Distr.: General
25 March 2024
Arabic
Original: English

مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

فريق الخبراء الحكوميين العامل المعني بالمساعدة التقنية

فيينا، 3 و4 حزيران/يونيه 2024

البند 3 من جدول الأعمال المؤقت*

الاحتيال المنظم

الاحتيال المنظم

ورقة معلومات أساسية من إعداد الأمانة

أولا- مقدمة

1- أعدت الأمانة ورقة المعلومات الأساسية هذه لتيسير المناقشة في إطار البند 3 من جدول الأعمال المؤقت للاجتماع الخامس عشر لفريق الخبراء الحكوميين العامل المعني بالمساعدة التقنية. وهي تقدم لمحة عامة موجزة غير شاملة عن مختلف فئات الاحتيال المنظم التي تُستخدم لاستهداف الأفراد أو المؤسسات لأغراض الحصول على منفعة مالية أو منفعة مادية أخرى، وتهدف إلى تشجيع اتخاذ تدابير أكثر فعالية للتصدي للاحتيال المنظم في إطار اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

2- وقد تطور الاحتيال تطورا كبير على مر السنين، وتكيَّف مع التطورات التكنولوجية والتغيرات في المجتمع. فهو يزداد تقدما باطراد، إذ يستخدم التلاعب النفسي والتكنولوجيا، ويطوِّع التعلم الآلي والذكاء الاصطناعي وغير ذلك من الأدوات التكنولوجية لأتمتة ارتكاب الجرائم. وتشكل كثرة حالات الاحتيال وشدتها خطورة كبيرة على الناس والاقتصادات والرخاء في جميع أنحاء العالم، وتخلف أثرا سلبيا على ثقة الناس في سيادة القانون. بيد أن الوصول إلى فهم دقيق للاحتيال ينطوي على تحديات عدة. فغالبا ما يكون معدل إبلاغ الضحايا عن الاحتيال منخفضا عن الواقع بسبب مشاعر الخجل أو لوم الذات أو الحَرَج، فضلا عن عدم الدراية بوقوع جريمة. وعلاوة على ذلك، يستهدف جزء كبير من عمليات الاحتيال الشركات، التي يختار كثير منها عدم الإبلاغ عن هذه الجرائم لتجنب الإضرار بسمعته. ويؤدي ارتباط الاحتيال بجهات مجهولة تعمل عن بعد إلى زيادة حجب هوية الجناة عن الضحايا والسلطات على حد سواء، مما يعوق الجهود المبذولة لتقييم أنماطه الأساسية والمخاطر المرتبطة به. وإضافةً إلى ذلك، فإن الطابع الديناميكي للاحتيال، الذي يتكيف باستمرار مع التغيرات في النظم القانونية والاجتماعية والتجارية والتكنولوجية، يستتبع احتمال إغفال أساليب الجريمة الجديدة والمبتكرة في البيانات الرسمية الثابتة.

* CTOC/COP/WG.2/2024/1.

3- وقد أقر المجتمع الدولي بالنطاق المقلق للاحتيال وضرورة بذل جهود مشتركة لمنع الاحتيال ومكافحته[1]. وأكدت الجمعية العامة مجددا، في قرارها 229/78، الولاية المسندة إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة والمتمثلة في التعاون التقني مع الدول الأعضاء وتزويدها بالمساعدة، بناء على طلبها، فيما يتعلق بجميع أشكال الجريمة المنظمة، بما في ذلك الاحتيال. ويتماشى ذلك مع الغرض من اتفاقية الجريمة المنظمة، التي تهدف إلى تعزيز التعاون على منع الجريمة المنظمة عبر الوطنية ومكافحتها بمزيد من الفعالية، على النحو المبين في المادة 1 منها. وإدراكا من الجمعية العامة للطبيعة المتغيرة للاحتيال وتزايد استخدام التكنولوجيا لتوسيع نطاقه، فقد أهابت، في قرارها 177/74، بالدول الأعضاء أن تستكشف تدابير وتضع استنتاجات وتوصيات ممكنة تهدف إلى توفير بيئة سيبرانية آمنة ومتينة، مع إيلاء اهتمام خاص للجرائم المتصلة بتزوير الهوية.

4- وثمة اعتراف واسع النطاق بأن الاحتيال يمكن أن يكون من الجرائم المنظمة والخطيرة[2]. وقد أدى تطور التكنولوجيا إلى جانب التوسع السريع في نطاق الجريمة المنظمة وحجمها إلى إنشاء مجموعة من الطرق الجديدة للاحتيال على الأفراد والشركات وحتى الحكومات على نطاق هائل وعالمي. ومكّن ذلك الجماعات الإجرامية المنظمة من استهداف الضحايا في جميع أنحاء العالم بمزيد من الفعالية[3].

5- ويتسم الاحتيال في مجال الجريمة المنظمة بخصائص مميزة. أولا، فالمسألة تتعلق بسرقة النقود في المقام الأول لا إنتاج السلع غير المشروعة أو توزيعها، مما يميزه عن الأنشطة الإجرامية الأخرى. ثانيا، كثير من الأنشطة الاحتيالية يُجرى عن بعد، بتيسير من التكنولوجيا التي تتيح الاتصال دون كشف الهوية وتحويل الأموال المسروقة دون تفاعل مادي بين الجاني والضحية. ثالثا، غالبا ما يعتمد الاحتيال على أن يتيح الضحايا الوصول إلى أموالهم بإرادتهم، حيث يتوقف نجاح الاحتيال على تكتيكات خادعة تطمس الخط الفاصل بين الكيانات المشروعة وغير المشروعة. وهذه العناصر هي التي تشكل الطرائق التي يستخدمها المحتالون، وتحدد القدرات اللازمة، وتؤثر في بنية الجماعات الإجرامية المنظمة.

6- ويكون بعض هؤلاء المحتالين منخرطين في أعمال أو مهن تبدو مشروعة. وتعتمد بعض الجماعات الإجرامية المنظمة هياكل مشابهة لأماكن العمل المشروعة بالارتكاز على المعلومات أو المهارات المكتسبة من العمل في مجالات مشبوهة أو غير خاضعة للتنظيم تقع خارج نطاق المعايير التقليدية للأعمال والتجارة. وقد ينطوي ذلك على إنشاء قوة عاملة بأجر وتنفيذ تقسيم محدد جيدا للعمل، يحاكي فعليا الأطر التنظيمية القائمة في المؤسسات المشروعة. ولا يوجد مثال نموذجي للجماعات الإجرامية المنظمة الضالعة في الاحتيال. فالاحتيال يمكن أن ترتكبه مجموعات شتى، منها الشبكات السيبرانية الإجرامية التي تتاجر في التكنولوجيا والبيانات وخدمات إجرامية أخرى دون الكشف عن هويتها؛ والجماعات الإجرامية المنظمة التي تتجمع حول منطقة محلية أو شبكات اجتماعية؛ والجماعات الإجرامية المنظمة التي تحاكي في تكوينها قوة عاملة مشروعة (مثل مراكز الاتصال)؛ والمجرمين من ذوي الياقات البيضاء الذين يرتكبون الاحتيال في إطار منظمات أو مهن مشروعة في الأصل. وعوضا عن التسلسل الهرمي، كثيرا ما تتميز الجماعات الإجرامية المنظمة بتعاون سلس بين أعضائها.

7- بيد أن الفهم المتعمق للاحتيال المنظم ليس مرتبطا بطريقة تنظيم الجناة بقدر ارتباطه بطريقة تنفيذ الأنشطة الاحتيالية. وتاريخيا، لم يُعطَ الاحتيال نفس مستويات الأولوية التي تُعطى لأنواع أخرى من الجريمة

(1) انظر قرارات المجلس الاقتصادي والاجتماعي 26/2004 و20/2007 و22/2009 و35/2011 و39/2013 بشأن التعاون الدولي على منع الاحتيال الاقتصادي والجرائم المتصلة بالهوية والتحقيق فيها وملاحقة مرتكبيها قضائيا ومعاقبتهم.

(2) European Union Agency for Law Enforcement Cooperation (Europol), *Internet Organized Crime Threat Assessment (IOCTA) 2023* (Luxembourg, Publications Office of the European Union, 2023)؛ والمنظمة الدولية للشرطة الجنائية (الإنتربول)، "اتجاهات الجريمة في العالم، الإنتربول: تقرير موجز لعام 2022" (تشرين الأول/أكتوبر 2022).

(3) الإنتربول، "تقييم الإنتربول للاحتيال المالي: تهديد عالمي تغذيه التكنولوجيا"، 11 آذار/مارس 2024.

المنظمة، حيث إن الاحتيال المنظم كثيرا ما ينظر إليه على أنه نشـــاط إجرامي تكميلي للجماعات الإجرامية المنظمة الضـــالعة في جرائم أخرى أكثر خطورة (مثل الاتجار بالمخدرات)[4]. وتعرِّف اتفاقية الجريمة المنظمة الجريمة الخطيرة بأنها جريمة يعاقَب عليها بالســجن لمدة لا تقل عن أربع ســنوات. غير أن دولا كثيرة لا تجرِّم الاحتيال في الممارســة العملية باعتباره جريمة خطيرة. ونتيجة لذلك، فإنه يقع خارج نطاق اختصـــاص اتفاقية الجريمة المنظمة. وعلاوة على ذلك، حتى في الحالات التي تصـــدر فيها عقوبة على الاحتيال باعتباره جريمة خطيرة، فإن الأحكام الصادرة لا تعكس بالضرورة هذه الخطورة.

ثانيا- فئات الاحتيال المنظم

8- الاحتيال جريمة تشمل أفعالا وسلوكيات شديدة التنوع تُرتكب على نطاق مجموعة واسعة من السياقات وضد ضحايا متباينين. وتقدم البحوث الأكاديمية تعريفا فضفاضا للاحتيال بأنه "الحصول على شيء ذي قيمة أو تجنب التزام عن طريق الخداع"[5]. ولذلك، وخلافا للأشـــكال الأخرى من جرائم الاســـتحواذ الخطيرة، يُرتكب الاحتيال عن طريق الخداع عوضـا عن القوة أو الإكراه. وعلاوة على ذلك، نادرا ما يلزم وجود الضـحية والجاني في نفس المكـان في الوقـت نفســـه، وكثيرا مـا تكون عمليـات الاحتيـال عـابرة للحـدود الوطنيـة والـدوليـة. ويظهر الاحتيال في القوانين الجنائية للعديد من البلدان، وإن كان يوصَـــف بطرق مختلفة وبدرجات متفاوتة من التحديد[6]. وتقدم بعض القوانين وصفا عاما للسلوكيات التي تشكل احتيالا، بينما تشير قوانين أخرى إلى أنشطة أو منتجات أو خدمات معينة بارزة في المخططات الاحتيالية، مثل انتحال صـــفة شـــخص في موقع ســـلطة أو التلاعب بالبيانات أو اسـتخدامها دون إذن. وقد اسـتحدثت بعض الدول تشـريعات منفصـلة لتناول مختلف جوانب جرائم الاحتيال، مثل الاحتيال الحاســـوبي أو الاحتيال الائتماني أو الاحتيال في المزادات أو الاحتيال ضـــد الأعمال التجارية. إلا أن ثمة عناصـــر أســـاســـية للاحتيال ترِد في معظم التعاريف القانونية، ألا وهي: اسـتخدام الخداع للحصـول على ميزة أو منفعة جائرة، مما يتسـبب في ضـرر لشـخص آخر أو منظمة أخرى. وعادة ما يُفهم الخداع على أنه خيانة للأمانة أو عروض كاذبة أو حيل أو مكائد أو مناورات احتيالية أو إسـاءة اسـتغلال للثقة أو إخفاء معلومات أو إغفالها. والضـرر الذي يلحق بشـخص آخر ينطوي في كثير من الحالات على منفعة للجناة، ولكن البعض يسلط الضوء على الضـرر الذي يلحق بشـخص آخر باسـتخدام مصـطلحات مثل التأثير على المصـــالح المالية للآخرين أو الإضـــرار بها، أو حدوث خســـارة غير مشـــروعة أو التعرض للاحتيال. ويمكن أن يقع الضرر على فرد أو شركة أو دولة.

9- وتتباين جرائم الاحتيال تباينا كبيرا من حيث الأسـاليب المسـتخدمة والكيانات المسـتهدفة والأثر على الضـحايا والنظم بصـفة أشـمل. ونتيجة لذلك، ابتُكر العديد من التصـنيفات لفهم طبيعة الاحتيال. وفي حين أن ثمة تصنيفات أخرى للاحتيال معترف بها على الصعيدين الوطني والدولي، تركز ورقة المعلومات الأساسية هذه على الاحتيال الذي يسـتهدف الأفراد أو المؤسـسـات العامة أو الخاصـة لأغراض تحقيق منفعة مالية أو منفعة مادية أخرى. ولغرض البيان، حُدِّدت الفئات الرئيسية التالية، التي سيرد شرحها بمزيد من التفصيل في الأقسام التـاليـة من ورقـة المعلومـات الأســـاســـيـة: (أ) الاحتيـال المتعلق بـالمنتجـات والخـدمـات الاسـتهلاكية؛ (ب) الاحتيال المتعلق باسـتثمارات المسـتهلكين؛ (ج) الاحتيال المتعلق بالتوظيف؛ (د) الاحتيال

(4) Michael Levi, “Organized fraud” in *The Oxford Handbook of Organized Crime*, Letizia Paoli, ed. (Oxford, Oxford University Press, 2014).

(5) Grace M. Duffield and Peter Grabosky, *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, No. 199 (Canberra, Australian Institute of Criminology, 2001).

(6) جرى الاطلاع على التعاريف القانونية في 26 بلدا في 7 مناطق مختلفة: أوروبا وأمريكا الشمالية؛ وأمريكا اللاتينية والكاريبي؛ وشمال أفريقيا وغرب آسيا؛ وأفريقيا جنوب الصحراء الكبرى؛ وجنوب وسط آسيا؛ وشرق وجنوب شرق آسيا؛ وأستراليا ونيوزيلندا.

المتعلق بالعلاقات والثقة؛ (هـ) الاحتيال الذي ينطوي على انتحال شخصية مسؤولين؛ (و) الاحتيال المتعلق بالهوية؛ (ز) الاحتيال ضد الشركات أو المنظمات.

10- وضمن هذه الفئات الرئيسية، يُسلَّط الضوء على الأشكال الأساسية للخداع التي تتعلق بالمنفعة أو النتيجة المتوقعة للضحية من المعاملة الاحتيالية. وعلى الرغم من أن هذه الفئات ليست حكرا على الجماعات الإجرامية المنظمة، فإن القدرة على ارتكاب الجرائم وإلحاق الضرر تزداد إلى حد كبير بضلوع تلك الجماعات فيها. وتمثل كل فئة أسلوبا مختلفا للتلاعب بالضحايا، ولكن جميع الفئات يمكن أن تكون عبر وطنية وتشمل شركاء في الجريمة ينتمون إلى جماعات إجرامية منظمة. وبعضها يُرتكب على نطاق كبير ويؤدي إلى تأثير إجمالي كبير، في حين يَلحق ضرر شديد بمجموعات أصغر من الضحايا في حالات أخرى.

ألف- الاحتيال المتعلق بالمنتجات والخدمات الاستهلاكية

11- يمثل الاحتيال المتعلق بالمنتجات والخدمات الاستهلاكية أحد أكثر أنواع الاحتيال انتشارا، حيث تبلغ أعداد كبيرة من أفراد الجمهور عن التعرض لاحتيال أو استهداف أو تلقّي اتصالات لبيع منتجات أو خدمات احتيالية. وينطوي هذا النوع من الاحتيال على بيع منتجات أو خدمات وهمية أو مختلفة اختلافا كبيرا عن المُعلَن عنه. وعادة ما يسوِّق المحتالون لمنتجات يكثر الطلب عليها أو يعرضون منتجات وخدمات بتكلفة أقل من المتاح في السوق المشروعة. ويستهدف بعض المحتالين بإعلاناتهم الفئات التي تعتبر أكثر عرضة لقبول مخطط معين. ويمكن أن تشمل عمليات الاحتيال بائعين وأصناف وهميين تماما ولكنها قد تشمل أيضا شركات تعرض وصفا مضللا للسلع أو الخدمات التي تقدمها. ويمكن أن ينطوي تأكيد وقوع الاحتيال على صعوبة عندما يكون المنتج أو الخدمة قد وصل إلى المستهلك ولكنه اعتُبر مختلفا عن الإعلان. وفي بعض الأحيان يستغل المحتالون افتقار الضحية إلى الإلمام بالأمور المالية من أجل بيع الخدمات المالية مثل القروض أو خطط التأمين أو المنتجات المتعلقة بالمعاشات التقاعدية. وتتعلق هذه الخدمات عادة بمنتجات تظهر قيمتها في المستقبل، وإما أن يُقدَّم للضحايا توقعات مفرطة التفاؤل للأداء في المستقبل أو لا تُشرَح لهم المخاطر كما يجب. وقد لا يفصح المحتالون للضحية أيضا عن الرسوم أو العمولات أو المتطلبات القانونية، مما قد يؤدي إلى مزيد من الخسائر والعقوبات[7].

12- وتشمل المنتجات والخدمات التي يكثر بصددها الاحتيال المتعلق بالمنتجات والخدمات الاستهلاكية الأحجار الكريمة والحيوانات الأليفة وتذاكر الفعاليات والمنتجات الطبية واليانصيب والسحب على جوائز واعدة بمكافآت كبيرة والمنتجات والخدمات المالية من قبيل التأمين. إلا أن المنتجات والخدمات التي يمكن استخدامها في المخططات الاحتيالية تكاد تكون بلا حصر، حيث يسعى المحتالون إلى التكيف باستمرار والاستفادة من الأسواق وطلبات المستهلكين الجديدة.

13- وتُستخدَم مجموعة متنوعة من الوسائط لتسويق المنتجات والخدمات، بما في ذلك الإنترنت. وتشمل هذه الوسائط المواقع المزيفة، ومواقع التسوق والمزادات المشروعة على الإنترنت، والرسائل الإلكترونية التطفلية، والبريد أو ما يسمى بـ"غرف المراجل (boiler rooms)" التي تجري كميات كبيرة من مكالمات التسويق والمبيعات. ويستغل بعض الجناة السوق النشطة لقوائم العملاء المحتملين التي تُجمَع بوسائل مشروعة أو غير مشروعة (مثل حملات اختراق البيانات أو التصيد الإلكتروني) أو حتى أدلة بيانات الأفراد الذين وقعوا ضحايا للاحتيال في الماضي (ما يسمى بقوائم "المغفلين"). وقد زادت تكنولوجيات المعلومات والاتصالات إلى حد كبير من القدرة على تسويق وبيع المنتجات والخدمات على نطاق عالمي وبتكلفة منخفضة نسبيا. وفي بعض

(7) انظر Michael Skidmore, *Protecting People's Pensions: Understanding and Preventing Scams* (London, The Police Foundation, 2020).

الحالات، قد يخسر فرادى المستهلكين المال ولكن قد تتكبد منصة مبيعات أو جهة مقدمة لخدمات مالية خسائر مالية حسب الظروف والأساليب التي يتبعها الجناة. وتشمل المنهجيات الرئيسية ما يلي:

(أ) مواقع شبكية مزيفة طُوِّرت لغرض تسويق و/أو بيع المنتجات والخدمات. وقد يسوِّق الجناة للموقع الشبكي باستخدام قنوات رقمية، مثل وسائل التواصل الاجتماعي أو الرسائل الإلكترونية التطفلية، أو قد يتلاعبون بمحركات البحث على الإنترنت لزيادة احتمالية وصول الباحثين عن المنتجات أو الخدمات ذات الصلة إلى موقعهم الشبكي؛

(ب) البائعون المزيفون على منصات البيع أو المزايدة أو وسائل التواصل الاجتماعي المشروعة الذين يستخدمون حسابات مفتوحة بهويات مزيفة أو مسروقة. ويستغل هؤلاء البائعون المنصات المشروعة التي تتيح وصول عدد كبير من المستخدمين الذين يبحثون عن منتجات وخدمات. فعلى سبيل المثال، نشرت جماعة إجرامية منظمة مئات أو آلاف القوائم لسلع عالية القيمة مثل السيارات في مواقع مزادات متعددة[8].

14- وليس من الضروري أن يتسم الاحتيال على المستهلكين عبر الإنترنت بأساليب متطورة أو معقدة. فإساءة استغلال موقع شبكي مشروع للبيع أو المزايدة لا يتطلب إلا فتح شخص واحد لحساب على موقع للمزادات ونشر إعلان لبيع منتج غير موجود. بيد أن جرائم الاحتيال على المستهلكين يكون بعضها عابرا للحدود الوطنية وتشارك فيه جماعات إجرامية منظمة. ونادرا ما يُكشف التنظيم أثناء التعامل مع الضحية، وإنما من فهم التخطيط والإعداد الكامنين وراءه. وتشمل المراحل الرئيسية إنشاء ملف تعريف الموقع الشبكي أو المنصة والتسويق له، والتواصل مع الضحايا للاستمرار في خداعهم (أو استدراجهم لدفع مبالغ أكبر)، وتحريك الأموال. ويتبع الجناة مجموعة متنوعة من الأساليب لتلقي المدفوعات دون ترك أثر مالي يُذكَر. وتشمل تلك الأساليب إقناع الجهات المقدمة لخدمات المدفوعات بأن شركاتهم مشروعة، أو تحويل العملاء إلى مواقع دفع مزيفة أو مطالبة الضحايا بالدفع باستخدام بطاقات السحب المدفوعة مسبقا أو استخدام حسابات أطراف ثالثة لوسطاء نقل المال المسمون ببغال الأموال أو حسابات فُتحت باستخدام هويات مسروقة أو مزيفة. وعادة ما تقوم الجماعات الإجرامية المنظمة التي تعمل من ولايات قضائية أخرى بتجنيد شركاء في الجريمة من داخل البلد المستهدف لتيسير غسل الأموال[9].

باء- الاحتيال المتعلق بالاستثمار

15- عادة ما ينطوي الاحتيال المتعلق بالاستثمار على بيع أسهم شركات أو سندات أو عملات، حيث تسوِّق بعض المخططات لاستثمارات في موجودات عينية تتراوح بين عقارات أو منشآت تجارية ونبيذ ومشروبات كحولية.

16- ويمكن أن يتطلب ارتكاب عمليات الاحتيال هذه وعيا شديدا بمعالم اللوائح والضوابط ذات الصلة التي تحكم الأسواق، ويمكن أن يكون الخط الفاصل بين الممارسات المشروعة وغير المشروعة قابلا للاختراق ومبهما. وفي بعض الحالات، يستغل الجناة آليات الثقة من خلال التسجيل بصفة كيان نظامي أو استغلال

(8) لمزيد من المعلومات، انظر مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (بوابة "شيرلوك")، قاعدة بيانات السوابق القضائية، *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*. على الرابط التالي: https://sherloc.unodc.org/.

(9) Christine Conradt, "Online auction fraud and criminological theories: the Adrian Ghighina case", vol. 6, No. 1, *International Journal of Cyber Criminology*, (January/June 2012)؛ و Jack M. Whittaker and Mark Button, "Understanding pet scams: a case study of advance fee and non-delivery fraud using victims' accounts", *Journal of Criminology*, vol. 53, No. 4 (September 2020).

جهات فاعلة مشروعة أخرى ذات وضع نظامي. وينشئ الجناة، باحتلال هذا الهامش الرمادي بين الممارسات المشروعة وغير المشروعة، عوائق أمام أجهزة إنفاذ القانون وغيرها من الجهات التنظيمية اللازمة لفحص وتقديم أدلة كافية وقوية على الخداع وإثبات وقوع جريمة. وفي الواقع، قد يستخدم البعض مخططات تسبب ضررا كبيرا للمستثمرين ولكن يتبين أنها ليست إجرامية رغم عدم أخلاقيتها. وتمثل مخططات الاحتيال الهرمي ومخططات بونزي نموذج عمل شائعا للجناة، حيث يعتمد مخطَّط الاستثمار على جذب مستثمرين جدد باستمرار للحفاظ على المخطط، عوضا عن إدرار عوائد من منتجات أو استثمارات حقيقية قد لا تكون موجودة أصلا.

17- ويبدو أن الاحتيال المتعلق بالاستثمار في ازدياد، فيما يعزى جزئيا إلى ارتفاع معدل الاحتيال الذي ينطوي على استثمارات في العملة المشفرة. ويستغل ذلك الوسيط الجديد للاحتيال المتصل بالاستثمار السرعة والمرونة اللتين توفرهما المساحات الرقمية، مما يسمح للجناة بالانخراط في التسويق الواسع النطاق بسرعة وبتكلفة منخفضة نسبيا[10]. وفي الأسواق المالية الجديدة، مثل سوق العملة المشفرة، تنشئ التحديات المتعلقة بالتنظيم فجوات أوسع يمكن استغلالها. وتتنوع الأساليب المستخدمة في عمليات الاحتيال المتعلقة بالاستثمار في العملة المشفرة من حيث درجة تعقيدها التقني وحداثتها، إذ تُنقَل بعض التقنيات من طرق أخرى مثل التلاعب بالسوق والاستمالة المالية، والتي تشمل تطوير منصات للاستثمارات الاحتيالية في العملة المشفرة والتسويق لها وما يسمى بـ "عمليات الإغلاق الاحتيالي" أو "سحب البساط" التي تنطوي على رفع مصطنع لقيمة العملات الرمزية الاحتيالية، ثم تصبح عديمة القيمة بمجرد سحب الجناة لجميع الأموال المستثمرة.

18- ويتوقف نجاح عمليات الاحتيال المتعلقة بالاستثمار على الاتصال الفعال، باستخدام تقنيات متنوعة لإقناع المستثمرين المحتملين مثل الحملات التسويقية المحددة الأهداف أو الواسعة النطاق؛ وأساليب البيع الشرسة؛ وإنتاج الموارد اللازمة لتأسيس المصداقية والثقة والحفاظ عليهما، بما في ذلك العلامات التجارية والمواقع الشبكية والمواد التسويقية الأخرى. ويمكن للجناة استخدام قنوات اتصال بعينها، أو توليفة منها، تُستعمَل في مراحل مختلفة من الجريمة. على سبيل المثال، قد يكون أول اتصال بالضحية من خلال موقع شبكي للتصيد الإلكتروني، تتبعه مكالمة مبيعات لاحقة، ثم يستمر التواصل من خلال موقع شبكي احتيالي. وقد يستخدم المحتالون الطرق التالية للتواصل مع الضحايا:

(أ) التسويق عبر الهاتف: استخدام مراكز الاتصال أو غرف المراجل للانخراط في حملات شرسة للتسويق والمبيعات، غالبا ما تتخذ هيئة مكالمات غير مرغوب فيها يُحدَّد الأشخاص المستهدفون بها باستخدام قوائم العملاء المحتملين التي تُجمَع أو تُشتَرى من جهات فاعلة أخرى مشروعة أو غير مشروعة تعمل على تجميع هذه المعلومات الشخصية المتعلقة بالمستهلكين وبيعها. وفي بعض الحالات، تشمل هذه القوائم أفرادا يُعرف أنهم وقعوا ضحايا سابقا، ومن ثم فهم عرضة لقبول نُهُج استثمار مماثلة، وهي مشكلة تزداد حدتها بالنسبة إلى الضحايا من كبار السن المعرضين للضرر. وقد يتولى الجناة الذين يديرون المخطط الاحتيالي إدارة مراكز الاتصال مباشرة أو يتعاقدون مع متخصصين قادرين على تقديم خدمات "غرفة المرجل" هذه. وقد تقع مقار هذه المراكز في بلدان أخرى غير الضحايا، وأحيانا في ولايات قضائية معروفة بقلة صرامة ضوابطها فيما يتعلق بهذه الأنشطة[11]؛

(ب) عبر الإنترنت: شهدت بعض البلدان ارتفاعا كبيرا في معدل الاحتيال المتعلق بالاستثمار عبر الإنترنت حيث يُجرى أول اتصال من خلال سبل التواصل عبر الإنترنت مثل وسائل التواصل الاجتماعي

(10) Arianna Trozze, Toby Davies and Bennett Kleinberg, "Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering", vol. 46, *Journal of Forensic Science International: Digital Investigation* (2023).

(11) Neal Shover, Glenn. S. Coffe and Clintin R. Sanders, "Dialing for dollars: opportunities, justifications, and telemarketing fraud", *Qualitative Sociology*, vol. 27, No. 1 (March 2004).

والمواقع الشبكية والتطبيقات الاحتيالية، التي تضطلع بدور رئيسي في الخداع. وتتيح سهولة الوصول إلى التكنولوجيا الرقمية ومجموعات البيانات الكبيرة المتعلقة بالمستهلكين تعزيز القدرة على الانخراط في التسويق على نطاق واسع ومحدد الأهداف إلى حد كبير. على سبيل المثال، يمكن استخدام حملات التصيد الإلكتروني لاستدراج وتحديد الأفراد المهتمين بالمنتج أو الخدمة المعروضَين، مما يوفر الأساس لتحديد أهداف الاتصالات اللاحقة. وعادةً ما يستغل الجناة وسائل التواصل الاجتماعي وتطبيقات الاتصال الرقمي لتسويق منتجاتهم، ويستخدمون في بعض الحالات رموزا من المشاهير أو الثقافة الشعبية لإقناع الضحايا باستثمار أموالهم. وعندما تخترق هذه المخططات الاحتيالية المتصلة بالعملة المشفرة الأسواق المالية الرئيسية، يمكن أن تؤدي إلى مستويات هائلة من الخسائر المالية؛

(ج) التواصل الشخصي: غالبا ما تنطوي الاستثمارات على مبالغ كبيرة من المال أهميتها فائقة للضحايا، وفي بعض الحالات يظل الاتصال وجها لوجه مهما لتحقيق مستويات كافية من الثقة لضمان الاستثمار. ويستهدف بعض المحتالين ضحايا من علاقات اجتماعية أو تجارية قائمة لاستغلال الثقة القائمة بالفعل.

19- ويبذل مرتكبو جرائم الاحتيال المتعلق بالاستثمار جهدا كبير لتهيئة ستار من المشروعية، وعادة ما يعتمدون هياكل المنظمات المشروعة الرسمية وعملياتها ولغتها، بما في ذلك تقسيم واضح للعمل، مع إنشاء تسلسل هرمي وتخصيص أدوار محددة للموظفين. وتتفاوت درجة تعقيد العملية، حسب مدى رغبة الجناة في تجنب الاشتباه أو الكشف ومواصلة ارتكاب الجرائم[12]. فيمكن أن تسري العمليات الخاطفة المسماة بعمليات "النزع والقطع (rip and tear)" لفترة قصيرة قبل أن يختفي الجناة بأموال المستثمرين، في حين يمكن أن تستمر مخططات أخرى دون اكتشافها لسنوات عديدة.

20- ويتكبد ضحايا الاحتيال المتعلق بالاستثمار أعلى خسائر مقارنةً بأنواع الاحتيال الأخرى التي تستهدف أفراداً من الجمهور[13]. ويُستمال الضحايا بتوقعات بعائد مالي تكون إما زائفة كليا أو مبالغا فيها جدا. ويفقد العديد من المستثمرين كل أموالهم أو جزءا كبيرا منها. وبصرف النظر عن الطريقة المستخدمة تحديدا، عادة ما يُقنَع الضحايا بتوقع متعلق بقيمة منتظَر اكتسابها من استثماراتهم في المستقبل، مما يعني أنهم قد يستغرقون سنوات بعد أول استثمار حتى يدركوا أنهم وقعوا ضحايا. ويمكن أن يكون التباين كبيرا بين خصوصيات المخططات المختلفة وأشكال الخداع التي تقوم عليها، ولكن النتيجة في مثل هذه المخططات تنطوي بصفة عامة على خسارة المستثمرين لأموالهم كلها أو جزء كبير منها. ومن الأمثلة عليها ما يلي:

(أ) أن يكون الأمر برمته خدعة لم تتضمن خدمة أو منتجا متصلا بالاستثمار قط؛

(ب) البيع المضلِّل لأسهم عديمة القيمة أو مبالغ في سعرها مقابل استثمارات عالية المخاطر من غير المرجح أن تحقق العائد الموعود أو قد تفشل ببساطة؛

(ج) تقنيات التلاعب بالسوق التي تصطنع لمستثمرين مطمئنين قيمة مبالَغا فيها للاستثمارات.

21- ويتوقف حجم الخسارة المالية التي يتكبدها الضحايا على ظروفهم المالية أو الشخصية. وقد يتوقف أيضا على المنهجيات التي يستخدمها الجناة، مثل استهداف مدخرات المعاشات التقاعدية للأشخاص، مما يمكن أن يخلف تأثيرا كبيرا على فرادى الضحايا[14]، في حين يمكن أن تركز بعض الاستثمارات المتصلة بالعملة

(12) Michael Levi, "Organized fraud and organizing frauds: unpacking research on networks and organization", *Criminology and Criminal Justice*, vol. 8, No. 4 (December 2008).

(13) انظر أيضا United States Department of Justice, "Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes", press release, 3 April 2023.

(14) انظر Skidmore, *Protecting People's Pensions*.

المشـفرة على تلقي مبالغ أصـغر ولكن من عدد أكبر من الضـحايا. وفي حالة ضـحايا المخططات الهرمية ومخططات بونزي، قد لا يخسـر أولئك الذين يسـتثمرون الأموال ويسـحبونها في مرحلة مبكرة أيا من مالهم. ولدى سرقة الأموال، قد يقع الأشخاص ضحية لنفس الجناة أو جناة آخرين مجددا، يُفترَض في بعض الحالات انتماؤهم إلى كيان مشـروع. ويؤكد هؤلاء الجناة قدرتهم على تتبع الأموال المفقودة واسـتردادها ولكنهم يطالبون برسوم مقدمة من الضحية، وهو مخطط يعرف باسم الاحتيال المتعلق بالاسترداد.

جيم- الاحتيال المتعلق بالتوظيف

22- ينطوي الاحتيال المتعلق بالتوظيف على التسويق الواسع النطاق لفرص عمل مزيفة أو مضلِّلة على مواقع الإعلان عن الوظائف. وقد زاد كثيرا اسـتخدام إعلانات الوظائف على الإنترنت في القطاع المشـروع، لا سـيما منذ الجائحة العالمية، حيث يعرض مسـؤولو التوظيف ترتيبات عمل أكثر مرونة وفرص عمل من المنزل. ويستغل المحتالون الطلب على الوظائف المرغوب فيها، وخصوصا لدى شرائح السكان التي تكون فيها الفرص المشـروعة من هذا النوع محدودة بسـبب عدم كفاية المؤهلات أو التدريب أو الافتقار إلى الوظائف المتاحة في الاقتصاد المحلي[15]. ويشير البحث إلى أن الباحثين عن عمل الذين يتسمون بأقل قدر من الأمان المالي أو بأوضاع ميؤوس منها هم من يستهدفهم هؤلاء المحتالون.

23- وعادة ما تتضمن عمليات الاحتيال هذه الإعلان عن فرصة عمل عبر الإنترنت تكون إما زائفة تماما أو أقل ربحية بكثير مما هو معلن عنه. ومن الأمثلة على ذلك الإعلانات عن فرص تجارية أو العمل من المنزل أو فرص لعرض الأزياء. وفي بعض الحالات، يطلب المحتالون من الضحايا دفع مبالغ مسبقة قبل شغل وظيفة؛ وتتعدد الأسباب التي يتذرعون بها، بما في ذلك مستلزمات بدء العمل أو السفر أو التدريب أو التحقق من الجدارة الائتمانية. ويترتب على ذلك في كثير من الأحيان خسارة الضحية للمال دون الحصول على فرصة العمل الموعودة. وفي مخططات أخرى، يرسـل المحتالون شـيكات مزورة إلى الضـحايا لدفع تكاليف بدء عمل الضـحايا ثم يدّعون أنهم دفعوا مبالغ زائدة ويطلبون من الضـحية إعادة الأموال إلى الجاني. فتفقد الضـحية الأموال المحولة ويُترَك لها تحمل تكلفة الشيك ما أن يُكتشَف أنه مزور.

24- ويمكن أن يتحرك المحتالون أيضا بدافع سرقة معلومات الهوية الشخصية، التي يقدمها الضحايا أثناء عملية تقديم الطلب، مما يعرضـهم لمزيد من الضـرر. وفي بعض الحالات، يتبين أن الوظيفة ذات طبيعة إجرامية. فعلى سبيل المثال، قد تتجرّ الضحية إلى تيسير غسل الأموال (كبغال الأموال مثلا) أو تولي تسليم أشـياء اشـتُريت عن طريق الاحتيال (أي الاحتيال المتعلق بالهوية). وفي أخطر الحالات، تصـبح الضـحية عرضة للاتجار بالأشخاص لأغراض السخرة والإجرام القسري[16].

دال- الاحتيال المتعلق بالعلاقات والثقة

25- تضـطلع عمليات بناء الثقة بدور مهم في أي نوع من أنواع الاحتيال. ولكن في حالة الاحتيال المتعلق بالعلاقات والثقة، يعزز الجناة قوة العلاقات الشـخصـية ويسـتغلونها في بناء الثقة اللازمة للتلاعب بالضـحايا

(15) Alexandrea J. Ravenelle, Erica Janko and Ken Cai Kowalski, "Good jobs, scam jobs: detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic", *New Media and Society*, vol. 24, No. 7 (July 2022), pp. 1591–1610؛ و Delali Kwasi Dake, "Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites", *International Journal of Computer Applications*, vol. 184, No. 51 (March 2023).

(16) لمزيد من المعلومات عن هذين الشكلين من الاستغلال، انظر أيضا *Global Report on Trafficking in Persons 2022* (منشورات الأمم المتحدة، 2022)، وكذلك UNODC, "Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia: policy report" (Bangkok, 2023).

وخداعهم، عدة مرات في بعض الأحيان. وفي حالات الاحتيال هذه، لا تتوقع الضحية الحصول على منتج أو خدمة وإنما تتوقع تكوين علاقة حقيقية مع الجاني. ولا يكمن تعقيد هذه الحالات من الاحتيال في استغلال النظم التقنية أو التكنولوجية بقدر ما يكمن في ديناميات العلاقة بين الضحية والجاني.

26- ويقيم العديد من المحتالين علاقات عبر الإنترنت ويستخدمون تقنيات الاستدراج الموجَّه على مدى أشهر أو حتى سنوات لكسب ثقة الضحية. ويتوقع الضحايا عادة علاقة رومانسية، ولكن العلاقة يمكن أن تتخذ أشكالا أخرى مثل صداقة موثوقة، أو حتى الرغبة في إقامة علاقة مع أحد أفراد أسرة الضحية. وقد حدد عدد من الدراسات نقاط ضعف لدى شريحة السكان المسنين والمتقدمين في السن متعلقة بعوامل من قبيل الشعور بالوحدة والعزلة الاجتماعية والرغبة في إقامة علاقات جديدة. ويستهدف المجرمون نقطة الضعف هذه ويستغلونها من خلال عملية إقامة صداقة أو ارتباط عاطفي. وإضافة إلى ذلك، قد ينتحل الجناة شخصية فرد من الأسرة أو صديق يواجه صعوبة شديدة ويحتاج إلى المال لمعالجة الموقف. وقد تكون عمليات الاحتيال هذه محددة الأهداف ويمكن أن تتضمن تفاصيل شخصية مأخوذة من منشورات وسائل التواصل الاجتماعي للصديق أو القريب لجعل التواصل مع الضحية أكثر مصداقية. وعادة ما يُبلَغ ذلك عن طريق رسائل نصية. وثمة أمثلة على استخدام الذكاء الاصطناعي لاستنساخ صوت أحد أفراد الأسرة أو الأصدقاء في مكالمة هاتفية.

27- ويتمثل أحد العناصر الأساسية في هذه الفئة من الاحتيال في الاحتيال العاطفي، حيث يعمل الجناة على إقامة علاقات عاطفية عبر الإنترنت بغرض خداع الضحايا وابتزازهم للحصول على المال. ويمكن أن تترتب عليها خسائر مالية كبيرة للأفراد. وتطال هذه المشكلة العديد من الضحايا في شتى أنحاء العالم، وتستفيد من تنامي ظاهرة إقامة العلاقات الاجتماعية عبر الإنترنت، وبصفة أكثر تحديدا، الاتجاه المجتمعي الأشمل إلى إقامة العلاقات العاطفية عبر الإنترنت. وعادة ما يبدأ الجاني التقرُّب من الضحايا على وسائل التواصل الاجتماعي أو مواقع وتطبيقات المواعدة باستخدام هوية مزيفة يصحبها سرد مقابل لمواصفاته. وقد يقوم جانٍ واحد بالتبديل بين الهويات لاستهداف ضحية محتملة واستدراجها. وبمجرد أن تنشأ العلاقة، قد يحصل الجاني على منفعة مالية بأن يطلب في البداية مبلغا صغيرا من المال ثم يتبعه بطلب مبالغ أكبر من الضحية، وغالبا ما يقدم سيناريو متعلقا بأزمة ما يؤدي إلى الضغط على الضحية وإشعارها بإلحاح الموقف (مثل حالة طوارئ صحية أو احتياج عاجل للسفر). وإذا جرى تبادل صور جنسية، فقد تُبتز الضحية أيضا للحصول على الأموال.

28- وشهد أحدث نموذج لهذه الطريقة تلاقي الاحتيال العاطفي مع الاحتيال المتعلق بالاستثمار في العملة المشفرة. فينطوي التغرير العاطفي أو ما يسمى باحتيال "ذبح الخنازير" – وهو مصطلح لا ينصح باستخدامه، احتراما لضحايا مثل هذه الجرائم – على إقامة الجاني علاقة شخصية مع ضحية عبر الإنترنت. وعوضا عن اختلاق سيناريو الأزمة، يستغل العلاقة الحميمة والثقة القائمة لاستدراج الضحية إلى مخطط استثماري احتيالي. ويمكن أن يستتبع ذلك للجناة مراحل إضافية من التخطيط والإعداد، بما في ذلك تطوير موقع شبكي أو تطبيق احتيالي يمكن للضحية الدخول عليه، وحتى توفير "خدمة العملاء" للمستثمرين[17]. ويترتب على دمج الاستثمار في العملة المشفرة في الخداع عدد من العواقب: فهو يوسِّع نطاق المجموعة المحتملة لتشمل ضحايا من فئات عمرية أصغر؛ ويدخل الضحايا سوقا غير مألوفة ومتقلبة وعالية المخاطر، مما يعني أن يقل احتمال إدراكهم أنهم ضحايا؛ ويطرح المزيد من الصعوبات أمام المحققين الجنائيين في تتبع الأموال للوصول إلى الجناة.

(17) Cassandra Cross, "Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud", *Current Issues in Criminal Justice* (2023)؛ و Fangzhou Wang and Xiaoli Zhou, "Persuasive schemes for financial exploitation in online romance scam: an anatomy on Sha Zhu Pan (杀猪盘) in China", *Victims and Offenders*, vol. 18, No. 5 (2023).

29- وقد ركز الكثير من البحوث المتعلقة بالاحتيال العاطفي على الضحايا وتجاربهم، وليس الجناة الذين هم أقل ظهورا. وتعتبر هذه الجرائم عادة جرائم عبر وطنية ترتكبها جماعات إجرامية منظمة، مع تركز بعضها داخل مناطق معينة. وفي سياق الاحتيال المسمى "ذبح الخنازير"، اعتمدت بعض الجماعات الإجرامية المنظمة هياكل أكثر تطورا أشبه بالأعمال التجارية يوجد فيها تقسيم واضح للعمل (مثل الاتصال بالضحايا، وتكنولوجيا المعلومات، وغسل الأموال) وتوظيف قوة عاملة من الأشخاص المحتاجين إلى المال والمعرضين لخطر الاستغلال، بما يشمل الاتجار بالأشخاص[18].

30- وبصرف النظر عن خصائص الضحايا، يمكن أن يكون تأثير الاحتيال المتعلق بالعلاقات والثقة كبيرا. فالضحايا، إلى جانب تعرضهم لخسائر مالية، يعانون أيضا من انكسار الثقة وفقد علاقة شخصية مهمة. وإضافةً إلى ذلك، فهم يعانون من ضرر نفسي وعاطفي كبير. وقد يرفض بعضهم حتى قبول أنهم كانوا أو لا يزالون ضحايا للاحتيال.

هاء- الاحتيال الذي ينطوي على انتحال شخصية مسؤولين

31- يتضمن الاحتيال الذي ينطوي على انتحال شخصية مسؤولين، أو الاحتيال المتعلق بانتحال الشخصية، التلاعب بالاتصالات بحيث تبدو وكأنها واردة من مسؤول عمومي أو مسؤول آخر، مثل الشرطة أو مصلحة الضرائب أو مصرف أو إدارة حكومية. وترتكز عمليات الاحتيال هذه على مجموعة من الذرائع والسيناريوهات بما في ذلك انتحال شخصية مسؤول في مصلحة ضرائب أو إدارة حكومية أخرى تدعي استحقاق دين غير مسدد؛ أو مسؤول مصرفي يدعي تعرض أموال في حساب مصرفي للتهديد من مجرمين؛ أو الشرطة مدعيةً اكتشافها جريمة ارتكبتها الضحية.

32- ومن السمات المميزة الرئيسية للاحتيال المتصل بانتحال الشخصية استخدام أساليب إقناع لا تستهدف رغبات الضحايا واحتياجاتهم (كما هو الحال في عمليات الاحتيال على المستهلكين) وإنما تثير مشاعر الخوف والرهبة والجزع والقلق. ويؤدي إحداث حالة الانفعال الشديد إلى إعاقة صنع القرار وجعل الضحايا أكثر عرضة للتلاعب. وتهدد هذه الرسائل بحدوث نتيجة سلبية، بما في ذلك شكل من أشكال الرد القانوني، إذا لم ترسل الضحية مدفوعات أو تحول أموال.

33- وعادة ما تُستخدَم في عمليات الاحتيال هذه وسائل الاتصال الجماهيري مثل البريد الإلكتروني التطفلي؛ أو الاتصالات باستخدام وسائل التواصل الاجتماعي؛ أو الرسائل النصية؛ أو المكالمات الهاتفية الآلية، أو ما يطلق عليه اسم "الاتصال الآلي (robodialling)"، حيث تجري أتمتة المكالمات الهاتفية باستخدام رسالة مسجلة. وتيسر هذه التكنولوجيا الاتصال شبه المتزامن مع آلاف الضحايا في وقت واحد، مما يتيح نطاق وصول هائلا.

واو- الاحتيال المتعلق بالهوية

34- ينطوي الاحتيال المتعلق بالهوية[19] على استخدام معلومات الهوية المسروقة أو المزيفة للوصول إلى السلع أو الخدمات أو الأموال من الضحايا مباشرةً، مثل استخدام المعلومات المسروقة لإجراء عمليات شراء أو الوصول إلى الحسابات المالية. ويمكن ارتكاب الاحتيال المتعلق بالهوية دون أي اتصال مباشر ولا اتخاذ إجراء من جانب الفرد الذي يُساء استخدام هويته، لأن الهدف غالبا ما يكون مقدم السلع أو الخدمات أو المال. وبهذه الطريقة ينتشر الضرر بين مختلف الجهات الفاعلة التي تقع ضحية الاحتيال، بما في ذلك الضحية التي

(18) UNODC, "Casinos, cyber fraud, and trafficking in persons".

(19) انظر أيضا UNODC *Handbook on Identity-related Crime* (Vienna, 2011).

يساء استخدام هويتها، والشركة المقدمة للخدمات المالية أو أي شركة أخرى تُهرَّب منها الأموال، وفي بعض الحالات، الجهة المقدمة للسلع أو الخدمات المشتراة باستخدام الأموال المسروقة.

35- وثمة أشكال مختلفة من معلومات الهوية يمكن الحصول عليها، ويمكن استغلال كل منها بطرق مختلفة. وتشمل المعلومات الشخصية، التي تتألف من الهويات الرقمية للأفراد في مختلف الأوساط على الإنترنت، مثل الاسم أو تاريخ الميلاد؛ وبيانات الحسابات المالية، مثل أرقام بطاقات الائتمان؛ ومعلومات الحساب عبر الإنترنت، بما في ذلك أسماء المستخدمين وكلمات المرور؛ والبيانات البيومترية، مثل بصمة رقمية مسروقة من جهاز إلكتروني.

36- ويمكن للجناة الوصول إلى هذه المعلومات عن طريق اختراق النظم؛ ومخططات الاستدراج الموجّه مثل حملات التصيد الإلكتروني أو الاحتيال عن طريق الرسائل النصية القصيرة؛ أو دخول الأسواق الإجرامية التي تبيع البيانات عبر الإنترنت. ويمكن استخدام البيانات لشراء السلع والخدمات، وتقديم طلبات للحصول على قروض وغيرها من أشكال التمويل، أو الوصول إلى الأموال وتحويلها من حسابات الضحايا. وتشمل المعلومات الإضافية المتعلقة بهذه الطرق ما يلي:

(أ) اختراق النظم: ينشط بعض المحتالين في الحصول على المعلومات الشخصية عن طريق تقنيات القرصنة غير المشروعة أو نشر البرامجيات الخبيثة أو التصيد الإلكتروني؛

(ب) الأسواق الإجرامية عبر الإنترنت: ثمة اقتصاد سري نشط معني بشراء معلومات الهوية وبيعها، حيث يمكن لمرتكبي الاحتلال المتعلق بالهوية استغلالها. وتزيل فرصة الحصول على المعلومات بهذه الطريقة بعض الحواجز التقنية أمام المحتالين الذين قد لا تتوافر لديهم القدرة على سرقة المعلومات الشخصية؛

(ج) الاستدراج الموجَّه: غالبا ما يتحقق ذلك عن طريق إعلان أو رسالة أخرى غير مرغوب فيها تُوجَّه عبر البريد الإلكتروني أو أي اتصال آخر عبر الإنترنت أو رسالة نصية أو مكالمة هاتفية غير مرغوب فيها، حيث يُخدَع الضحايا لتقديم معلومات شخصية. وتتفاوت درجة تطور هذه الأساليب، ولكن أكثرها تعقيدا، مثل محاكاة المواقع الشبكية المشروعة يمكن أن يؤدي إلى مكاسب أكبر فيما يتعلق بتزويد الجناة بإمكانية الوصول المباشر إلى الحسابات عبر الإنترنت.

37- ويستعمل الجناة مجموعة من التقنيات لارتكاب الاحتيال المتعلق بالهوية. وتتضمن بعض الطرق الرئيسية الاستيلاء على الحسابات، والمعاملات التي لا تتطلب وجود بطاقة، والاحتيال المتعلق بالتطبيقات، والتي تُعرَّف كما يلي:

(أ) الاستيلاء على الحسابات: في عمليات الاحتيال هذه، يحصل الجناة على بيانات اعتماد مشروعة لدخول حسابات المستخدمين. ويمكن أن تشمل هذه الحسابات حسابات مصرفية، ولكنها تشمل أيضا أنواعا أخرى من الحسابات المالية (مثل مقدمي خدمات العملات الافتراضية) أو مواقع البيع بالتجزئة أو أي جهات مقدمة للسلع والخدمات. ويمكن الاستفادة من الحسابات لعدد من الأغراض، بما في ذلك تحويل الأموال مباشرة إلى حسابات يسيطر عليها الجناة أو شراء السلع أو الخدمات عن طريق الاحتيال باستخدام الحساب. وفي بعض الحالات، يمثل الحصول على معلومات لدخول حساب الضحية الخطوة الأولى في سلسلة من الخطوات اللازمة للوصول إلى الأموال أو السلع أو الخدمات من خلال اختراق النظام لاحقا. وقد يتضمن ذلك التغلب على تدابير أمنية من قبيل الاستيقان بعاملَيْن. ونتيجة لذلك، يلجأ الجناة إلى تقنيات إضافية مثل استبدال شرائح الهواتف المحمولة وطرق الدفع البديلة؛

(ب) المعاملات التي لا تتطلب وجود بطاقة: عمليات شراء غير مصرح بها تُجرى عن بعد مع بائع، سواء عبر الإنترنت أو عبر الهاتف. ويكفي الحصول على بيانات الاعتماد المالية للضحايا لخداع كل من

مقدم الخدمات المالية والبائع التجاري، دون الحاجة إلى التفاعل مع الضحية مباشرة أو الوصول إلى بطاقة الدفع المادية. وثمة عدد من الخطوات الرئيسية اللازمة عادةً لاستغلال مرتكبي الاحتيال المتعلق بالهوية لبيانات الاعتماد المالية للضحايا:

'1' اكتساب المعرفة والموارد وبيانات الاعتماد المالية من الأسواق الإجرامية عبر الإنترنت؛

'2' إخفاء الطلبات لتجنب تشغيل خوارزميات الكشف عن الاحتيال على المواقع الشبكية التجارية؛

'3' تلقي الطلبات على عنوان لا يمكن ربطه بالجناة؛

'4' إعادة بيع الأصناف كبائع فردي أو بيعها بكميات كبيرة عن طريق انتحال شخصية تاجر مشروع في الأسواق الإلكترونية الرئيسية؛

(ج) الاحتيال المتعلق بالتطبيقات: تستغل عمليات الاحتيال هذه التوافر الواسع النطاق للمعلومات الشخصية وتستخدمها للتقدم بطلب للحصول على ائتمان باسم الضحية. ويتم ذلك عادة بهدف الحصول على قرض من جهة مقدمة لخدمات مالية. ويلزم على الجناة الوصول إلى مجموعة من المعلومات الشخصية (مثل الاسم أو العنوان أو تاريخ الميلاد) حتى يتمكنوا من انتحال شخصية الفرد على نحو جدير بالتصديق. ويتمثل أحد الأنماط الناشئة في استخدام التكنولوجيا لإنشاء هويات اصطناعية من خلال الجمع بين معرِّفات حقيقية وملفقة للهوية. وبمجرد إنشاء هذه الهويات، يمكن تعزيزها بمرور الوقت لرفع جدارتها الائتمانية قبل تقديم طلبات للحصول على منتجات مالية عالية القيمة في نهاية المطاف.

38- ومن الجدير بالاهتمام أن ارتكاب الاحتيال المتعلق بالهوية لا يرتبط بضلوع الجريمة المنظمة والجماعات الإجرامية المنظمة. بيد أن القدرة على ارتكاب الاحتيال المتعلق بالهوية على نطاق واسع وتحقيق أرباح عالية تتعزز إلى حد كبير بالمهارات والموارد المتاحة للجريمة المنظمة. ويزداد هذا التهديد حدة بوضوح إثر انتشار الأهداف المتاحة عبر الإنترنت في ظل الاقتصادات الرقمية المتنامية. ويمكن أن يؤدي التلاعب بالهوية وإساءة استخدامها مجموعة متنوعة من الوظائف فيما يتعلق بارتكاب الجرائم المنظمة، بما في ذلك الجهود الرامية إلى تعقب النشاط الإجرامي للوصول إلى الجناة[20].

زاي- الاحتيال ضد الشركات أو المنظمات

39- عادة ما ينطوي الاحتيال ضد الشركات أو المنظمات على إساءة استخدام النظم الداخلية أو علاقة تجارية بهدف الاحتيال على الضحية. ويمكن أن يرتكب عمليات الاحتيال هذه شخص من داخل المنظمة أو خارجها. وبعضها ترتكبه مؤسسات وجهات فاعلة مشروعة في الأساس أو تستخدم منتجات مشروعة، عوضا عن أن تكون مخططات مصممة منذ البداية لارتكاب احتيال، استجابة لضغوط داخلية أو ممارسات أو ثقافة عمل مشبوهة في بعض الأحيان.

40- ومن الأمثلة على الاحتيال ضد الشركات أو المنظمات ما يلي:

(أ) الاحتيال عن طريق اختراق البريد الإلكتروني للأعمال التجارية هو نوع من الاحتيال عبر الإنترنت يُرتكَب بمعدلات كبيرة. وتقع الشركات والمنظمات من جميع الأحجام ومن مختلف القطاعات ضحية لهذا النوع من الاحتيال، الذي يرتكبه عادةً مجرمون من خارجها. فيخترق الجناة النظم ويستخدمون تقنيات الاستدراج الموجّه لإقناع الموظفين بإجراء تحويلات للأموال غير مصرح بها إلى حسابات تحت سيطرة الجناة.

(20) Simon Baechler, "Document fraud: will your identity be secure in the twenty-first century?", *European Journal on Criminal Policy and Research*, vol. 26, No. 3 (June 2020).

ويمكن أن تكون الخسائر التي تلحق بالضحايا كبيرة جدا. وتتمثل الخطوة الأولى في اختراق نظم الاتصال الخاصة بالمنظمة للمساعدة في إقناع متلقيّ الرسائل بشرعية الجناة. وتشمل الطرق الرئيسية اختراق حسابات البريد الإلكتروني للموظفين؛ أو توجيه رسائل التصيد الإلكتروني بالبريد الإلكتروني من أجل الحصول على تفاصيل حسابات الموظفين؛ أو استغلال الجهات المقدمة لخدمات الاتصالات لانتحال أسماء النطاقات المألوفة لدى المنظمة المستهدفة[21]. ويتبنى الجناة سرديات عدة، تشمل استغلال علاقة قائمة بين شركتين من خلال إصدار فاتورة مزيفة؛ أو إرسال بريد إلكتروني يُزعم أنه موجه من موظف كبير يقدم طلبا عاجلا للحصول على أموال؛ أو انتحال شخصية محام يطلب تحويلا برقيا لمعالجة مسألة حساسة[22]. ويمكن أن يحدث الاتصال على مدى فترة من الزمن وقد يستثمر الجناة وقتا في فهم المنظمة ونظمها والهجوم عليها مرات متعددة؛

(ب) تشمل عمليات الاحتيال المتعلقة بالبيانات المالية العديد من الأساليب التي يقوم فيها مختصون بسوق مالية مشروعون في الأصل بتضليل وتشويه رؤية الآخرين من قبيل المستثمرين والمنظمين والجهات الفاعلة الأخرى في السوق للسلامة المالية والآفاق المستقبلية لشركة أو صندوق ما. وقد تواري أنواع مماثلة من الاحتيال المحاسبي أيضا اختلاس الأموال أو سوء استخدامها أو التصرف فيها. ويمكن ارتكاب عمليات الاحتيال هذه استجابة لضغوط لتلبية توقعات الأداء. ومن الأمثلة على ذلك المديرون التنفيذيون للشركات أو السماسرة الماليون المارقون أو مديرو صناديق التحوط الذين يقدمون تقارير عن الأداء المالي. وفي بعض الحالات، يُستشعَر تأثير عمليات الاحتيال هذه خارج نطاق ذلك العمل التجاري، بما في ذلك الأعمال التجارية أو القطاعات الخارجية أو حتى الاقتصاد بنطاقه الأوسع[23]؛

(ج) يمكن أن تُرتكب عمليات احتيال الشركات الطويلة الأمد أو القصيرة الأمد من جانب شركات تجارية قائمة أو شركات ربما جرى شراؤها أو إنشاؤها لغرض احتيالي. فتنشئ تلك الشركات تاريخا ائتمانيا أو ثقة أو مصداقية، تستخدمها لخداع المشتري أو البائع أو الدائن لتوريد السلع أو التمويل. وتقوم بذلك مع العلم بأنها إما لا تستطيع السداد أو لا نية لديها للسداد.

ثالثا- مواضيع مطروحة للنظر فيها

41- لعل الفريق العامل يود أن يوجه تركيز مداولاته إلى المواضيع التالية:

(أ) طبيعة الاحتيال المنظم في مختلف الولايات القضائية؛

(ب) استخدام اتفاقية الجريمة المنظمة لمنع ومكافحة الاحتيال المنظم، وكذلك تجريم الاحتيال باعتباره جريمة خطيرة، حسب التعريف الوارد في المادة 2 من الاتفاقية؛

(ج) فرص التعاون الدولي الفعال، بما في ذلك التعاون مع القطاع الخاص؛

(21) Norah Saud Al-Musib and others, “Business email compromise (BEC) attacks”, *Materials Today: Proceedings*, (vol. 81, Part 2 (2023)) و Geoffrey Simpson, Tyler Moore and Richard Clayton, “Ten years of attacks on companies using visual impersonation of domain names”، ورقة بحثية قُدمت في الندوة المتعلقة بأبحاث الجريمة الإلكترونية (eCrime)، التي استضافها الفريق العامل المعني بمكافحة التصيد وعُقدت في بوسطن، الولايات المتحدة الأمريكية، في الفترة من 16 إلى 19 تشرين الثاني/نوفمبر 2020.

(22) Alessandro E. Agazzi, “Business Email Compromise (BEC) and cyberpsychology”. الرابط الشبكي: https://arxiv.org/؛ و Al-Musib and others, “Business email compromise (BEC) attacks”.

(23) United Kingdom of Great Britain and Northern Ireland, Serios Fraud Office, “Senior bankers sentenced to 9 years for rigging EURIBOR rate”, 1 April 2019.

(د) تبادل المعلومات بشأن منع الاحتيال المنظم، وحماية ضحايا الاحتيال والشهود، وكذلك المبلغين عن المخالفات، وملاحقة الجماعات الإجرامية المنظمة الضالعة في الاحتيال المنظم، وتعزيز الشراكات لتحقيق تلك الأهداف؛

(هـ) تحديد الاحتياجات ذات الصلة من المساعدة التقنية فيما يتعلق بتنفيذ اتفاقية الجريمة المنظمة لمنع الاحتيال المنظم ومكافحته.

رابعا- المتابعة والتوصيات الممكنة

42- لعل الفريق العامل يود أن يقدم التوصيات التالية:

(أ) تشجيع الدول الأطراف على النظر في تجريم الاحتيال باعتباره جريمة خطيرة، إن لم تكن قد فعلت ذلك بعد، حسب التعريف الوارد في الفقرة الفرعية (ب) من المادة 2 من اتفاقية الجريمة المنظمة، بغرض ضمان توفير التعاون الفعال على الصعيد الدولي بموجب الاتفاقية في الحالات التي يكون فيها الجرم ذا طابع عبر وطني وثمة جماعة إجرامية منظمة ضالعة فيه؛

(ب) حث الدول الأطراف على استخدام الأدوات التي تتيحها اتفاقية الجريمة المنظمة لوضع تشريعات وطنية أو تعديلها، حسب الضرورة والاقتضاء، لمنع الاحتيال ومكافحته، بما في ذلك الاحتيال الذي ترتكبه جماعات إجرامية منظمة؛

(ج) تشجيع الدول الأطراف على إجراء تحليلات، بالتشاور مع أصحاب المصلحة المعنيين الآخرين، تتناول، عند الاقتضاء، الاتجاهات السائدة فيما يتعلق بأنشطة الجماعات الإجرامية المنظمة المتصلة بالاحتيال المنظم، وعلى تبادل هذه المعلومات والبيانات مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة؛

(د) الطلب إلى مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، رهناً بتوافر موارد من خارج الميزانية، جمع معلومات بشأن الاحتيال المنظم وتحليلها ونشرها؛

(هـ) حث الدول الأطراف على التعاون الدولي المتبادل على أوسع نطاق ممكن، بما في ذلك تبادل المساعدة القانونية، في التحقيقات والملاحقات الجنائية والإجراءات القضائية المتعلقة بالاحتيال المنظم والجرائم ذات الصلة المشمولة باتفاقية الجريمة المنظمة والبروتوكولات الملحقة بها؛

(و) تشجيع الدول الأطراف على تعزيز تعاونها مع أصحاب المصلحة المعنيين، بما في ذلك القطاع الخاص ومنظمات المجتمع المدني ووسائل الإعلام والأوساط الأكاديمية والعلمية، على منع الاحتيال المنظم ومكافحته، بسبل منها حملات التثقيف والتوعية؛

(ز) الطلب إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن يواصل، رهنا بتوافر موارد من خارج الميزانية، استحداث أدوات للمساعدة التقنية وتقديم المساعدة التقنية، بما في ذلك بناء القدرات، إلى الدول الأطراف، بناء على طلبها، لأغراض دعم جهودها الرامية إلى تنفيذ اتفاقية الجريمة المنظمة تنفيذا فعالا في مجال منع الاحتيال المنظم ومكافحته؛

(ح) الطلب إلى الدول الأطراف أن تحدِّث سجلاتها التشريعية المتعلقة بتجريم الاحتيال المنظم في بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (بوابة شيرلوك)، إن لم تكن قد حدثتها بعد.