمة المواطن، وأن إطار تطويرها يجب أن يتم عبر قنوات التعاون الدولي، مع الالتزام بالامتناع عن استخدامها للتعرض للهوية الإنسانية، أو لحقوق الإنسان أو الحياة الخاصة أو الحريات الفردية والعامة كما نص هذا القانون على أن كل شخص له الحق في اتخاذ القرار في السيطرة على استخدامات بياناته الشخصية¹.

وتجدر الإشارة أن ما كان معمولاً به سابقاً قبل تعديل قانون العقوبات الفرنسي لسنة 2011 في القضاء الفرنسي بخصوص معالجة قضايا انتحال الهوية الرقمية هو وضع عدة تكييفات قانونية على غرار جريمة النصب، جريمة الولوج عن طريق الغش لنظام معالجة آلية للمعطيات، الدخول غير الشرعي لنظام المعالجة الآلية للمعطيات، جريمة التقليد، جمع المعطيات الشخصية.

وهذا ما يتضح من خلال القرارات القضائية الصادرة و من بينها قيام أحد مستخدمي الانترنت بتصميم وإنشاء على مستوى موقعه الالكتروني الشخصي صفحة تسجيل مماثلة تماماً لصفحة Microsoft MSN Messenger من أجل القيام بجمع المعطيات الشخصية للمستخدمين.

¹ - المادة الأولى من القانون الفرنسي المتعلق بالمعلوماتية، الملفات، والحريات، رقم 78-17 المؤرخ في 1978/01/06 <http://www.legifrance.gouv.fr/1978/01/06>

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

والملاحظ أن بعض السلوكيات غير المشروعة بقيت خارج مجال التجريم لأنه لا ينطبق عليها أي تكييف قانوني ضمن التشريع الفرنسي وبقيت دون وصف قانوني¹.

أمام هذا الوضع، تدخل المشرع الفرنسي لسدّ هذا الفراغ القانوني وقام بتجريم فعل انتحال الهوية الرقمية لأول مرة في فرنسا سنة 2011، بمقتضى المادة الثانية من القانون (LOPPSI 2)²، والذي بموجبه تم إدراج المادة 1-4-226 ضمن أحكام قانون العقوبات الفرنسي.

ونلاحظ للوهلة الأولى أن المشرع الفرنسي قام بإدراج جريمة انتحال الهوية الرقمية في قانون العقوبات ضمن أحكام القسم الثاني المعنون ب:"الاعتداءات على الحياة الخاصة" (المواد من 1-226 إلى 2-226)، من الفصل السادس المعنون الاعتداءات على الشخصية (المواد من 1-226 إلى 2-226) مما يؤكد بأن الأفعال المتعلقة بانتحال الهوية الرقمية تعتبر من جرائم القانون العام، وتم تجريمها في فرنسا كحماية جزائية لحقوق الشخصية droits de la personnalité، باعتبارها انتهاك خطير للحياة الخاصة لاسيما الحق في الخصوصية الرقمية³.

¹ www.dalloz.fr

² - Loi n° 2011-267. <http://www.legifrance.gouv.fr/>

³ - تنص المادة 1-4-226 من قانون العقوبات الفرنسي المعدل بتاريخ 2011/03/16 بموجب القانون (LOPPSI2) على مايلي:"أي فعل يقوم بانتحال هوية الغير أو استعمال معطيات أو عدة معطيات مهما كانت طبيعتها من شأنها التعريف بالشخص و التي تؤدي إلى الإخلال بالطمأنينة ، أو المساس بشرفه أو باعتباره ، يعاقب بسنة حبس و 15000 أورو غرامة مالية. و تطبق نفس العقوبة إذا ارتكبت الجريمة عن طريق شبكة اتصالات موجهة للعامة على الخط".

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

وبتاريخ 2020/08/01 تم تعديل المادة 1-4-226 أين أضيفت الفقرة الثالثة التي شددت العقوبة بعامين حبس وغرامة مالية في حالة ارتكاب الجريمة من طرف زوج أو عشيق الضحية أو شريك مرتبط بالضحية بعقد مدني.¹ ومن خلال هذا النص القانوني يتضح أن المشرع الفرنسي عاقب على جريمة انتحال الهوية بنفس العقوبة سواء ارتكبت في الواقع المادي أو الواقع الافتراضي.

كما نصت المادة الأولى من القانون الفرنسي، المتعلق بحماية المعطيات ذات الطابع الشخصي، على أن حماية المعطيات ذات الطابع الشخصي هو "حق أساسي"².

أما العناصر المشكلة للجريمة، في واقع الأمر وحسب أحكام التشريع الفرنسي فإن مجرد انتحال الهوية غير كافٍ لقيام الجريمة، حيث يشترط المشرع الفرنسي ما يلي:

أن تنصب على هوية الغير بما في ذلك الشخص المعنوي لكونه يتمتع بهوية قابلة للانتحال.³

¹ - المادة 19، من القانون رقم 936-2020، المؤرخ في 30 جويلية 2020 المتعلق بحماية ضحايا العنف الزوجي التي أضافت الفقرة الأخيرة من المادة 1-4-226 من قانون العقوبات الفرنسي «Lorsqu'ils sont commis par le conjoint ou le concubin de la victime ou par le partenaire lié à la victime par un pacte civil de solidarité, ces faits sont punis de deux ans d'emprisonnement et de 30 000 euros d'amende».

² - القانون الفرنسي المتعلق بحماية المعطيات ذات الطابع الشخصي تحت رقم 63. 2004 المؤرخ في 2004/07/27.

³ - اعتبر القضاء الفرنسي أن هوية الشخص المعنوي كذلك قد تتعرض للانتحال، لتفاصيل أكثر أنظر:

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

أو تنصب على معطيات تعريفية. les données d'identification.
أن يؤدي ارتكاب الفعل إلى المساس بطمأنينة المعني بالأمر أو الغير، أو
المساس بشرفه أو اعتباره.

الفرع الثاني: الآليات القانونية الدولية

تتمثل الآليات القانونية الدولية في اتفاقية بودابست (أولا)،
واتفاقية الأمم المتحدة بشأن مكافحة استخدام تكنولوجيا المعلومات
والاتصالات للأغراض الإجرامية (ثانيا)

أولا: اتفاقية بودابست BUDAPEST

تطرقت اتفاقية بودابست إلى بعض صور الجرائم السيبرانية من خلال
توفير أحكام قانونية نموذجية يمكن للبلدان اعتمادها وتكييفها حسب
احتياجاتها الخاصة، كما تساعد الاتفاقية على تعزيز التعاون الدولي من خلال
تجريم التهديدات السيبرانية الأساسية.

وفي إطار حماية الحق في الهوية الرقمية من الاعتداءات الماسة بها على
غرار الانتحال الرقمي، قامت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة
الالكترونية بإصدار مذكرة توجيهية بشأن انتحال الشخصية والتصيد المرتبطين
بالاحتيال تتضمن عدة توجيهات وكيفية تطبيق مواد وأحكام قانونية من
الاتفاقية على هذه الصورة من الإجرام الالكتروني، ولقد استخدمت المذكرة
التوجيهية عدة مصطلحات تحمل نفس المدلول للتعبير على هذا النوع من

Paris, pôle 1, ch. 2, 11 avr. 2019, RG n° 18/21298, Légipresse 2019. 332 , n° 372 ; –
TJ Paris, 17^e ch., 11 mars 2022, n° 18-271000552, Légipresse 2022.
209, www.dalloz.fr

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الإجرام: سرقة الهوية، الاحتيال المتصل بالهوية. ومن بين الأحكام القانونية المطبقة على تجريم انتحال الشخصية المرتبط بالاحتيال بمقتضى اتفاقية بودابست نجد تجريم السلوك المتعلق بالنفاذ الغير قانوني لنظام الكمبيوتر (م2) ، والاعتراض الغير قانوني للبيانات (م3) ، التدخل في البيانات (م4) ، التدخل في نظام الكمبيوتر (م5) ، التزوير المرتبط بالكمبيوتر والمتعلق بإدخال أو تغيير أو حذف أو إتلاف بيانات الكمبيوتر وجعلها تبدو كبيانات أصلية (م7) والاحتيال المتصل بالكمبيوتر (م8) كما يعاقب على المحاولة والمساعدة والتحريض (م8) من الاتفاقية¹.

كما حثت المادة 13 من الاتفاقية والمذكرة التوجيهية السالف ذكرها الى ضرورة إدخال تعديلات على التشريعات الوطنية للدول لاسيما بالنسبة للعقوبات المقررة للجرائم المتصلة بسرقة الهوية بأن تكون عقوبات فعالة، متناسبة وراعية بما في ذلك العقوبات السالبة للحرية. ويجوز للأطراف تشديد العقوبة في حالة مثلا إذا ما امتدت آثار جريمة سرقة الهوية إلى عدد كبير من الأشخاص.

¹ - لمزيد من التفاصيل أنظر الاتفاقية الأوروبية لمكافحة الجرائم الالكترونية، الموقعه ببودابست بتاريخ 23 نوفمبر 2001، وبروتوكولها الإضافي الأول الموقع بستراسبورغ بتاريخ 28 جانفي 2003 بشأن تجريم الأفعال المرتبطة بالتميز العنصري وكرهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، والبروتوكول الإضافي الثاني المؤرخ في 17/11/2021 بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية، والمذكرة التوجيهية رقم 4 بشأن انتحال الشخصية والتصيد المرتبطين بالاحتيال المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية خلال اجتماعها العام التاسع بتاريخ 4 و5 جوان 2013، موقع مجلس أوروبا، www.int.coe اطلع عليه في 2024/05/02 .

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

ثانيا: اتفاقية الأمم المتحدة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية.

اعتمدت الجمعية العامة للأمم المتحدة بتاريخ 2024/12/24، اتفاقية أممية جديدة و التي تعتبر خطوة تاريخية و أول معاهدة عالمية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية بعد مرور خمس سنوات من المفاوضات ، و سيتم الاعلان عن فتحها للتوقيع بهانوي (الفيتنام) بتاريخ 25 و 26 اكتوبر 2025 ، وستدخل حيز التنفيذ بعد مرور (90) يوما من التصديق عليها من طرف أربعون (40) دولة .

و تهدف هذه الاتفاقية لمنع ومكافحة الجرائم الإلكترونية و حماية الاشخاص وحقوقهم عبر الإنترنت بكفاءة و فعالية ، من خلال تعزيز آليات و أدوات التعاون الدولي لاسيما في مجال تبادل الادلة الالكترونية في الجرائم الخطيرة ، و تشجيع ودعم المساعدة التقنية وبناء القدرات .

و تجدر الإشارة، أن الدولة الجزائرية كانت الرائدة في إعداد هذه الاتفاقية الاممية، وهذا ما يتبين من خلال لجنة صياغة الاتفاقية التي كانت برئاسة السفيرة الجزائرية مباركي فوزية ، بعد انتخابها بالأغلبية خلال سنة 2021. أين باشرت اللجنة جهود مكثفة و عدّة مساعي و مفاوضات لتقريب وجهات النظر بين الدول بخصوص مكافحة الجرائم السيبرانية ، وكُلّلت هذه الجهود باعتماد النص الكامل للاتفاقية الأممية بإجماع كافة الدول الأعضاء .

و بالرجوع لأحكام الاتفاقية نجد أنها تطرقت لمختلف الأفعال الغير مشروعة و المرتكبة عمدا و بدون وجه حق بواسطة تكنولوجيا المعلومات و الاتصالات و من بينها انتحال الهوية الرقمية لاسيما الوصول غير المشروع (المادة 7 من الاتفاقية)، الاعتراض غير المشروع (المادة 8)، التدخل في البيانات

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

الالكترونية (المادة 9)، التزوير المتعلق بنظام تكنولوجيا معلومات و اتصالات (المادة 12)، السرقة أو الاحتيال المتعلقان بنظام تكنولوجيا معلومات و اتصالات (المادة 13).¹

الخاتمة:

من خلال دراستنا، يتعين التأكيد بأن الهوية الرقمية أصبحت واقعا تكنولوجيا وشكلا جديدا لحضور الشخص المعاصر نتيجة تطور الوسائل التكنولوجية الحديثة، والتي ساهمت بشكل كبير في تطور الإجرام السيبراني ومن بينها انتحال الهوية الرقمية إذ أصبح من السهل الحصول على المعلومات والبيانات الشخصية للأشخاص المخزنة في شبكة الإنترنت وبالتالي يجب التصدي لمخاطر استخدام الهوية الرقمية باعتبارها امتدادا للهوية الحقيقية. إن مسألة المعالجة القانونية والقضائية للهوية الرقمية تُشكل أحد أهم محاور اهتمام الدول نظرا لانتشار وتنامي صور التعدي على الحق في الهوية الرقمية نتيجة تطور وتعمّد أساليب وتقنيات ارتكابها مما يُحتم على الدول ضرورة تكييف منظومتها التشريعية وتطويرها من أجل مكافحة هذا النوع من الإجرام السيبراني ولمسايرة التطورات التكنولوجية الحديثة. مع ضرورة إقامة موازنة بين الحق في استخدام الوسائل الحديثة للكشف عن الجريمة وبين الحق في الخصوصية المعلوماتية والحريات الشخصية للأفراد، وعلى هذا الأساس تم التوصل للنتائج الآتية:

¹. الاتفاقية الصادرة عن الجمعية العامة للأمم المتحدة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية بتاريخ 2024/12/24 موقع www.un.org الرابط

[https://www.unodc.org/unodc/ar/cybercrime/convention/text/convention-full-](https://www.unodc.org/unodc/ar/cybercrime/convention/text/convention-full-text.html)

[text.html](https://www.unodc.org/unodc/ar/cybercrime/convention/text/convention-full-text.html) اطلع عليه بتاريخ 2025/06/27 .

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

أولاً: تعتبر الهوية الرقمية كالهوية الحقيقية الموجودة في العالم المادي وهي في حاجة إلى سُبُل وآليات الحماية القانونية قصد الحفاظ عليها وضمان فعالية الأداء في البيئة الرقمية.

ثانياً: الهوية الرقمية دعامة أساسية للتحويل الرقمي في جميع الدول وتشكل عنصراً أساسياً للثقة الرقمية إلا أن ضبط مفهومها لا يزال يشكل تحدياً كبيراً بالنسبة للدول.

ثالثاً: تطبيق التدابير والآليات الوقائية الفعالة من طرف الأشخاص يساهم بشكل كبير في الحدّ من مخاطر استخدام الهوية الرقمية. وبناءً على ما سبق نقترح:

أولاً: تطوير وتحسين المنظومة التشريعية الوطنية وإثرائها لاسيما قانون العقوبات والقوانين الخاصة ذات الصلة المتعلقة بمكافحة الجرائم السيبرانية بما يتماشى مع التطورات الرقمية الحديثة والمستجدات التشريعية.

ثانياً: ضرورة تدخل المشرع الجزائري لإدراج أحكام قانونية جزائية ضمن قانون العقوبات، تُجرّم فعل انتحال الهوية الرقمية قصد ضمان حماية قانونية لحق الأشخاص في الهوية الرقمية ولمسايرة التطورات التكنولوجية.

ثالثاً: ضرورة توفير البيئة القانونية والتنظيمية والرقمية الملائمة والفعالة لتبني نظام الهوية الرقمية.

رابعاً: تعزيز التعاون الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نظراً لخطورتها ولكونها ذات طابع دولي.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

قائمة المصادر والمراجع:

أولا/ قائمة المصادر والمراجع العربية:

قائمة المصادر:

أ. الاتفاقيات والمواثيق الدولية والإقليمية:

1. الاتفاقية الأوروبية لمكافحة الجرائم الالكترونية، الموقع ببودابست بتاريخ 23 نوفمبر 2001، وبرتوكولها الإضافي الأول الموقع بستراسبورغ بتاريخ 28 جانفي 2003 بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، والبرتوكول الإضافي الثاني المؤرخ في 2021/11/17 بشأن تعزيز التعاون و الكشف عن الأدلة الالكترونية، والمذكرة التوجيهية رقم 4 بشأن انتحال الشخصية والتصيد المرتبطين بالاحتيال المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية خلال اجتماعها العام التاسع بتاريخ 4 و 5 جوان 2013.
2. الاتفاقية الصادرة عن الجمعية العامة للأمم المتحدة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية بتاريخ 2024/12/24.

ب. النصوص القانونية

1. الدستور: التعديل الدستوري لسنة 2020 بموجب المرسوم الرئاسي رقم 442/20 المؤرخ في 2020/12/30، ج ر عدد 82
2. القانون رقم 04-09، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
3. الأمر رقم 156-66 المتضمن قانون العقوبات. المعدل والمتمم
4. الأمر رقم 156-66 المتضمن قانون الاجراءات الجزائية المعدل والمتمم .
5. القانون رقم 07-18، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي، ج ر، عدد 34.
6. القانون الليبي رقم 5 لسنة 2022، بشأن مكافحة الجرائم الالكترونية، منشور في الجريدة الرسمية الليبية لسنة 2023، العدد 1، السنة الأولى.
7. مرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الالكترونية

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

ج-قرارات قضائية:

1. قرار صادر بتاريخ 20/07/2016، غ ج ملف رقم 1146677 ،مجلة المحكمة العليا 2016 ع2، ص394 .

قائمة المراجع:

أ- الكتب:

1. أرزقي سي حاج محند، "حماية المعطيات ذات الطابع الشخصي في القانون الجزائري والمقارن"، منشورات بغداددي، الجزائر، 2023.
2. باسم محمد فاضل، حماية الخصوصية عبر البيئة الرقمية دراسة تحليلية مقارنة، دار الفكر الجامعي، الطبعة الأولى،الجزائر، 2021.
3. جيلالي بغداددي، الاجتهاد القضائي في المواد الجزائية، ج 3، الديوان الوطني للأشغال التربوية، الجزائر، 1996.
4. طاهري حسين، المواقع الالكترونية و حقوق الملكية الفكرية المتضمنة فيها، دار الأولى ،طبعة 2024 ، الجزائر، 2024.
5. ليندة رقيق، القرصنة الالكترونية لحقوق الملكية الأدبية والفنية، اشغال الملتقى الوطني الافتراضي حول: الجرائم الماسة بالملكية الفكرية وآليات مكافحتها، مؤلف جماعي، المنعقد بتاريخ 2022/02/17، كلية الحقوق جامعة الجزائر 1، دار بيت الأفكار، الطبعة 1، الجزائر، سبتمبر 2022.
6. مازوني كوثر، واقع حقوق الملكية الفكرية في البيئة الرقمية، دار هومة، الجزائر، 2020.
7. مناصرة يوسف، شرعية حجب المواقع الالكترونية بين التشريع الجزائري والمقارن وأثره على حرية التعبير، دارالخلدونية،الجزائر،طبعة2022 .
8. منى الأشقر جبور، محمود جبور، " البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد"، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت لبنان، 2018.
9. محاربة الجريمة المعلوماتية أشغال الملتقى الدولي بالجزائر مركز البحوث القانونية والقضائية، بتاريخ 5-6 ماي 2010،مطبعة دار النخلة، الطبعة الأولى، الجزائر، 2011/2012.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

ب- المقالات :

1. إبراهيم عطية محمود المهدي، "الحق في الهوية الرقمية في ضوء حماية البيانات الشخصية والخصوصية المعلوماتية دراسة وصفية تحليلية مقارنة"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة دمياط، العدد 84، مصر، جوان 2023.
2. الويزة حدة، خلفاوي شمس ضيات، الهوية الرقمية في العالم الافتراضي دراسة في الفرص ومخاطر الاستخدام، مجلة رقمنة للدراسات الإعلامية والاتصالية، جامعة الجزائر3، المجلد 02، العدد 03، ديسمبر 2022.
3. واضح الحاج، التنظيم القانوني لعنوان بروتوكول الانترنت، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 07، العدد 01، 2021.
4. يوسف منصرة، " التوفيق بين حوكمة الانترنت والأمن السبيري للدول"، مجلة صوت القانون، جامعة خميس مليانة، العدد 2 لسنة 2023، الجزائر، ص 318.
5. لامية طالة، مقال بعنوان "من مجتمع المعلومات إلى مجتمع المعرفة: نحو مقاربة مفاهيمية"، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، المجلد 11، العدد 01، 2021.
6. علي حميدوش، "الجرائم الاقتصادية الإلكترونية: الدواعي والمآلات والحلول"، أشغال الملتقى الوطني "الأشكال المتعددة للجريمة الاقتصادية والمالية وسبل مواجهتها"، النادي الوطني للجيش، بتاريخ 23 و 24 فيفري 2022.
7. علي نابتي، " الهوية الرقمية: واقع تكنولوجي وشكل جديد لحضور الفرد المعاصر"، مجلة متون كلية العلوم الاجتماعية والإنسانية، جامعة سعيدة ، المجلد الثامن، العدد الرابع، الجزائر، جانفي 2017.
8. سيرجيو بيلغاكوف، مداخله بعنوان "استرداد الأصول من الدول الأجنبية: تجربة روسيا الاتحادية، المشاكل والاتجاهات الحالية"، أشغال الندوة المنظمة من طرف وزارة العدل الجزائرية حول التجربة الروسية في مجال مكافحة الجرائم المعلوماتية ومكافحة الفساد في إطار التعاون مع الفيدرالية الروسية (أعضاء من النيابة العامة الروسية)، إقامة القضاة، الجزائر، 2023/12/27.

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

9. شفيقة حداد، أسماء بلاغماس، "الهوية الرقمية والأمن الهوياتي الجزائري في ظل تحديات المجتمع الشبكي، المجلة الجزائرية للأمن والتنمية، جامعة الحاج لخضر باتنة، المجلد 10، عدد 02، الجزائر.

ثانيا / قائمة المصادر والمراجع الأجنبية:

1. Loi 78-17 du 06/01/1978 relative à l'informatique aux fichiers et aux libertés modifiées
2. Loi 2004-63 du 27/07/2004 relative à la protection des données à caractère personnelles.
3. Loi n° 2011-267, du 14 mars 2011, d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure dite (LOPPSI2).
4. Loi n°2020-936 ; du 30 juillet 2020 ; visant à protéger les victimes de violences conjugales.
5. Loi n°2004-575 .du 21 juin 2004, pour la confiance dans l'économie numérique ; dite LCEN ; JORF. n°143.22 JUIN 2004.
6. Tribunal judiciaire de Paris (17e ch.), 11 mars 2022, n° 18-27-1000552, Sté Hutchinson c/ A. K
7. Paris, pôle 1, ch. 2, 11 avr. 2019, RG n° 18/21298, Légipresse 2019. 332, n° 372; – TJ Paris, 17^e ch., 11 mars 2022, n° 18-271000552, Légipresse 2022. 209
8. Myriam QUÉMÉNER, Yves CHARPENEL :Cybercriminalité, droit pénal appliqué, Edition Economica, 2010.
9. Frédéric DECHAMPS, Caroline LAMBILOT .Cybercriminalité état des lieux ;Anthémis ;2016 .
10. Solange GHERNAOUTI, la cybercriminalité les nouvelles armes de pouvoir, édition 2018, ITCIS.Algerie.
11. Olivier ITEANU ,L'identité numérique en question, édition EYROLLES, France, 2008.
12. Christiane Feral-Schull, cyberdroit, le droit à l'épreuve de l'identité, Dalloz, 6ème Edition, France, 2011/2012

المجلة الجزائرية للقانون والعدالة

انتحال الهوية الرقمية

13. Nicolas CHAMBARDON, "L'identité numérique de la personne humaine: Contribution à l'étude du droit fondamental à la protection des données à caractère personnel"; thèse doctorat , université de LYON , école doctorale de droit, présenté et soutenue le 27/09/2018
14. Bahmed et Hassane Boumriga ; la protection de la vie privée dans un système de gestion d'identité ;master ; Universite Abou Bekr Belkaid Tlemcen Algeria ;2012 .
15. Reinhold Sojer.l'usurpation d'identité sur Internet.<https://www.semanticscholar.org/paper/L%E2%80%99usurpation-d%E2%80%99identit%C3%A9-sur-Internet-Sojer/74621d81e697a52f11fec701cbc432258afe5951>
16. Myriam QUEMENER ;"La cybercriminalité à l'heure de la Covid-19".<https://cybercercle.com/la-cybercriminalite-a-lheure-de-la-covid-19-par-myriam-quemener-magistrat-docteur-en-droit/>
17. الأمم المتحدة www.un.org
18. www.dalloz.fr
19. <http://www.legifrance.gouv.fr>
20. مجلس أوروبا www.int.coel
21. www.meltingmots.com
22. Commission nationale de l'informatique et des libertés www.cnil.fr
23. موقع الإنتربول: www.interpol.int
24. موقع مجموعة العمل لمكافحة التصيد الاحتيالي WWW.APGW.ORG
25. موقع مبادرة العطاء الرقمي لنشر الوعي التقني www.attaa.sa
26. موقع شركة تصميم وتطوير تقنيات حديثة للأمن السيبراني WWW.CEREBRA.SA