جامعة الدول العربية
مجلس وزراء العدل العرب
المركز العربي للبحوث القانونية والقضائية
بيروت - لبنان

دراسة موجزة حول الإحتيال الإلكتروني في القانون اللبناني

إعداد القاضي الدكتور وسيم شفيق الحجار

أولاً- مقدمة

جريمة الإحتيال هي من الجرائم المالية القديمة في التاريخ، وقد ظهرت منذ بدء إستقرار الإنسان في مجتمعات وتعامله مع غيره. ويهدف الجاني فيها عبر مناورات إحتيالية إلى إيقاع الغير أي الضحية في الغلط لحمله على تسليم المال بصورة رضائية ودون معرفة أن الجاني سيستولي على ماله. وهذا النوع من الجرائم يُرتكب من قبل أشخاص يظهرون في غالب الأحيان بمظهر لائق يوحي بالثقة ويكونون على درجة معينة من العلم، وغالباً ما يستغلون ذلك للإيقاع بضحاياهم.

ووفق دراسة مُجراة من قبل الاتحاد الأوروبي في شهر كانون الثاني 2020، فقد تعرض 56% من الراشدين في الإتحاد الأوروبي للإحتيال خلال السنتين الماضيتين. وتشكل أعمال الإحتيال المتعلقة بالجوائز واليانصيب نسبة 28% منها وإنتحال الهوية 22% وأعمال إحتيال على الكمبيوتر ومشاكل في الإنترنت 21% ووعود مقابل تحويل مبالغ من المال 14% وطلب للدفع لوجود مشاكل بالنسبة لحساب مصرفي 12%. ويستخدم الجناة البريد الإلكتروني في 43% من الحالات والمكالمات الهاتفية في 28% من الحالات، والخسائر لكل فرد تراوحت بمعظمها بين يورو وخمس مئة يورو.[1]

وفي الولايات المتحدة الأميركية، يفيد مكتب التحقيقات الفدرالية في تقريره السنوي أن عدد ضحايا الإحتيال المُبلّغ عنه عام 2019 هو /114,702/ في الولايات المتحدة الأميركية، وقد بلغت الخسائر ما مجموعه /57,836,379/ دولار أميركي، كما بلغ عدد ضحايا عمليات الإحتيال

[1] - European Commission, Survey on scams and frauds experienced by consumers, file:///C:/Users/wassim/Documents/MD/Laws%20Studies/Droit%20de%20l'informatique/scams/factsheet_fraud_survey.pdf, February 2020, p 1.

المتعلقة بالتحاويل المصرفية /23,775/ بمجموع خسائر بقيمة /1,776,549,688/ دولار اميركي.[2]

وفي أوستراليا على سبيل المثال، بلغت الخسائر الناتجة عن عمليات الإحتيال الإلكتروني 13,1 مليون دولار أوسترالي في العام 2018 و15,7 مليون دولار أوسترالي في العام 2017.[3]

وفي إحصاءات في كندا، 40% من الهجمات الإلكترونية على قطاع الأعمال في العام 2017 تضمنت محاولة لسرقة المال أو لطلب فدية وأن حوالي عشرين بالمئة من الشركات قد بلّغت أنها تعرضت لحوداث سيبرانية في العام 2017.[4]

وفي دراسة أجريت على عينة من 1408 شخص في الولايات المتحدة الأميركية، تبين أن 47% منهم لم يتجاوبوا مع عمليات الإحتيال ولم تنطلي عليهم وأن 30% منهم تعاملوا مع المحتالين ولم يخسروا مالاً وأن 23% منهم خسروا أموالاً نتيجة لعمليات الإحتيال.[5]

ويمكن تعريف الإحتيال بأنه الإستيلاء على مال مملوك للغير عن طريق مناورات إحتيالية بخداعه وحمله على تسليم ذلك المال. ويعني هذا التعريف أن الإحتيال ينال بالإعتداء حق الملكية، سواء في ذلك الملكية المنقولة والعقارية، ويتميز بالأسلوب الذي يتحقق عن طريقه هذا الإعتداء: ذلك أن المحتال يصدر عنه فعل خداع يتخذ صورة المناورات الإحتيالية، فيترتب عليه وقوع المجني عليه في الغلط وإقدامه على تصرف مالي أوحى به إليه المحتال وجعله يعتقد أنه في مصلحته أو في مصلحة غيره، ومن شأنه هذا التصرف تسليم مال إلى المحتال الذي يستولي عليه بنية تملكه.[6]

وقد ورد في الفقه الفرنسي تعريفات مشابهة بأن جريمة الإحتيال هي إستخدام أساليب ومناورات معينة من أجل إيقاع الضحية في الغلط وتسليم المال للغير.

---

[2] - FBI, Federal Burau of investigation, USA, Internet Crime report 2019, https://pdf.ic3.gov/2019_IC3Report.pdf, p 19, 20.

[3] - Consumers International, Social media scams: Understanding the consumer experience to create a safer digital world, May 2019, https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf, February 2020, p 9.

[4] - Little book on big scams, A guide to fraud prevention from small to medium sized businesses, https://www.rbc.com/cyber-security/_assets-custom/pdf/RBC_Book_of_Scams_Final_EN.pdf, February 2020, 13.

[5] - International Association for better business bureaus Inc, Exposed to scams, What separates victims from non-victims, https://www.bbb.org/globalassets/local-bbbs/council-113/media/financial-fraud/pdf/ScamTrackerIssueBrief-ExposedToScams-ConsumerTips-09.12.19.pdf, February 2020, p 1.

[6] - د. محمود نجيب حسني، جرائم الإعتداء على الأموال في قانون العقوبات اللبناني، المجلد الأول، منشورات الحلبي الحقوقية، بيروت، طبعة ثالثة، 1998، ص 291.

“L’ecroquerie consiste dans l’utilisation de certains procédés ou manoeuvres en vue de tromper la victim et se faire remettre le bien d’autrui”.[7]

“L’escroquerie est le fait de provoquer la remise de la chose par son propriétaire en trompant celui-ci sur la réalité des choses, par des manoeuvres frauduleuses.”[8]

ويحمي قانون العقوبات الإرادة في مجال القانون المدني من أن يعيبها محتال بغية سلب الغير ماله، فيجرم الإحتيال.[9]

ولقد أصبحت تعرف عمليات الإحتيال الإلكتروني باللغة الإنكليزية بـscams.

ثانياً- النصوص الجزائية في لبنان المتعلقة بالإحتيال الإلكتروني

لقد نص قانون العقوبات اللبناني (المرسوم الإشتراعي رقم 340 صادر في 1943/3/1 والمعدل لجهة جريمة الإحتيال بموجب المادة 40 من المرسوم الاشتراعي رقم 112 تاريخ 1983/9/16، والمعدل لجهة الغرامة الواردة فيه بموجب المادة 111 من القانون رقم 239 تاريخ 1993/5/27) على جريمة الإحتيال في المادة 655 وما يليها منه.

وتنص المادة 655 من القانون المذكور على أن "كل من حمل الغير بالمناورات الاحتيالية على تسليمه مالاً منقولاً أو غير منقول أو اسناداً تتضمن تعهداً أو ابراءً أو منفعةً وإستولى عليها يعاقب بالحبس من ستة أشهر الى ثلاث سنوات وبالغرامة من مئة ألف الى مليون ليرة.

وتعتبر من المناورات الاحتيالية:

1 - الاعمال التي من شأنها إيهام المجنى عليه بوجود مشروع وهمي أو التي تخلق في ذهنه أملاً بربح أو تخوفاً من ضرر.

2 – تلفيق أكذوبة يصدقها المجنى عليه نتيجة تأييد شخص ثالث ولو عن حسن نية أو نتيجة ظرف مهد له المجرم أو ظرف إستفاد منه.

3 - التصرف بأموال منقولة أو غير منقولة ممن ليس له حق أو صفة للتصرف بها أو ممن له حق او صفة للتصرف فأساء استعمال حقه توسلاً لابتزاز المال.

---

[7]- Corinne Mascala, Escroquerie, Rép. Pen. Dalloz, 2013, p. 2, n1.

[8] - Michèle-Laure Rassat, Escroquerie, J.C.I. code pénal 2013, Article 313-1 à 313-3, Fasc. 20, p. 5, n.10.

[9] - القاضي سمير عالية، أصول قانون العقوبات، القسم العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، الطبعة الثانية، 1996، ص 30.

4 - إستعمال إسم مستعار أو صفة كاذبة للمخادعة والتأثير. ويطبق العقاب نفسه في محاولة إرتكاب هذا الجرم."

وتقضي المادة 656 منه بتشديد عقوبة الإحتيال في حالات معينة، إذ تنص على أنه "تضاعف العقوبة إذا إرتكب الجرم في إحدى الحالات الآتية:

1 - بحجة تأمين وظيفة أو عمل في ادارة عمومية.

2 - بفعل شخص يلتمس من العامة مالاً لإصدار أسهم أو سندات أو غيرها من الوثائق لشركة أو لمشروع ما.

3 - بفعل أي مفوض بالتوقيع عن شركة أو جمعية أو مؤسسة أو أي شخص معنوي آخر."

كما تجرم المادة 657 من ذات القانون استغلال احتياجات قاصر للإحتيال عليه، فتنص على أن "كل من استغل احتياجات أو عدم خبرة أو أهواء قاصر دون الثامنة عشرة من عمره أو مجذوب أو معتوه فحمله على إجراء عمل قانوني من شأنه الاضرار بمصالحه أو مصالح الغير، عوقب بالحبس من شهرين الى سنتين وبغرامة توازي قيمة الضرر ولا تنقص عن خمسين ألف ليرة."

وتعرف المواد 658 و659 و660 من ذات القانون جرائم ذات طابع خاص من جرائم الإحتيال سمتها "فيما جرى مجرى الاحتيال"، وتتعلق المادة الأولى بحمل الضحية على تسليم بضاعة مع حق الخيار او لوعدة إحتيالاً، وتتعلق المادة الثانية بتوفير الجاني منامة أو طعام مع النية المسبقة بعدم الدفع، وتتعلق المادة الثالثة بإتخاذ واسطة نقل برية او بحرية او جوية بالغش؛ إذ تنص المادة 658 على أن "كل من حمل الغير على تسليمه بضاعة مع حق الخيار أو لوعدة وهو ينوي عدم دفع ثمنها أو كان يعرف أنه لا يمكنه الدفع، عوقب بالحبس، حتى ستة أشهر وبغرامة حتى مايتي ألف ليرة اذا لم يردها أو لم يدفع ثمنها بعد انذاره." كما تنص المادة 659 على أن "كل من وفر لنفسه منامة أو طعاماً أو شراباً في محل عام وهو ينوي عدم الدفع او يعلم انه لا يمكنه أن يدفع، عوقب بالتوقيف التكديري وبالغرامة من عشرين ألف الى مئة ألف ليرة." وتنص المادة 660 من ذات القانون على أنه "يقضى بالعقوبة نفسها على كل من اتخذ بالغش واسطة نقل برية أو بحرية أو جوية دون أن يدفع اجرة الطريق."

وتعتبر جريمة الإحتيال في القانون اللبناني من قبيل الجنحة كون عقوبتها، وهي الحبس من قبيل العقوبات الجناحية وفق المادة 39 من قانون العقوبات، وهي لا تتجاوز الثلاث سنوات حبس.

في الواقع، لم تحدد المادة 655 من قانون العقوبات اللبناني طبيعة المناورات الإحتيالية التي يمكن إرتكابها، فقد تكون تتم بين أشخاص حاضرين في مجلس واحد أي في مقابلة أو مواجهة بعضهم البعض أو قد تتم عن بعد أو بالواسطة.

كما إن الإحتيال الجزائي يمر بخطوات ومراحل صعبة متنوعة في إطار ترابط منطقي إضافة على إشتراط أن تكون المناورات الإحتيالية سابقة أو على أبعد تقدير معاصرة لعملية التسليم وليس لاحقة لها حتى وإن سلمنا بأن مرحلة تنفيذ التعاقد لا تدخل إطلاقاً في إطار إكتمال الجرم.[10]

والسؤال الذي يثيره نص المادة 655 عقوبات هو تحديد ما إذا كان الشارع قد ذكر هذه الصور على سبيل الحصر أم على سبيل المثال. يبدو من سياق عبارة الشارع، وقوله "وتعتبر من المناورات الإحتيالية" أنه يذكرها على سبيل المثال، وقد ذكر أهم هذه الصور في التطبيق. وبناءً على ذلك فإنه إذا توافرت صورة للمناورات الإحتيالية، تطور المعاملات، ولم تكن فيه بين الصور التي وردت في النص، فإن للقاضي أن يقدر قيام الإحتيال بها.[11] وهذا دليل إضافي أن نص المادة 655 عقوبات يمكن تطبيقه على جريمة الإحتيال الإلكتروني دون حاجة لنص جديد أو تعديل تشريعي.

في الواقع، لم يلحظ القانون اللبناني نصاً يبيح للقاضي اللجوء إلى القياس في حال عدم شمول النص أفعالاً مضرة بالمجتمع كالأفعال التي قرر تجريمها في قانون العقوبات وإنزال العقاب بفاعلها. ويترتب على ذلك أنه يحظر على القاضي تجريم مثل هذه الأفعال وإن إعتقد في قرارة نفسه بعدم جواز ترك فاعلها دون عقاب بالنظر للخطر الذي يشكله على المجتمع. إلا أن مهمة التشريع غير منوطة به وبالتالي تتعدى سلطته وصلاحيته.[12]

ويعاقب في القانون اللبناني على محاولة الإحتيال وفق صراحة نص الفقرة لأخيرة من المادة 655 من قانون العقوبات والمذكورة أعلاه. وفي الواقع، لا يعاقب في القانون اللبناني على محاولة إرتكاب جنحة إلا إذا ورد نص صريح على ذلك، إذ تنص المادة 202 من قانون العقوبات المعدل على أنه لا يعاقب على المحاولة في الجنحة وعلى الجنحة الناقصة الا في الحالات التي ينص عليها القانون صراحة.

ثم جاء قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي (قانون رقم 81 تاريخ 2018/10/18)، والذي أُقرّ في العام 2018، ليتضمن باباً خاصاً هو الباب السادس حول الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية والبطاقات المصرفية، فأنشأ جرائم جديدة في القانون اللبناني لم تكن موجودة قبل ذلك. فمن المعلوم أن لا جريمة ولا عقوبة دون نص قانوني، وأن النصوص الجزائية العقابية تفسر على سبيل الحصر.[13] والجرائم الجديدة التي أنشأها قانون المعاملات

---

[10] - د. فيلومين يواكيم نصر، قانون العقوبات الخاص- جرائم وعقوبات، المنشورات الحقوقية صادر، طبعة العام 2009، ص 154.

[11]- د. محمود نجيب حسني، جرائم الإعتداء على الأموال في قانون العقوبات اللبناني، المجلد الأول، منشورات الحلبي الحقوقية، بيروت، طبعة ثالثة، 1998، ص 308.

[12] - القاضي مصطفى العوجي، القانون لجنائي العام، النظرية العامة للجريمة، الجزء الأول، مؤسسة نوفل، بيروت، الطبعة الثانية، 1988، ص 294.

[13] - وقد أقرت المادة الثامنة من الدستور اللبناني هذا المبدأ إذ تنس على أن "الحرية الشخصية مصونة وفي حمى القانون ولا يمكن أن يقبض على أحد أو يحبس أو يوقف إلا وفاقاً لأحكام القانون ولا يمكن تحديد جرم أو تعيين عقوبة إلا بقتضى القانون".

الإلكترونية والبيانات ذات الطابع الشخصي الجديد هي جرائم الولوج غير المشروع أو بالغش إلى نظام معلوماتي (ما يعرف ب Illegal Access أو Hacking) وجرائم إدخال بيانات معلوماتية بنية الغش في نظام معلوماتي أو تعديلها أو محوها (ما يعرف ب Data Interference) وجرائم إعاقة عمل نظام معلوماتي أو تعطيله عن العمل (ما يُعرف ب System Interference or Denial of service) وجرائم إساء إستعمال تجهيزات أو برامج معلوماتية بهدف إرتكاب أي من الجرائم المذكورة سابقاً (ما يُعرف ب Misuse of devices).
إلا أن قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي الصادر عام 2018 لم يتطرق إلى جريمة الإحتيال الإلكتروني.

ويمكن القول أن قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي الجديد لم يحتج إلى إستعادة تجريم جريمة موجودة في القانون العقوبات اللبناني، والذي حدد عناصر وشروط جريمة الإحتيال ولم يمنع أن تكون المناورات الإحتيالية مُرتكبة بوسائل معلوماتية وعن بعد أو بإستعمال هوية إلكترونية غير صحيحة أو منتحلة او بواسطة البريد الإكتروني أو بإستعمال مواقع إلكترونية ذات محتوى خادع أو غير صحيح.

في الواقع، يقتضي التفريق بين نوعين من الجرائم المعلوماتية (والتي تُعرف أيضاً بالجرائم السيبرانية أو الجرائم الإلكترونية أو جرائم الحاسوب). النوع الأول من الجرائم المعلوماتية هو حيث تكون التجهيزات والبرامج المعلوماتية هي الوسيلة المُستعملة لإرتكاب جريمة تقليدية، مثل السرقة، عبر خرق النظام المصرفي الإلكتروني عن بعد والتحويل المصرفي الإلكتروني من حساب إلى آخر، أو مثل جرائم القدح والذم (جرائم القذف والسباب) عبر إستعمال مواقع إلكترونية على شبكة الإنترنت لنشر الأقوال المسيئة... أما في النوع الثاني من الجرائم المعلوماتية، فتكون التجهيزات والبرامج المعلوماتية هي الموضوع أو المحل الذي يقع عليه الفعل الجرمي، كالإعتداء على البرامج المعلوماتية أو البيانات المعلوماتية.

وإن جريمة الإحتيال هي من قبيل النوع الأول من الجرائم، فهي من الجرائم التقليدية التي قد تتم إما بطرق تقليدية أما عبر إستخدام الوسائل المعلوماتية. وبالتالي لا حاجة لنص قانون جديد لتجريم جريمة الإحتيال الإلكتروني في القانون اللبناني.

كما تنص المادة الأولى من قانون العقوبات على أنه لا تفرض عقوبة ولا تدبير إحترازي أو إصلاحي من أجل جرم لم يكن القانون قد نص عليه حين إقترافه. وتنص المادة السادسة من ذات القانون على أنه لا يقضى بأي عقوبة لم ينص القانون عليها حين إقتراف الجرم.

بالفعل، هناك الجرائم المعلوماتية التي تُرتكب بواسطة نظام معلوماتي، ويطبق قانون العقوبات على هذه الجرائم، فالوصف القانوني يرتبط بجرائم تقليدية مثلا حالة إستخدام إحتيالي أرقام بطاقة مصرفية من أجل معاملة على الإنترنت.[14]

ولعل البعض قد يرى ضرورة إضافة نص تشريعي لتشديد العقوبة المتعلقة بالإحتيال الإلكتروني، لاسيما في مجال جرائم الإحتيال الإلكتروني المنظمة، والتي تطال عدد كبير جداً من المستخدمين على شبكة الإنترنت ومن خلال مواقع إلكترونية معروفة أو عناوين رقمية IP معروفة. ومن الجدير ذكره أن قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي الجديد قد تشدد في مسائل حجب المواقع الإلكترونية، فلم تجز المادة 125 منه حجب المواقع الإلكترونية أو وقف خدمات إلكترونية عليها أو إلغاء حسابات عليها إلا في جرائم الإرهاب أو المتعلقة بالمواد الإباحية للقاصرين أو بألعاب مقامرة ممنوعة أو بعمليات الإحتيال الإلكتروني المنظمة أو تبييض الأموال أو الجرائم الواقعة على الأمن الداخلي أو الخارجي أو المتعلقة بالتعدي على سلامة الأنظمة المعلوماتية كنشر الفيروسات. ويبدو أن المشرع اللبناني قد وعى لأهمية عمليات الإحتيال الإلكتروني المنظمة فساواها بجرائم أخرى ذات أهمية كجرائم الإرهاب، وأجاز حجب المواقع الإلكترونية الصادرة عنها هذه الجرائم.

وتعد جرائم الإحتيال من الجرائم القصدية التي تقوم على توافر النية الجرمية والقصد الجرمي أي على معرفة الجاني بطبيعة فعله والنتيجة المترتبة عليه وإتجاه إرادته لتحقيق الفعل الجرمي والنتيجة الجرمية. ولا يتصور أن تكون جريمة الإحتيال ناتجة عن عمل غير مقصود نتيجة الإهمال أو قلة إحتراز أو عدم مراعاة القوانين والأنظمة.

ويفترض لتوافر عناصر جرم الإحتيال أن يكون قد وقع على شخص آخر أي على إنسان، وليس على جهاز كمبيوتر. ويرى البعض أنه وراء كل نظام معلوماتي يوجد شخص، وبالتالي فيكون الخداع قد وقع على هذا الشخص من خلال النظام المعلوماتي.

وتجدر الإشارة إلى أن القانون اللبناني لا يعتبر إنتحال الهوية الإلكترونية على شبكة الإنترنت جريمة بذاتها إلا إذا وقعت من ضمن سياق المناورات الإحتيالية وفق ما تنص عليه المادة 655 عقوبات، هذا مع مراعاة ما تنص عليه المادتان 405 و406 من قانون العقوبات لجهة تجريم إنتحال هوية في سياق تحقيق قضائي أو محاكمة أو أمام قاضي أو الضابطة العدلية فقط. وقد عمد المشرع الفرنسي

[14] - Christiane Féral-Schuhl, Cyberdroit, Le droit l’épreuve de l’internet, Dalloz, 7ème edition, 2018, p 1480.

إلى إضافة فقرة إلى المادة 226-4-1 من قانون العقوبات الفرنسي بموجب القانون رقم 267/2011 تاريخ 2011/3/14، وذلك حول جريمة إنتحال الهوية الإلكترونية.[15]

ثالثاً- خصائص جرائم الإحتيال الإلكتروني بالمقارنة مع جرائم الإحتيال التقليدي

لقد وفرت الوسائل المعلوماتية والإلكترونية وسائل أكثر فعالية وجدوى للإيقاع بالضحايا. ولقد ساهمت العولمة وتحول الكون كله إلى قرية عبر وسائل الإتصال الحديثة وتكنولوجيا المعلومات إلى تفشي ظاهرة جرائم الإحتيال الإلكتروني. وتمتاز جرائم الإحتيال الإلكتروني عن تلك التقليدية بأنها في معظمها هي جرائم عابرة للحدود، حيث أصبح الجناة يستغلون واقع إنفتاح العالم عبر شبكات نقل وتبادل البيانات لإستهداف أشخاص في دول أخرى.

على سبيل المثال، إزادات بشكل مستمر الهجمات الإلكترونية بحيث بلغت في العام 2014 42,8 مليون هجوم إلكتروني في العالم[16]، ما يوازي 117,339 هجوم سيبراني في اليوم؛ ثم إزدادت هذه الهجمات في العام 2015.[17]

في الواقع، تُرتكب جرائم الإحتيال الإلكتروني في بيئة إفتراضية Virtuel environment في حين تحصل جرائم الإحتيال التقليدية في بيئة حقيقة واقعية، ومن هنا تنشأ الإشكاليات الخاصة بالنوع الأول من جرائم الإحتيال. وهي جريمة تُرتكب دون عنف بل بإستعمال الذكاء والمعرفة التقنية. ويمكن إستعمال ليس فقط أجهزة الكمبيوتر الثابتة Desktop والمحمولة Laptop بل أيضاً الهواتف الذكية Smart phones وغيرها من الألواح الإلكترونية Tablets لإرتكاب جرائم الإحتيال الإلكتروني أو حتى الهواتف الخليوية العادية (الجوالة) Mobile phones من خلال الرسائل القصيرة sms.

تُرتكب معظم حالات جرائم الإحتيال الإلكتروني عن بعد من قبل الجناة بخلاف حالات الإحتيال التقليدي، إذ يتيح هذا النوع المُستجد من الجرائم للجاني الحصول على منافع مالية دون تعريض نفسه إلى خطر، إذ أنه لا ينتقل أبداً إلى موقع الجريمة للتصادم مع الضحايا أو للتعرض للتوقيف من قبل

---

[15] - La loi n 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 a consacré une nouvelle infraction pénale d'usurpation d'identité codifié à l'article 226-4-1 du de penal: "Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou de plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquilité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa consideration, est puni d'un an d'emprisonnement et de 15 000 euro d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un reseau de communication au public en ligne".

[16] - C. Desjardins, Quand le cauchemar de la cyberattauqe devient réalité, Les Echos, 5 février 2015.

[17] - Etude mené par le binet PriceWaterhouseCoopers.

الشرطة، بل غالباً ما يوقع بضحاياه وهو موجود بكل طمأنينة أو أمان في مكتبه أو في منزله. كما يقلل الجاني من خطر تعرضه للملاحقة القانونية من خلال إستهداف الأفراد أو المستخدمين على الإنترنت بمبالغ مالية صغيرة، ولكن تتراكم بفعل العدد الكبير من الأشخاص المستهدفين، فيعمد معظم الأشخاص إلى عدم الادعاء لعدم تكبد مصاريف توكيل محامين أو مشقة التحقيقات، وأحياناً بسبب الإحراج الذي يتعرضون له من وقوعهم ضحايا لضروب من الغش قد تكون أحياناً بديهية، وأحياناً أيضاً بسبب إنتفاء ثقتهم في وصول التحقيقات القضائية إلى إكتشاف الجناة بالنظر للصعوبات التقنية وحرفية الجناة وتواجدهم في دول أخرى بعيدة.

ووفق دراسة مُجراة من قبل الاتحاد الأوروبي في شهر كانون الثاني 2020، فقد تقدم فقط 21% من الضحايا بشكاوى جزائية عن جرائم إحتيال تعرضوا لها.[18]

ومن الأسباب المهمة لصعوبة إكتشاف الجريمة هي إحجام الضحايا عن الإبلاغ عن الجرائم المعلوماتية التي تعرضوا لها، وذلك إما خوفاً من التشهير بهم أو الإساءة إلى سمعة شركتهم وفقدان ثقة المستثمرين والزبائن بهم.[19]

وبالتالي تمتاز جرائم الإحتيال الإلكتروني بالتباعد الجغرافي بين الجناة والضحايا، لا بل بين الأفعال الجرمية المقترفة والنتائج الجرمية المترتبة عليها، والتي قد تحصل في مكان جغرافي أو دول أخرى. إذ يمكن إرتكاب جريمة بإستعمال كمبيوتر موجود في دولة معنية في حين تتحقق النتيجة الجرمية في دولة أخرى، ما يعني أن أماكن متعددة في دول متعددة قد تتأثر في وقت واحد بالأفعال الجرمية.[20] وتساهم هذه الإشكالية في صعوبة تحديد الدولة التي تكون محاكمها مختصة لنظر الدعوى الجزائية، وكذلك في صعوبة تحديد القانون الواجب التطبيق بالإضافة إلى الإشكاليات الناتجة عن الملاحقة الجزائية وإجراءات التحقيق وتجميع الأدلة، ولاسيما الإدلة المعلوماتية. فقد تكون هذه الأدلة لدى دول أخرى أو على شبكة الإنترنت وهي معرضة للزوال بسرعة أو لدى مقدمي الخدمات التقنيين خارج حدود الدولة القائمة بالتحقيق، مما لا يمنح الأخيرة سلطة عليهم لطلب الأدلة منهم، هذا بالإضافة إلى ما يعاصر ذلك من جهد يقوم به الجاني لإخفاء آثاره المعلوماتية ومحو الأدلة عبر إستعماله مثلاً عناوين رقمية IP عائدة لمواقع عامة أو متغيرة Dynamic أو محاولة إخفاء عنوانه الرقمي الحقيقي أو بالإختباء وراء حاسب proxy server...

---

[18] - European Commission, Survey on scams and frauds experienced by consumers, file:///C:/Users/wassim/Documents/MD/Laws%20Studies/Droit%20de%20l'informatique/scams/factsheet_fraud_survey.pdf, February 2020, p 2.

[19] - David Wall, Cybercrimes and the internet, Taylor and Francis group, 2001, first edition, p 8.

[20] - Mascla Corinne, Criminalité et contrat éléctronique, Travaux de l'association Capitant Henir, Journée nationale, Paris 2000, p 119.

كما قد يستغل الجناة الطابع الدولي لجريمة الإحتيال الإلكتروني والنظام القانوني بين الدول، إذ ينطلقون في أعمالهم من دول لا تربطها إتفاقيات تعاون قضائي وإسترداد للمجرمين مع الدول المستهدفة.

فقد أصبح بإمكان الجاني الوصول إلى عدد غير محدود من الأشخاص عبر شبكة الإنترنت يتجاوز الملايين، أي إلى أي شخص وفي أي دولة في العالم، أي إلى كل شخص موصول بشبكة الإنترنت، أي أكثر من ثلث عدد سكان الكون، في حين كان سابقاً مقيداً بهامش لا يتعدى الأشخاص الذي يمكن أن يلتقي بهم بصورة مباشرة مادية وجهاً لوجه في محيطه الضيق، والذين قد لا يتجاوزن بضع مئات أو بضعة آلاف. كما أتاحت الإنترنت وتطبيقاتها كالبريد الإلكتروني ووسائل التواصل الاجتماعي Social media والمواقع الإلكترونية وغرف الدردشة الإلكترونية إمكانية التواصل مع أي شخص قد يرغب الجاني بإستهدافه، في حين أن التواصل في الشكل التقليدي قد يكون مرهون بوجود فرصة للإلتقاء شخصياً بالضحية أو مراسلتها عبر البريد الورقي والغير مضمونة مفاعليه.

كما أتاحت الوسائل المعلوماتية للجاني إنتحال هوية إلكترونية مغايرة لهويته الحقيقية ولإخفائها، ما يُعرف بظاهرة Impersonation، ومن ذلك على سبيل المقال إنشاء حسابات بأسماء وهمية أو مستعارة على وسائل التواصل الاجتماعي كفيسبوك أو على مقدمي خدمات البريد الإلكتروني أو حتى إنشاء مواقع إلكتروني وهمية. فغالباً ما قد لا تلتقي الضحية بالجاني أبداً أثناء تنفيذ جرائم الإحتيال الإلكتروني، إذ أن التعامل يتم عن بعد. ويستغل الجاني حاجات المستخدمين لخدمات أو سلع يطلبونها على الإنترنت، وغالباً من مواقع أجنبية موجودة في دول أخرى بعيدة، وذلك من أجل إستسهال إخفاء هويته وعدم الكشف عنها.

ويعرّف البعض الهوية الإلكترونية أو الهوية الرقمية بأنها تمثيل تقني للشخص ولأعماله في العالم السيبراني، وهي الأقرب إلى هوية الشخص الحقيقية التي تترجم أعماله إلى بيانات رقمية.[21] وفي الحقيقة، فإن الهوية الإلكترونية هي الهوية التي يتخذها شخص ويظهر بها على المستخدمين الآخرين على شبكة الإنترنت، وقد تكون مطابقة لهويته الحقيقية أو قد تكون مخادعة ومستعارة. كما تشمل عناصر الهوية الإلكترونية على الإنترنت الوسائل التقنية التي تسمح بتحديد الهوية الحقيقة للشخص من خلال ربط العنوان الرقمي IP التي ينطلق منه بمكان إقامة أو عمل مادي أو ببريد إلكتروني شخصي أو بحساب شخصي على وسائل التواصل الاجتماعي معروف صاحبه. وقد إعتبرت محكمة إستئناف باريس أنه يمكن إعتماد العنوان الرقمي أو عنوان الإنترنت IP وحساب البريد الإلكتروني Email Address وإسم المستخدم Username على شبكة الإنترنت من أجل التعرف على الهوية الإلكترونية الوهمية والتحقق منها.

[21] - Mouron P., Internet et identité virtuelle des personnes, Revue de la recherche juridique-Droit prospectif, n 124, 2008.

وفي الواقع، لقد أصبحت وسائل إغتصاب الهوية على شبكة الإنترنت أكثر عدوانية وهجومية وأصبحت من الأدوات الرئيسية لتحقق الجرائم.[22]

إن الغفلية أي إخفاء الإسم تعزز الشعور بالتهرب من العقاب لمرتكبي الجرائم في البيئة الرقمية؛ وخلافاً لمجرمي الماضي حيث كانت المخاطر مادية، فالمجرم السيبراني ينشط في أمان مغيراً مفهوم المخاطرة التي يتعرض لها.[23]

وكنتيجة لما تقدم، لا يترك الجناة في جرائم الإحتيال الإلكتروني في معظم الأحيان أدلة مادية ملموسة في مسرح الجريمة يمكن جمعها توصلاً لإثبات الجرائم وتحديد هوية مرتكبيها، بل أن معظم الأدلة هي من قبيل الأدلة الرقمية التي يمكن محوها بسرعة وسهولة أو تعديلها.

ومما قد يصعب الأمور أيضاً أنه قد لا تعرف الضحية أنها قد تعرضت لعملية خداع وإحتيال إلا بعد مرور فترة زمنية كبيرة، بحيث يصعب بعدها تعقب الجناة وضبط الأدلة الرقمية حولهم، كقيامهم مثلاً بإقفال الموقع الإلكتروني المُستعمل أو التعويل على عدم تخزين معلومات حركة البيانات من قبل مقدمي الخدمات التقنية إلا لفترات قصيرة.

وتعد من الحالات الشائعة للإحتيال الإلكتروني حالات الإحتيال على المستخدمين على شبكة الإنترنت المتعلقة باليانصيب وببطاقات الإئتمان وإنتحال الشخصية وعمليات بيع السلع والخدمات أو جمع الإعانات من المتبرعين بعد إنتحال صفة جمعية خيرية.

ويسعى المحتالون الى عزل ضحاياهم، فالأكثر عرضة للخطر هم الذين يحسون بالوحدة، ويجب بالتالي على المستهدفين أن يتصلوا فوراً باشخاص موثوقين من قبلهم كأصدقاء لهم أو شركات متخصصة أو مؤسسات لأخذ النصيحة. ف51% من الأشخاص الذي أبلغوا عن تدخل شخص ثالث لمصلحتهم (كمحاسب أو موظفي مصرف أو موظف خبير) تمكنوا من تجنب خسارة الأموال، كذلك الأشخاص الذين سمعوا بعمليات إحتيال مشابهة هم أقل عرضة للإنخداع بهذه العمليات.[24]

وفي الواقع، في الغالب قد لا يستهدف الجناة أشخاص محددين، بل قد يرسلون آلاف رسائل البريد الإلكتروني إلى علب بريد إلكتروني يجمعونها على شبكة الإنترنت، أو لأشخاص من فئات محددة، كالمهندسين أو البائعين في قطاع معين، ويحصل الجناة على البريد الإلكتروني للفئات المذكورة من

---

[22]- Céline Castets-Renard, Droit de l'internet: Droit français et européen, Montchrestien, 2 ème édidion, 2012, p 450.

[23] - Christiane Féral-Schuhl, Cyberdroit, Le droit l'épreuve de l'internet, Dalloz, 7ème edition, 2018, p 1476.

[24] - International Association for better business bureaus Inc, Exposed to scams, What separates victims from non-victims, https://www.bbb.org/globalassets/local-bbbs/council-113/media/financial-fraud/pdf/ScamTrackerIssueBrief-ExposedToScams-ConsumerTips-09.12.19.pdf, February 2020, p 1.

الدليل المنشور عنهم، وذلك على أمل أن يوقعوا ولو قسم بسيط من مستقبلي رسائلهم بالغلط والخداع لحملهم عل تسليم المال.

ويكون في الغالب لعمليات الإحتيال جانب عاطفي، إذ تحس الضحية أنها خُدعت وقد تشعر بالأذى والإنتهاك ومحاولة إستغبائها.[25] مما يترك أثر نفسي عميق لديها بالإضافة إلى الخسارة المادية التي تعرضت لها. وقد تسعى للمطالبة أمام المحاكم بالتعويض عن الضرر المادي وكذلك المعنوي الذي لحق بها من جراء الإحتيال الإلكتروني.

وقُضي في فرنسا بأنه تحصل جريمة الإحتيال الإلكتروني بإستعمال إسم مستعار وبطاقة مصرفية مزورة وذلك لشراء على شبكة الإنترنت أغراض قيمة وذات قيمة أثرية وطلب إرسالها إلى عنوان مختلف عن العنوان الحقيقي للجاني لتجنب كشف هويته وملاحقته.[26] كما قُضي بأنه يعد الإحتيال متوافراً عندما يتصل الجاني بالضحية هاتفياً مدعياً أنه مندوب للمصرف ويطلب تأكيد معلومات البطاقة المصرفية كرقم الحساب وتاريخ إنتهاء صلاحية البطاقة، ويعمد الجاني إلى إستعمال المعلومات المذكورة لإستلام النقود إلكترونياً بفعل المناورة الإحتيالية المذكورة.[27] كما إعتبرت محكمة إستئناف باريس من قبيل الإحتيال تشغيل شركة إتصالات للخليوي نظام معلوماتي للإتصال بشكل مكثف بمستخدمين على الهاتف الخليوي وقطع الاتصالات حتى قبل إعطاء الوقت للمُتصل بهم للإجابة على الهاتف.[28]

من أجل محاربة ظاهرة الإحتيال الإلكتروني، أنشأت دول كثيرة مواقع إلكترونية رسمية لها على شبكة الإنترنت لتنبيه المواطنين والأفراد حول الأشكال المستخدمة يومياً لعمليات الإحتيال الإلكتروني، لاسيما تلك المنظمة منها. كما وضعت تلك الدول على تلك المواقع إرشادات مفصلة للمواطنين لتفادي وقوعهم ضحايا لجرائم الإحتيال الإلكتروني. على سبيل المثال، يجب على المستخدم على الإنترنت التعامل قدر الإمكان مع مواقع إلكترونية مشهورة أو معروفة وذات سمعة جيدة معروفة، وأن لا ينغرّ بعروض هي أفضل من أن تكون حقيقة، وأن يتحرى حول المواقع الإلكترونية والخدمات المقدمة من خلال البحث على الإنترنت من خلال محركات البحث كغوغل على تعليقات المستخدمين السابقين حول الموقع الإلكتروني المستعمل، وأن يقرأ بدقة المعلومات

---

[25] - Charles Schwab, Protect yourself from financial fraud, file:///C:/Users/wassim/Documents/MD/Laws%20Studies/Droit%20de%20l'informatique/scams/Consumers%20International,%20Social%20media%20scams-%20Understanding%20the%20%20consumer%20experience%20to%20create%20a%20safer%20digital%20world_May%202019.pdf, May 2019, p 3.

[26]- Cour d'Appel Paris, Chambre correctionnelle 12, 29/5/2007, N 07/02517, JurisData: 2007-338700.

[27]- Cour d'Appel Paris, 9 ch, sect A, 18 nov 1992, Juris-Data, n 23257.

[28] - Cour d'Appel Paris, pole 5, Chambre 11, 26/9/2014, RG n 11/22949.

الواردة على الموقع وأن يحاول أن يربطه بمكان أو شخص مادي ممكن التحري أكثر عنه من خلال رقم هاتف أو عنوان مكان أو رقم تسجيل الشركة في السجل التجاري أو لدى الإدارة الضريبية...

في الواقع، قد يعمد معظم مستخدمي وسائل التواصل الاجتماعي إلى نشر تجاربهم في حال تعرضهم لمحاولة إحتيال إلكتروني فاشلة على الإنترنت، لكن معظم الضحايا يمتنعون عن نشر تجاربهم في حال نجاح عمليات الإحتيال الحاصلة بحقهم.[29]

كخلاصة، يبدو أن جرائم الإحتيال الإلكتروني بالنظر للمزايا التي تتمتع بها بالنسبة للجناة قد أصبحت مغرية لعدد كبير من الناس للقيام بها بالنظر لمردودها المادي الكبير عليهم ولصعوبة إكتشافهم وإثبات الجرم بحقهم وضآلة المخاطر المحدقة بهم.

رابعاً- الطرق المعتمدة في الإحتيال الإلكتروني

1-حالة إستخدام بطاقة مصرفية أو البيانات العائدة لها

يمكن أن يقوم الجاني بالإستيلاء بشكل إحتيالي على بطاقة مصرفية صحيحة عبر مناورات إحتيالية وإستعمالها لتسديد دفعات عن نفسه. كما يمكن أن يقوم بإستعمال بطاقة مصرفية أقدم على تزويرها عبر نسخ البيانات المعلوماتية لبطاقة مصرفية صحيحة إستولى عليها بالخداع من صاحبها لنسخها. كما يمكن أن يقوم الجاني بخداع صاحب البطاقة المصرفية للحصول على رقمها وتاريخ إنتهاء صلاحيتها لإستعمالها عنه في مدفوعات على شبكة الإنترنت أو لطباعتها وبيعها في السوق السوداء. ويمكن أن يقوم الجاني بإختراق قاعدة بيانات لبعض المواقع الإلكترونية التي تتعاطى التجارة الإلكترونية، والتي تخزن في قواعد بياناتها البيانات العائدة لبطاقات الزبائن الذين تعاملوا معها، فيعمد الجاني إلى إعادة إستعمال بيانات البطاقات المصرفية، لكن البعض يرى أنه في هذه الحالة لا يعد فعله من قبيل الإحتيال لعدم وقوع إنسان في الغلط لتسليم المال. وقد إعتبرت محكمة التمييز الفرنسية أن أخذ مال الغير عن طريق الحصول على بطاقة الإئتمان خفية أو عنوة وإستعمالها لسحب الأموال من الصراف الآلي يعتبر من قبيل جريمة السرقة.[30]

2-تقنيات الهندسة الإجتماعية

[29] - Consumers International, Social media scams: Understanding the consumer experience to create a safer digital world, May 2019, https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf, February 2020, p 14.

[30]- Cass., arrêt 4/7/2013, publié au Bulletin, n 11 rev 101; C. Appel Basse-Terre, 2 chambre, civ., 23L5L2013, Numéro Jurisdata 2013-016466.

في الواقع، لا تتطلب عمليات الإحتيال الإلكتروني معارف تقنية كبيرة لدى الجناة، إذ غالباً ما يلجأ هؤلاء، وقد يكونون بلا معرفة تقنية متخصصة في المعلوماتية، إلى أفكار بسيطة للإيقاع بضحاياهم. وتعرف هذه الأساليب بتقنيات الهندسة الاجتماعية Social engineering.

ويمكن تعريف الهندسة الاجتماعية بأنها تقنية تعتمد على التلاعب النفسي البشري، وتهدف إلى الحصول على معلومات سرية من شخص مستهدف. فهي تستند إلى فن إختراق العقول، حيث يتقن الضليعون بهذا الفن إستغلال الجوانب النفسية، ويعتمدون لذلك على أساليب الخداع والإستغلال والتضليل والإستفادة من نقاط الضعف في الجوانب البشرية للإنسان، وذلك لإختراق أكثر النظم أماناً عبر الحصول بكل بساطة على المعلومات الحساسة والتي تمكن من تفادي نظم الأمان. يُراجع.[31]

وتدخل ضمن هذا الإطار ما يعرف بعمليات التصيد Phishing. ويتم ذلك من خلال حمل المستخدم إحتيالاً على تقديم بياناته الشخصية (ككامل إسمه وتاريخ ولادته...) أو المالية أو بيانات بطاقته المصرفية أو كلمة السر وإسم المستخدم العائدة له أو بريده الإلكتروني بصورة رضائية. مثلاً قد ينشأ المحتال موقع إلكتروني مشابه لموقع المصرف المُستخدم في العمليات المصرفية على الإنترنت، إذ يتضمن ذات شكل الشاشات وألوانها وشعار المصرف وعبارات مشابهة لتلك الواردة على الموقع الإلكتروني الحقيقي، ويرسل رابط الموقع البديل الوهمي لزبائن المصرف ليستعملوه، فيستولي على كلمات السر العائدة لهم عندها.

كما قد يعيد المحتال توجيه المستخدمين من الموقع الحقيقي إلى الموقع الوهمي البديل من خلال وضع شاشة فيها رابط فوق الشاشة الحقيقة للموقع الصحيح. كما قد يتم إستغلال الأخطاء الشائعة في طرق كتابة بعض أسماء المواقع الإلكترونية المهمة حيث يتم توجيه المستخدمين حينها إلى مواقع إلكترونية شبيهة وهمية بغية تصيدهم.

كما قد يوهم الجاني صاحب حساب مصرفي أنه موظف لدى المصرف ويرسل له رسالة بريد إلكتروني طالباً منه تزويده بكلمة السر وإسم المستخدم من أجل إتمام تصليحات على النظام المعلوماتي أو تحديث نظام الأمان أو لإجراء معاملات روتينية في المصرف. وقد ينخدع العميل ويزود المحتال بالبيانات المطلوبة، فيستعملها الجاني للدخول إلى حساب العميل المصرفي من خلال شبكة الإنترنت عبر ما يعرف Internet Banking لسحب أموال منه.

أما ما يعرف بعمليات الصيد الهادفة Spear phishing، فهي تقنيات من الهندسة الاجتماعية تستهدف أشخاص محددين أو فئات محددة من الأشخاص عبر تجميع معلومات عنهم وعن عاداتهم وحساباتهم وذلك لزيادة فرص إنجاح عمليات التصيد. مثلاً قد يعلم الجاني أن مستخدم معين له

[31]- Jacquet Laurent, Lexique du renseignement de l'information et l'influence, l'esprit du livre, edition 2010, p 102.

حسابات مصرفية لدى أحد المصارف وأنه يستعمل الإنترنت في عمله المصرفي، فيرسل له بريد إلكتروني يبدو أنه صادر عن المصرف مع رابط Link، ويطلب منه إستعمال هذا الرباط لتحديث نظامه المعلوماتي حتى يتمكن من الإستمرار بإلدخول إلى حسابه المصرفي على الإنترنت.

ويمكن للمحتال أن يستهدف فئات محددة من الأشخاص إذا كان من شأن ذلك أن يعزز فرصه بالنجاح.

كما يمكن أن يكون التصيد عبر الإستنساخ (Clone Phishing) عبر رسالة بريد إلكتروني صحيحة مُرسلة سابقاً ولكن يتم تغيير الرابط فيها من رابط صحيح إلى رابط يؤدي إلى الموقع الإلكتروني الوهمي، على أن تصدر الرسالة عن عنوان إلكتروني مزور (spoofed) مشابه للعنوان الرقمي الحقيقي للمؤسسة المعنية أو المصرف. ويمكن أن يتم التصيد لأشخاص عالي المستوى في الإدارة وهو ما يُعرف (Whale phishing).

كما قد يقوم المحتال بتزوير عناوين المواقع الإلكترونية، ما يُعرف Pharming. وهذا يعني إعادة توجيه المستخدم نحو الموقع الوهمي، ولكن يظهر العنوان الصحيح في شريطة المتصفح، مما يصعب إكتشافها، وذلك من خلال:

إختراق الحواسب الخادمة لأسماء النطاق للمواقع الإلكترونية (DNS) وتغيير العنوان الرقمي الحقيقي لإسم الموقع، فهذه الحواسب تترجم إسم الموقع إلى العنوان الرقمي المقابل له.

إختراق الحاسب العائد لمستخدم وتغيير العنوان الرقمي للرمز المعطى لجهاز كمبيوتر مربوط بالشبكة (Hostname) وذلك في ملف موجود في النظام التشغيلي (Operating System).

كما قد يعمد الجاني إلى إخفاء مصدر رسالة البريد الإلكتروني ووضع مصدر كاذب لها أي عنوان رقمي IP لمصدرها غير صحيح أو مختلق وذلك لإضفاء الثقة عليها من خلال ما يعرف بعمليات IP Address Spoofing، حيث يقوم الجاني بتزوير العنوان الرقمي الوارد في حزمة البيانات المُرسلة، بحيث يظهر أنه عنوان صحيح صادر من داخل الشبكة المعلوماتية، مما يسمح بإستغلال بروتكول نقل المعلومات لصالح الجاني لإخفاء عنوانه الرقمي الحقيقي.

وعلي سبيل المثال أيضاً، يرسل الجاني رسالة بريد إلكتروني لعدد كبير من المستخدمين يعدهم فيها بتقاسم حساب مصرفي لشخص متوفي دون ورثة، زاعماً أنه يعمل في مصرف ويرغب في تقاسم هذا الحساب منهم لوجود تشابه في إسمهم وإسم صاحب الحساب أو قرابة معينة، ويطلب منهم إرسال بعض الأموال لتغطية تكاليف المعاملة المصرفية.

كما قد يعد الجاني في رسالة البريد الإلكتروني المُرسلة منه المستخدمين بحضور مؤتمر أو بربح جائزة مقابل أن يدفعوا ولو مبلغ بسيط للعمولات أو لتأسيس الملف أو لتغطية النفقات.

كما قد يوهم الجاني الضحية، من خلال رسالة بريد إلكتروني يُرسلها لها، أنه يتوجب له بذمتها دين ناشئ عن معاملة ما ويطلب منها تسديده عبر تحويل مبلغ من المال.

وتعد وسائل التواصل الاجتماعي من البيئات التي يعتبرها الجناة جنة لأعمالهم الإحتيالية. فأربعين بالمئة من سكان الكون لهم حسابات على وسائل التواصل الاجتماعي كفيسبوك وتوتير وواتس اب وبإزدياد مليون مشترك كل يوم. فهذه الشعبية بالإضافة على الطبيعة المفتوحة لمنصات وسائل التواصل الاجتماعي، تتيح للمجرمين الوصول على عدد خيالي من المستخدمين وإلى كميات هائلة من البيانات الشخصية والتي يمكن إستعمالها لإستهداف فئات خاصة من المستخدمين ولشخصنة عمليات الإحتيال لتكون أكثر إقتناعاً. كما تتيح وسائل التواصل الاجتماعي للمجرمين إخفاء هويتهم الحقيقية خلف حسابات وهمية.[32]

3- تقنيات الإختراق

قد يقوم الجاني في جرائم الإحتيال الإلكتروني بأعمال القرصنة وإختراق قواعد بيانات أو حسابات المستخدمين أو علب بريدهم الإلكتروني للإستحصال على أرقام سر أو بيانات شخصية أو بيانات البطاقات المصرفية أو لإنتحال هوية الآخر الإلكترونية وذلك كله في معرض المناورات الإحتيالية التي قد يقوم بها لإرتكاب جرمه بالإحتيال. وعادةً يقوم بذلك أشخاص لهم معارف تقنية معلوماتية ويعرفون بالهاكرز Hackers، وهم قد يلجأون إلى تقنيات لإختراق البرامج المعلوماتية إما عن طريق تنزيل برامج تجسس spyware or intrusion software في كمبيوترات الضحايا من خلال إغراء المستخدمين بفتح بعض الوصلات المُرسلة لهم في رسالة بريد إلكتروني أو إستغلال الثغرات أو مكامن الضعف في نظام التشغيل Windows أو البرامج المعلوماتية أو من خلال إستعمال خاصية تحديث البرامج وصيانتها عن بعد أو من خلال دمج البرمجيات الخبيثة وإخفائها ضمن برامج أخرى مجانية تؤدي وظائف أخرى للمستخدمين.

وتقوم برامج التجسس بمراقبة نشاط المستخدم وقراءة كل ما يكتبه المستخدم أو يرسله على شبكة الإنترنت أو بتحديد المواقع الإلكترونية التي يتصفحها، أو قد تنسخ محتوى الذاكرة الصلبة، وكل ذلك بهدف إيجاد معلومات حساسة عن المستخدم، ككلمات السر أو البيانات الشخصية أو المالية له. قد يقوم المحتال بإستعمال برامج لإلتقاط كلمة السر العائدة للمستخدم لإختراق حسابه على موقع تواصل إجتماعي أو بريد إلكتروني أو الموقع الإلكتروني لمصرف وهي البرامج معروفة ب Password Sniffer. فهذه البرامج تقوم بمراقبة وضبط حركة حزم البيانات packets المُرسلة من خلال

[32] - Consumers International, Social media scams: Understanding the consumer experience to create a safer digital world, May 2019, https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf, February 2020, p 6.

الشبكة المعلوماتية بهدف رصد وتصفية البيانات السرية فيها، ولاسيما كلمات السر بقصد الإستيلاء عليها.

وقد يستعمل المخترق آلاف الكمبيوترات العائدة لأشخاص آخرين على شبكة الإنترنت، والتي يتحكم بها عن بعد من خلال إصابتها ببرامج للتحكم، وهي ما تعرف بشبكة Bot net، فتصبح هذه الكمبيوترات تعرف بالزومبي كونها تخدم سيد واحد يتحكم بها Bot Master، وهي تطيع أوامره دون أن يعلم صاحبها طبيعة العمل الذي تنفذه بالرغم من أنه قد يعمل عليها يومياً بشكل عادي. ويستعمل الجناة هذه الكمبيوترات في عملياتهم بدلاً من إستعمال كمبيوترهم وذلك لإخفاء آثارهم.

وقد يعمد الجاني، بعد إختراق حساب المستخدم على وسائل التواصل الاجتماعي كفيسبوك أو بريده الإلكتروني، إلى إنتحال هوية هذا المستخدم وإرسال رسائل بريد إلكتروني لكامل لائحة المستخدمين يطلب منهم فيها إرسال مبلغ من المال له كونه قد تعرض مثلاً للسرقة في أحد البلدان أثناء سفره وبحاجة لبعض الأموال لتدبير أموره. وفي حالة مثيرة حصلت في لبنان، تمكن هاكر محترف من إختراق مئات حسابات البريد الإلكتروني لمئات الأشخاص في لبنان، حيث كان يعمد إلى مراقبة كل بريد على حدة ليتمكن من معرفة التعابير وأسلوب الكتابة المُستعمل من قبل كل مستخدم، ثم يعمد بإستعمال ذات أسلوب التخاطب المُستعمل عادةً من قبل صاحب البريد الإلكتروني، للإقناع بصدقية الرسالة وأنه هو صاحب الحساب، للإتصال بلائحة معارف الأخير لطلب تحويل عدد من وحدات الإتصال Units لتعبئة خط الهاتف الخليوي (الجوال) العائد لبطاقة مسبقة الدفع بحجة توقف خط هاتفه، ثم يقوم ببيع هذه الوحدات.

ويبدو أن معظم الناس معرضون لأخطار إختراق حواسبيهم بالنظر لعدم إحتياطهم بصورة مستمرة عبر تفعيل الحوائط النارية أو برامج مكافحة التجسس أو الفيروسات أو تحديث النظام التشغيلي أو البرامج المذكورة بشكل مستمر، لا بل يميلون إلى فتح رسائل بريد إلكتروني مُرسلة من مصادر مجهولة...

خامساً- الخلاصة

يتضح من إستعراض الطرق المختلفة المستعملة من قبل الجناة لإرتكاب الإحتيال الإلكتروني أنها تنطبق على الصور التي أوردتها المادة 655 من قانون العقوبات اللبناني، فهي تتجلى بإيهام الضحية بوجود مشروع وهمي، كوعد بجائزة أو بالحصول على حساب مصرفي متروك أو المشاركة في مؤتمر، أو تلفيق أكذوبة تصدقها الضحية نتيجة ظرف إستفاد منه الجاني، وبالأخص من خلال إستعمال إسم مستعار أو صفة كاذبة للمخادعة أو للتأثير، ألا وهي الهوية الإلكترونية التي يظهر بها

الجاني[33]. كما إعتبرت محكمة إستئناف باريس أن إدخال المدعى عليه لبيانات غير صحيحة إلى نظام معلوماتي بعد إختراقه، مما سمح له بالقيام بعمليات تحويل للأموال لحسابات مصرفية أخرى، يعد كافياً لإثبات وجود جريمة الإحتيال.[34]

- وقد صدرت أحكام كثيرة عن القضاء اللبناني سنداً للمادة 655 عقوبات (جريمة الإحتيال) إعتبرت أن إستدراج الشخص عبر الإنترنت للحصول على بيانات البطاقة المصرفية (Credentials) هو من قبيل المناورات الإحتيالية، وبالتالي تمت إدانة المدعى عليه سنداً للمادة القانونية المذكورة.

في الواقع، إن مسؤولية مراقبة عمليات الإحتيال على وسائل التواصل الاجتماعي تقع على عاتق الشرطة وجمعيات حماية المستهلك ومشغلي وسائل التواصل الاجتماعي. وتعمل شركات التكنولوجيا على إستخدام برمجيات مبتكرة لمكافحة الإحتيال الإلكتروني قبل وصوله للضحايا، فموقع Ebay الإلكتروني طور برمجيات للتعرف على النشاطات التي تخالف المعايير الموضوعة منه، وبإختباره على 300,000 معاملة تعرف على 40% من 492 حالة إحتيال وأخطأ فقط بالنسبة 29 حالة غير إحتيال صنفها كإحتيال. ويسعى غوغل إلى تحليل ومنع البريد الإلكتروني Gmail المُستعمل في عمليات الإحتيال من خلال التحقق من البريد المحتوي على برمجيات خبيثة وإطلاق تحذير للمستخدم إذ اقدم على الرد على شخص غير وارد في لائحة معارفه أو على فتح رباط غير آمن[35].

وبموازاة جهد الشرطة، من المهم أيضاً إطلاق حملات توعية للمستخدمين من عمليات الإحتيال الإلكتروني، ويمكن أن يؤدي ذلك إلى إنخفاض كبير في عدد عمليات الإحتيال الإلكتروني الناجحة. وتشمل التوعية كيفية التعرف على عمليات الإحتيال وكيفية الحماية منها وكيفية التبليغ عنها في حال التعرض لها.

ويمكن للمستخدمين أن يتخذوا بعض التدابير لحماية نفسهم من عمليات الإحتيال، مثل التحقق من عمليات التحويل الإلكتروني مع المستحقين لها وطلب وثائق عنها، وإجراء بحث على محركات البحث حول المنتج أو الشخص أو حول ملاحظات المستخدمين حولها وإستعمال وسائل دفع مناسبة وتجنب النقود الإلكترونية وبطاقات الهدية والبطاقات الدائنة المسبقة الدفع، ومحاولة معاينة البضاعة شخصياً قبل الدفع وإكتمال إستلام الخدمة قبل الدفع وعدم الدفع إلا لأشخاص سبق اللقاء بهم

---

[33] - وقد صدر حكم جزائي عن القاضي المنفرد الجزائي في بعبدا بتاريخ 2012/6/13 (غير منشور) أدان مدعى عليه بجريمة الإحتيال لإستيلائه على أموال الناس عبر قرصنة حسابات بريد إلكتروني لأشخاص وإستعمالها عبر مراسلة أقارب وأصدقاء لهم منها منتحلاً هوية صاحب البريد الإلكتروني وذلك لحملهم عل إرسال وحدات مسبقة الدفع لهاتف خلوي (جوال).

[34] - Cour d'Appel Paris, 13/2/1990, Juris Data n 022903.

[35] - Consumers International, Social media scams: Understanding the consumer experience to create a safer digital world, May 2019, https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf, February 2020, p 17.

شخصياً...[36] وفي حال عدم معرفة المُرسل عدم فتح الملفات المرتبطة برسالة البريد الإلكتروني والإنتباه من العبارات الغريبة أو المتطرفة أو التي تصف الموضوع بالمستعجل والإنتباه إلى كون الرسالة موجهة بشكل عام دون ذكر إسم الشخص الموجه له (فهذا دليل على أنها محاولة إحتيالية موجهة لأعداد كبيرة من المستخدمين)، والتدقيق في الصياغة والأخطاء اللغوية فرسائل المحتالين تكون مليئة بها من حيث المبدأ، والإنتباه إلى عبارات تخويف المستخدم (وهي إستراتيجة يعتمدها المحتالون لحمل المستخدم على كشف بياناته الحساسة)، أو محاولة طلب بيانات شخصية والإنتباه إلى الروابط والملفات المرتبطة بالرسالة.[37] كما يتوجب على المستخدم تنزيل برامج للحوائط النارية Firewalls وبرامج أخرى لمحاربة الفيروسات Antivirus وبرامج أخرى لمكافحة التجسس المعلوماتي Antispyware وتفعليها وتحديثها بشكل دائم، كما تحديث البرامج التشغيلية Operating system/windows بشكل دائم.

ويتضمن على سبيل المثال الموقع الإلكتروني لمكتب التحقيقات الفيدرالية في الولايات المتحدة توجيهات مفصلة للمستخدمين عن مختلف أشكال عمليات الإحتيال المكتشفة وذلك لمساعدتهم على عدم الوقوع ضحية لها.[38] ومن الإرشادات المهمة للمستخدمين: إستعمال المواقع الإلكترونية المعروفة والشهيرة في تعاملاتهم وتجنب المواقع غير المعروفة، ومحاولة التحقق من الموقع الإلكتروني من خلال ربطه بمعطيات مادية كالإتصال برقم الهاتف المذكور عليه أو التحقق من مركز الشركة المذكور على الموقع أو من رقم تسجيلها في السجل التجاري والإدارة الضريبية والواردين على الموقع الإلكتروني والتحقق من كون البريد الإلكتروني للشركة يعمل وغير وهمي...

---

[36] - Charles Schwab, Protect yourself from financial fraud, file:///C:/Users/wassim/Documents/MD/Laws%20Studies/Droit%20de%20l'informatique/scams/Consumers%20International,%20Social%20media%20scams-%20Understanding%20the%20%20consumer%20experience%20to%20create%20a%20safer%20digital%20world_May%202019.pdf, May 2019 2020, p 4.

[37] - US Bank, Cyber scam spotter Signs of scams, 2019, https://www.usbank.com/dam/documents/pdf/online-security/cyber-scam-spotter-10-19.pdf, p 1.

[38] - FBI Federal Bureau Investigation Website, https://www.fbi.gov/scams-and-safety/common-fraud-schemes.