-- Journal of Criminal Law Research------
Spring 2025, 13 (50), 73-110
Jclr.atu.ac.ir
DOI: 10.22054/jclr.2025.82798.2714

ATU PRESS

Original Research
Received: 08/Nov/2024 *** Accepted: 30/June/2025
ISSN: 2345-3575
eISSN: 2476-6224

Computer Fraud in Iranian, England, and Welsh Penal Systems

Amir E'temadi*

Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, University of Qom, Qom, Iran

Abstract

Computer fraud refers to criminal behaviors carried out specifically through the use of computer networks. These offences have created new opportunities for fraudulent activity, particularly because computer-based fraud encompasses a wide range of deceptive conduct aimed at obtaining benefits without due entitlement. Evidence suggests that the financial and personal costs of such frauds—especially through methods such as identity theft and phishing—are substantial for both individual victims and society as a whole. Moreover, with the increasing accessibility of the internet—no longer confined to desktop computers but also available via tablets,

* Corresponding Author: Am.etemadi@gmail.com
How to Cite: Etemadi, A. (2025). Computer Fraud in Iranian, England, and Welsh Penal Systems. *Journal of Criminal Law Research*, 13 (50), 73- 110. doi: 10.22054/jclr.2025.82798.2714

smartphones, and handheld devices—the potential for individuals to fall victim to computer fraud has dramatically increased.

In the Iranian penal system, computer fraud is addressed independently from traditional (non-computer) fraud. This distinction arises from the nature of the offence: computer fraud is not merely a case of fraud committed using a computer as a tool. Rather, the computer plays a fundamental and constitutive role in shaping the *actus reus* of the offence. Therefore, computer fraud in Iranian law falls under the category of offences committed within a computer-based context, rather than offences committed by means of a computer.

According to Iranian law, any person who unlawfully obtains money, property, services, or financial advantages for themselves or another—by inputting, altering, deleting, creating, or suppressing data, or by disrupting a computer or telecommunications system—is considered to have committed computer fraud. For criminal liability to be established, both general intent and specific intent must be proven. General intent involves knowingly and willfully engaging in prohibited behaviors while being aware of the lack of authorization and the fact that the property belongs to another. Specific intent involves the aim to obtain financial gain or benefits for oneself or another individual.

In contrast, under the English and Welsh legal system, computer fraud is not categorized as a standalone offence but is prosecuted under the broader umbrella of the general offence of fraud, as defined in the Fraud Act 2006. This includes three primary types: fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. For example, in fraud by false representation, the

dishonest act may include phishing, pharming, presenting someone else's credit card, or using another person’s PIN at an ATM. These acts are not limited by medium and can be performed through digital platforms.

Fraud by failing to disclose information can also occur via digital means—such as failing to disclose essential facts when renewing a television license online or applying for car insurance through an internet portal. In all such cases, the perpetrator must act with malicious intent, and ignorance may serve as a defense against establishing this element. However, in the context of fraud by false representation, recklessness can also satisfy the mental element required for liability. If the perpetrator is aware of the possibility that their representation is false but proceeds regardless, this may be sufficient to establish criminal liability. That said, recklessness may not suffice as *mens rea* for other forms of computer fraud, such as failure to disclose information or abuse of position.

In both legal systems, specific intent remains a key requirement: the perpetrator must have acted with the intention of gaining a benefit or causing harm, even if that outcome is not ultimately realized.

This article critically examines the key elements of computer fraud under Iranian, English, and Welsh law. It concludes that certain deficiencies exist in the Iranian legislative framework. These include the absence of a comprehensive general offence of fraud and the failure to recognize recklessness as a valid form of *mens rea* in the context of computer fraud. Addressing these shortcomings is essential for more effective legal responses to cyber-enabled criminal conduct. Furthermore, doing so would help reduce the over-proliferation of

criminal statutes and eliminate the need for speculative interpretations concerning the offender's mental state.

Keywords: Computer or telecommunication systems, Computer fraud, Fraud by false representation, Fraud by failing to disclose information, Fraud by abuse of position

مقاله پژوهشی

-- فصلنامه علمی پژوهش حقوق کیفری ---------
دوره ۱۳، شماره ۵۰، بهار ۱٤۰٤، ۷۳-۱۱۰
Jclr.atu.ac.ir
DOI: 10.22054/jclr.2025.82798.2714

کلاهبرداری رایانه‌ای در نظام‌های کیفری ایران، انگلستان و وِیلز

امیر اعتمادی* استادیار گروه حقوق کیفری و جرم شناسی، دانشکده ی حقوق دانشگاه قم، ایران، قم

چکیده

جرم رایانه‌ای اصطلاحی است که دلالتِ ضمنی بر استفاده از شبکه‌های رایانه‌ای به طور خاص دارد. چنین جرایمی فرصت‌های جدیدی برای ارتکاب کلاهبرداری فراهم آورده اند، به ویژه از آن رو که این جرم دربرگیرنده‌ی انواع مختلفی از رفتارها است که با قصد فریب دادن و کسب منافعِ بدون زحمت شناخته شده اند. افزون بر این، بدون شک دسترسیِ افزایش‌یافته به اینترنت موجب می‌شود که افراد مختلف آسان‌تر بزهدیده‌ی کلاهبرداری رایانه‌ای شوند. بر این اساس، در نظام کیفری ایران، جرم کلاهبرداری رایانه‌ای به طور مستقل از کلاهبرداری سنتی (غیر رایانه‌ای) پیش‌بینی شده است، ولی در نظام کیفری انگلستان و وِیلز، جرم مذکور ممکن است زیر عنوان یکی از شیوه‌های سه‌گانه‌ی جرم عامِ کلاهبرداری، شامل کلاهبرداری با اظهار کذب، کلاهبرداری با کوتاهی در افشای اطلاعات و یا کلاهبرداری با سوءاستفاده از موقعیت، رسیدگی شود. نوشتار حاضر، با بررسی عنصرهای سازنده‌ی جرمِ کلاهبرداری رایانه‌ای در نظام‌های کیفری یادشده، به این نتیجه رسیده است که برخی نقص‌ها در رویکرد قانونگذار ایرانی وجود دارند، از جمله میزان مجازات کمتر کلاهبرداری رایانه‌ای در مقایسه با کلاهبرداری سنتی (حتی از گونه‌ی ساده)، که رفع آن‌ها در راستای مقابله‌ی مؤثرتر با مرتکبان جرم مزبور ضروری است.

کلیدواژه‌ها: سامانه‌های رایانه‌ای یا مخابراتی، کلاهبرداری رایانه‌ای، کلاهبرداری با اظهار کذب، کلاهبرداری با کوتاهی در افشای اطلاعات، کلاهبرداری با سوءاستفاده از موقعیت.

* نویسنده مسئول: Am.etemadi@gmail.com

تاریخ دریافت: ۱۴۰۳/۰۸/۱۸ *** تاریخ پذیرش: ۱۴۰۴/۰۴/۰۹
ISSN: ۲۳۴۵-۳۵۷۵ eISSN: ۲۴۷۶-۶۲۲۴

مقدمه

جرم رایانه‌ای یا جرم سایبری، اصطلاحی است که در کل برای توصیف فعالیت مجرمانه‌ای به کار می‌رود که در آن، رایانه‌ها یا شبکه‌های رایانه‌ای حسب مورد ابزار، آماج و یا مکان فعالیتِ مجرمانه هستند. در جهت تفکیک جرم سایبری از جرم رایانه‌ای گفته شده است که اولی دلالتِ ضمنی بر استفاده از شبکه‌های رایانه‌ای به طور خاص دارد، اما دومی ممکن است شامل شبکه‌های رایانه‌ای باشد یا نباشد (Stallings & Brown, 2018: 601).[1] چنین جرایمی فرصت‌های جدیدی برای ارتکاب کلاهبرداری فراهم آورده، به ویژه از آن رو که این جرم دربرگیرنده‌ی انواع مختلفی از رفتارها است که با قصد فریب دادن و کسب منافعِ بدون زحمت توصیف شده اند (Coderre, 2009: 3)، بدون اینکه محدود به دنیای واقعی یا فضای سایبر باشد. افزون بر این، دسترسی به اینترنت دیگر محدود به رایانه‌های رومیزی نیست، بلکه اشخاص ممکن است از طریق تَبلت، تلفن هوشمند و یا رایانه‌ی دستی به اینترنت دسترسی داشته باشند. بدون شک این دسترسیِ افزایش‌یافته به اینترنت موجب می‌شود که افراد مختلف آسان‌تر بزهدیده‌ی کلاهبرداری سایبری شوند.

برخی معتقدند که بعضی از جرایم دنیای واقعی نظیر کلاهبرداری شباهت‌های آشکاری با جرایم سایبری دارند، حال آنکه جرایم سایبری معینی، از قبیل ورود غیرمجاز به سیستم[2] و پراکندن بدافزار،[3] وجود دارند که وابسته به کسب معلومات درباره‌ی عملکردِ فناوری رایانه‌ای/ اینترنتی هستند (Stalans & Donner, 2018: 25-40). جرایم دسته‌ی اخیر، جرایم وابسته به فضای سایبر نامیده شده اند، چراکه تنها ممکن است با استفاده از رایانه، شبکه‌های رایانه‌ای یا سایر اَشکال فناوریِ انتقال اطلاعات ارتکاب یابند، ولی جرایم دسته‌ی نخست ممکن است بدون چنین فناوری‌هایی نیز ارتکاب یابند (Button & Cross, 2017: 9).[4] شواهدی نیز ذکر شده که هزینه‌های کلاهبرداری برای بزهدیدگان آن و مردم به طورکلی، به ویژه از طریق اَشکال کلاهبرداریِ برخط مانند سرقت هویت و

1. See also (Lushbaugh & Weston, 2016: 263).
2. Hacking.
3. Spreading malware.
4. See also (Jewkes & Yar, 2010, 3 & 4).

فیشینگ (داده‌گیریِ وانمودی)، هنگفت است و بر هزینه‌های سرقت از فروشگاه، رایج‌ترین سرقت ثبت‌شده در بریتانیا، غلبه می‌کند (Cross, 2020: 115).

در حقوق کیفری ایران، جرم کلاهبرداری رایانه‌ای به طور مستقل از کلاهبرداری سنتی (غیر رایانه‌ای) پیش‌بینی شده است، ولی در حقوق کیفری انگلستان و وِیلز، جرم مذکور ممکن است زیر عنوان یکی از شیوه‌های سه‌گانه‌ی جرم عامِ کلاهبرداری رسیدگی شود. بر این اساس، نوشتار حاضر درصدد پاسخ‌دهی به این پرسش است که چه نقیصه‌هایی در رویکرد قانونگذار ایرانی در جهت مقابله‌ی مؤثرتر با کلاهبرداران رایانه‌ای یافت می‌شود؟ و کدام راهکار(ها) ممکن است در راستای تقویت مقابله با کلاهبرداران مذکور مدنظر قرار گیرد؟ پاسخ به این پرسش‌ها مستلزم این است که اجزای سازنده‌ی عنصر مادی و عنصر روانی جرمِ کلاهبرداری رایانه‌ای در نظام‌های کیفری ایران، انگلستان و وِیلز تحلیل شود تا نقیصه‌های مورد نظر آشکار گردد. بنابراین، در نوشتار حاضر، نخست مفهوم قانونیِ کلاهبرداری رایانه‌ای در پرتو عنصر قانونی آن شناسایی می‌شود، و سپس، با بررسی عنصرهای سازنده‌ی کلاهبرداری رایانه‌ای و نیز وجوه افتراق و اشتراک نظام‌های یادشده در خصوص این جرم، به ارائه‌ی پیشنهاد(ها) پرداخته خواهد شد.

۱. شناخت مفهوم قانونیِ کلاهبرداری رایانه‌ای

در خصوص قوانین مربوط به رایانه‌ها که گاهی‌اوقات زیر عنوان حقوق رایانه از آن‌ها یاد شده است، اصل مهمی که وجود دارد، این است که رایانه‌ها از مقررات از پیش موجود معاف نیستند. برای نمونه، کاربران رایانه باید از قوانین مخالفِ کلاهبرداری، مزاحمت و سرقت خدمات تبعیت کنند (Downing, 2009: 115). با این حال، قوانین خاصِ مرتبط با اَعمال مجرمانه‌ی رایانه‌ای نیز وجود دارند، به طوری که قانونگذار ایرانی کلاهبرداری رایانه‌ای را جداگانه در ماده‌ی ۱۳ قانون جرایم رایانه‌ای ۱۳۸۸ (اصلاحی ۱۴۰۳)[1] پیش‌بینی کرده است. این ماده اعلام می‌دارد: «هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای یا

---

۱. ر.ک. تصویب‌نامه‌ی شماره‌ی۵۶۲۶۱/ت۶۲۲۹۸ه هیئت وزیران در خصوص اصلاح میزان مبالغِ مربوط به جرایم و تخلفات مندرج در قوانین مختلف مورخ ۱۴۰۳/۴/۴، پیوست ۱ـ جرایم، ردیف ۵.

مخابراتی با ارتکاب اَعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف‌کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن، به حبس از یک تا پنج سال یا جزای نقدی از صد و شصت و پنج میلیون (۱۶۵/۰۰۰/۰۰۰) ریال تا هشت‌صد و بیست و پنج میلیون (۸۲۵/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

در ارتباط با دلیل پیش‌بینی کلاهبرداری رایانه‌ای اظهار شده است که این جرم صرفاً کلاهبرداری از رهگذر رایانه نیست تا به واسطه‌ی آن نقش رایانه به اندازه‌ی یک ابزارِ جرم شناسانده شود، بلکه جرمی است که رایانه در آن نقش بنیادین ایفا می‌کند و بر بعضی از اجزای سازنده‌ی عنصر مادی کلاهبرداری تأثیر می‌گذارد، لذا کلاهبرداری رایانه‌ای از کلاهبرداری عام (سنتی) جدا می‌شود (عالی‌پور، ۱۳۹۵: ۲۵۰). بنابراین، باید گفت که کلاهبرداری رایانه‌ای در دسته‌ی جرایم ارتکابی در بستر رایانه‌ها (جرایم «سنتیِ» ارتکابی در محیطی که رایانه‌ها نقش مهمی ایفا می‌کنند) قرار می‌گیرند، نه در دسته‌ی جرایم ارتکابی به وسیله‌ی رایانه (رایانه به عنوان ابزار جرم) (See Hildebrandt, 2020: 165). افزون بر این، باید متذکر شد که با الحاق قانون جرایم رایانه‌ای ۱۳۸۸ به قانون تعزیرات ۱۳۷۵، شماره‌ی مواد ۱ تا ۵۴ این قانون به عنوان مواد ۷۲۹ تا ۷۸۲ قانون تعزیرات ۱۳۷۵ منظور شد؛[1] درنتیجه، ماده‌ی ۱۳ یادشده هم‌اکنون ماده‌ی ۷۴۱ قانون اخیر (الحاقی ۱۳۸۸) قلمداد می‌شود.[2]

---

۱. ر.ک. ماده‌ی ۵۵ قانون جرایم رایانه‌ای ۱۳۸۸.

۲. باید خاطرنشان کرد که ماده‌ی ۶۷ قانون تجارت الکترونیکی ۱۳۸۲ هم به کلاهبرداری کامپیوتری پرداخته که تنها در بستر مبادلات الکترونیکی ارتکاب‌یافتنی است. ماده‌ی مذکور مقرر می‌دارد: «هر کس در بستر مبادلات الکترونیکی، با سوءاستفاده و یا استفاده‌ی غیرمجاز از داده‌پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستمِ رایانه‌ای و غیره، دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازشِ خودکار و نظایر آن شود، و از این طریق، برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببَرد، مجرم محسوب و علاوه بر رد مال به صاحبان اموال، به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذ محکوم می‌شود». برخی درباره‌ی ماده‌ی بالا اظهار داشته اند که به وسیله‌ی ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) نسخ ضمنی شده است (آقایی‌نیا و رستمی، هادی، ۱۴۰۱: ۱۰۸)؛ با این حال، چنانچه ماده‌ی اخیر به عنوان مقرره‌ای از قانون عام تلقی شود، نسخ ماده‌ی ۶۷ قانون تجارت الکترونیکی ۱۳۸۲، به

در حقوق کیفری انگلستان و ویلز، ماده‌ی ۲ قانون کلاهبرداری ۲۰۰۶م.[1] که به «کلاهبرداری با اظهار کذب»[2] می‌پردازد، دربرگیرنده‌ی موقعیتی نیز است که رفتار شخص صرفاً (یا عمدتاً) از طریق «دستگاه» صورت گیرد. یک نمونه شامل جایی می‌شود که شخص کارت اعتباری[3] و شماره‌ی رمز[4] متعلق به دیگری را به دست می‌آورد و از آن برای خرید کالا استفاده می‌کند، خواه از طریق اینترنت باشد خواه با استفاده از تراشه‌ی رایانه‌ای[5] یا دستگاه کارت‌خوان در فروشگاه (Lloyd, 2017: 241). درواقع، اظهار کذب ممکن است نسبت به یک دستگاه نیز صورت گیرد، مانند جایی که متهم عددی را در دستگاه خودپرداز بانک وارد می‌کند، با علم به اینکه اختیار انجام این کار را ندارد (Thomas, 2023: 1361). بند (۱) ماده‌ی ۲ قانون یادشده مقرر می‌دارد: «شخص نقض‌کننده‌ی این ماده است، اگر وی (الف) با سوءنیت اظهار کذب کند، و (ب) با اظهار کذب قصد داشته باشد: (۱) منفعتی را برای خودش یا دیگری کسب کند، یا (۲) سبب ضرر غیر شود یا دیگری را در معرض احتمالِ ضرر قرار دهد».[6]

اما دو شیوه‌ی دیگر از ارتکاب جرمِ کلاهبرداری در این نظام کیفری در مواد ۳ و ۴ از قانون کلاهبرداری ۲۰۰۶م. پیش‌بینی شده اند. ماده‌ی ۳ قانون مزبور درباره‌ی «کلاهبرداری با کوتاهی در افشای اطلاعات»[7] مقرر می‌دارد: «شخص نقض‌کننده‌ی این ماده است، هرگاه وی (الف) با سوءنیت در افشای اطلاعات نسبت به شخص دیگری کوتاهی کند، اطلاعاتی که وظیفه‌ی قانونی برای افشای آن‌ها دارد، و (ب) با کوتاهی در افشای اطلاعات قصد داشته باشد: (۱) برای خودش یا دیگری منفعتی را کسب کند، یا (۲) سبب ضرر غیر شود

منزله‌ی قانون خاص، به وسیله‌ی آن مورد تردید است.

1. Fraud Act 2006.
2. Fraud by false representation.
3. Credit card.
4. PIN number.
5. A chip.
6. (1) A person is in breach of this section if he (a) dishonestly makes a false representation, and (b) intends, by making the representation – (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.
7. Fraud by failing to disclose information

یا دیگری را در معرض احتمالِ ضرر قرار بدهد».[1]

بند (۱) ماده‌ی ۴ قانون موردبحث در خصوص «کلاهبرداری با سوءاستفاده از موقعیت»[2] اعلام می‌دارد: «شخص نقض‌کننده‌ی این ماده است، چنانچه وی (الف) موقعیتی را دارا باشد که در آن، از او انتظار می‌رود تا منافع مالیِ فرد دیگری را حفظ کند یا علیه آن اقدام نکند، (ب) با سوءنیت از آن موقعیت سوءاستفاده کند، و (پ) به وسیله‌ی سوءاستفاده از آن موقعیت قصد داشته باشد: (۱) برای خودش یا دیگری منفعتی را کسب کند، یا (۲) سبب ضرر غیر شود یا دیگری را در معرض احتمالِ ضرر قرار دهد».[3]

بر این اساس، باید در مورد امکان ارتکاب شیوه‌های سه‌گانه‌ی کلاهبرداری به‌صورت رایانه‌ای بیش‌تر توضیح داده می‌شود، موضوعی که در ادامه به آن پرداخته خواهد شد. پیش از آن، باید در نظر داشت که همسو با پیشرفت‌ها در حوزه‌ی جرم رایانه‌ای به طورکلی، بعضی از مقرره‌های دیگر قانون کلاهبرداری ۲۰۰۶م. انواع مختلفِ معاملاتی را جرم‌انگاری کرده اند که مربوط به ابزارهایی می‌شوند که ممکن است نقشه‌ی کلاهبرداری را تسهیل کنند. در این راستا، ماده‌ی ۶ قانون مزبور اعلام می‌دارد که دارا بودن شیء‌ای برای استفاده در جریان کلاهبرداری یا در ارتباط با آن جرم است و ماده‌ی ۷ همان قانون مقرر می‌دارد که ساختن، سازگار کردن، تهیه و یا پیشنهاد تهیه‌ی هر شیء‌ای، با آگاهی از اینکه به منظور استفاده در جریان کلاهبرداری یا در ارتباط با آن در نظر گرفته شده یا همساز گردیده است، یا با قصد اینکه در ارتکاب کلاهبرداری یا مساعدت در ارتکاب آن به کار گرفته شود، جرم به حساب می‌آید. ماده‌ی ۸ قانون کلاهبرداری ۲۰۰۶م. نیز اضافه می‌کند که شیء[4] دربرگیرنده‌ی هر برنامه یا داده‌ای است که به صورت الکترونیکی نگه

---

1. A person is in breach of this section if he (a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and (b) intends, by failing to disclose the information – (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.
2. Fraud by abuse of position
3. A person is in breach of this section if he (a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person, (b) dishonestly abuses that position, and (c) intends, by means of the abuse of that position – (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.
4. Article .

داشته می‌شود.

بنابراین، در ارتباط با ماده‌ی ۶ قانون مذکور، برنامه‌ی رایانه‌ای که برای ایجاد شماره‌های کارت اعتباری استفاده می‌شود،[1] یا فایل‌های رایانه‌ای شامل فهرستی از جزئیات کارت‌های اعتباریِ اشخاص،[2] و در خصوص ماده‌ی ۷ همان قانون، نوشتن جاسوس‌افزار[3] که جهت کنترل داده‌های شخصی طراحی شده است تا بعدها در ارتکاب کلاهبرداری با اظهار کذب به کار رود، آماده‌سازی یک ایمیل برای فیشینگ[4] و طراحی وب‌سایتِ ساختگی[5] که برای جمع‌آوری اطلاعات شخصی از قبیل کُدهای شناسایی و رمزهای عبور در نظر گرفته شده است، در چارچوب تعریف شیء قرار می‌گیرند.

۲. تحلیل عنصرهای سازنده‌ی کلاهبرداری رایانه‌ای

باید پذیرفت که نقص‌هایی که ممکن است در رویکرد قانونگذار ایرانی نسبت به هر یک از عنصر مادی و یا عنصر روانیِ جرمِ کلاهبرداری رایانه‌ای وجود داشته باشد روشن نمی‌شود، مگر اینکه تمامی اجزای سازنده‌ی عنصرهای یادشده به صورت تطبیقی بررسی شوند. از این رو، این قسمت از نوشتار به تحلیل عنصرهای متشکله‌ی جرم مزبور در ایران، انگلستان و ویلز اختصاص داده شده است.

---

1. A computer program used to generate credit card numbers.
2. Computer files containing lists of other people's credit card details.
3. Spyware.

۴. این عمل که معادل انگلیسی آن Phishing است، از استعاره‌ای آمده است که توصیف می‌کند، چگونه مجرمان رایانه‌ای از تله‌های ای‌میلی برای صید رمزهای عبور و داده‌های مالی از دریایِ کاربران اینترنت استفاده می‌کردند. هجی کردن آن با Ph شاید نوعی تکریمِ هکرهای اولیه، یعنی هکرهای تلفنی (Phone Phreaks)، باشد. این اصطلاح در دهه‌ی ۱۹۹۰م. توسط هکرهایی که حساب‌های America Online را با تحصیل رمزهای عبور از مشترکان آن سرقت می‌کردند، ساخته شد. تا سال ۱۹۹۶م. حساب‌های هک‌شده Phis خوانده می‌شدند. با گذشت سال‌ها، تعریف آنچه حمله‌ی فیشینگ را تشکیل می‌دهد، گسترش یافته است، به طوری که این اصطلاح در حال حاضر نه‌تنها به دست آوردن جزئیات حسابِ کاربر، بلکه دسترسی به تمامی داده‌های شخصی و مالی را نیز دربرمی‌گیرد (Rosoff, 2020: 525-528).

5. Bogus website.

۱-۲. عنصر مادی کلاهبرداری رایانه‌ای

عنصر مادی جرمِ کلاهبرداری رایانه‌ای، با توجه به مفاد ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) در حقوق ایران و با لحاظ مقرره‌های پیش‌گفته از قانون کلاهبرداری ۲۰۰۶م. در حقوق انگلستان و وِیلز، شامل اجزای سازنده‌ی مشخصی می‌شود که در زیر شرح داده می‌شوند.

۱-۱-۲. رفتار مجرمانه

در ایران، رفتار مجرمانه در جرمِ کلاهبرداری رایانه‌ای شامل اَعمالی نظیر واردکردن، تغییر، محو، ایجاد یا متوقف‌کردن داده‌ها و یا مختل‌کردن سامانه می‌شود که توسط هر کس اعم از شخص عادی یا کارمند دولت ممکن است ارتکاب یابد. این رفتارها که همگی ایجابی (فعل) هستند، با توجه به عبارت «از قبیل» در قسمت ابتدایی ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) جنبه‌ی تمثیلی دارند، نه حصری. از این رو، دسترسی به شناسه‌های کارت عابر بانک دیگری و انتقال وجه از حساب دیگری به حساب خود از طریق سامانه‌ی رایانه‌ای از مصادیق کلاهبرداری رایانه‌ای قلمداد شده، با این استدلال که اقدام مرتکب درواقع، استفاده‌ی غیرمجاز از سامانه‌ی رایانه‌ای است که به بُردن مال متعلق به دیگری منجر شده و ماده‌ی یادشده با ذکر مصادیق تمثیلیِ استفاده‌ی غیرمجاز از سامانه‌ی رایانه‌ای، بُردن مال از این طریق را جرم‌انگاری کرده است (دادنامه‌ی شماره‌ی ۹۲۰۹۹۷۰۲۷۰۱۰۰۱۱۹ مورخ ۱۳۹۲/۲/۱۸، شعبه‌ی ۵۶ دادگاه تجدیدنظر استان تهران). با وجود این، نظر به اینکه شناسه‌های کارت عابر بانک به صورت اعداد و ارقام است و مرتکب ناگزیر به درج آن‌ها در سامانه‌ی رایانه‌ای یا مخابراتی برای انتقال وجه است، رفتار ارتکابی در چنین موردی زیر همان عنوان واردکردن داده‌ها بررسی‌کردنی است.

در انگلستان و وِیلز، «کلاهبرداری با اظهار کذب» نسبت به انواع گسترده‌ای از موقعیت‌ها صدق می‌کند. به عبارت دیگر، اظهار کذب به عنوان رفتار مجرمانه‌ی این شیوه از کلاهبرداری منحصر به گونه‌ی خاصی از فعل‌ها نیست و شامل فیشینگ، فارمینگ،[1]

---

۱. این رفتار مجرمانه که در زبان انگلیسی با اصطلاحِ Pharming از آن یاد می‌شود، به معنای تغییر دادن مسیر ترافیکِ

ارائه‌ی کارت اعتباریِ دیگری برای پرداخت و واردکردن شماره‌ی رمز متعلق به غیر در دستگاه خودپرداز[۱] می‌شود. حتی داده‌های جمع‌آوری‌شده با استفاده از جاسوس‌افزار ممکن است بعدها به منظور اظهار کذب به کار گرفته شوند، و درنتیجه، کلاهبرداری با اظهار کذب را به طور نامستقیم محقق سازند، مانند اینکه اطلاعات حساب بانکیِ بزهدیده که با جاسوس‌افزار به دست آمده اند، جهت برداشت وجه به سامانه‌ی بانک ارسال شوند.

«کلاهبرداری با کوتاهی در افشای اطلاعات» نیز به صورت رایانه‌ای متصور است. در واقع، با توجه به شمار رو به افزایش معاملات بین مؤسسه‌های دولتی و اشخاص و یا بین مصرف‌کنندگان و بنگاه‌های تجاری، در حال حاضر امکان ارتکاب این شیوه از کلاهبرداری حداقل به صورت برخط وجود دارد. ارائه‌ی الکترونیکیِ اظهارنامه‌ی مالیاتی،[۲] درخواست تمدید جوازهای تلویزیونی به طور الکترونیکی[۳] و تقاضای بیمه‌نامه‌ی وسیله‌ی نقلیه به صورت برخط[۴] نمونه‌هایی از این شیوه‌ی کلاهبرداری محسوب شده اند (Bainbridge, 2008: 426)؛ مشروط بر اینکه شخص در زمان انجام آن‌ها در افشای اطلاعاتِ موردنیاز کوتاهی کرده باشد.

بالاخره، در «کلاهبرداری با سوءاستفاده از موقعیت» هم می‌توان به جایی اشاره کرد که کارمند یک شرکت نرم‌افزار[۵] از موقعیتش سوءاستفاده می‌کند و از نرم‌افزارهای کارفرما به طور غیرمجاز کپی می‌گیرد تا به نفع خودش بفروشد. کلاهبرداری به شیوه‌ی مذکور همچنین در مواردی ارتکاب می‌یابد که یک کارمند ای‌میلی که حاوی اطلاعات

وب‌سایت اصلی، مثلاً یک وب‌سایت مشهور، به وب‌سایت ساختگی است، جایی که اطلاعات شخصیِ بازدیدکنندگان بدون آگاهی آن‌ها به دست آورده شده و به‌منظور تحصیل وجوه‌شان به کار گرفته می‌شود.

۱. از این موارد به طور خاص زیر عنوان کلاهبرداری با کارت اعتباری (Credit card fraud) یا کلاهبرداری با دستگاه خودپرداز (ATM (cash machine) fraud) هم سخن گفته می‌شود. کلاهبردار ممکن است اطلاعات شخصی یا خودِ کارت اعتباری دیگری را سرقت کند تا بتواند وجوهی را از حساب بزهدیده برداشت یا کالاهایی را با استفاده از کارت اعتباری وی خریداری کند. مرتکب همچنین احتمال دارد، زمانی که دیگری از دستگاه خودپردازِ بانک استفاده می‌کند، کارت اعتباری او یا اطلاعات آن را بَردارد.

2. Electronic submission of tax returns.
3. Applying for or renewing television licences electronically.
4. Applying for motor vehicle insurance online.
5. Software company.

محرمانه‌ی[1] متعلق به کارفرمایش است، را به شرکت رقیب ارسال کند، اعم از اینکه برای منفعت شخصی‌اش باشد یا با قصد ایراد ضرر به کارفرمای خود (Bainbridge, 2008: 427). با این همه، به نظر می‌رسد که این شیوه از کلاهبرداری زمانی که به صورت رایانه‌ای ارتکاب می‌یابد، تنها از طریق فعل امکان‌پذیر باشد، نه ترک فعل، در حالی که ماهیت کلاهبرداری با کوتاهی در افشای اطلاعات به گونه‌ای است که اساساً با ترک فعل تحقق می‌پذیرد، خواه به‌صورت رایانه‌ای انجام گیرد خواه به شکل سنتی.

اما شرح رفتارهای تمثیلیِ کلاهبرداری رایانه‌ای در نظام حقوقی ایران از قرار زیر است: **واردکردن داده‌ها**،[2] درج اطلاعاتی از قبیل مشخصات هویتی و اعداد و ارقام در سامانه‌ی رایانه‌ای یا مخابراتی است. این اطلاعات که ممکن است صحیح یا ناصحیح باشند، با استفاده از صفحه‌کلید یا سایر تجهیزات ورودیِ سامانه وارد می‌شوند. برای مثال، هرگاه شخصی مشخصات و شماره‌حساب دیگری را به دست آورد، یا مشخصات ناواقعی‌ای را جعل کند، و سپس، با درج آن‌ها در وب‌سایت فروش کالا یا دستگاه خودپردازِ بانک حسب مورد مال، وجه و یا خدمات مالی تحصیل نماید، مرتکب این رفتار مجرمانه شده است.

تغییر داده‌ها[3] به معنای دست‌کاری در اطلاعات موجود در سامانه‌ی رایانه‌ای یا مخابراتی است. چنین دست‌کاری‌ای ممکن است شامل تبدیل داده‌ها یا کم‌وزیاد کردن آن‌ها شود. بنابراین، در موردی که فردی با دست‌کاری در اطلاعات خروجیِ سامانه‌ی حساب‌داریِ شرکتی که در آن کار می‌کند، موجب شود که فیش حقوقی با مبلغ بالاتر برای او صادر گردد، و از این طریق، حقوق بیشتری دریافت کند، رفتار مجرمانه‌ی مذکور انجام گرفته است.

محو داده‌ها[4] عبارت است از حذف همه یا بخشی از اطلاعاتی که در سامانه‌ی رایانه‌ای یا مخابراتی وجود دارند. شیوه‌های مختلفی برای محو داده‌ها ممکن است به کار گرفته شوند،

1. Confidential information.
2. Input of data.
3. Alteration of data.
4. Deletion of data.

ازجمله حذف متن، فایل و یا بخشی از سند الکترونیکی که به منظور حذف اطلاعات انجام گیرد (Haynes, 2002: 151). پس، هرگاه کسی بعد از دریافت طلب خود از یک شرکت خصوصی، اسناد الکترونیکی مربوط به آن را که در سامانه‌ی رایانه‌ایِ شرکت وجود دارند حذف کند و دوباره وجوهی به عنوان طلبش تحصیل کند، این رفتار مجرمانه ارتکاب یافته است.

ایجاد داده‌ها،[1] به وجود آوردن اطلاعات ساختگی‌ای است که پیش‌تر در سامانه‌ی رایانه‌ای یا مخابراتیِ مورد نظر وجود نداشته اند. این عمل مجرمانه ممکن است به واسطه‌ی واردکردن اطلاعات به سامانه‌ی مربوط انجام گیرد. چنانچه شخصی در سامانه‌ی رایانه‌ایِ یکی از بانک‌ها اطلاعاتی وارد کند، مبنی بر اینکه دارای حساب سپرده‌ی سرمایه‌گذاریِ کوتاه‌مدت با مبلغ معینی است، و از این راه، ماهانه سود بانکی دریافت کند، مرتکب رفتار مجرمانه‌ی مورد بحث شده است.

متوقف‌کردن داده‌ها[2] به معنای جلوگیری از انتقال و تبادل اطلاعات در سامانه‌ی رایانه‌ای یا مخابراتی است که به شیوه‌های مختلفی امکان‌پذیر است. برای نمونه، در صورتی که فردی، در زمان خرید کالا از فروشگاه، به جای وجه نقد از دستگاه کارت‌خوان استفاده کند، اما پیش از تکمیل فرآیند انتقال داده‌ها، بدون اطلاع فروشنده آن را لغو و کالای مورد نظر را دریافت نماید، رفتار مجرمانه‌ی یادشده انجام گرفته است.

مختل‌کردن سامانه[3] شامل انواع دست‌کاری‌ها در سخت‌افزار یا نرم‌افزار سامانه‌ی رایانه‌ای یا مخابراتی می‌شود که باعث ایجاد اختلال در عملکرد آن مثلاً در پردازش اطلاعات یا جریان انتقال داده‌ها شود. بر این اساس، اگر کسی با دست‌کاری در سخت‌افزار دستگاه خودپردازِ بانکی بتواند مبالغ زیادی وجه نقد به دست آورد، مرتکب این رفتار مجرمانه شده است.

در هر حال، با محور قرار دادن رفتار مجرمانه، برخی معتقدند که کلاهبرداری رایانه‌ای دو رفتاری است و لذا جرمی مرکب به حساب می‌آید؛ رفتار نخست، یکی از موارد تمثیلی

1. Creation of data.
2. Suppression of data.
3. System interference.

پیش‌گفته است و رفتار دوم، تحصیل است که اعم از دریافت واقعی، مجازی و یا منظور کردن اعتبار مالی برای خود است (عالی‌پور، ۱۳۹۵: ۲۸۰ و ۲۸۱). این دیدگاه در معرض انتقاد قرار می‌گیرد، زیرا شیوه‌ی نگارش ماده‌ی ۷۴۱ قانون مذکور حاکی از این است که ارتکاب یکی از رفتارهای تمثیلی یادشده برای تحقق کلاهبرداری رایانه‌ای کافی است و تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی در واقع، نتیجه‌ی این جرم است؛ پس، باید پذیرفت که کلاهبرداری رایانه‌ای جرمی ساده است.

۲-۱-۲. شرایط پیرامونی

در نظام کیفری ایران، شرایط پیرامونی که لازم است رفتار مجرمانه به شرح پیش‌گفته را احاطه کنند تا کلاهبرداری رایانه‌ای تحقق یابد، از قرار زیر هستند:

- مرتکب مجوز نداشته باشد؛ و
- موضوع جرم، سامانه‌ی رایانه‌ای یا مخابراتی باشد؛ و
- مال (در مفهوم عام خود) متعلق به دیگری باشد.

در مورد شرط اول باید متذکر شد که عبارت «به طور غیرمجاز» در قسمت ابتدایی ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) دلالت بر این دارد که شخص فقط در صورتی ممکن است به این گونه‌ی خاص از کلاهبرداری محکوم شود که افزون بر سایر مقتضیات این جرم، احراز گردد که وجه، مال و یا خدمات مالی را بدون مجوز[1] تحصیل کرده است. در نظام کیفری انگلستان و ویلز، اصطلاح اخیر در ارتباط با جرایمی که مستلزم دسترسی غیرمجاز هستند،[2] به این صورت معنا شده است که شخص یا اشخاصی که حق کنترلِ دسترسی به داده‌های مورد نظر را دارند، رضایت یا اجازه‌ی استفاده از اطلاعات یا بخشی از آن‌ها را به دیگری نداده باشند.[3] از این رو، هرگاه کسی، به خاطر دسترسی نداشتن به اینترنت، نام کاربری و رمز عبورِ سامانه‌ی اینترنت بانکی را که کاربر آن است به دیگری بدهد و از او بخواهد که مبلغی معینی را به حساب شخص ثالثی انتقال دهد، شرط مذکور

1. Unauthorized.
2. Offences of unauthorised access.
3. See, S 17 (5) of the Computer Misuse Act 1990.

تحقق نمی‌یابد، زیرا عمل مرتکب به طور غیرمجاز نبوده، بلکه با تجویز صاحب حساب بوده است.

در خصوص شرط دوم باید توجه داشت که تحقق عنصر مادی کلاهبرداری رایانه‌ای منوط به این است که سامانه‌ی رایانه‌ای یا مخابراتی موضوع جرم قرار گیرد، به این معنا که جرم نسب به یکی از سامانه‌های مذکور واقع شود. سامانه‌ی رایانه‌ای[1] مجموعه‌ای از نرم‌افزارها و سخت‌افزارهای مرتبط است که از طریق یک شبکه‌ی رایانه‌ای جهت اجرای فرایندهای کار مشخصی، به یکدیگر متصل اند (بند (ب) ماده‌ی ۱ آیین‌نامه‌ی نحوه‌ی استفاده از سامانه‌های رایانه‌ای یا مخابراتی ۱۳۹۵)؛ رایانه‌ی رومیزی یا دستی. دستگاه‌های جنبی مانند مودم[2] (Horak, 2008: 317) نیز در مفهوم سامانه‌های مذکور گنجانده می‌شود، زیراکه سخت‌افزاری وابسته به رایانه هستند. نرم‌افزار به طور معمول بخشی از سامانه‌ی رایانه‌ای تلقی نمی‌شود، گرچه سیستم‌عامل[3] که سخت‌افزار را فعال می‌کند، معروف به نرم‌افزارِ سیستم[4] است. اما سامانه‌ی مخابراتی[5] هر سیستمی است که از طریق آن منبع اطلاعات قادر باشد که اطلاعات را با رعایت دقیقِ کارآیی و اطمینان‌پذیری به مقصدی انتقال بدهد؛ چنین سیستمی ممکن است دارای بیش از یک منبع و یا بیشتر از یک مقصد باشد، که در این صورت، شبکه‌ی ارتباطی[6] خوانده می‌شود (Butterfield & Ekembe Ngondi, 2016: 540)، مانند تلفن همراه. به عبارت دیگر، هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها که برای انتقال الکترونیکی اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله‌ی قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد، به کار گرفته شود، سامانه‌ی مخابراتی نامیده می‌شود (بند (پ) ماده‌ی ۱ آیین‌نامه‌ی نحوه‌ی استفاده از سامانه‌های رایانه‌ای یا مخابراتی ۱۳۹۵).

1. Computer system.
2. Modem.
3. Operating system.
4. System software.
5. Communications system.
6. Communication network.

در حقوق انگلستان و وِیلز، بند (۵) ماده‌ی ۲ قانون کلاهبرداری ۲۰۰۶م. اعلام می‌دارد که اظهار کذب ممکن است نسبت به هر دستگاه یا وسیله‌ای صورت گیرد که به منظور دریافت، انتقال و یا پاسخ به ارتباط‌ها (با دخالت انسان یا بدون آن) طراحی شده باشد. این در حالی است که تا پیش از تصویب قانون یادشده، مسئله‌ی پُردردسر در ارتباط با جرایمی که مستلزم اثبات فریب‌کاری بودند این بود که آیا یک دستگاه ممکن است فریب داده شود یا اینکه چنین عملی تنها ممکن است نسبت به انسان‌ها انجام گیرد (For further reading, See, Rowland et. al., 2017: 279-282).

بنابراین، هم‌اکنون رایانه یا تلفن همراه به عنوان یک دستگاه یا وسیله ممکن است برای اهداف بالا به کار گرفته شود، و در نتیجه، موضوع جرمِ کلاهبرداری قرار گیرد. در این راستا، بی‌تردید اظهارات کذبی که با ای‌میل نسبت به رایانه[1] یا به وسیله‌ی پیام کوتاه به تلفن همراه[2] صورت می‌گیرند، زیر عنوان کلاهبرداری با اظهار کذب تعقیب‌شدنی اند. اظهار کذب همچنین زمانی صورت خواهد گرفت که برای تجهیزات یا نرم‌افزارِ تمام‌خودکار،[3] مثلاً به بانکی برخط[4] با دستورهایی جهت واریز پول به حساب دیگری، ارسال شود (Bainbridge, 2008: 425). بر این اساس، چنانچه فردی با استفاده از تلفن همراهش آگهی‌ای در صفحه‌ی فِیس‌بوک خود درج کند و اشخاصی را فریب دهد که مدیر کارخانه‌ای است که درصدد جذب نیروی جدید است، و از این راه، متقاضیان کار را متقاعد کند که برای مصاحبه مبلغی وجه به حساب معینی واریز کنند، کلاهبرداری سنتی تحقق یافته، چراکه از سامانه‌ی مخابراتیِ مزبور تنها به عنوان وسیله‌ای جهت فریفتن دیگران استفاده شده است،[5] حال آنکه، در کلاهبرداری رایانه‌ای، سامانه‌های یادشده فقط وسیله‌ی

1. By e-mail to a computer.
2. By SMS to a mobile phone.
3. Fully automated equipment or software.
4. An online bank.

۵. اداره‌ی حقوقی قوه‌ی قضائیه هم در نظریه‌ی مشورتی شماره‌ی ۷/۹۵/۲۹۲۲ مورخ ۱۳۹۵/۱۱/۱۶ اظهار داشته است: «ملاک تحقق بزه موضوع ماده‌ی ۷۴۱ قانون مجازات اسلامی [تعزیرات] ۱۳۷۵ـ الحاقی ... ۱۳۸۸ ... این است که «وجه یا مال یا منفعت یا خدمات یا امتیازات» با استفاده‌ی غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی و با ارتکاب اَعمالی از قبیل وارد کردن، تغییر، محو، ایجاد، متوقف کردن داده‌ها یا مختل کردن سامانه‌ها تحصیل گردد، وگرنه، اگر کسی

ارتکاب جرم نیستند، بلکه به طور مستقل موضوع جرم قرار می‌گیرند؛ ضمن اینکه فریب بزهدیده هم شرط نیست.

درباره‌ی شرط سوم باید گفت که در کلاهبرداری رایانه‌ای، وجه، مال، منفعت، خدمات و یا امتیازات مالی باید متعلق به دیگری باشد. البته، در این خصوص، اموالی که داده‌های رایانه‌ای معرف آن‌ها هستند، غیرمادی اند، مانند سپرده‌ها، مطالبه‌ها، ارزش اعتبارات و نتایج محاسبه‌های ترازنامه‌ها. خلاصه‌ی کلام، در این نوع از کلاهبرداری، داده‌ها به عنوان نماینده‌ی اموال مادی قلمداد شده اند (زیبر، ۱۳۹۰: ۲۰). پس، اگر زنی بدون اطلاع شوهرش اطلاعات حساب بانکی او را در وب‌سایت فروش کالا وارد کند و به اندازه‌ی نفقه‌ی خود کالاهایی را خریداری کند، عنصر مادی این جرم محقق نمی‌شود، زیراکه وجه انتقال داده‌شده درواقع، متعلق به او است.

۳-۱-۲. نتیجه‌ی حاصله

کلاهبرداری رایانه‌ای در ایران در زمره‌ی جرایم مقید قرار می‌گیرد و قسمت میانی ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) حاکی از این است که تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی[1] نتیجه‌ی آن محسوب می‌شود. با این حال، برخی

بدون ارتکاب چنین اَعمالی ولی با استفاده از سامانه‌های رایانه‌ای یا مخابراتی موجب فریب فرد یا افرادی گردد و مالی از آنان تحصیل نماید، موضوع از مصادیق کلاهبرداری ماده‌ی ۱ قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری [۱۳۶۷] خواهد بود. به عنوان مثال، چنانچه فردی با استفاده از سامانه‌های رایانه‌ای یا مخابراتی به قصد فریب با امیدوار کردن به امر واهی، افراد شرکت‌کننده در قرعه‌کشیِ واهی را فریب دهد، و از این طریق، وجوه آن‌ها را تصاحب کند، موضوع از مصادیق بزه ماده‌ی ۱ قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری [۱۳۶۷] خواهد بود».

۱. خدمات مالی به هر نوع خدمتی اطلاق می‌شود که در ماهیت و ذات مالی است و بیشتر به‌وسیله‌ی مؤسسه‌های مالی نظیر بانک‌ها و مؤسسه‌های مالی‌ـاعتباری ارائه می‌شوند، مانند پرداخت وام قرض‌الحسنه یا صدور ضمانت‌نامه‌ی بانکی؛ اما امتیازات مالی به هرگونه امتیازی گفته می‌شود که دستاوردی مالی برای شخص داشته باشد، از قبیل مجوز ساختن یک آپارتمان ده طبقه در محل یک ساختمان قدیمیِ دو طبقه. بدیهی است که هر یک از این موارد باید با ارتکاب یکی از رفتارهای مجرمانه‌ی مذکور در ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) و از سامانه‌ی مؤسسه یا سازمان مربوط تحصیل شوند تا کلاهبرداری رایانه‌ای تحقق یابد.

نویسندگان حقوق کیفری، ضمن پذیرش مقید بودن جرم مورد بحث، اظهار داشته اند که رفتار مرتکب (تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی) باید به ورود زیان به صاحب مال منتهی شده باشد تا عنصر مادی آن به طور کامل تحقق یابد (منصورآبادی و منصورآبادی، ۱۴۰۳: ۱۵۸). چنین نظرگاهی در معرض انتقاد قرار می‌گیرد، به این دلیل که از یک طرف، استفاده از واژه‌ی **اَعمالی** و ذکر تمثیلی برخی مصادیق آن نشان می‌دهد که در ماده‌ی مذکور رفتار مجرمانه از نتیجه‌ی حاصله تفکیک شده است، و در واقع، موارد پیش‌گفته همان نتیجه محسوب می‌شوند، و از طرف دیگر، هرچند که اگر مرتکب موفق به تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی شود، ایراد نوعی ضرر به بزهدیده احرازشدنی است، اساساً در جرم کلاهبرداری، ضرر دیگری افزون بر آن لازم نیست (اعتمادی، ۱۴۰۳: ۵۵)؛ به ویژه از آن رو که قانونگذار به لزوم ورود زیانِ مازاد به صاحب مال اشاره نکرده است.

اما ماده‌ی مذکور پیش از اشاره به تحصیل موارد یادشده از عبارت «برای خود یا دیگری» استفاده کرده است؛ این عبارت حکایت از آن دارد که تحصیل هر یک از موارد پیش‌گفته برای خودِ متهم ضروری نیست، بلکه شامل تحصیل برای دیگری نیز می‌شود. از این رو، برخی نویسندگان اظهار داشته اند که تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی برای خود یا دیگری نتیجه‌ی جرمِ کلاه‌برداری رایانه‌ای محسوب می‌شود (محمدنسل، ۱۳۹۲: ۱۱۱). برای مثال، اگر کسی از اطلاعات شماره‌حساب دیگری برای ورود به همراه بانک استفاده کند، و سپس، مبلغی وجه به حساب خود یا یکی از فرزندانش انتقال دهد، کلاهبرداری رایانه‌ای تحقق می‌یابد. در این فرض، چنانچه مرتکب به واسطه‌ی عامل خارج از اراده‌اش، از قبیل اختلال در فرآیند ارسال داده‌ها، نتواند عملیات انتقال وجه را به انجام برساند، زیر عنوان شروع به کلاهبرداری رایانه‌ای[1] تعقیب و مجازات می‌شود. در این راستا، باید متذکر شد که مجازات کلاهبرداری رایانه‌ای با توجه به تبصره‌های ۲ و ۳ ماده‌ی ۱۹ قانون مجازات اسلامی ۱۳۹۲ تعزیر درجه‌ی پنج است، لذا شروع به این جرم تحت شمول بند (پ) ماده‌ی ۱۲۲ قانون اخیر قرار می‌گیرد و شروع‌کننده به حبس تعزیری،

1. Attempted computer fraud.

شلاق و یا جزای نقدی درجه‌ی شش محکوم می‌شود.

برخی نویسندگان اظهار داشته اند که به دلیل مرکب بودن جرمِ کلاهبرداری رایانه‌ای، رفتارهای مجرمانه‌ی این جرم به‌خودی‌خود کلاهبرداری نیست و آخرین فرآیند رُکن مادی (بُردن مال، امتیاز، منفعت و یا خدمات مالی) نیز باید تحقق یابد (آقایی‌نیا و رستمی، ۱۴۰۱: ۱۰۸ و ۱۰۹). در خصوص این دیدگاه، هرگاه منظور از آخرین فرآیند رُکن مادی، نتیجه‌ی حاصله باشد، باید گفت که لزوم تحقق نتیجه در یک جرم ممکن نیست بر مبنای مرکب بودن آن استوار شود، زیرا همان‌گونه که در بحث از کلاهبرداری سنتی اشاره شد، تقسیم‌بندی جرایم به ساده یا مرکب در اصل مبتنی بر چندگانگی رفتارهای مجرمانه است، نه محاسبه‌ی رفتار مجرمانه و نتیجه؛ لزوم یا عدم لزوم نتیجه نیز مبنای دسته‌بندی جرایم به مطلق و مقید است.

در واقع، ضرورت تحقق نتیجه در جرمی اساساً ارتباطی با ساده یا مرکب بودن آن ندارد، در حالی که دیدگاه مذکور با تکیه بر مرکب بودن کلاهبرداری رایانه‌ای، لزوم تحقق آخرین جزء از عنصر مادی را استنباط کرده است. از این گذشته، از یک‌سو، همان‌طور که قبلاً بیان شد، جرم مزبور مستلزم انجام بیش از یک رفتار مجرمانه نیست و ارتکاب هر یک از رفتارهای مجرمانه‌ای که پیش‌تر اشاره شدند، ممکن است باعث تحقق این جرم شود، یعنی این گونه‌ی خاص از کلاهبرداری جرمی ساده است، و از سوی دیگر، ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) از تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی یاد کرده است، نه بُردن هر یک از آن‌ها.

در مقابل، در انگلستان و وِیلز، از مواد ۲، ۳ و ۴ از قانون کلاهبرداری ۲۰۰۶م. استنباط می‌شود که کلاهبرداری رایانه‌ای جرمی مطلق قلمداد می‌شود، و از این حیث، تفاوتی نمی‌کند که مرتکب کدام‌یک از شیوه‌های سه‌گانه‌ی این جرم را برگزیند. دلیل این دیدگاه آن است که قانونگذار انگلیسی و وِیلزی صرف اظهار کذب، کوتاهی در افشای اطلاعات و سوءاستفاده از موقعیت را با لحاظ شرایط پیرامونیِ لازم موجب تحقق جرمِ کلاهبرداری رایانه‌ای می‌داند. به این ترتیب، حصول نتیجه‌ی خاصی از رفتار مرتکب مانند کسب منفعت ضروری نیست و هرگاه وی یکی از رفتارهای مذکور را انجام دهد، در صورت احراز

شرایط پیرامونیِ مربوط، عنصر مادی جرمِ کلاهبرداری رایانه‌ای تحقق می‌یابد.

در هر حال، در کلاهبرداری رایانه‌ای، در مواردی که مبدأ انتقال وجه و مقصد آن در حوزه‌های قضایی مختلف بوده، اختلاف در صلاحیت محلی بین مراجع قضایی موجب اظهارنظر هیئت عمومی دیوان عالی کشور به شرح زیر شده است:

«نظر به اینکه در صلاحیت محلی، اصلْ صلاحیت دادگاه محل وقوع جرم است[1] و این اصل در قانون جرایم رایانه‌ای نیز ـ مستفاد از ماده‌ی ۲۹[2] ـ مورد تأکید قانونگذار قرار گرفته، بنابراین، در جرم کلاهبرداری مرتبط با رایانه، هرگاه تمهید مقدمات و نتیجه‌ی حاصله از آن در حوزه‌های قضایی مختلف صورت گرفته باشد، دادگاهی که بانک افتتاح‌کننده‌ی حسابِ زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده، در حوزه‌ی آن قرار دارد، صالح به رسیدگی است ... ».[3]

این رویکرد دیوان عالی کشور در بسیار از آرای دادگاه‌های کیفری مورد استناد یا متابعت قرار گرفته است.[4] در برخی آرای کیفری نیز اعلام شده است که اگر وجهی از

---

۱. قسمت ابتدایی ماده‌ی ۳۱۰ قانون آیین دادرسی کیفری ۱۳۹۲ مربوط به این اصل می‌شود؛ ماده‌ای که اعلام می‌دارد: «متهم در دادگاهی محاکمه می‌شود که جرم در حوزه‌ی آن واقع شود. ... ».

۲. این ماده‌ی قانونی که در سال ۱۳۸۸ به ماده‌ی ۷۵۷ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) تبدیل شد، طبق ماده‌ی ۶۹۸ قانون آیین دادرسی کیفری ۱۳۹۲ نسخ صریح شده، چراکه ماده‌ی اخیر به صراحت از لغو مواد ۷۵۶ تا ۷۷۹ الحاقی ۱۳۸۸ به قانون تعزیرات ۱۳۷۵ سخن گفته است. با وجود این، ماده‌ی ۶۶۵ قانون آیین دادرسی کیفری ۱۳۹۲ جایگزین ماده‌ی ۲۹ قانون جرایم رایانه‌ای (ماده‌ی ۷۵۷ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)) شده است که با اندکی تغییر مقرر می‌دارد: «چنانچه جرم رایانه‌ایِ در صلاحیت دادگاه‌های ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. در صورتی که محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و در صورت اقتضا صدور کیفرخواست می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند».

۳. رأی وحدت رویه‌ی شماره‌ی ۷۲۹ مورخ ۱۳۹۱/۱۲/۱، هیئت عمومی دیوان عالی کشور.

۴. ازجمله، ر.ک. دادنامه‌ی شماره‌ی ۹۳۰۹۹۷۰۹۱۰۶۰۰۲۸۶ مورخ ۱۳۹۳/۳/۱۰، شعبه‌ی ۳۳ دیوان عالی کشور؛ مبنی بر اینکه دادگاهی صلاحیت رسیدگی به کلاهبرداری رایانه‌ای را دارد که بانک محل افتتاح حسابِ بزهدیده و عملیات برداشت یا انتقال وجه در حوزه‌ی آن واقع شده باشد. نیز دادنامه‌ی شماره‌ی ۹۳۰۹۹۷۰۹۲۵۲۰۲۱۷۹ مورخ ۱۳۹۳/۶/۸، شعبه‌ی ۳۷ دیوان عالی کشور؛ دادنامه‌ی شماره‌ی ۹۳۰۹۹۷۰۹۲۵۱۰۱۹۵۳ مورخ۱۳۹۳/۷/۷، شعبه‌ی ۳۶ دیوان عالی کشور؛ دادنامه‌ی شماره‌ی ۹۳۰۹۹۷۰۹۲۵۱۰۲۹۵۱ مورخ ۱۳۹۳/۱۰/۲۹، شعبه‌ی ۳۶ دیوان عالی کشور؛ و دادنامه‌ی

شهری به شهر دیگر منتقل شود، نظر به اینکه به محض برداشت وجه از حساب شاکی در مبدأ جرم تحقق یافته و حساب مقصد که وجوه به آن انتقال داده شده، تأثیری در صلاحیت محلی ندارد، دادگاه مبدأ جرم، یعنی جایی که پول از حساب شاکی خارج شده، صالح به رسیدگی است (دادنامه‌ی شماره‌ی ۹۱۰۹۹۷۰۹۱۰۵۰۰۸۵۴ مورخ ۱۳۹۱/۱۱/۲۵، شعبه‌ی ۳۲ دیوان عالی کشور). به این ترتیب، دادگاهی که بانک افتتاح‌کننده‌ی حساب مقصد در حوزه‌ی آن قرار دارد، صلاحیت محلی برای رسیدگی به جرم کلاهبرداری رایانه‌ای ندارد. البته، رسیدگی به جرم کلاهبرداری رایانه‌ای توسط اتباع بیگانه در صلاحیت دادسرا و دادگاه تهران است[1] و موضوع از شمول رأی وحدت رویه‌ی پیش‌گفته خارج است (دادنامه‌ی شماره‌ی ۹۴۰۹۹۷۰۹۲۵۲۰۵۳۷۶ مورخ ۱۳۹۴/۱۱/۱۹، شعبه‌ی ۳۷ دیوان عالی کشور).

۲-۲. عنصر روانی کلاهبرداری رایانه‌ای

در حقوق ایران، عنصر روانی کلاهبرداری رایانه‌ای مشتمل بر دو جزء اصلی می‌شود: قصد عام و قصد خاص. قصد عام زمانی احراز می‌شود که به اثبات برسد، مرتکب با علم به شرایط پیرامونی، از جمله نداشتن مجوز و تعلق مال به دیگری، یکی از رفتارهای مجرمانه‌ی پیش‌گفته را با عمد و اراده انجام داده است. از این رو، چنانچه شخصی با واردکردن اطلاعات اشتباه در اینترنت بانک به طور اتفاقی به حساب دیگری دسترسی پیدا کند و بدون توجه به اینکه حساب بانکی خودش نیست، وجوهی را برای خرید اینترنتی انتقال دهد، قصد عام ندارد.

اما قصد خاص در مواردی احراز می‌شود که مرتکب قصد تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی برای خود یا دیگری داشته باشد. پس، هرگاه قصد شخص از ارتکاب عالمانه و عامدانه‌ی یکی از رفتارهای مجرمانه‌ی کلاهبرداری رایانه‌ای نشان دادن توانایی‌اش برای ایجاد اختلال در سامانه‌ی رایانه‌ای یا مخابراتی نزد همکاران خود باشد،

شماره‌ی ۹۴۰۹۹۷۰۹۲۵۰۰۰۰۴۱ مورخ ۱۳۹۴/۱/۲۹، شعبه‌ی ۳۵ دیوان عالی کشور.

۱. ر.ک. مواد ۲۶ و ۳۱۶ از قانون آیین دادرسی کیفری ۱۳۹۲.

قصد خاص ندارد. اعتقاد به اینکه با احراز انجام فعل از سوی شخص، سوءنیت او مفروض انگاشته شده و بار اثبات نداشتن سوءنیت با متهم است (حیدری، ۱۳۹۶: ۲۴۰). از ظاهر ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) برداشت نمی‌شود و با لزوم احراز قصد نتیجه در جرایم مقید به‌موجب ماده‌ی ۱۴۴ قانون مجازات اسلامی ۱۳۹۲ هم سازگار نیست؛ ضمن اینکه تفسیری به ضرر متهم است، از آنجا که باعث جابجایی بار اثبات از شاکی یا دادستان به متهم می‌شود، و درنتیجه، اثبات جرم آسان‌تر می‌گردد.

در حقوق انگلستان و وِیلز نیز پیش از همه لازم است قصد عام مرتکب احراز شود، به این معنا که وی در ارتکاب هر یک از رفتارهای اظهار کذب، کوتاهی در افشای اطلاعات و سوءاستفاده از موقعیت عمد و اراده داشته باشد که خود مستلزم آگاهی از شرایط پیرامونیِ مربوط است. قانونگذار انگلیسی و وِیلزی هم در قسمت (الف) بند (۱) ماده‌ی ۲، قسمت (الف) ماده‌ی ۳ و قسمت (ب) بند (۱) ماده‌ی ۴ از قانون کلاهبرداری ۲۰۰۶م. پیش از اشاره به رفتار مجرمانه‌ی موردنظر، با استفاده از اصطلاح «با سوءنیت»[1] به نوعی بر این امر تأکید کرده است؛ برای نمونه، در ابتدای قسمت (الف) ماده‌ی ۳ قانون مذکور مقرر می‌دارد: «با سوءنیت در افشای اطلاعات نسبت به شخص دیگری کوتاهی کند ... ». باید افزود که دیوان عالی بریتانیا[2] در یکی از پرونده‌های اخیر[3] رهنمونی را که باید در خصوص مفهومِ سوءنیت به هیئت‌منصفه ارائه شود دوباره پی‌ریزی کرده است.

پس، چنانچه در نوشیدنی شخصی بدون اطلاع او مشروب الکلی ریخته شده باشد و وی در حالت مستی مرتکب یکی از رفتارهای بالا شود، به خاطر کلاهبرداری تعقیب‌شدنی نیست، چراکه قصد عام متزلزل شده است. به همین ترتیب، در کلاهبرداری با اظهار کذب، متهمِ ناآگاه، یعنی کسی که اشتباه کرده، گیج شده و یا اظهاری را با حُسن‌نیت صورت داده است (با این اعتقاد که اظهارش صحیح است)، سوءنیتِ لازم را ندارد (Hutchinson & Hendy, 2015: 212). باید دانست که اگرچه مواد یادشده از قانون مذکور از لزوم علم به شرایط پیرامونی سخن نگفته اند، اما همان‌طور که برخی حقوق‌دانان انگلیسی اشاره

1. Dishonestly.
2. UK Supreme Court.
3. See, *Ivey v Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67.

کرده اند (Martin & Storey, 2015: 526). ناآگاهی مرتکب ممکن است در احراز سوءنیت به شرحی که گفته شد، اختلال ایجاد کند، و در واقع، به این معنا است که وی سوءنیت ندارد.

در اینجا، باید خاطرنشان کرد که اگرچه قانون کلاهبرداری ۲۰۰۶م. در خصوص کافی بودنِ بی‌پروایی[1] برای احراز عنصر روانیِ کلاهبردار صراحتی ندارد، به نظر می‌رسد که در این نظام حقوقی، افزون بر علم مرتکب، بی‌پروایی او نیز موجب تحقق سوءنیتِ لازم برای جرم کلاهبرداری رایانه‌ای خواهد شد. بی‌پروایِ مجرمانه،[2] به عنوان گونه‌ای از عنصر روانی، به این معنا است که متهم خطر را پیش‌بینی می کرده، اما پیش رفته و تن به آن داده است (کراس، ۱۳۹۸: ۸۳ـ۷۹). بر این اساس، در کلاهبرداری با اظهار کذب که طبق قسمت (الف) بند (۲) ماده‌ی ۲ قانون کلاهبرداری ۲۰۰۶م. اظهار باید خلاف واقع یا گمراه‌کننده باشد تا کذب به شمار آید، به‌موجب قسمت (ب) بند مذکور، اظهارکننده نیز باید آگاه باشد که اظهار خلاف واقع یا گمراه‌کننده است یا چه‌بسا باشد. عبارت اخیر حکایت از این دارد که اگر متهم احتمال بدهد که اظهار دارای یکی از ویژگی‌های یادشده است، همانند موردی که نسبت به این مسئله آگاهی دارد، با لحاظ سایر شرایط، مرتکب کلاهبرداری با اظهار کذب شده است. با وجود این، به نظر می‌رسد که بی‌پروایی در خصوص سایر شیوه‌های ارتکاب جرم کلاهبرداری رایانه‌ای سوءنیتِ لازم را برآورده نکند، زیراکه در مواد ۳ و ۴ از قانون کلاهبرداری ۲۰۰۶م. عبارتِ مشابهی یافت نمی‌شود.

اما قصد خاص در جرم کلاهبرداری رایانه‌ای در نظام کیفری مورد بحث عبارت است از قصد کسب منفعت برای خود یا دیگری، یا ایراد ضرر به غیر. در این خصوص، باید توجه داشت که چنین قصدی که به طور مشابهی در قسمت انتهایی بند (۱) ماده‌ی ۲، ماده‌ی ۳ و بند (۱) ماده‌ی ۴ از قانون کلاهبرداری ۲۰۰۶م. ذکر شده است، لازم نیست در عمل محقق شده باشد، یعنی کسب منفعت یا ایراد ضررِ عملی ضرورتی ندارد، به ویژه از آن رو که مواد یادشده تصریح دارند که اگر مرتکب قصد داشته باشد که دیگری در معرض احتمال ضرر قرار دهد، کفایت می کند. بنابراین، اگرچه این جرم مطلق است، با توجه به

1. Recklessness.
2. Criminal recklessness.

اینکه مطلق یا مقید بودن جرم با عنصر مادی آن و لزوم یا عدم لزومِ قصد خاص با عنصر روانیِ جرم ارتباط دارد، و در نتیجه، مطلق بودن جرمی با لزوم قصد خاص در آن جمع‌پذیر است، احراز قصد خاصِ مذکور در مورد هر سه شیوه‌ی کلاهبرداری رایانه‌ای ضروری است.

باید افزود که استفاده از حرف ربط «یا» در میان عبارت‌های مربوط به عنصر روانی در مواد بالا حکایت از آن دارد که یکی از قصدهای کسب منفعت یا ایراد ضرر به غیر کافی است، قصد کسب منفعت ممکن است برای خود یا دیگری باشد و ضرورتی ندارد که مرتکب درصدد کسب منفعت برای خودش برآید. در *پرونده‌ی حکومت علیه وای یو تسانگ* [۱۹۹۱][1]، متهم در بانکی استخدام شد و با کارمندان دیگر توافق کرد که به بانک اطلاع ندهند که چک‌های حاصله پرداخت‌نشدنی بوده اند. وی با دیگران قرار گذاشت که اطلاعات مربوط به چک‌های پرداخت‌نشدنی را در سوابق بانک وارد نکند. در این پرونده، متهم به طور شخصی منفعتی کسب یا ضرری ایجاد نکرده، ولی کارفرمایش کسب نموده بود؛ مطابق با قانون کلاهبرداری ۲۰۰۶م. هم قصدِ متهم بررسی می‌شود، نه اینکه در عمل سبب منفعت یا ضرری شده است یا خیر.

پرسشی که در اینجا مطرح می‌شود این است که منفعت یا ضرر که تنها قصد یکی از آن‌ها ضروری است، چه مفهومی دارند؟ در پاسخ به این پرسش، ماده‌ی ۵ قانون کلاهبرداری ۲۰۰۶م. به تبیین اصطلاح‌های مذکور پرداخته است. بر این اساس، منفعت و ضرر فقط نسبت به پول[2] یا اموال دیگر[3] تعمیم داده شده (قسمت (الف) بند (۲) ماده‌ی ۵ قانون مذکور) و شامل هرگونه منفعت یا ضرر، اعم از موقت یا دائمی، شده اند (قسمت (ب) بند (۲) ماده‌ی ۵ همان قانون). بنابراین، متهم لازم نیست قصد به طور دائمی محروم کردن را داشته باشد، بلکه منفعت یا ضررِ قصدشده ممکن است موقت یا دائمی باشد. قسمت انتهایی بند (۲) ماده‌ی ۵ قانون کلاهبرداری ۲۰۰۶م. نیز در تبیین مفهوم مال[4] در

1. *R v Wai Yu- tsang* [1991] 4 All ER 664.
2. Money.
3. Other property.
4. Property.

قسمت (الف) همین بند تصریح دارد که به معنای هر مالی، اعم از منقول یا غیرمنقول (شاملِ اموال ناعینی[1]) است.

۳. واکنش قانونی در برابر کلاهبرداری رایانه‌ای

در حقوق کیفری ایران، مطابق با قسمت انتهایی ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، کسی که مرتکب جرم کلاهبرداری رایانه‌ای شود، افزون بر رد مال به صاحب آن،[2] به حبس از یک تا پنج سال یا جزای نقدی از صد و شصت و پنج میلیون (۱۶۵/۰۰۰/۰۰۰) ریال تا هشت‌صد و بیست و پنج میلیون (۸۲۵/۰۰۰/۰۰۰) ریال و یا هر دو مجازات محکوم خواهد شد. بنابراین، اگرچه میزان جزای نقدی مقرر در ماده‌ی مذکور تعدیل شده و کلاهبردار ملزم به رد مال به صاحبش است، میزان حبس کمتر از حتی کلاهبرداری سنتیِ ساده است و جزای نقدی همچنان از نوع ثابت با تعیین حداقل و حداکثر است، حال آنکه در کلاهبرداری سنتی، اعم از ساده یا مشدد، جزای نقدی از گونه‌ی نسبی است، چراکه باید معادل مال اخذشده تعیین شود.[3]

باید افزود که در پرونده‌های کلاهبرداری رایانه‌ای، چنانچه با تحقیقات قضاییْ تمامی یا بخشی از وجوه برداشتی از حساب شاکی در حساب اشخاص دیگر اعم از اشخاص

---

1. Intangible property.

۲. اداره‌ی حقوقی قوه‌ی قضائیه، در خصوص مواردی که مال موضوع کلاهبرداری رایانه‌ای از نوع ارز دیجیتال (رمز ارز) بوده باشد، در نظریه‌ی مشورتی شماره‌ی ۷/۱۴۰۰/۱۶۲۳ مورخ ۱۴۰۱/۸/۲۳ اظهار عقیده کرده است: « ... با عنایت به مقررات مربوط ازجمله ماده‌ی ۳۱۲ قانون مدنی و ماده‌ی ۷۴۱ قانون مجازات اسلامی [تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)] ... معادل آنچه از کیف پول الکترونیکی بُرده شده است، باید به مالباخته مسترد شود. ازآنجاکه مال موضوع [جرم] ... مثلی تلقی می‌شود، دادگاه باید حکم به پرداخت ارز دیجیتال صادر کند، و در صورت امتناع، با عنایت به اینکه معامله‌ی ارزهای دیجیتال بر اساس مقررات بانک مرکزی و تصویب‌نامه‌ی شماره‌ی ۵۸۱۴۴/ت ۵۵۶۳۷ هـ مورخ ۱۳۹۸/۵/۶ هیأت وزیران در مبادلات داخلی رسمیت ندارد، لذا توقیف و فروش آن به وسیله‌ی اجرای احکام ممکن نیست؛ بنابراین، در حکم مالی است که دسترسی به آن ممکن نیست و با توجه به ملاک ماده‌ی ۴۶ قانون اجرای احکام مدنی مصوب ۱۳۵۶ قیمت آن به تراضی طرفین، و در صورت عدم تراضی، بهای آن به قیمت یوم‌الاداء به‌وسیله‌ی کارشناس و خبره محاسبه و از محکومٌ‌علیه وصول و به محکومٌ‌له پرداخت می‌شود». اداره‌ی مذکور در نظریه‌ی مشورتی شماره‌ی ۷/۱۴۰۰/۱۵۵۵ مورخ ۱۴۰۱/۸/۲۵ نیز دیدگاه مشابهی ابراز کرده است.

۳. ر.ک. ماده ی ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری ۱۳۶۷.

حقیقی یا حقوقی یافت و توقیف شود، با درخواست ذی‌نفع صدور دستور عودت وجه مزبور قانونی است و لزومی به صدور حکم قطعی در این مورد نیست. در واقع، مطابق با ماده‌ی ۱۴۸ قانون آیین دادرسی کیفری ۱۳۹۲ و ماده‌ی ۲۱۵ قانون مجازات اسلامی ۱۳۹۲ رد عین مال موجود یا وجوه تحصیل‌شده از ارتکاب جرم با رعایت شرایط مذکور در این موادْ تکلیف قانونیِ مقام قضایی رسیدگی‌کننده به موضوع اعم از بازپرس یا دادرس دادگاه است و لذا صدور حکم قطعی ضرورتی ندارد (نظریه‌ی مشورتی شماره‌ی ۷/۹۹/۹۶ مورخ ۱۳۹۹/۳/۷ اداره‌ی حقوقی قوه‌ی قضائیه).

از این گذشته، چنانچه کلاهبرداری رایانه‌ای به صورت شبکه‌ای و سازمان‌یافته ارتکاب یابد، مشمول ماده‌ی ۴ قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری ۱۳۶۷ نمی‌شود، زیراکه کلاهبرداری رایانه‌ای عمل مجرمانه‌ی خاصی است که مؤخر بر قانون مذکور جرم‌انگاری شده و از ماده‌ی ۴ قانون اخیر که ناظر بر کلاهبرداری سنتی موضوع ماده‌ی ۱ همان قانون است، انصراف دارد (نظریه‌ی مشورتی شماره‌ی ۷/۹۹/۱۴۹۴ مورخ ۱۳۹۹/۱۲/۵ اداره‌ی حقوقی قوه‌ی قضائیه). ضمن اینکه افتتاح حساب بانکیِ جعلی در راستای ارتکاب کلاهبرداری رایانه‌ای مقدمه‌ی این جرم تلقی می‌شود، و در نتیجه، کیفر مستقل ندارد، بلکه تنها مجازات کلاهبرداری رایانه‌ای اِعمال می‌شود (دادنامه‌ی شماره‌ی ۹۴۰۹۹۷۰۲۲۲۳۰۰۱۸۹ مورخ ۱۳۹۴/۲/۱۹، شعبه‌ی ۲۳ دادگاه تجدیدنظر استان تهران).

در حقوق کیفری انگلستان و وِیلز، مجازات شیوه‌های سه‌گانه‌ی کلاهبرداری رایانه‌ای در ماده‌ی ۱ قانون کلاهبرداری ۲۰۰۶م. یافت می‌شود. مطابق با قسمت (الف) بند (۳) ماده‌ی ۱ قانون کلاهبرداری ۲۰۰۶م.، شخصی که به جرم کلاهبرداری (رایانه‌ای) مقصر شناخته می‌شود، در محکومیت اختصاری،[1] به حبس برای مدتی که متجاوز از دوازده ماه نباشد یا جزای نقدی که از حداکثر قانونی تجاوز نکند، یا هر دو مجازات، از سوی دادگاه صلح[2] محکوم خواهد شد. در خصوص تعیین میزان مجازات توسط قاضی انگلیسی و وِیلزی باید به چند مسئله اشاره کرد: نخست اینکه اگرچه در قسمت (الف) بند (۳) ماده‌ی

1. Summary conviction.
2. Magistrates' court.

۱ قانون کلاهبرداری ۲۰۰۶م. فقط حداکثر مجازات حبس (دوازده ماه) تعیین شده است، اما دادگاه صلح نمی‌تواند به کمتر از پنج روز حبس حکم صادر کند؛[1] دوم آنکه جزاهای نقدی که دادگاه مذکور می‌تواند مورد حکم قرار دهد، در پنج سطح در نظر گرفته شده اند که جزای نقدیِ سطح پنج[2] (بالاترین سطح) هرچند پیش‌تر سقفِ ۵/۰۰۰ پوند داشت، اما متعاقب اصلاحِ قانون معاضدت حقوقی، صدور حکم و مجازاتِ مجرمان ۲۰۱۲م.[3] به جزای نقدی با «هر مبلغی»[4] تغییر کرد[5] (Elliott & Quinn, 2016: 480). در هر حال، پرداخت جزای نقدی لازم است بلافاصله باشد، اما در مواردی که امکان‌پذیر نباشد، دادگاه دوره‌های زمانی برای جزای نقدی تعیین می‌کند تا به صورت اقساط هفتگی یا ماهانه پرداخت شود. البته، دادگاه‌ها به طورمعمول به دنبال آن هستند که جزای نقدی در طول دوره‌ی دوازده‌ماهه تسویه شود (Gibson, 2009: 96-97).

اما طبق قسمت (ب) بند (۳) ماده‌ی ۱ قانون کلاهبرداری ۲۰۰۶م.، شخصی که کلاهبردار (رایانه‌ای) شناخته می‌شود، در محکومیت برحسب کیفرخواست،[6] مشمول حبس برای مدتی که متجاوز از ده سال نباشد یا جزای نقدی و یا هر دو مجازات می‌شود. اگرچه مرجع قضاییِ انگلیسی و ویلزی (در اینجا، دادگاه جنایی[7]) بار دیگر می‌تواند حکم به یکی از دو مجازات حبس یا جزای نقدی و یا هر دو مجازات صادر کند، حداکثر میزان حبس (ده سال) به‌مراتب بیشتر از میزان حبسی است که ممکن است در محکومیت اختصاری بر کلاهبردار تحمیل شود. افزون بر این، هیچ حداکثرِ جزای نقدی در خصوص تعیین مجازات از سوی دادگاه جنایی تعیین نشده، اما این دادگاه لازم است اطمینان حاصل کند که مبلغ جزای نقدیِ تعیین‌شده انعکاس‌دهنده‌ی شدت جرم[8] است، ضمن اینکه

---

1. See, s. 132 of the Magistrates' Courts Act 1980.
2. A level five fine.
3. Legal Aid, Sentencing and Punishment of Offenders Act 2012.
4. Fine of 'any amount'.
۵. شایان ذکر است که هرچند جزای نقدی ممکن است برای هر جرمی تحمیل شود، ولی پیش از اصلاح قانونیِ یادشده تنها دادگاه جنایی بود که مجاز به تعیین جزای نقدی با هر مبلغی برای مجرم بود (مارتین، ۱۴۰۱: ۲۳۳).
6. Conviction on indictment.
7. Crown Court.
8. Seriousness of the offence.

استطاعتِ مجرم، کاهش یا افزایش آن را به عنوان نتیجه در نظر گیرد.[1] با وجود این، درصدد کمی از مجرمان در دادگاه جنایی با محکومیت به جزای نقدی مواجه می‌شوند. یکی از معضل‌های مربوط، شمار جزاهای نقدیِ پرداخت‌نشده[2] است که هم موجب بی‌تأثیری این مجازات و هم حبس شدنِ مجرم به خاطر نپرداختن آن می‌شود (Huxley-Binns e. al., 2017: 553).

٤. وجوه افتراق و اشتراک نظام‌های کیفری

بررسی عنصرهای سازنده‌ی کلاهبرداری رایانه‌ای در نظام‌های کیفری ایران، انگلستان و ویلز، به شرحی که گذشت، روشن می‌سازد که وجوه افتراق و اشتراکی بین این نظام‌ها وجود دارند. این وجوه به اختصار در جدول زیر به تصویر کشیده می‌شوند:

الف. عنصر قانونی
قانون‌گذار ایرانی کلاهبرداری رایانه‌ای را جداگانه در ماده‌ی ۱۳ قانون جرایم رایانه‌ای ۱۳۸۸ (هم‌اکنون ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)) پیش‌بینی کرده، ولی قانونگذار انگلیسی و ویلزی جرم عامِ کلاهبرداری را مقرر کرده است که امکان ارتکاب آن به صورت رایانه‌ای نیز وجود دارد.
ب. عنصر مادی
۱. در ایران، رفتار مجرمانه در جرمِ کلاهبرداری رایانه‌ای شامل اَعمالی نظیر واردکردن، تغییر، محو، ایجاد یا متوقف‌کردن داده‌ها و یا مختل‌کردن سامانه می‌شود که همگی ایجابی (فعل) هستند. در انگلستان و ویلز، رفتار مجرمانه‌ی کلاهبرداری رایانه‌ای ممکن است به صورت اظهار کذب، کوتاهی در افشای اطلاعات و یا سوءاستفاده از موقعیت جلوه‌گر شود. شیوه‌ی اخیر از کلاهبرداری زمانی که به صورت رایانه‌ای ارتکاب می‌یابد، تنها از طریق فعل امکان‌پذیر است، نه ترک فعل، در حالی که ماهیت کلاهبرداری با کوتاهی در افشای اطلاعات به گونه‌ای است که اساساً با ترک فعل تحقق می‌پذیرد. ۲. در نظام کیفری ایران، شرایط پیرامونی کلاهبرداری رایانه‌ای عبارت اند از: مرتکب مجوز نداشته باشد؛ و موضوع جرم، سامانه‌ی رایانه‌ای یا مخابراتی باشد؛ و مال (در مفهوم عام خود) متعلق به دیگری باشد. در نظام کیفری انگلستان و ویلز نیز بدون مجوز عمل ارتکابی شرط است و اظهار کذب ممکن است نسبت به هر دستگاه یا وسیله‌ای صورت گیرد که به منظور دریافت، انتقال و یا پاسخ به ارتباط‌ها (با دخالت انسان یا بدون آن) طراحی شده باشد.

1. See s. 164 of the Criminal Justice Act 2003.
2. Unpaid fines.

ادامه جدول

ب. عنصر مادی
۳. کلاهبرداری رایانه‌ای در ایران در زمره‌ی جرایم مقید قرار می‌گیرد و تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی نتیجه‌ی آن محسوب می‌شود؛ حال آنکه این جرم در انگلستان و وِیلز در شمار جرایم مطلق قرار می‌گیرد، لذا حصول نتیجه‌ی خاصی از رفتار مرتکب مانند کسب منفعت ضروری نیست.
پ. عنصر روانی
در حقوق ایران، عنصر روانی کلاهبرداری رایانه‌ای مشتمل بر دو جزء قصد عام (ارتکاب یکی از رفتارهای مجرمانه‌ی پیش‌گفته با عمد و اراده و نیز با علم به شرایط پیرامونی، از جمله نداشتن مجوز و تعلق مال به دیگری) و قصد خاص (قصد تحصیل وجه، مال، منفعت، خدمات و یا امتیازات مالی برای خود یا دیگری) می‌شود. در حقوق انگلستان و وِیلز نیز لازم است قصد عام مرتکب احراز شود، به این معنا که وی در ارتکاب هر یک از رفتارهای اظهار کذب، کوتاهی در افشای اطلاعات و سوءاستفاده از موقعیت عمد و اراده داشته باشد که خود مستلزم آگاهی از شرایط پیرامونیِ مربوط است. اما قصد خاص در جرم کلاهبرداری رایانه‌ای در این نظام کیفری عبارت است از قصد کسب منفعت برای خود یا دیگری، یا ایراد ضرر به غیر.
ت. مجازات
در حقوق کیفری ایران، مطابق با قسمت انتهایی ماده‌ی ۷۴۱ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، کسی که مرتکب جرم کلاهبرداری رایانه‌ای شود، افزون بر رد مال به صاحب آن، به حبس از یک تا پنج سال یا جزای نقدی از صد و شصت و پنج میلیون (۱۶۵/۰۰۰/۰۰۰) ریال تا هشتصد و بیست و پنج میلیون (۸۲۵/۰۰۰/۰۰۰) ریال و یا هر دو مجازات محکوم خواهد شد. در حقوق کیفری انگلستان و وِیلز، مطابق با قسمت (الف) بند (۳) ماده‌ی ۱ قانون کلاهبرداری ۲۰۰۶م.، شخصی که به جرم کلاهبرداری (رایانه‌ای) مقصر شناخته می‌شود، در محکومیت اختصاری، به حبس برای مدتی که متجاوز از دوازده ماه نباشد یا جزای نقدی که از حداکثر قانونی تجاوز نکند، یا هر دو مجازات، از سوی دادگاه صلح محکوم خواهد شد. اما طبق قسمت (ب) بند (۳) ماده‌ی ۱ قانون کلاهبرداری ۲۰۰۶م.، شخصی که کلاهبردار (رایانه‌ای) شناخته می‌شود، در محکومیت برحسب کیفرخواست، مشمول حبس برای مدتی که متجاوز از ده سال نباشد یا جزای نقدی و یا هر دو مجازات می‌شود.

نتیجه

تحلیل عنصرهای سازنده‌ی کلاهبرداری رایانه‌ای در نظام‌های کیفری ایران، انگلستان و وِیلز حکایت از آن دارد که با وجود جرم‌انگاری این عمل از سوی قانونگذار، برخی نقص‌ها در رویکرد اتخاذی در راستای مقابله با کلاهبرداران رایانه‌ای یافت می‌شوند که تلاش برای رفع آن‌ها، به ویژه در جهت صدور آرای کیفریِ منسجم، تأثیر مطلوبی خواهد داشت. بر این اساس، راهکارهای زیر به قانونگذار ایرانی پیشنهاد می‌شود:

- **پیش‌بینی جرم عامِ کلاهبرداری**؛ همان‌طور که در نظام کیفری انگلستان و وِیلز جرم عامِ کلاهبرداری پیش‌بینی شده است و با توجه به اینکه هم‌اکنون بسیاری از جرایم مالی به صورت رایانه‌ای نیز ارتکاب می‌یابند، در راستای جلوگیری از ازدیاد مواد قانونی در مقررات کیفری، مناسب است که قانونگذار ایرانی در اصلاحاتی که در مجموعه‌ی قوانین کیفری اِعمال می‌کند، ارتکاب کلاهبرداری به هر دو شکل سنتی و رایانه‌ای آن را در قالب یک ماده‌ی قانونی پیش‌بینی کند.

- **پذیرش بی‌پروایی به‌منزله‌ی عنصر روانی جرمِ کلاهبرداری رایانه‌ای**؛ در حقوق انگلستان و وِیلز، بی‌پروایی نوعی از حالت ذهنی است که در مرز بین تقصیر جزایی و قصد مجرمانه در حقوق ایران قرار می‌گیرد. ایده‌ی ورای بی‌پروایی این است که متهم خطر صدمه (نتیجه‌ی ممنوعه) را پیش‌بینی کرده، و با این حال، پیش رفته و تن به آن داده است (هِرینگ، ۱۴۰۳: ۴۵). این در حالی است که در حقوق ایران چنین حالت ذهنی‌ای به رسمیت شناخته نشده است. به نظر می‌رسد که، در راستای مقابله مؤثرتر با کلاهبرداران رایانه‌ای، لازم باشد که قانونگذار ایرانی نیز حالت ذهنی پیش‌گفته را به طور مستقلی در قانون منعکس سازد.

- **افزایش میزان کیفرهای جرمِ کلاهبرداری رایانه‌ای**؛ در حال حاضر میزان حبس کلاهبرداری رایانه‌ای کمتر از حتی کلاهبرداری سنتی از گونه‌ی ساده است و جزای نقدی مقرر برای آن همچنان از نوع ثابت با تعیین حداقل و حداکثر است، در حالی که در کلاهبرداری سنتی، اعم از ساده یا مشدد، جزای نقدی از گونه‌ی نسبی است و باید معادل مال اخذشده تعیین شود. چنین رویکردی در معرض انتقاد قرار می‌گیرد، زیرا به طور معمول یکی از اهداف پیش‌بینی جرایم خاص این است که برخورد سخت‌گیرانه‌تری نسبت به مرتکبان این جرایم اِعمال شود، در حالی که مجازات کلاهبرداری سنتی تعزیر درجه‌ی چهار است، در حالی که مجازات کلاهبرداری رایانه‌ای تعزیر درجه‌ی پنج محسوب می‌شود. هرگاه مواردی نظیر ناشناس بودنِ هویت کلاهبردارهای رایانه‌ای، صرف زمان و هزینه‌ی بیشتر جهت تعقیب آن‌ها و زیان‌های واردشده به بزهدیده(ها)ی کلاهبرداری رایانه‌ای مدنظر قرار گیرد، انتقاد مذکور بیش‌تر جلوه خواهد کرد.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID

Amir E'temadi https://orcid.org/0000-0003-1748-4825

منابع

آقایی‌نیا، حسین و رستمی، هادی (۱۴۰۱)، جرایم علیه اموال و مالکیت، چاپ سوم، تهران، بنیاد حقوقی میزان.

اعتمادی، امیر (۱۴۰۳)، جرایم علیه اموال و مالکیت، چاپ اول، تهران، بنیاد حقوق میزان.

حیدری، علی‌مراد (۱۳۹۶)، جرایم علیه اموال و مالکیت، چاپ اول، قم، انتشارات دانشگاه حضرت معصومه.

زیبر، اولریش (۱۳۹۰)، جرایم رایانه‌ای، ترجمه‌ی محمدعلی نوری و دیگران، چاپ دوم، تهران، انتشارات کتابخانه‌ی گنج دانش.

عالی‌پور، حسن (۱۳۹۵)، حقوق کیفری فناوری اطلاعات، چاپ چهارم، تهران، انتشارات خرسندی.

کراس، نوئل (۱۳۹۸)، درآمدی بر حقوق کیفری و عدالت کیفری در انگلستان و ویلز، ترجمه‌ی امیر اعتمادی، چاپ دوم، تهران، انتشارات مجد.

مارتین، جکلین (۱۴۰۱)، نظام حقوقی انگلستان: نکته‌های کلیدی ـــ پرونده‌های کلیدی، ترجمه‌ی امیر اعتمادی، چاپ اول، تهران، بنیاد حقوقی میزان.

محمدنسل، غلامرضا (۱۳۹۲)، حقوق جزای اختصاصی: جرایم رایانه‌ای در ایران، چاپ اول، تهران، نشر میزان.

منصورآبادی، عباس و منصورآبادی، علیرضا (۱۴۰۳)، حقوق جرایم رایانه‌ای و مجازی، چاپ اول، تهران، بنیاد حقوقی میزان.

هرینگ، جاناتان (۱۴۰۳)، مقدمات حقوق کیفری، ترجمه‌ی امیر اعتمادی، چاپ اول، تهران، بنیاد حقوقی میزان.

پژوهشگاه قوه‌ی قضائیه (۱۳۹۴)، *مجموعه‌ی آرای قضایی دادگاه‌های تجدیدنظر استان تهران (کیفری)، بهار ۱۳۹۲*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۴۰۲)، *مجموعه‌ی آرای قضایی دادگاه‌های تجدیدنظر استان تهران (کیفری)، سال ۱۳۹۴*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۳۹۳)، *مجموعه‌ی آرای قضایی شعب دیوان عالی کشور (کیفری)، بهمن ۱۳۹۱*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۳۹۶)، *مجموعه‌ی آرای قضایی شعب دیوان عالی کشور (کیفری)، بهار ۱۳۹۳*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۴۰۱)، *مجموعه‌ی آرای قضایی شعب دیوان عالی کشور (کیفری)، تابستان ۱۳۹۳*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۳۹۷)، *مجموعه‌ی آرای قضایی شعب دیوان عالی کشور (کیفری)، مهر، آبان و آذر ۱۳۹۳*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۴۰۱)، *مجموعه‌ی آرای قضایی شعب دیوان عالی کشور (کیفری)، زمستان ۱۳۹۳*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

پژوهشگاه قوه‌ی قضائیه (۱۴۰۱)، *مجموعه‌ی آرای قضایی شعب دیوان عالی کشور (کیفری)، سال ۱۳۹۴*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه‌ی قضائیه.

آیین‌نامه‌ی نحوه‌ی استفاده از سامانه‌های رایانه‌ای یا مخابراتی ۱۳۹۵.

تصویب‌نامه‌ی شماره‌ی ۵۶۲۶۱/ت۶۲۲۹۸ه هیأت وزیران در خصوص اصلاح میزان مبالغ مربوط به جرایم و تخلفات مندرج در قوانین مختلف مورخ ۱۴۰۳/۴/۴.

References

Bainbridge, David I. (2008), Introduction to Information Technology Law, Sixth Edition, Harlow, Pearson Education Limited

Butterfield, Andrew and Ekembe Ngondi, Gerard (Eds) (2016), A Dictionary of Computer Science, Seventh Edition, Oxford, Oxford University Press

Button, Mark and Cross, Cassandra (2017), Cyber Frauds, Scams and their Victims, London, Routledge, First Published

Coderre, David (2009), Computer-aided Fraud Prevention and Detection, New Jersey, John Wiley & Sons, Inc.

Cross, Noel (2020), Criminal Law for Criminologists: Principles and Theory in Criminal Justice, London, Routledge

Downing, Douglas A. et. al. (2009), Dictionary of Computer and Internet Terms, Tenth Edition, Hauppauge, Barron's Educational Series, Inc.

Elliott, Catherine and Quinn, Frances (2016), English Legal System, Seventeenth Edition, London, Pearson Education Limited

Gibson, Bryan (2009), The Magistrates' Court: An Introduction, Fifth Edition, Hampshire, Waterside Press

Haynes, Sandra (Ed) (2002), Microsoft Computer Dictionary, Fifth Edition, Washington, Microsoft Press

Hildebrandt, Mireille (2020), Law for Computer Scientists and Other Folk, First Edition, Oxford, Oxford University Press

Horak, Ray (2008), Webster's New World Telecom Dictionary, Indiana, Wiley Publishing, Inc.

Huxley-Binns, Rebecca et. al. (2017), Unlocking the English Legal System, Fifth Edition, London, Routledge

Hutchinson, Odette and Hendy, John (2015) Optimize Criminal Law, London, Routledge, First Published

Jewkes, Yvonne and Yar, Majid (2010), Handbook of Internet Crime, Devon (UK), Willan Publishing, First Published

Lloyd, Ian J. (2017), Information Technology Law, 8th Edition, Oxford, Oxford University Press

Lushbaugh, Charles A. and Weston, Paul B. (2016), Criminal Investigation: Basic Perspectives, Thirteenth Edition, New York, Pearson Education, Inc.

Martin, Jacqueline and Storey, Tony (2015), Unlocking Criminal Law, Fifth Edition, London, Routledge

Rosoff, Stephen M. et. al. (2020), Profit without Honor: White Collar Crime and the Looting of America, Seventh Edition, Hoboken, Pearson Education, Inc.

Rowland, Diane et. al. (2017), Information Technology Law, Fifth Edition, London, Routledge

Stalans, Loretta J. and Donner, Christopher M. (2018), "Explaining Why Cybercrime Occurs: Criminological and Psychological Theories",

Published in Cyber Criminology, Edited by Hamid Jahankhani, London, Springer, 2018, PP. 25-40

Stallings, William and Brown, Lawrie (2018), Computer Security: Principles and Practice, Fourth Edition, Harlow, Pearson Education Limited

Thomas, Mark (2023), Criminal Law, Third Edition, Saltford, Hall and Stott Publishing Ltd.

Statutes

Computer Misuse Act 1990

Criminal Justice Act 2003

Fraud Act 2006

Legal Aid, Sentencing and Punishment of Offenders Act 2012

Magistrates' Courts Act 1980

Cases

Ivey v Genting Casinos (UK) Ltd t/a Crockfords [2017] UKSC 67

R v Wai Yu- tsang [1991] 4 All ER 664

Translated References into English

Books

Aghaeinia, Hossein and Rostami, Hadi (2022), *Crimes against the Property and Ownership*, Third Edition, Tehran, Mizan Legal Foundation. [In Persian]

E'temadi, Amir (2024), *Crimes against Property and Ownership*, First Edition, Tehran, Mizan Law Foundation. [In Persian]

Heydari, Ali-Morad (2017), *Crimes against the Property and Ownership*, First Edition, Qom, Hazrat Masoumeh University Press. [In Persian]

Zieber, Ulrich (2011), *Computer Crimes*, Translated by Mohammad Ali Nouri and Others, Second Edition, Tehran, Ganj-E-Danesh Library Publications. [In Persian]

Alipour, Hassan (2016), *Criminal Law of Information Technology*, 4th edition, Tehran, Khorsandi Publications. [In Persian]

Cross, Noel (2019), *An Introduction to Criminal Law and Criminal Justice in England and Wales*, Translated by Amir E'temadi, Second Edition, Tehran, Majd Publications. [In Persian]

Martin, Jacqueline (2022), *The English Legal System: Key Points-Key Cases*, Translated by Amir E'temadi, First Edition, Tehran, Mizan Legal Foundation. [In Persian]

Mohammad-Nasal, Gholamreza (2013), *Specialized Criminal Law: Computer Crimes in Iran*, First Edition, Tehran, Mizan Publishing House. [In Persian]

Mansourabadi, Abbas and Mansourabadi, Alireza (2024), *Computer and Virtual Crimes Law*, First Edition, Tehran, Mizan Legal Foundation. [In Persian]

Herring, Jonathan (2024), *Introduction to Criminal Law*, Translated by Amir E'temadi, First Edition, Tehran, Mizan Legal Foundation. [In Persian]

Judicial Procedure

Judiciary Research Institute (2015), *Collection of Judicial Decisions of Tehran Province Courts of Appeal (Criminal), Spring 2013*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2023), *Collection of Judicial Decisions of Tehran Province Courts of Appeal (Criminal), Year 2015*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2014), *Collection of Judicial Decisions of the Supreme Court Branches (Criminal), February 2012*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2017), *Collection of Judicial Decisions of the Supreme Court Branches (Criminal), Spring 2014*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2022), *Collection of Judicial Decisions of the Supreme Court Branches (Criminal), Summer 2014*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2018), *Collection of Judicial Decisions of the Supreme Court Branches (Criminal), September, October and December 2014*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2022), *Collection of Judicial Decisions of the Supreme Court Branches (Criminal), Winter 2014*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Judiciary Research Institute (2022), *Collection of Judicial Decisions of the Supreme Court Branches (Criminal), Year 2015*, First Edition, Tehran, Judiciary Press and Publications Center. [In Persian]

Statutes & Regulations

Regulations on the Use of Computer or Telecommunications Systems 2016. [In Persian]

Resolution No. 56261/T62298H of the Council of Ministers Regarding the Amendment of the Amounts Related to Crimes and Violations Stipulated in Various Laws Dated 4/4/1403. [In Persian]

استناد به این مقاله: اعتمادی، امیر. (۱۴۰۴). کلاهبرداری رایانه ای در نظام‌های کیفری ایران، انگلستان و وِیلز. *پژوهش حقوق کیفری*، (۵۰) ۱۳، ۷۳-۱۱۰.

Doi: 10.22054/jclr.2025.82798.2714