University of Tehran Press

Comparative Law Review

Online ISSN: 2423-3404

Volume: 16, **Issue:** 2
Autumn & Winter
2025-2026

Homepage: https://jcl.ut.ac.ir

Computer Theft in the Face of Unauthorized Access to Computer Material in Iranian, English and Welsh Law

Amir E'temadi✉

Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, Qom University, Qom, Iran. Email: Am.etemadi@gmail.com

Article Info

Article Type:
Research Article

Received:
2024/10/29
Received in revised form:
2025/06/27
Accepted:
2025/07/05
Published online:
2025/12/22

Keywords:
Data belonging to another, computer or communications systems, unauthorised access, copying data, cutting data.

Abstract

In the offence of theft, traditionally, property that is observable and tangible (concrete) is stolen. However, human advances, especially in the field of information technology, have led to the emergence of information that is no longer written on paper sheets but stored in spaces such as computer hard disks. Such data, which in many cases also have property characteristics, are considered intangible (inconcrete) property. In Iranian criminal law, the offences of computer theft and unauthorized access have been introduced to criminally protect such data. However, an examination of the approach of the Iranian legislator makes it clear that some flaws exist, including the lack of clarity in distinguishing certain components of the physical element of computer theft and the lack of clarification on whether the computer data belonging to another must be legitimate in both crimes. In contrast, under English and Welsh criminal law, information is not considered property, and theft of information is not recognized as an offence. Nevertheless, when someone attempts to gain unauthorized access to computer data, they may be prosecuted under the criminal offence of unauthorized access to computer material, which is classified as a conduct offence. Accordingly, the present article, by analyzing the constituent elements of the offences of computer theft and unauthorized access to computer material in the mentioned penal systems, proposes solutions to the Iranian legislator, such as separately specifying criminal behavior and result in computer theft, as well as restricting the definition of data to legitimate data.

How To Cite

E'temadi, Amir (2025). Computer Theft in the Face of Unauthorized Access to Computer Material in Iranian, English and Welsh Law. *Comparative Law Review*, 16 (2), 433-457.
DOI: https://doi.com/10.22059/jcl.2025.384374.634691

DOI

10.22059/jcl.2025.384374.634691

Publisher

The University of Tehran Press.

مطالعات حقوق تطبیقی

Homepage: https://jcl.ut.ac.ir

University of Tehran Press

شاپا الکترونیکی: ۳۴۰۴-۲۴۲۳

دوره: ۱۶، شماره: ۲

پاییز و زمستان ۱۴۰۴

سرقت رایانه‌ای در رویارویی با دسترسی غیرمجاز به داده‌های رایانه‌ای در حقوق کیفری ایران، انگلستان و ویلز

امیر اعتمادی✉

استادیار گروه حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق دانشگاه قم، قم، ایران. رایانامه: Am.etemadi@gmail.com

اطلاعات مقاله

نوع مقاله: پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۸/۰۸

تاریخ بازنگری:
۱۴۰۴/۰۴/۰۶

تاریخ پذیرش:
۱۴۰۴/۰۴/۱۴

تاریخ انتشار برخط:
۱۴۰۴/۱۰/۰۱

کلیدواژه‌ها:
بُرش داده‌ها، داده‌های متعلق به دیگری، دسترسی غیرمجاز، رونوشت گرفتن از داده‌ها، سامانه‌های رایانه‌ای یا مخابراتی.

چکیده

در جرم سرقت به‌طور سنتی اموالی ربوده می‌شوند که محسوس هستند و به‌مثابه مال عینی (ملموس) تلقی می‌شوند، اما پیشرفت‌های بشری، به‌ویژه در حوزهٔ فناوری اطلاعات، موجب شکل‌گیری اطلاعاتی شده است که دیگر روی برگه‌های کاغذی نگاشته نمی‌شوند، بلکه در فضاهایی مانند دیسک‌های سخت موجود در رایانه‌ها ذخیره می‌شوند. چنین داده‌هایی که در بسیاری از موارد از ویژگی مالیت نیز برخوردار هستند، به‌منزلهٔ مال ناعینی (ناملموس) درنظر گرفته می‌شوند. در حقوق کیفری ایران جرایمِ سرقت مرتبط با رایانه و دسترسی غیرمجاز در راستای حمایت کیفری از داده‌های پیش‌گفته پیش‌بینی شده است، ولی بررسی رویکرد قانون‌گذار ایرانی روشن می‌سازد که برخی نقص‌ها، ازجمله عدم وضوح در تفکیک برخی اجزای سازندهٔ عنصر مادیِ سرقت رایانه‌ای و عدم تصریح به لزوم مشروع بودنِ داده‌های رایانه‌ای متعلق به دیگری در هر دو جرم، در آن یافت می‌شوند. در مقابل، در حقوق کیفری انگلستان و وِیلز، اطلاعات در زمرهٔ اموال به‌شمار نمی‌آیند و سرقت اطلاعاتْ جرم قلمداد نمی‌شود. اما در شرایطی که کسی درصدد برآید تا به داده‌های رایانه‌ای به‌طور غیرمجاز دسترسی پیدا کند، ممکن است زیر عنوان مجرمانهٔ دسترسی غیرمجاز به داده‌های رایانه‌ای تعقیب شود؛ جرمی که به‌وضوح مطلق محسوب می‌شود. بر این اساس، نگارندهٔ مقالهٔ حاضر، با تحلیل عنصرهای سازندهٔ جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز به داده‌های رایانه‌ای در نظام‌های کیفری پیش‌گفته، راهکارهایی نظیر تصریح جداگانه به رفتار مجرمانه و نتیجهٔ حاصله در سرقت رایانه‌ای و نیز مقید ساختن اطلاق داده‌ها به مشروع بودن آنها را به قانون‌گذار ایرانی پیشنهاد کرده است.

استناد

اعتمادی، امیر (۱۴۰۴). سرقت رایانه‌ای در رویارویی با دسترسی غیرمجاز به داده‌های رایانه‌ای در حقوق کیفری ایران، انگلستان و ویلز. *مطالعات حقوق تطبیقی*، ۱۶ (۲)، ۴۳۳- ۴۵۷.

DOI: https://doi.com/10.22059/jcl.2025.384374.634691

DOI 10.22059/jcl.2025.384374.634691

ناشر مؤسسه انتشارات دانشگاه تهران.

۱. مقدمه

در جرم سرقت به‌طور سنتی اموالی ربوده می‌شوند که محسوس بوده و در دنیای واقعی لمس‌پذیر باشند، به‌طوری‌که از آنها به‌مثابه «مال عینی (ملموس)» یاد شود. اما پیشرفت‌های بشری، به‌ویژه در حوزهٔ فناوری اطلاعات[1]، موجب دگرگونی‌های زیادی در حیات انسان‌ها شده است که از جملهٔ آنها می‌توان به شکل‌گیری اطلاعاتی اشاره کرد که دیگر روی برگه‌های کاغذی نمی‌توان آنها را دید، بلکه در فضاهایی مانند دیسک‌های سخت موجود در رایانه‌ها یا حامل‌های داده ذخیره می‌شوند. چنین داده‌هایی که در بسیاری از موارد از ویژگی مالیت نیز برخوردار هستند، به‌منزلهٔ «مال ناعینی (ناملموس)» درنظر گرفته می‌شوند، و به همین سبب، رفتار مجرمانهٔ ربایش نسبت به آنها شکل نوینی به خود می‌گیرد که با ربودن در قالب سنتی آن کاملاً متفاوت است، و به‌تبع آن، نتیجهٔ حاصله نیز شکل دیگری پیدا می‌کند.

در ایران، عنوان مجرمانهٔ «سرقت مرتبط با رایانه»[2] در فصل سوم (سرقت و کلاهبرداری مرتبط با رایانه) از بخش یکمِ (جرایم و مجازات‌ها) قانون جرایم رایانه‌ای ۱۳۸۸ پیش‌بینی شده است. با وجود این، چنین عنوان مجرمانه‌ای انتقادپذیر است، زیرا قلمرو وسیعی دارد و تمامی سرقت‌هایی را که فقط مرتبط با رایانه هستند، دربر می‌گیرد. برای نمونه، هرگاه کسی از رایانه برای متوقف ساختن عملکرد تدابیر امنیتی نظیر دوربین‌های مداربسته در محل ارتکاب سرقت استفاده کند، یا شخصی دست به ربودن خودِ رایانه و یا تجهیزات رایانه‌ای بزند، از عمل ارتکابی ممکن است زیر عنوان سرقت مرتبط با رایانه یاد شود؛ این در حالی است که هیچ‌یک از اَعمال اخیر زیر عنوان «سرقت رایانه‌ای»[3] تعقیب‌شدنی نیست، بلکه حسب مورد با سرقت‌های تعزیری دیگر تطبیق‌پذیر است. افزون بر این، لحن قانون‌گذار در عنصر قانونی سرقت رایانه‌ای به نحوی است که تفکیک بین رفتار مجرمانه و نتیجه با دشواری روبه‌رو می‌شود. این درحالی است که عنصر قانونی جرمِ دسترسی غیرمجاز که جداگانه پیش‌بینی شده، از وضوحِ لازم در این خصوص برخوردار است.

در انگلستان و وِیلز، اگرچه بند نخست مادهٔ ۴ قانون سرقت ۱۹۶۸، اموال ناعینی را در مفهومِ مال گنجانده، ولی *پروندهٔ آکسفورد و ماس* (۱۹۷۹)[4] تعیین تکلیف کرده است که «اطلاعات» در زمرهٔ اموال به‌شمار نمی‌آیند. به‌طور مشابه، در پروندهٔ *اسکاتلندیِ گرانت علیه دادستانِ بخش* [۱۹۸۸][5] نیز کارمندی که در ازای ۴۰۰ پوند پیشنهاد ارائهٔ رونوشتی از خروجی‌های چاپیِ[6] رایانهٔ کارفرمایش را به شرکت رقیب

1. Information technology
2. Computer-related theft
3. Computer theft
4. *Oxford and Mass* (1979) 68 Cr App R 183
5. Scottish case of *Grant v Procurator Fiscal* [1988] RPC 41
6. Printouts

داد، تبرئه شد. مقرر شد که هیچ مرجعی برای این قضیه که بهره‌جویی از اطلاعات محرمانهْ جرمی کیفری باشد، وجود ندارد. بدیهی است که اگر اطلاعات موردنظر روی برگه‌های کاغذ متعلق به غیر- همچون کارفرمای مرتکب- رونویس شوند، جرمِ سرقت در خصوص برگه‌های کاغذ ارتکاب خواهد یافت.

در واقع، با اینکه پروندهٔ *آکسفورد و ماس* (۱۹۷۹) شامل جرمی مرتبط با رایانه[1] نمی‌شود، برخی محدودیت‌ها آنچه را که در چارچوب قانون بالا مال محسوب می‌شود، روشن می‌سازد. از این رو، اطلاعات، اعم از اینکه روی برگهٔ کاغذ باشد یا در قالب رکورد رایانه‌ای[2]، مال نیست و در نتیجه، «سرقت اطلاعات»[3] جرم شمرده نمی‌شود. در مواردی که اطلاعات روی کاغذ یا دیسکِ نرم[4] باشد، مرتکب فقط ممکن است به سرقت برگه یا دیسک یادشده متهم شود؛ حتی اگر اطلاعات روی آنها ارزش بسیاری زیادی برای ازدست‌دهنده داشته باشد (Edwards et. al., 1990: 150 & 151).

در نظام کیفری اخیر، کمیسیون حقوقی در خصوص «رونوشت گرفتنِ الکترونیکی»[5] که شامل جابه‌جایی فیزیکیِ ابزاری که داده یا برنامهٔ رایانه‌ای روی آن ذخیره شده باشد، نمی‌شود، بلکه تنها دربرگیرندهٔ «رونوشت برداشتنِ غیرمجاز»[6] از آنهاست. گفته شده است حتی اگر اطلاعات یا داده‌ها در چارچوب بند نخست مادهٔ ۴ قانون سرقت ۱۹۶۸، مال قلمداد شوند، به‌ندرت صدق می‌کند که چنین حقی با قصد به‌طور دائمی محروم کردن جرم‌دیده از آنها، تصاحب شود. اغلب، صاحب اطلاعات معلوماتش را دربارهٔ آنها حفظ می‌کند، حتی اگر شخص دیگری اطلاعات را به‌دست آورد. البته ممکن است وضعیت‌هایی هم وجود داشته باشد که قصد یادشده احراز شود، مانند جایی که رونوشت‌گیرنده اطلاعات اصلی را پس از گرفتن رونوشت پاک کند[7] یا همهٔ ارزش اطلاعات ازبین رفته باشد، ولی اصولاً چنین مواردی کمتر صدق خواهد کرد (The Law Commission, Working Paper No. 110, 1988: 45-47).

بر این اساس، پرسش‌های مقالهٔ حاضر عبارت‌اند از: اجزای سازندهٔ عنصرهای مادی و روانی جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز به داده‌های رایانه‌ای در ایران، انگلستان و وِیلز کدام‌اند؟ رویکرد اتخاذشده در برابر مرتکبان جرایم یادشده در نظام‌های کیفری ایران، انگلستان و وِیلز چگونه ارزیابی می‌شود؟ و راهکارهای مؤثر برای مقابله با آنها شامل چه مواردی است؟ در پاسخ به این پرسش‌ها، ابتدا

---

1. Computer-related crime
2. Computer record
3. Theft of information
4. Floppy disk
5. Electronic copying
6. Unauthorised copying

۷. در چنین مواردی، مرتکب ممکن است زیر عنوان دست‌کاری غیرمجازِ داده‌های رایانه‌ای (Unauthorised modification of computer material)، به‌موجب مادهٔ ۳ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰، تعقیب و محاکمه شود (See: E'temadi (B), 284-309).

عنصرهای سازندهٔ جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز به داده‌های رایانه‌ای در نظام‌های حقوقی یادشده بررسی می‌شود و سپس با کنکاش در وجوه افتراق و اشتراک آنها، به نتیجه‌گیری و ارائهٔ راهکار پرداخته خواهد شد.

۲. عنصر قانونی سرقت رایانه‌ای/ دسترسی غیرمجاز به داده‌های رایانه‌ای

در حقوق ایران، قانون‌گذار سرقت رایانه‌ای را به‌طور مستقل در مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)[۱] به‌صورت زیر پیش‌بینی کرده است:

«هر کس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا صد و شصت و پنج میلیون (۱۶۵/۰۰۰/۰۰۰) ریال، و در غیر این صورت، به حبس از نود و یک روز تا یک سال یا جزای نقدی از شصت و شش میلیون (۶۶/۰۰۰/۰۰۰) ریال تا دویست و شصت و چهار میلیون (۲۶۴/۰۰۰/۰۰۰) ریال[۲] یا هر دو مجازات محکوم خواهد شد».

با توجه به مفاد این ماده روشن می‌شود که در سرقت تعزیری موردبحث، رایانه و یا شبکه‌های رایانه‌ای حسب مورد ممکن است آماج یا مکان فعالیت مجرمانه[۳] باشند، اما صرفاً ابزاری که برای ارتکاب فعالیت مجرمانه به‌کار گرفته شود[۴]، به‌شمار نیایند؛ چراکه داده‌های رایانه‌ای در زمرهٔ اموال عینی و ملموس نیستند که رایانه تنها نقش ابزاری برای ربایش آنها ایفا کند. از این رو، سرقت رایانه‌ای را باید «جرمی وابسته به فضای سایبر»[۵] محسوب کرد که در محیط دیجیتال ارتکاب می‌یابد و مستلزم به‌کارگیری سامانه‌های رایانه‌ای و حداقل بعضی از مهارت‌های فناوری اطلاعات است.

در حقوق انگلستان و وِیلز، در شرایطی که کسی درصدد برآید تا دسترسی غیرمجاز به داده‌های رایانه‌ای را به‌دست آورد، ممکن است زیر عنوان مجرمانهٔ «دسترسی غیرمجاز به داده‌های رایانه‌ای»[۶] طبق مادهٔ ۱ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰[۷] تعقیب کیفری شود[۸]. مادهٔ اخیر اعلام می‌دارد:

---

۱. باید یادآور شد که این ماده درواقع، مادهٔ ۱۲ قانون جرایم رایانه‌ای ۱۳۸۸ بوده که با الحاق مواد ۱ تا ۵۴ همین قانون به ادامهٔ قانون تعزیرات ۱۳۷۵ به‌عنوان مواد ۷۲۹ تا ۷۸۲، شمارهٔ آن به ۷۴۰ تغییر یافته است.

2. See: Amendment of the Amounts related to Crimes and Violations Contained in Various Laws Dated 24/6/2024, Appendix 1- Crimes, Row 5

3. Target or place of criminal activity

4. Instrument used to commit a criminal activity

5. A cyber-dependent crime; cf. cyber-enabled crime in Kranenbarg & Leukfeldt, 2021: 196 (See also: Reichel et. al., 2019: 145).

6. Unauthorised access to computer material

7. Computer Misuse Act 1990

۸. در مواردی هم که شخصی با ورود به یک سامانهٔ رایانه‌ای بتواند داده‌های شخصی، یعنی اطلاعات مرتبط با تشخیص

«(۱) شخص در صورتی مقصرِ جرم است که:

(الف) با قصد تأمین دسترسی به هر برنامه یا دادهٔ نگه داشته‌شده در هر رایانه‌ای یا میسرسازی اینکه چنین دسترسی‌ای فراهم گردد، موجب شود که رایانه هرگونه عملیاتی را اجرا کند؛

(ب) دسترسی‌ای که او قصد داشته باشد تأمین یا میسرسازی نأمین آن را فراهم سازد، غیرمجاز باشد؛ و

(پ) وی در زمانی که موجب می‌شود رایانه عملیات موردنظر را اجرا کند، آگاه باشد که مورد یادشده صدق می‌کند.

(۲) برطبق این ماده، قصد شخص برای ارتکاب جرم، لازم نیست متوجهٔ موارد زیر باشد:

(الف) هرگونه برنامه یا دادهٔ خاص؛

(ب) برنامه یا داده از هر نوعِ معین؛ و

(پ) برنامه یا دادهٔ نگه داشته‌شده در هر رایانهٔ خاص. ...»[1].

بند سوم این مادهٔ قانونی نیز مجازات مرتکب را برحسب نوع محکومیت پیش‌بینی کرده است که در بحث از مجازات سرقت رایانه‌ای/ دسترسی غیرمجاز به داده‌های رایانه‌ای به آن اشاره می‌شود. از این گذشته، باید درنظر داشت که قانون‌گذار انگلیسی و وِیلزی، مطابق با قانون پلیس و عدالت ۲۰۰۶[2]، اصلاحاتی را در قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰ اِعمال کرده که در متن مادهٔ ۱ به شرح پیش‌گفته لحاظ شده است. ناگفته نماند که جرم دسترسی غیرمجاز در حقوق کیفری ایران مستقل از جرمِ سرقت رایانه‌ای پیش‌بینی شده است. در این راستا، مادهٔ ۷۲۹ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) اِشعار می‌دارد:

«هر کس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای و یا مخابراتی که به‌وسیلهٔ تدابیر امنیتی حفاظت شده است، دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از شصت و شش میلیون (۶۶/۰۰۰/۰۰۰) ریال تا دویست و شصت و چهار میلیون (۲۶۴/۰۰۰/۰۰۰) ریال[3] یا هر دو مجازات محکوم خواهد شد».

هویتِ اشخاص زنده، را بدون رضایتِ کنترل‌کنندهٔ آنها به‌دست آورد یا افشا کند، ممکن است مطابق با مادهٔ ۱۷۰ قانون حفاظت از داده‌ها ۲۰۱۸ (Data Protection Act 2018) تعقیب‌شدنی باشد.

1. Section 1 of the Computer Misuse Act 1990 provides: "(1) A person is guilty of an offence if —
   (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;
   (b) the access he intends to secure or to enable to be secured, is unauthorised; and
   (c) he knows at the time when he causes the computer to perform the function that that is the case.
   (2) The intent a person has to have to commit an offence under this section need not be directed at —
   (a) any particular program or data;
   (b) a program or data of any particular kind; or
   (c) a program or data held in any particular computer. …"
2. Police and Justice Act 2006
3. See: Amendment of the Amounts related to Crimes and Violations Contained in Various Laws Dated 24/6/2024, Appendix 1- Crimes, Row 5

بر این اساس، در تحلیل جرمِ سرقت رایانه‌ای در رویارویی با دسترسی غیرمجاز به داده‌های رایانه‌ای در نظام‌های حقوقی موردبحث به مناسبت از مادهٔ اخیر نیز سخن گفته خواهد شد تا بتوان ارزیابی جامع‌تری از رویکرد قانون‌گذاران ایرانی، انگلیسی و وِیلزی به‌دست داد.

۳. عنصر مادی سرقت رایانه‌ای/دسترسی غیرمجاز به داده‌های رایانه‌ای

مفاد مواد قانونی پیش‌گفته دربارهٔ جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز به داده‌های رایانه‌ای، حسب مورد در ایران، انگلستان و وِیلز، حاکی از آن است که این جرم از لحاظ عنصر مادی زمانی کامل می‌شود که اجزای سازندهٔ آن به شرح زیر به‌اثبات برسد.

۳. ۱. رفتار مجرمانه

در نظام کیفری ایران، قسمت ابتدایی مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، حاکی از این است که رفتار مجرمانه در سرقت رایانه‌ای همچنان ربایش است، اما با توجه به ماهیتِ متفاوت آنچه در این نوعِ خاص از سرقت‌های تعزیری ربوده می‌شود (داده‌های رایانه‌ای)، چگونگی ارتکاب ربایش شکل نوینی پیدا می‌کند که در سرقت‌های غیررایانه‌ای، اعم از حدی یا تعزیری، متصور نیست. بنابراین، باید دانست که ربایش در مفهوم رایانه‌ای آن به دو صورت بُریدن یا رونوشت گرفتن امکان‌پذیر است. در اصطلاح رایانه‌ای، «بُریدن (بُرش)»[1] به معنای برداشتن بخشی از یک سند به‌طور معمول با قرار دادن موقتی آن در حافظه است، به نحوی که قسمت بُریده‌شده ممکن باشد که جای دیگری قرار داده (چسبانده) شود (Haynes, 2002: 137)؛ و «رونوشت گرفتن»[2] در مفهومِ نسخه‌برداری از اطلاعات در محل دیگری است، درحالی‌که اصلِ اطلاعات بدون تغییر باقی می‌ماند (Downing et. al., 2009: 115). در این عملیات، نسخهٔ بدل از داده‌های ذخیره‌شده در بخش دیگری از حافظه یا روی ابزار ذخیره‌سازیِ متفاوتی ایجاد می‌شود. ناگفته پیداست که رفتارهای یادشده تنها به‌صورت «ایجابی (فعل)» متصور هستند، نه سلبی (ترک فعل).

بر این اساس، هرگاه کسی به رایانهٔ دستیِ متعلق به دیگری وارد شود و بتواند عین برخی داده‌های او را به یک ابزار حامل داده منتقل کند و فردی با دستیابی به دیسک سختِ خارجی[3] متعلق به غیر موفق شود که از تمامی اطلاعات موجود در آن رونوشت بگیرد و آنها را در دیسک سختِ خارجی متعلق به خودش ذخیره کند، به‌ترتیب مرتکب بُریدن یا رونوشت گرفتن از داده‌های رایانه‌ایِ دیگری شده و لذا ربایش با مفهومی که اشاره شد، تحقق یافته است.

---

1. Cut
2. Copy
3. External hard disk

اما برطبق قسمت میانی مادهٔ ۷۲۹ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، رفتار مجرمانه در جرمِ دسترسی غیرمجاز همانا «دسترسی» است که گونه‌ای از نفوذ به داده‌ها و یا سامانه‌های رایانه‌ای/ مخابراتی است. پس، درصورتی که شخصی به رایانهٔ دیگری نفوذ کند و سپس با استفاده از تلفن همراه خود به عکس‌برداری از اطلاعات موردنظر مبادرت ورزد و یا خلاصه‌ای از آنها را به ذهن بسپارد، مرتکب سرقت رایانه‌ای نشده، چراکه ربایش به‌صورت بُریدن یا رونوشت گرفتن که تنها در فضای رایانه‌ای متصور است، اساساً انجام نگرفته است. در این فرض، عمل ارتکابی با لحاظ سایر مقتضیات، ازجمله این‌که داده‌ها یا سامانهٔ رایانه‌ای مربوط به تدابیر امنیتی حفاظت‌شده باشد، زیر عنوان مجرمانهٔ «دسترسی غیرمجاز»[1] در چارچوب مادهٔ اخیر تعقیب‌شدنی است.

در نظام انگلستان و وِیلز، به‌رغم اینکه جرمِ دسترسی غیرمجاز به داده‌های رایانه‌ای به‌موجب مادهٔ ۱ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰، در تداولِ عام، ورود غیرمجاز به سامانهٔ رایانه‌ای[2] توصیف می‌شود (Marion & Twede, 2020: 205-209)، لزومِ «دسترسی غیرمجاز» در آن بسیار گسترده‌تر از ورود غیرمجاز است و هرگونه فعالیتی غیر از صرف خواندن اطلاعات روی صفحهٔ نمایش را دربر می‌گیرد. جرم یادشده حتی شامل دسترسی به محتویاتِ ابزارهای ذخیره‌سازیِ حمل‌کردنی[3] از قبیل دیسک‌ها[4] و کارت‌های حافظه[5] نیز می‌شود، مشروط بر اینکه چنین دسترسی در حالی انجام شده باشد که ابزارهای پیش‌گفته در رایانه قرار گرفته باشند (Rowland et. al., 2017: 288 & 289). با وجود این، هرگاه محتوای داده‌های رایانه‌ای از سوی کاربر مُجازی[6] پرینت گرفته شود و سپس، شخص دیگری مبادرت به خواندن غیرمجاز[7] آنها کند، بار دیگر عمل ارتکابی در چارچوب قانون موردبحث قرار نمی‌گیرد (Rowland & Macdonald, 2000: 466).

باید افزود، مطابق قسمت «الف» بند نخست مادهٔ ۱ قانون بالا، دسترسی غیرمجاز به داده‌های رایانه‌ای زمانی ارتکاب می‌یابد که شخص با قصد تأمین دسترسی به داده‌ها یا برنامه‌های رایانه‌ای موجب شود که رایانه هرگونه عملیاتی[8] را اجرا کند، مانند اینکه اقدام به روشن کردن رایانه نماید. مفاد مادهٔ پیش‌گفته حاکی از آن است که هرگاه مرتکب تلاش کند که به‌طور غیرمجاز وارد رایانه‌ای شود، اما موفق نشود، همچنان ممکن است به سبب جرم موردبحث تعقیب کیفری شود. از این گذشته، تأمین

1. Unauthorised access
2. Proscribing hacking
3. Portable storage devices
4. Disks
5. Memory sticks
6. An authorised user
7. Unauthorised reading
8. Any function

دسترسی به‌طور موسعی تعریف می‌شود، به‌طوری‌که دربرگیرندهٔ هر عملی است که موجب اجرای عملیاتی به‌وسیلهٔ رایانه شود. نمونه‌هایی از چنین عملیاتی عبارت‌اند از: تغییر یا حذف برنامه یا دادهٔ رایانه‌ای، رونوشت گرفتن یا انتقال هریک از آنها به فضای دیگری در وسیلهٔ ذخیره‌سازی که در آن نگه‌داری می‌شوند، استفاده از برنامه یا دادهٔ رایانه‌ای و یا داشتن برون‌دادِ هریک از آنها از رایانه‌ای که در آن ذخیره شده‌اند (Bainbridge, 2008: 441). پس، با توجه به اینکه رونوشت گرفتن در مفهومِ تأمین دسترسی می‌گنجد، رونوشت گرفتنِ غیرمجاز از برنامه یا دادهٔ رایانه‌ای و یا دانلود رونوشت غیرمجاز از برنامه یا دادهٔ رایانه‌ای ممکن است طبق مادهٔ ۱ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰ جرم تلقی شود.

در مقابل، در ایران، چنانچه کسی به‌جای ارتکاب یکی از رفتارهای بُرش یا رونوشت گرفتن، دست به ربایش در مفهوم سنتی آن بزند، مانند اینکه به برداشتن و جابه‌جایی رایانهٔ دستی و یا ابزار حامل دادهٔ متعلق به دیگری اقدام کند، هرچند تجهیزات رایانه‌ای اخیر ممکن است حاوی اطلاعات زیادی باشند، سرقت رایانه‌ای رخ نداده، بلکه سرقت در مفهوم سنتی آن روی داده است و در نتیجه، باید با لحاظ مقررات مربوط به سرقت‌های غیررایانه‌ای مورد حکم قرار گیرد. البته، احتمال دارد که ربایش داده‌های رایانه‌ای توأم با ربودن سامانهٔ رایانه‌ای یا ابزار حامل داده باشد؛ برای مثال، مرتکب نخست، داده‌هایی را که روی دیسک سختِ داخلی نصب و در رایانهٔ دیگری ذخیره شده است، از طریق بُرش برمی‌دارد و پس از آن، دیسک یادشده را نیز از رایانه جدا کرده، می‌رباید. در چنین مواردی، حکم قضیه باید مطابق با قواعد تعدد جرم صادر شود، ولی پرسشی که مطرح می‌شود، این است که آیا ضوابط تعدد رفتاری باید جاری شود یا تعدد عنوانی؟ در پاسخ باید گفت، هرچند اصطلاح «ربایش» در خصوص هم سرقت رایانه‌ای و هم سرقت سنتی به‌کار می‌رود، ربودن رایانه‌ای در عمل با رفتارهایی انجام می‌گیرد که اساساً در ربایش سنتی مصداق پیدا نمی‌کند. پس، هرگاه قرار باشد که ربایش در مفهوم رایانه‌ای و سنتی توأمان ارتکاب یابد، ناگزیر رفتارهای متعدد (و نه واحدی) رخ می‌دهد و در این صورت، اِعمال ضوابط «تعدد رفتاری» مندرج در مادهٔ ۱۳۴ قانون مجازات اسلامی ۱۳۹۲ (اصلاحی ۱۳۹۹) لازم می‌آید.

باید یادآور شد که ربایش به‌صورت بُریدن یا رونوشت گرفتن از داده‌های رایانه‌ای مستلزم دسترسی به داده‌های یادشده است، ولی این دسترسی حتی اگر تمامی مقتضیات جرمِ دسترسی غیرمجاز طبق مادهٔ ۷۲۹ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) را داشته باشد، اصولاً به‌مثابه «جرم مقدمه‌ای» خواهد بود و لذا مرتکب فقط به سبب سرقت رایانه‌ای تعقیب و محاکمه می‌شود. استثنای این وضعیت در مواردی صدق می‌کند که شخص عنصر مادی و عنصر روانیِ هر دو جرم یادشده را به‌طور مستقل دارا باشد. در شرایطی هم که مرتکب بعد از دسترسی غیرمجاز به داده‌های رایانه‌ای متعلق به دیگری و قبل از اتمام سرقت رایانه‌ای دستگیر شود، درصورتی که مقتضیات جرمِ دسترسی غیرمجاز به اثبات برسد، تنها امکان محاکمهٔ او به علت همین جرم وجود دارد.

در واقع، در فرض اخیر، گرچه شخص در مرحلهٔ شروع به جرم قرار دارد، با توجه به اینکه مجازات سرقت رایانه‌ای با ملاک قرار دادن کیفر حبسْ «تعزیر درجهٔ شش» است و مادهٔ ۱۲۲ قانون مجازات اسلامی ۱۳۹۲ (اصلاحی ۱۳۹۹) شروع به جرایمی را که مجازات قانونی آنها «حبس تعزیری درجهٔ یک تا پنج» باشد، جرم‌انگاری کرده است، اصل قانونی بودن جرم و مجازات[1] اقتضا دارد که شروع به سرقت رایانه‌ای تعقیب‌شدنی نباشد.

در انگلستان و وِیلز، به‌موجب مادهٔ ۲ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰، «دسترسی غیرمجاز با قصد ارتکاب یا تسهیل ارتکاب جرایم دیگر»[2] نیز به‌طور خاص جرم‌انگاری شده است. این جرم در مواردی رخ می‌دهد که کسی با ورود غیرمجاز به سامانهٔ رایانه‌ای[3] متعلق به غیر، قصد ارتکاب جرم دیگری مانند سرقت، اخاذی و کلاهبرداری را داشته یا قصد کرده باشد که ارتکاب چنین جرمی را از طریق خودش یا دیگری تسهیل کند. در این خصوص، طبق بند سوم مادهٔ یادشده، اهمیتی ندارد که جرمِ دیگر قرار باشد که در همان رویدادِ دسترسی غیرمجاز ارتکاب یابد یا در واقعهٔ دیگری در آینده. فراتر از این، حتی اگر وقایع آن‌چنان باشد که ارتکاب جرمِ دیگر مُحال[4] باشد، همچنان مرتکب ممکن است به دلیل جرم یادشده محکوم شود[5]. نمونه‌ای از این وضعیت اخیر در شرایطی صدق می‌کند که مرتکب قصد داشته باشد جزئیاتِ بدهی خود را پاک کند، درحالی‌که شخصی که به او بدهکار است، پیش‌تر دِین را سوخته تلقی نموده یا اینکه مرتکب اساساً دربارهٔ داشتن بدهی اشتباه کرده باشد.

۳. ۲. شرایط پیرامونی

در حقوق کیفری ایران، تحقق عنصر مادی جرایمِ سرقت رایانه‌ای/ دسترسی غیرمجاز مستلزم آن است که حسب مورد شرایط پیرامونی زیر، رفتار مجرمانه به شرح پیش‌گفته را احاطه کند:

- موضوع جرم باید حسب مورد داده‌های متعلق به دیگری و یا داده‌ها یا سامانه‌های رایانه‌ای/ مخابراتی باشد؛
- رفتار مرتکب به‌طور غیرمجاز انجام گرفته باشد؛
- داده‌ها یا سامانه‌های رایانه‌ای به‌وسیلهٔ تدابیر امنیتی حفاظت شده باشند.

در مورد شرط اول باید یادآور شد که در سرقت رایانه‌ای، آنچه ربایش نسبت به آن انجام می‌گیرد،

1. Computer Misuse Act 1990
2. Unauthorised access with intent to commit or facilitate commission of further offences
3. Computer system
4. Impossible
5. See: s 2 (4) of the Computer Missuse Act 1990

باید «داده» بوده و داده‌های موردنظر لازم است متعلق به دیگری باشد. «داده‌ها»[1] به معنای هر شکل از اطلاعات[2] هستند که برنامه‌های رایانه‌ای روی آنها پردازش می‌کنند (Butterfield & Ekembe Ngondi, 2016: 610). در این مفهوم، ممکن است داده‌ها یک فایل متنی، صوتی، تصویری و یا ترکیبی از آنها باشند. پس، اگر کسی برخی کتاب‌های الکترونیکی متعلق به غیر را که در تَبلت او ذخیره شده است، از طریق بُرش آنها برباید؛ دانشجویی از فایل‌های صوتیِ هم‌کلاسی خود که در کلاس‌های درسی ضبط و روی رایانهٔ دستی‌اش منتقل کرده است، رونوشت بگیرد؛ شخصی تعدادی از فیلم‌های سینمایی یک ویدئوکلوب را از آرشیو موجود در رایانهٔ رومیزی آن به‌واسطهٔ بُرش برباید؛ فردی از برخی عکس‌ها که دیگری در تلفن همراه خودش دارد، رونوشت بردارد، دست به ربایش داده‌ها زده است. اما موضوع جرم در «دسترسی غیرمجاز» ممکن است شامل سامانه‌های رایانه‌ای یا مخابراتی شود. سامانهٔ رایانه‌ای عبارت است از مجموعه‌ای از نرم‌افزارها و سخت‌افزارهای مرتبط که از طریق یک شبکهٔ رایانه‌ای جهت اجرای فرایندهای کار مشخصی به یکدیگر متصل باشند (S 1 (B) of the Regulations on How to Use Computer or Telecommunications Systems 2016)؛ و سامانهٔ مخابراتی شامل هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکیِ اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارسازِ نوری از طریق یک یا چند مسیر ارتباطی به‌وسیلهٔ قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد، می‌شود (S 1 (C) of the Regulations on How to Use Computer or Telecommunications Systems 2016).

افزون بر این، اطلاق واژهٔ «داده‌ها» حاکی از آن است که داده‌های ربوده‌شده، هم شامل داده‌هایی که ارزش مالی دارند، از قبیل برخی مقاله‌های علمی که با پرداخت وجه خریداری شده‌اند و هم داده‌هایی که ارزش مالی ندارند، مانند فیلم‌های مستهجن، می‌شود. با وجود این، هرگاه ضابطهٔ اصلی برای تشخیص ارزش مالی چیزی، معیار شرعی باشد، حداقل باید پذیرفت که اگر صاحب داده‌هایی که از لحاظ شرعی مالیت ندارند، مسلمان باشد، ربایش آنها از سوی دیگری زیر عنوان سرقت رایانه‌ای تعقیب‌شدنی نیست[3]؛ چراکه حمایت کیفری قانون‌گذار ایرانی از داده‌هایی که مطابق با موازین شرعی مالیت ندارند، امری لغو است و موجب ترغیب اشخاص به حفظ و نگه‌داری چنین داده‌هایی در پرتو ضمانت اجرای کیفری برای سرقت آنها می‌شود. آری، چنانچه صاحب داده‌های یادشده نامسلمان باشد، با درنظر گرفتن عرف نامسلمانان، ممکن است بتوان قائل به این شد که ربایش آنها زیر عنوان سرقت تعزیری، تعقیب‌شدنی است.

---

1. Data
2. Information
۳. برای ملاحظهٔ نظرگاهی که تمامی داده‌های رایانه‌ای را به‌طور مطلق مشمول مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) قلمداد می‌کند، See: Aalipour, 2015: 257 & 258; Heydari, 2016: 101.

در هر حال، ربودن داده‌ها تنها زمانی موجب تحقق سرقت رایانه‌ای می‌شود که داده‌های موردنظر «متعلق به دیگری» باشد. بنابراین، هرگاه کسی از داده‌های رایانه‌ای متعلق به خودش که با تجویز همکارش روی رایانهٔ دستی او ذخیره کرده است، رونوشت بگیرد یا شخصی بعضی از فایل‌های خود را که مربوط به آموزش زبان انگلیسی است و به دیگری برای استفادهٔ موقت داده است، از طریق بُرش برباید، مرتکب سرقت رایانه‌ای نشده، زیراکه آن داده‌ها متعلق به خودش بوده است. باید درنظر داشت که تعلق داده‌ها به شخص زمانی معنا دارد که آنها در فضای مناسب جهت حفظ و نگه‌داری قرار داده شده باشد، لذا اگر کسی داده‌هایش را در وب‌سایت اینترنتی بارگذاری کند، به‌طوری که در دسترس همگان قرار گیرد، حتی اگر فایل‌های اشتباهی‌ای را در وب‌سایت قرار داده باشد، دریافت آن از سوی بازدیدکنندهٔ آن وب‌سایت اینترنتی، سرقت رایانه‌ای نیست.

ناگفته نماند که صاحب داده‌ها لازم نیست پدیدآورندهٔ آنها باشد، چراکه شرط تعلق به دیگری اعم از این است که دارندهٔ داده‌ها خودش آنها را پدید آورده یا به‌صورت قانونی مثلاً از راه خرید به‌دست آورده باشد. البته ربایش داده‌هایی که دارنده خود آنها را پدید آورده است، احتمال دارد که به نقض حقِ دارنده منتهی شود، و در نتیجه، با عنوان مجرمانهٔ دیگری نیز تطبیق پیدا کند. برای مثال، حق نشر، عرضه، اجرا و حق بهره‌برداری مادی و معنوی از نرم‌افزار رایانه‌ای، متعلق به پدیدآورندهٔ آن است و با وجود شرایطی ممکن است نرم‌افزار به‌عنوان اختراع تشخیص داده شود[1]. در این خصوص، هر کس حق‌های یادشده را نقض کند، افزون بر جبران خسارت، مستحق کیفر نیز شناخته می‌شود[2]؛ مشروط به اینکه انحصار بهره‌برداری از نرم‌افزار رایانه‌ای متعلق به پدیدآورنده باشد؛ امری که مستلزم ثبت نرم‌افزار در شورای عالی انفورماتیکِ وزارت فرهنگ و ارشاد اسلامی و یا مرجع ثبت شرکت‌ها دانسته شده است (See: Decision No. 9109970907900376 dated 3/10/1391, Branch 19 of the Supreme Court).

بر این اساس، در مواردی که شخصی دست به ربودن نرم‌افزاری از روی رایانهٔ دیگری می‌زند که دارندهٔ آن پدیدآورندهٔ نرم‌افزار موردنظر است و سپس مبادرت به نشر، عرضه، اجرا و یا نوعی بهره‌برداری مادی یا معنوی از آن می‌کند، با توجه به انجام این رفتارهای متعدد (و نه واحدی)، قاضی دادگاه باید مطابق با ضوابط «تعدد رفتاری» حکم صادر نماید.

---

1. See: ss 1 & 2 of the Protection of the Rights of Computer Software Creators Act 2000

۲. مادهٔ ۱۳ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای ۱۳۷۹ (اصلاحی ۱۴۰۳) اِعلام می‌دارد: «هر کس حقوق مورد حمایتِ این قانون را نقض نماید، علاوه بر جبران خسارت، به حبس از نود و یک روز تا شش ماه و جزای نقدی از سیصد و سی میلیون (۳۳۰/۰۰۰/۰۰۰) تا ششصد و شش میلیون (۶۶۰/۰۰۰/۰۰۰) ریال محکوم می‌گردد». همچنین، ر.ک. تصویب‌نامهٔ شمارهٔ ۵۶۲۶۱/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 ۱۷

در حقوق مالکیت فکریِ انگلستان و ویلز[1]، از یک طرف، برنامه‌های رایانه‌ای یا داده‌های اولیهٔ طراحیِ برنامهٔ رایانه‌ای، از قبیل روندنماها[2]، به‌موجب قسمت «ب» بند نخست مادهٔ ۳ قانون حقوق انحصاری آثار، طرح‌ها و اختراع‌های ثبت‌شده مصوب ۱۹۸۸[3] به‌عنوان اثر ادبی[4] برشمرده شده‌اند، و از طرف دیگر، اَعمالی مانند فروش، اجاره و توزیعِ آثار ادبی که با نقض حقوق انحصاری‌شان از آنها رونوشت گرفته شده، طبق مادهٔ ۱۰۷ همان قانون، مستوجب مسئولیت کیفری دانسته شده است. پس، هرگاه شخصی بدون مجوزِ صاحب حقوق انحصاریِ یک برنامهٔ رایانه‌ای، از آن رونوشت بگیرد و سپس به یکی از اَعمال یادشده مبادرت کند، مطابق مادهٔ ۱۷ قانون پیش‌گفته مرتکبِ «نقض حقوق انحصاری به‌وسیلهٔ رونوشت گرفتن»[5] شده است و به سبب اَعمالی که بعدها روی آن انجام می‌دهد، مسئولیت کیفری خواهد داشت[6].

در خصوص شرط دوم باید درنظر داشت که عبارتِ «به‌طور غیرمجاز» در قسمت ابتدایی مواد ۷۲۹ و ۷۴۰ از قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) حکایت از این دارد که ربودن داده‌های متعلق به دیگری، یا دسترسی به داده‌ها یا سامانه‌های رایانه‌ای، در صورتی ممکن است عنصر مادی جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز را تحقق بخشد که عملِ مرتکب «غیرمجاز»[7] باشد. اصطلاح اخیر ناظر بر رفتاری دانسته شده است که از سوی مالک یا اداره‌کننده تأیید نگردیده یا مجاز شمرده نشده باشد (Gattiker, 2004: 340). از این رو، هرگاه مرتکب رضایتِ صاحب داده‌ها یا مجوز قانونی برای بُریدن یا رونوشت گرفتن از داده‌ها را نداشته باشد، به‌طور غیرمجاز اقدام کرده است.

در مقابل، هرگاه شخصی به دیگری اجازه بدهد که به داده‌های متعلق به او از قبیل برخی تصویرها که برای امور گرافیکی استفاده می‌شوند، دسترسی پیدا کند یا آنها را به‌واسطهٔ بُرش به ابزار حامل دادهٔ خود منتقل نماید، گرچه دسترسی به داده‌های متعلق به غیر یا ربایش آن ارتکاب یافته است، با توجه به اینکه صاحب داده‌ها عملِ رونوشت را تجویز کرده، رفتار مرتکب به‌صورت غیرمجاز انجام نشده است و لذا شرط موردبحث احراز نمی‌شود. به همین ترتیب، اگر مقام قضایی در شرایطی که ظنّ قوی به کشف جرم، شناسایی متهم و یا ادلهٔ جرم وجود دارد، دستور تفتیش و توقیف داده‌ها را بدهد (See: s 671 of the Criminal Procedure Code 2013)، درصورتی‌که ضابطان قضایی نسبت به دستیابی به داده‌ها و

1. English and Welsh intellectual property law
2. Flow-charts
3. Copyright, Designs and Patents Act 1988
4. Literary work
5. Infringement of copyright by copying
6. For further reading, See: ss 107 to 110 of the Copyright, Designs and Patents Act 1988 (Also, Davis, 2012: 71-76, and Bainbridge, 2009: 239-296).
7. Unauthorised

گرفتن رونوشت از آنها اقدام کنند (See ss 674 & 675 of the Criminal Procedure Code 2013) یا اصل داده‌ها را توقیف نمایند (See s 680 of the Criminal Procedure Code 2013)، ازآنجا که عمل ارتکابی با مجوز مقام قضایی است، غیرمجاز به‌شمار نمی‌آید.

در حقوق کیفری انگلستان و وِیلز، قسمت «ب» بند نخست مادهٔ ١ قانون سوءاستفادهٔ رایانه‌ای ١٩٩٠، تأکید می‌کند که دسترسی‌ای که شخص قصد تأمین یا میسر ساختن تأمین آن را دارد، باید «غیرمجاز» باشد. در این نظام کیفری و همچنین در نظام حقوقی اسکاتلند، اصطلاحِ اخیر در خصوص جرایمی که مستلزم دسترسی غیرمجازند[1]، به این معنا آمده است که شخص یا اشخاصی که حق کنترلِ دسترسی به داده‌های موردنظر را دارند، رضایت یا اجازهٔ استفاده از اطلاعات یا بخشی از آنها را به دیگری نداده باشند[2]. در این راستا، بند ٥ مادهٔ ١٧ قانون سوءاستفادهٔ رایانه‌ای ١٩٩٠، در تفسیر اصطلاح یادشده اِشعار می‌دارد که هر نوع دسترسیِ شخص به هر برنامه یا دادهٔ ذخیره‌شده در رایانه، درصورتی که وی خودش حق هرگونه کنترلِ دسترسی نسبت به برنامه یا دادهٔ موردنظر را نداشته باشد، غیرمجاز محسوب می‌شود (قسمت «الف» بند پیش‌گفته)؛ و از رضایت هر شخصی که به این صورت حق داشته باشد، برای هر نوع دسترسی به برنامه یا دادهٔ مربوط برخوردار نباشد (قسمت «ب» بند یادشده).

باید توجه داشت که در بسیاری از موارد، شخصی که حق کنترل دسترسی را دارد، صاحب خودِ سامانهٔ رایانه‌ای است، ولی در موارد دیگر سامانهٔ رایانه‌ای ممکن است به‌عنوان میزبان[3] خدمت کند و فضای ذخیره‌سازی[4] و امکاناتِ دسترسی به برنامه‌ها یا داده‌های رایانه‌ای[5] را که از سوی طرف‌های دیگری کنترل می‌شوند، در اختیار بگذارد. در این موقعیت، این مسئله که چه کسی حق رضایت دادن به دسترسی را دارد، چه‌بسا پیچیده‌تر باشد. بیشتر سامانه‌های رایانه‌ایِ دانشگاهی[6] نمونه‌هایی از چنین وضعیتی را به‌دست می‌دهند. در این موارد، این واقعیت که حق‌های دسترسی به دانشجو داده می‌شود، موجب نمی‌شود که وی حق انتقال دسترسی به شخص ثالث را داشته باشد (Lloyd, 2011: 227).

در برخی موارد، شخص احتمال دارد که از رایانه‌ای استفاده کند که شخص دیگری پیش‌تر وارد سیستم آن شده، ولی فراموش کرده است که از آن خارج شود؛ در این صورت، حتی اگر داده‌های مورد دسترسی از مواردی باشند که در ارتباط‌های اینترنتی به‌طور رایگان در دسترسِ عموم قرار دارند، مرتکب ممکن است به سبب جرمِ دسترسی غیرمجاز به داده‌های رایانه‌ای محکوم شود. در *پروندهٔ الیس علیه*

1. Offences of unauthorised access
2. See: s 17 (5) of the Computer Misuse Act 1990 and Clause 1 (3) of the Computer Crime (Scotland) Bill
3. Host
4. Storage space
5. Access facilities for programs or data
6. University computer systems

دادستان [۲۰۰۱][1]، اِلیس، دانشجوی سابقِ دانشگاه نیوکاسل و عضو انجمن دانش‌آموختگان دانشگاه، از رایانه‌ها با دسترسی غیرعمومی[2] در دانشگاه استفاده کرد تا در وب‌سایت‌هایی گشت‌زنی کند. رایانهٔ موردنظر از سوی کاربر پیشین به‌صورت وارد سیستم‌شده[3] رها شده بود. مأمور اداری به اِلیس اظهار داشت که اجازهٔ استفاده از رایانه‌ها با دسترسی غیرعمومی را ندارد و اِلیس در بازجویی به‌وسیلهٔ مأمور پلیس بیان داشت که از این رایانه‌ها استفاده کرده و رمز عبور برای استفاده از آنها نداشته است. همچنین وی به استفاده از رایانه‌ای که به‌صورتِ وارد سیستم‌شده رها شده بود، برای دسترسی به وب‌سایت‌ها اعتراف کرد. دادگاه صلح[4] اِلیس را به سه فقره دسترسی غیرمجاز به داده‌های رایانه‌ای طبق مادهٔ ۱ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰محکوم نمود و محکومیت او در دادگاه‌های بالاتر نیز تأیید شد.

دربارهٔ شرط سوم باید دانست که در جرم دسترسی غیرمجاز در چارچوب مادهٔ ۷۲۹ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، داده‌ها یا سامانه‌های رایانه‌ای که دسترسی غیرمجاز نسبت به آنها صورت می‌گیرد، باید با تدابیر امنیتی حفاظت شده باشند. مُراد از تدابیر امنیتی، هرگونه محدودیت فنی (سخت‌افزاری یا نرم‌افزاری) برای مصون ماندن از دسترسی سایر اشخاص است. بارزترین نمونهٔ این محدودیت‌ها، ایجاد گذرواژه یا دیوارهٔ آتش (فایروال) و یا موارد دیگرِ اعتبارسنجی جهت ورود یک کاربر به سامانه و دسترسی او به داده‌های موجود در آن است (Mansourabadi & Mansourabadi, 2024: 43). از این رو، هرگاه شخصی با ورود به رایانهٔ دیگری که هیچ تدبیر امنیتی ندارد، به داده‌های آن دسترسی پیدا کند، از شمول مادهٔ یادشده خارج است؛ با وجود این، در مواردی که مرتکب بعد از آن دست به ربایش داده‌های موردنظر بزند، به دلیل سرقت رایانه‌ای تعقیب و محاکمه خواهد شد.

۳. ۳. نتیجه

در نظام حقوقی ایران، سرقت رایانه‌ای «جرمی مقید» است. اما باید توجه داشت که نتیجه در سرقت رایانه‌ای، برحسب اینکه ربایش به‌صورت بُریدن انجام شود یا رونوشت گرفتن، متفاوت است. توضیح بیشتر اینکه هرگاه مرتکب دست به ربایش داده‌های متعلق به غیر از طریق بُرش بزند، در جریان طبیعی امور صاحب داده‌ها از عین آنها محروم می‌شود. اما درصورتی که سارق مرتکب ربودن داده‌های دیگری به‌واسطهٔ رونوشت گرفتن از آنها شود، صاحب داده‌ها از رونوشت داده‌ها محروم می‌شود؛ پس «محروم شدن صاحب داده‌ها از عین یا رونوشت آنها» به‌عنوان نتیجه در سرقت رایانه‌ای لحاظ می‌شود. تفکیک

1. *Ellis v DPP* [2001] EWHC 362 (Admin)
2. Non-open access computers
3. Logged on
4. Magistrates' Court

قانون‌گذار بین وضعیتی که «عین داده‌ها در اختیار صاحب آن باشد» و «در غیر این صورت» در مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) به‌نوعی اشاره به همین مطلب دارد.

در واقع، استفاده از عبارت‌های اخیر حکایت از دو مطلب دارد: از یک سو، چگونگی ارتکاب ربایش داده‌ها را تبیین کرده که حسب مورد با جابه‌جایی عین داده‌ها (بُریدن) یا بدون جابه‌جایی آنها (رونوشت گرفتن) امکان‌پذیر است و از سوی دیگر، تأثیر گونه‌های رفتاریِ موردنظر بیان شده است که حسب مورد سبب محرومیت صاحب داده‌ها از عین یا رونوشت آنها می‌شود. البته، چنین محرومیتی لازم نیست دائمی یا همراه با نفع‌رسانی به مرتکب باشد؛ از این رو، هرگاه مرتکب پس از بُریدن یا رونوشت گرفتن از داده‌های متعلق به غیر و انتقال آنها به رایانهٔ رومیزی که در محل سکونتش دارد، بی‌درنگ از سوی مأموران پلیس دستگیر شود، درحالی که تنها ساعتی از اتمام سرقت سپری شده و هیچ بهره‌ای از داده‌ها نبُرده باشد، همچنان مسئولیت کیفری‌اش به سبب جرم تامِ سرقت رایانه‌ای پابرجا است.

بنابراین، نویسندهٔ حاضر با این دیدگاه موافق نیست که سرقت رایانه‌ای جرمی است که نتیجهٔ آن ربوده شدن به‌محض ربودن است؛ محروم شدن دارنده یا بهره‌مند شدنِ رباینده نتیجه نیست، بلکه اثر نتیجه است، زیرا اگر نتیجه بود، بر پایهٔ اصل قانونی بودن باید به‌عنوان یکی از پاره‌های عنصر مادی به آن اشاره می‌شد (Aalipour, 2015: 258). دلایل تردید در پذیرش این نقطه‌نظر از قرار زیر است:

اول، درنظر گرفتن «ربودن شدن» به‌عنوان نتیجهٔ سرقت رایانه‌ای تأکیدی دوباره بر همان رفتار مجرمانهٔ ربودن با عبارتِ تا اندازه‌ای متفاوت است و توسل به چنین رویکردی در خصوص جرایم دیگری که وضعیت کمابیش مشابهی دارند، به برداشت‌های نامعقولی منجر خواهد شد. برای نمونه، در جرم ایراد ضرب که در زمرهٔ جرایم مقید است، هرگاه اظهار شود که نتیجهٔ آن مضروب شدن جرم‌دیده است، تأکیدی دوباره بر عمل مجرمانه‌ای شده است که زیر عنوان ایراد ضرب از آن یاد می‌شود؛ بدون اینکه از نتیجه در این جرم صحبتی شده باشد. این درحالی است که تردیدی وجود ندارد که نتیجه در جرمِ ایراد ضرب در واقع، برخی صدمه‌ها نظیر تغییر رنگ پوست و تورم، بدون خون‌ریزی است.

دوم، نتیجه اثری است که به‌طور مستقیم از رفتار مجرمانه حاصل می‌شود. چنین اثری در اصل باید از سوی قانون‌گذار تصریح گردد، ولی برخی جرایم وجود دارند که هرچند از نتیجهٔ حاصله در عنصر قانونی‌شان سخنی گفته نشده است، از لحاظ مفهومی یا در جریان طبیعی امور تنها زمانی تصورپذیر هستند که رفتار مجرمانهٔ آنها به نتیجهٔ معینی منتهی شود. دلیل این نظرگاه آن است که جرایم از امور اعتباریِ صرف نیستند، بلکه از اموری‌اند که در عالم خارج تحقق می‌یابند و لذا توجه به واقعیت‌های امور در آنها ضروری است.

برای مثال، جرم ایراد جراحت[1] در مواردی تحقق می‌یابد که رفتار مجرمانهٔ موردنظر مثلاً چاقو زدن به عضوی از اعضای بدنِ دیگری سبب ازهم‌گسیختگی لایه‌های درونی و بیرونیِ پوست و جاری شدن خون او شود (E'temadi, 2016: 77). به‌رغم اینکه قانون‌گذار به چنین نتیجه‌ای تصریح نکرده است، از لحاظ مفهومی شکی نیست که ایراد جراحت تنها با حصول نتیجهٔ یادشده تحقق می‌یابد و صدمه‌های کمتر کافی نیستند. در میان جرایم مالی هم اختلاس جرمی است که در جریان طبیعی امور لازم است به نتیجهٔ معینی منجر شود، وگرنه تحقق عنصر مادی آن معنا پیدا نمی‌کند. در جرم اخیر، زمانی می‌توان گفت عنصر مادی آن کامل شده است که برداشت و تصاحب به نفع خود یا دیگری (به‌مثابه رفتار مجرمانه) باعث محروم شدنِ هرچند موقتِ حکومت از مال یا نوشتهٔ امانی (نتیجه) گردد، درحالی که قانون‌گذار به چنین اثری اشاره نکرده است (E'temadi (A), 2022: 426).

به‌طور مشابه، این نظرگاه که نتیجه در سرقت رایانه‌ای تصاحب داده‌ها است و لذا عمل ربایش باید به بُردن (تصاحب من غیر حق داده‌ها) منجر شود، ممکن است در معرض انتقاد قرار گیرد (Mohammad Nasl, 2012: 103)؛ زیراکه تصاحب نوعی رفتار را به ذهن متبادر می‌کند که با توجه به مفهوم عامی که دارد، ممکن است از طریق ربایش نیز انجام گیرد. به عبارت دیگر، زمانی که شخص اقدام به ربودن داده‌های متعلق به غیر می‌کند، با توجه به اینکه حق‌های صاحب داده‌ها را برای خودش فرض نموده، به‌نوعی مبادرت به تصاحب آنها نیز کرده است. از این رو، تفکیک بین ربایش به‌منزلهٔ رفتار مجرمانه از یک سو و تصاحب به‌مثابه نتیجه از سوی دیگر، پذیرفتنی نیست. ضمن اینکه اصطلاح «بُردن» مترادف با تصاحب نیست که به‌جای یکدیگر استفاده شوند؛ گرچه تصاحبِ چیزی ممکن است به‌واسطهٔ بُردن آن انجام گیرد.

بر این اساس، باید پذیرفت که اثر ربایش داده‌های متعلق به دیگری، همانا محروم شدن صاحب داده‌ها از عین یا رونوشت آنهاست. پس، اگر کسی با نفوذ به رایانهٔ رومیزیِ دیگری، بُرش داده‌ها و انتقال آنها به ابزار حامل داده‌اش را آغاز کند و درست در همین لحظه صاحب داده‌ها یا پلیس از راه برسد و مانع ادامهٔ عملیات از جانب مرتکب شود، یا قطع برق باعث ناکامی شخص در عمل ربایش گردد، عنصر مادی سرقت رایانه‌ای هنوز کامل نشده است و مرتکب در مرحلهٔ شروع به جرم قرار دارد. در مقابل، هرگاه عملیات بُریدن و انتقال داده‌ها به پایان برسد، عنصر مادی جرمِ موردبحث کامل می‌شود و صرف اینکه داده‌های موردنظر با نرم‌افزارهای ویژهٔ بازیابی اطلاعات ممکن است دوباره در اختیار صاحب آنها قرار گیرد، در تحقق سرقت رایانه‌ای که پیش‌تر واقع شده است، تأثیری ندارد. در این موارد، بازیابی داده‌ها به‌وسیلهٔ نرم‌افزارْ کارکردی مشابه با بیمهٔ سرقت از منازل مسکونی دارد که مال‌باخته با دریافت غرامت از شرکت بیمه می‌تواند دوباره اموالش را به‌دست آورد.

---

1. Wounding

در نظام حقوقی انگلستان و وِیلز، اگرچه جرمِ دسترسی غیرمجاز به داده‌های رایانه‌ای برطبق مادهٔ ١ قانون سوءاستفادهٔ رایانه‌ای ١٩٩٠، دربرگیرندهٔ هر عملی است که موجب اجرای عملیاتی به‌وسیلهٔ رایانه شود، ضرورتی ندارد که نتیجهٔ خاصی بر اثر آن پدید آید. بنابراین، جرم یادشده در زمرهٔ «جرایم مطلق» قرار می‌گیرد؛ به‌ویژه از آن رو که تحقق عملیِ دسترسی به داده‌ها یا برنامه‌های رایانه‌ای ضروری نیست. به‌طور مشابه در حقوق ایران، دسترسی غیرمجاز در چارچوب مادهٔ ٧٢٩ قانون تعزیرات ١٣٧٥ (الحاقی ١٣٨٨)، جرمی مطلق است؛ چراکه عنصر مادی آن با صرف دسترسی به داده‌ها یا سامانه‌های رایانه‌ای به‌طور غیرمجاز، به علت نقض محرمانگی داده‌ها یا سامانه‌ها تحقق می‌یابد و تحقق نتیجهٔ خاصی مانند تسلط بر داده‌های رایانه‌ای ضرورت ندارد.

۴. عنصر روانی سرقت رایانه‌ای/ دسترسی غیرمجاز به داده‌های رایانه‌ای

در حقوق کیفری ایران، در مواد ٧٢٩ و ٧۴٠ قانون تعزیرات ١٣٧٥ (الحاقی ١٣٨٨) از واژه‌هایی نظیر عالماً، عامداً و مشابه آن استفاده نشده است، ولی با توجه به «اصل عمدی بودن جرایم»، جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز در زمرهٔ جرایم عمدی قرار می‌گیرد. بر این اساس، به‌موجب بخش نخست مادهٔ ١۴۴ قانون مجازات اسلامی ١٣٩٢ که در تحقق جرایم عمدی، احراز «علم مرتکب به موضوع جرم» و «قصد او در ارتکاب رفتار مجرمانه» را ضروری می‌داند- اجزایی که روی‌هم‌رفته زیر عنوان «قصد عام» از آنها یاد می‌شود- باید دانست که برای تحقق عنصر روانیِ جرایم موردبحث، لازم است ثابت شود که مرتکب حسب مورد نسبت به تعلق داده‌ها یا سامانه‌های رایانه‌ای/ مخابراتی به شخص دیگر عالم بوده و در ارتکاب ربایش، خواه به‌صورت بُرش و خواه به‌واسطهٔ رونوشت گرفتن و یا ارتکاب دسترسی، تعمد داشته است.

بنابراین، چنانچه دانشجویی در زمان رونوشت گرفتن از داده‌های متعلق به خودش که در رایانهٔ دستی‌ای ذخیره کرده و از سوی دانشگاه محل تحصیل او در اختیار وی و یکی دو نفر از دانشجویان دیگر برای امور پژوهشی قرار گرفته است، به‌اشتباه به داده‌های متعلق به غیر دسترسی یابد یا از آنها رونوشت بگیرد یا شخصی که به‌عنوان مهمان به خانهٔ دیگری رفته است، شب‌هنگام در حالت خواب‌گردی به ربایش داده‌های متعلق به صاحب‌خانه از روی تَبلت او مبادرت کند، یا به رایانهٔ او که با تدابیر امنیتی حفاظت شده است نفوذ کند، حسب مورد به دلیل نداشتن علم به موضوعِ جرم یا عمد در رفتار، قصد عامِ مرتکب احراز نمی‌شود. به‌طور مشابه، اگر کسی با تصور اینکه بُریدن یا رونوشت گرفتن از داده‌های موردنظر یا دسترسی به آنها مجاز است، اقدام به این کار کرده باشد، عنصر روانی‌اش احراز نخواهد شد؛ مانند اینکه کسی از داده‌های ذخیره‌شده در رایانهٔ دستیِ موجود در یک کتابخانهٔ عمومی رونوشت بگیرد، یا وارد سیستم‌عامل رایانهٔ نامبرده

شود، با این تصور که چنین عملی برای تمامی مراجعه‌کنندگان مجاز است، درحالی که رایانهٔ موردنظر متعلق به مسئول کتابخانه بوده و هیچ‌گونه رضایتی به این کار نداشته است.

افزون بر این، مطابق با بخش دومِ مادهٔ ۱۴۴ قانون اخیر، «قصد نتیجه» یا «علم به وقوع آن» از سوی متهم به سرقت رایانه‌ای باید محرز شود، اما لزومی به اثبات آن در مورد مرتکب دسترسی غیرمجاز نیست؛ چراکه این قسمت از مادهٔ یادشده بر لزوم احراز «قصد خاص» در جرایم مقید تأکید دارد، نه جرایم مطلق. ضمن اینکه بخش یادشده از مادهٔ ۱۴۴ قانون موردبحث روشن می‌سازد که این جزء از عنصر روانیِ سرقت رایانه‌ای ممکن است به‌طور مستقیم باشد یا نامستقیم. از این رو، «قصد محروم کردن دائمی صاحب داده‌ها از عین یا رونوشت آنها» که به‌منزلهٔ قصد خاص در جرم موردبحث است؛ هم در مواردی که شخص از ربایش داده‌های متعلق به غیر قصد داشته باشد که صاحب داده‌ها را به شرح بالا محروم سازد و هم در شرایطی که مرتکب هرچند قصد یادشده را ندارد، ولی علم دارد که رفتار ارتکابی‌اش در عمل باعث محروم شدن صاحب داده‌ها از عین یا رونوشت آنها می‌شود، احراز خواهد شد.

نمونهٔ وضعیت اخیر جایی است که کسی بعضی از کتاب‌های الکترونیک متعلق به دیگری را بدون اجازهٔ او از دیسک سختِ خارجی‌اش به‌واسطهٔ بُرش جابه‌جا و به رایانهٔ دستی خود منتقل می‌کند تا به امانت نگه‌داری کند. در چنین موردی، مرتکب حتی اگر بتواند ثابت کند که قصد محروم‌سازی دائمیِ صاحب داده‌ها از عین آنها را نداشته، با توجه به اینکه علم به وقوع نتیجه داشته است، قصد خاص او احراز می‌شود.

بدیهی است که اگر قصد خاص مرتکب به شرح یادشده اساساً به اثبات نرسد، عنصر روانی احراز نمی‌شود و در نتیجه، وی از اتهام سرقت رایانه‌ای تبرئه خواهد شد. برای مثال، هرگاه کسی که بنابه تقاضای دوستش مشغول نصب سیستم‌عامل ویندوز روی رایانهٔ رومیزی اوست، بعد از اتمام نصب ویندوز، عین داده‌های ذخیره‌شده در آن رایانه را به ابزار حامل دادهٔ خویش منتقل کند تا در زمان قسمت‌بندی دیسک سخت داخلیِ رایانه به‌طور اتفاقی حذف نشود و قصد داشته باشد که دوباره عین داده‌ها را سر جای خود بازگرداند، گرچه بدون مجوز و با علم به تعلق داده‌ها به غیر دست به بُرش عمدی آنها زده است، به دلیل نداشتن قصد محروم کردن دائمیِ صاحب داده‌ها از عین آنها، مرتکب سرقت رایانه‌ای نشده است. باید یادآور شد که محروم شدن دائمیِ جرم‌دیده از عین یا رونوشت داده‌ها در عمل لازم نیست، بلکه آنچه اهمیت دارد این است که مرتکب، قصد محروم‌سازی دائمی او به شرح پیش‌گفته را داشته باشد.

در حقوق کیفری انگلستان و وِیلز، احراز عنصر روانی جرمِ دسترسی غیرمجاز به داده‌های رایانه‌ای مستلزم اثبات این است که شخص قصد دسترسی به هرگونه داده یا برنامهٔ ذخیره‌شده در هر رایانه‌ای را داشته و در هنگام اجرای عملیات مربوط به‌وسیلهٔ رایانه، آگاه باشد که دسترسی موردنظر غیرمجاز است[1].

1. See: s (1) (a) & (c) of the Computer Misuse Act 1990

با وجود این، قصدِ مرتکب به شرح پیش‌گفته لازم نیست متوجهٔ هرگونه برنامه یا دادهٔ خاص، برنامه یا داده از هر نوع معین و یا برنامه یا دادهٔ ذخیره‌شده در رایانهٔ خاصی باشد[1]. ناگفته پیداست که تحقق عملیِ دسترسی به داده‌ها یا برنامه‌های رایانه‌ای ضروری نیست، بلکه احراز قصد مرتکب به شرح پیشین کافی است؛ از این رو، دسترسیِ بی‌پروا یا همراه با بی‌دقتی[2] کفایت نمی‌کند.

۵. مجازات سرقت رایانه‌ای/دسترسی غیرمجاز به داده‌های رایانه‌ای

در ایران، مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) مجازات سرقت رایانه‌ای را در دو فرض پیش‌بینی کرده است: «چنانچه عین داده‌ها در اختیار صاحب آن باشد»، مرتکب به جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا صد و شصت و پنج میلیون (۱۶۵/۰۰۰/۰۰۰) ریال محکوم می‌شود. این فرض ناظر بر مواردی است که سرقت رایانه‌ای از طریق «رونوشت گرفتن» از داده‌های متعلق به دیگری انجام گرفته باشد و به همین خاطر، عین داده‌ها هنوز در اختیار صاحب آنهاست و امکان بهره‌مندی از داده‌ها برای او وجود دارد. اما «در غیر این صورت»، یعنی در فرضی که عین داده‌ها در اختیار صاحب آنها نباشد، سارق به حبس از نود و یک روز تا یک سال یا جزای نقدی از شصت و شش میلیون (۶۶/۰۰۰/۰۰۰) ریال تا دویست و شصت و چهار میلیون (۲۶۴/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. فرض اخیر مربوط به شرایطی است که مرتکب با «بُریدن» داده‌های متعلق به غیر دست به سرقت رایانه‌ای بزند و در نتیجه، عین داده‌ها دیگر در اختیار صاحب آنها نباشد که بتواند از آنها بهره‌مند شود. در این صورت، با توجه به اینکه داده‌های ربوده‌شده ممکن است برگشت‌ناپذیر باشند[3] یا به‌صورت ناقص بازیابی شوند، سارق مستحق کیفرِ شدیدتری دانسته شده است. بر طبق مادهٔ ۷۲۹ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، مجازات دسترسی غیرمجاز مشابه با فرض اخیر از سرقت رایانه‌ای پیش‌بینی شده است.

شایان ذکر است، چنانچه مجازات حبس ملاک تعیین درجهٔ تعزیر قرار گیرد، با توجه به مادهٔ ۱۹ قانون مجازات اسلامی ۱۳۹۲، مجازات مقرر در مواد ۷۲۹ و ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، «تعزیر درجهٔ شش» محسوب می‌شود. البته، در سرقت رایانه‌ای، در فرضی که عین داده‌ها در اختیار صاحب آنها باشد، کیفر حبس پیش‌بینی نشده است؛ لذا ممکن است بتوان گفت که این جرم در زمرهٔ

1. S (2) of the Computer Misuse Act 1990
2. Careless or reckless access
۳. باید خاطرنشان ساخت که چنانچه برگشت‌ناپذیر بودن داده‌های متعلق به غیر در نتیجهٔ بُرش، حذف یا تخریب داده‌ها نیز محسوب شود، رفتار واحد مشمول عناوین مجرمانهٔ متعددی (سرقت رایانه‌ای طبق مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) و تخریب کیفریِ رایانه‌ای به‌موجب مادهٔ ۷۳۶ همان قانون) است، که در این صورت، مطابق با قاعدهٔ تعدد عنوانی مندرج در مادهٔ ۱۳۱ قانون مجازات اسلامی ۱۳۹۲، مرتکب به مجازات اشد محکوم می‌شود.

«جرایم تعزیریِ دودرجه‌ای» است. توضیح بیشتر اینکه در فرض اخیر جزای نقدی مقرر «تعزیر درجهٔ هفت» به‌شمار می‌آید و مجازات حبس وجود ندارد که با مادهٔ ۱۹ قانون مجازات اسلامی ۱۳۹۲ تطبیق داده شود. ولی در فرضی که عین داده‌ها در اختیار صاحب آنها نیست، کیفر حبس به شرح پیش‌گفته ملاک قرار می‌گیرد و در نتیجه، مجازات مقرر «تعزیر درجهٔ شش» تلقی می‌شود.

در هر حال، قطع نظر از درجهٔ مجازات تعزیری، مقایسهٔ مادهٔ ۶۶۱ قانون تعزیرات ۱۳۷۵ (سرقت تعزیری ساده) با مادهٔ ۷۴۰ همان قانون ((الحاقی ۱۳۸۸) مربوط به سرقت رایانه‌ای) روشن می‌سازد که مادهٔ اخیر مجازات کمتری را پیش‌بینی کرده، و به این وسیله، سرقت رایانه‌ای را به خفیف‌ترین نوع از سرقت‌های تعزیری تبدیل کرده است. این درحالی است که پیش‌بینی سرقت رایانه‌ای به‌طور خاص، از یک سو، و ارتکاب رو به افزایشِ ربایش‌های رایانه‌ای بر اثر پیشرفت‌های مرتبط با فناوری اطلاعات، از سوی دیگر، اقتضا می‌کرد که مجازات سرقت رایانه‌ای حداقل از سرقت تعزیری ساده بیشتر درنظر گرفته شود.

در انگلستان و وِیلز، طبق بند ۳ مادهٔ ۱ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰، شخصی که به سبب دسترسی غیرمجاز به داده‌های رایانه‌ای مجرم تشخیص داده می‌شود، در محکومیت اختصاری[1] مشمول حبس برای مدتی که از ۱۲ ماه متجاوز نباشد، یا جزای نقدی که از حداکثر مقررِ قانونی فراتر نرود و یا هر دو مجازات می‌شود؛ درحالی که در محکومیت برحسب کیفرخواست[2] مستوجب حبس که متجاوز از دو سال نباشد یا جزای نقدی و یا هر دو خواهد بود.

۶. وجوه افتراق و اشتراک نظام‌های کیفری

تحلیل عنصرهای سازندهٔ جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز به داده‌های رایانه‌ای در نظام‌های کیفری ایران، انگلستان و وِیلز، به شرحی که گذشت، روشن می‌سازد که وجوه افتراق و اشتراکی بین این نظام‌ها وجود دارد. این وجوه به‌اختصار در جدول زیر به تصویر کشیده شده است:

الف. عنصر قانونی
در حقوق ایران، عنوان مجرمانهٔ سرقت مرتبط با رایانه به‌طور مستقل از دسترسی غیرمجاز پیش‌بینی شده است؛ درحالی که در حقوق انگلستان و وِیلز، ازآنجا که اطلاعات در زمرهٔ اموال به‌شمار نمی‌آید، تنها عنوان مجرمانهٔ دسترسی غیرمجاز به داده‌های رایانه‌ای در دسترس قضات دادگاه‌های کیفری است.
ب. عنصر مادی
۱. در نظام کیفری ایران، رفتار مجرمانه در سرقت، به شکل ربایش در مفهوم رایانه‌ای آن، شامل بُریدن یا رونوشت

1. Summary conviction
2. Conviction on indictment

گرفتن می‌شود و در دسترسی غیرمجاز، همانا دسترسی است. اما در نظام کیفری انگلستان و وِیلز، رفتار مجرمانهٔ دسترسی غیرمجاز به داده‌های رایانه‌ای دربرگیرندهٔ هرگونه فعالیتی، غیر از صرف خواندن اطلاعات روی صفحهٔ نمایش است.

۲. در حقوق کیفری ایران، تحقق عنصر مادی جرایمِ سرقت رایانه‌ای/ دسترسی غیرمجاز مستلزم اثبات برخی شرایط پیرامونی است که عبارت‌اند از: موضوع جرم باید حسب مورد داده‌های متعلق به دیگری و یا داده‌ها یا سامانه‌های رایانه‌ای/ مخابراتی باشد؛ رفتار مرتکب به‌طور غیرمجاز انجام گیرد و داده‌ها یا سامانه‌های رایانه‌ای به‌وسیلهٔ تدابیر امنیتی حفاظت شده باشند. در حقوق کیفری انگلستان و وِیلز نیز شرط است که دسترسی‌ای که شخص قصد تأمین یا میسر ساختن تأمین آن را دارد، غیرمجاز باشد.

۳. در نظام حقوقی ایران، سرقت رایانه‌ای جرمی مقید است و نتیجه در این جرم همانا محروم شدن صاحب داده‌ها از عین یا رونوشت آنهاست، اما دسترسی غیرمجاز جرمی مطلق محسوب می‌شود. در نظام حقوقی انگلستان و وِیلز هم ضرورتی ندارد که رفتار مرتکب به نتیجهٔ خاصی منجر شود؛ لذا دسترسی غیرمجاز به داده‌های رایانه‌ای در زمرهٔ جرایم مطلق قرار می‌گیرد.

پ. عنصر روانی

در حقوق کیفری ایران، برای تحقق عنصر روانیِ سرقت رایانه‌ای/ دسترسی غیرمجاز، لازم است ثابت شود که مرتکب حسب مورد نسبت به تعلق داده‌ها یا سامانه‌های رایانه‌ای/ مخابراتی به شخص دیگر عالم بوده و در ارتکاب ربایش، خواه به‌صورت بُرش و خواه به‌واسطهٔ رونوشت گرفتن یا دسترسی، عمد داشته است (قصد عام). البته، قصد محروم کردن دائمی صاحب داده‌ها از عین یا رونوشت آنها (قصد خاص) نیز در سرقت رایانه‌ای ضرورت دارد. در حقوق کیفری انگلستان و وِیلز، احراز عنصر روانی جرمِ دسترسی غیرمجاز به داده‌های رایانه‌ای مستلزم اثبات این است که شخص قصد دسترسی به هرگونه داده یا برنامهٔ ذخیره‌شده در هر رایانه‌ای را داشته باشد و در زمانی که موجب اجرای عملیات مربوط به‌وسیلهٔ رایانه می‌شود، آگاه باشد که دسترسی موردنظر غیرمجاز است.

ت. مجازات

در حقوق کیفری ایران، به‌موجب مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، مجازات سرقت رایانه‌ای در دو فرض پیش‌بینی شده است: چنانچه عین داده‌ها در اختیار صاحب آن باشد، مرتکب به جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا صد و شصت و پنج میلیون (۱۶۵/۰۰۰/۰۰۰) ریال محکوم می‌شود؛ اما در فرضی که عین داده‌ها در اختیار صاحب آنها نباشد، سارق به حبس از نود و یک روز تا یک سال یا جزای نقدی از شصت و شش میلیون (۶۶/۰۰۰/۰۰۰) ریال تا دویست و شصت و چهار میلیون (۲۶۴/۰۰۰/۰۰۰) ریال و یا هر دو محکوم خواهد شد. مجازات دسترسی غیرمجاز نیز مشابه با فرض اخیر از سرقت رایانه‌ای پیش‌بینی شده است.

در انگلستان و وِیلز، طبق بند ۳ مادهٔ ۱ قانون سوءاستفادهٔ رایانه‌ای ۱۹۹۰، شخصی که به سبب دسترسی غیرمجاز به داده‌های رایانه‌ای مجرم تشخیص داده می‌شود، در محکومیت اختصاری مشمول حبس برای مدتی که از ۱۲ ماه متجاوز نباشد، یا جزای نقدی که از حداکثر مقررِ قانونی فراتر نرود و یا هر دو مجازات می‌شود؛ درحالی که در محکومیت برحسب کیفرخواست مستوجب حبس که متجاوز از دو سال نباشد، یا جزای نقدی و یا هر دو خواهد بود.

۷. نتیجه‌گیری

بررسی عنصرهای سازندهٔ جرایمِ سرقت رایانه‌ای و دسترسی غیرمجاز به داده‌های رایانه‌ای در نظام‌های کیفری ایران، انگلستان و وِیلز حکایت از آن دارد که با وجود جرم‌انگاری این اَعمال از سوی قانون‌گذار ایرانی، برخی نقص‌ها در رویکرد اتخاذی در راستای مقابله با مرتکبان آن یافت می‌شود که تلاش برای رفع آنها، به‌ویژه در جهت صدور آرای کیفریِ منسجم، تأثیر مطلوبی خواهد داشت. بر این اساس، راهکارهای زیر به قانون‌گذار ایرانی پیشنهاد می‌شود:

ـ تصریح جداگانه به رفتار مجرمانه و نتیجهٔ حاصله در سرقت رایانه‌ای. مفاد مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸)، به‌ویژه تفکیک بین وضعیتی که عین داده در اختیار صاحب آن باشد و حالتی که عین داده در اختیار صاحب آن نباشد؛ همچنین اینکه تحقق سرقت رایانه‌ای در جریان طبیعی امور مستلزم محروم شدن صاحب داده از عین یا رونوشت آنها است، تقویت‌کنندهٔ این نظرگاه است که سرقت رایانه‌ای جرمی مقید است. با وجود این، عدم تصریح قانون‌گذار ایرانی به نتیجهٔ ممنوعه موجب اختلاف نظر حقوق‌دانان کیفری و قضات دادگاه‌های کیفری است. بنابراین، ضرورت دارد که یا قانون‌گذار ایرانی به نتیجهٔ حاصله تصریح کند و یا مشابه با رویکرد اتخاذی در جرم دسترسی غیرمجاز، نیز رویکرد قانون‌گذار انگلیس و وِیلزی در دسترسی غیرمجاز داده‌های رایانه‌ای، عبارت‌پردازی مادهٔ یادشده را به نحوی اصلاح کند که سرقت رایانه‌ای به جرمی مطلق تبدیل گردد.

ـ مقید ساختن اطلاق عبارتِ داده‌های متعلق به دیگری به مشروع بودن آنها. با لحاظ اینکه ضابطهٔ اصلی برای تشخیص ارزش مالی چیزی در مقررات ایران همانا معیار شرعی است و حمایت کیفری قانون‌گذار ایرانی از داده‌هایی که مطابق با موازین شرعی مالیت ندارند، امری لغو است و موجب ترغیب اشخاص به حفظ و نگه‌داری چنین داده‌هایی در پرتو ضمانت اجرای کیفری برای سرقت یا دسترسی غیرمجاز به آنها می‌شود، حداقل لازم است قانون‌گذار ایرانی در قالب تبصره‌ای در عنصر قانونی جرایمِ سرقت رایانه‌ای/ دسترسی غیرمجاز، تصریح کند که اگر صاحب داده‌هایی که از لحاظ شرعی مالیت ندارند، مسلمان باشد، ربودن (اعم از بُریدن (بُرش) یا رونوشت گرفتن) یا دسترسی به آنها زیر عنوان سرقت رایانه‌ای یا دسترسی غیرمجاز تعقیب‌شدنی نیست.

ـ افزایش میزان کیفر جرمِ سرقت رایانه‌ای. در حال حاضر، سرقت رایانه‌ای خفیف‌ترین نوع از سرقت‌های تعزیری محسوب می‌شود، چراکه مجازات آن حتی از سرقت تعزیری ساده (مادهٔ ۶۶۱ قانون تعزیرات ۱۳۷۵) کمتر است. این درحالی است که پیش‌بینی سرقت رایانه‌ای به‌طور خاص از یک سو، و ارتکاب رو به افزایشِ ربایش‌های رایانه‌ای بر اثر پیشرفت‌های مرتبط با فناوری اطلاعات از سوی دیگر، اقتضا می‌کند که مجازات سرقت رایانه‌ای حداقل از سرقت تعزیری ساده بیشتر درنظر گرفته شود. در

انگلستان و وِیلز، قاضی رسیدگی‌کننده مجاز به تعیین هر دو مجازاتِ حبس و جزای نقدی برای مرتکبِ دسترسی غیرمجاز به داده‌های رایانه‌ای است. از این رو، مناسب است که قانون‌گذار ایرانی نیز حداقل چنین صلاحدیدی را برای دادرس در چارچوب مادهٔ ۷۴۰ قانون تعزیرات ۱۳۷۵ (الحاقی ۱۳۸۸) پیش‌بینی کند.

ـ اصلاح عنوان «سرقت مرتبط با رایانه» در فصل سوم (سرقت و کلاهبرداری مرتبط با رایانه) از بخش یکمِ (جرایم و مجازات‌ها) قانون جرایم رایانه‌ای ۱۳۸۸. با توجه به اینکه عنوان یادشده قلمرو وسیعی دارد که تمامی سرقت‌هایی که فقط مرتبط با رایانه هستند و نه لزوماً سرقت رایانه‌ای به معنای خاص کلمه را دربر می‌گیرد، مناسب است که قانون‌گذار نسبت به حذف عبارتِ «مرتبط با» و اصلاح واژهٔ «رایانه» به‌صورتِ «رایانه‌ای» مبادرت ورزد تا از هرگونه توسیع بلاوجه قلمرو جرمِ سرقت رایانه‌ای به اعمال مجرمانه‌ای که در مفهوم سرقتِ سنتی گنجانده می‌شوند، جلوگیری به‌عمل آید.

References

1. 1 Approval Letter No. 56261/T62298H of the Council of Ministers regarding the Amendment of the Amounts related to Crimes and Violations Contained in Various Laws Dated 24/6/2024 (In Persian).
2. Aalipour, Hassan (2015). *Information Technology Criminal Law*. 4th edition, Tehran: Khorsandi Publications (In Persian).
3. Bainbridge, David I. (2008). *Introduction to Information Technology Law*. 6th Edition, Harlow: Pearson Education Limited
4. Bainbridge, David I. (2009). *Intellectual Property*. 7th Edition, Harlow: Pearson Education Limited
5. Butterfield, Andrew & Ekembe Ngondi, Gerard (Eds) (2016). *A Dictionary of Computer Science*. 7th Edition, Oxford: Oxford University Press
6. Computer Crime (Scotland) Bill
7. Computer Misuse Act 1990
8. Computer Offences Act 2018 (In Persian).
9. Copyright, Designs and Patents Act 1988
10. Criminal Procedure Code 2013 (In Persian).
11. Data Protection Act 2018
12. Davis, Jennifer (2012). *Intellectual Property Law*. 4th Edition, Oxford: Oxford University Press
13. Downing, Douglas A. et. al. (2009). *Dictionary of Computer and Internet Terms*. 10th Edition, New York: Barron's Educational Series, Inc.
14. Edwards, Chris et. al. (1990). *Information Technology & the Law*. 2nd Edition, London: Macmillan Publishers Ltd.
15. *Ellis v DPP* [2001] EWHC 362 (Admin)
16. E'temadi, Amir (2016). *Specific Comparative Criminal Law: Assault against the Person*. First Edition, Tehran: Mizan Legal Foundation (In Persian).
17. E'temadi, Amir (2022 A). *Specific Criminal Law: Property offences*. Vol 1: Fraud and Breach of Trust, 2nd Edition, Tehran: Mizan Legal Foundation (In Persian).
18. E'temadi, Amir (2022 B). *Specific Criminal Law: Property offences*. Vol 3: Criminal

Damage and Issuance of Bad Check, First Edition, Tehran: Mizan Legal Foundation (In Persian).
19. Gattiker, Urs E. (2004). *The Information Security Dictionary*. Boston: Kluwer Academic Publishers
20. *Grant v Procurator Fiscal* [1988] RPC 41
21. Haynes, Sandra (Ed) (2002). *Microsoft Computer Dictionary*, Fifth Edition, Washington: Microsoft Press
22. Heydari, Ali Murad (2016). Offence against Property and Ownership. First Edition, Qom: Hazrat Masoumeh University Publications (In Persian).
23. Islamic Penal Code 2013 (In Persian).
24. Judiciary Research Institute (2013). Collection of Judicial Decisions of Supreme Court Branches (Criminal). December 2011, First Edition, Tehran: Judiciary Press and Publishing Center (In Persian).
25. Kranenbarg, Marleen Weulen and Leukfeldt, Rutger (Eds) (2021). *Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing*. Springer Nature Switzerland AG
26. Lloyd, Ian J. (2011). *Information Technology Law*. 6th Edition, Oxford: Oxford University Press
27. Mansourabadi, Abbas & Mansourabadi, Alireza (2024). Computer and Virtual Crimes Law. First Edition, Tehran: Mizan Legal Foundation (In Persian).
28. Marion, Nancy E. & Twede, Jason (2020). *Cybercrime: An Encyclopedia of Digital Crime*. First Edition, Santa Barbara: ABC-CLIO
29. Mohammad Nasl, Gholamreza (2012). *Computer Crimes in Iran*. First Edition, Tehran: Mizan Publishing (In Persian).
30. Police and Justice Act 2006
31. Protection of the Rights of Computer Software Creators Act 2000 (In Persian).
32. Regulations on How to Use Computer or Telecommunications Systems 2016 (In Persian).
33. Reichel, Philip L. et. al. (2019). *Global Crime: An Encyclopedia of Cyber theft, Weapons Sales, and Other Illegal Activities*. Santa Barbara: ABC-CLIO
34. Rowland, Diane et. al. (2017). *Information Technology Law*. 5th Edition, London: Routledge
35. Rowland, Diane & Macdonald, Elizabeth (2000). *Information Technology Law*. 2nd Edition, London: Cavendish Publishing Limited
36. *Taezirat* Act 1996 (In Persian).
37. The Law Commission, Working Paper No. 110, *Computer Misuse*, London: First Published 1988