Criminal Law and Criminology Studies Online ISSN: 2588-5901

Journal of the Faculty of Law and Political Science Volume: 54, Issue:2

Homepage: https://clcs.ut.ac.ir Autumn & Winter 2024

Comparative Study of Ruling Approaches on the Criminalization of Identity Theft

Meysam Abbasi Lahroudi[1]✉| Mohammad Rasaei[2]| Mohammad Bahrami Khoshkar[3]| Seyyed Abolghasem Naghibi[4]

1. Corresponding Author: Ph.D Student of Jurisprudence and Criminal Law, University of Shahid Motahari, Tehran, Iran. Email: meysamabbasi004@gmail.com
2. Assistant Professor, Department of Jurisprudence and Criminal Law, University of Shahid Motahari, Tehran, Iran. Email: m.rasaei@motahari.ac.ir
3. Associate Professor, Department of Jurisprudence and Private Law, University of Shahid Motahari, Tehran, Iran. Email: m.khoshkar@motahari.ac.ir
4. Professor, Department of Jurisprudence and Private Law, University of Shahid Motahari, Tehran, Iran. Email: da.naghibi@motahari.ac.ir

Article Info

Article type:
Research Article

Article history:
Manuscript Received:
5 December 2024
Final revision received:
6 February 2025
Accepted:
23 February 2025
Published online:
5 March 2025

Keywords:
Identity information, Identity related crimes, Criminalization, Legislative approaches, Identity theft.

ABSTRACT

Identity theft is a type of deception and fraud in which a person uses the identity information of another person to introduce himself instead of that person. This action can allow him to gain financial benefits in various ways. The process of transition from industrial societies to information societies has left a tremendous impact on the development of identity theft. This criminal phenomenon, which includes various forms and degrees and includes the unauthorized use of credit cards to the complete appropriation of a person's identity, is considered one of the most dangerous crimes today and sometimes causes irreparable damages. Considering that stealing people's identity, both in the real world and in cyberspace, can lead to committing illegal acts, this act has been criminalized in some countries and especially in many criminal laws of American states. The current research with descriptive-analytical method and using library resources while explaining the basics of research deals with the dominant approaches to the criminalization of this phenomenon and finally, it provides suggestions for drafting appropriate criminal laws in this field.

Cite this article: Abbasi Lahroudi, Meysam; Rasaei, Mohammad; Bahrami Khoshkar, Mohammad; Naghibi, Seyyed Abolghasem (2024). "Comparative Study of Ruling Approaches on the Criminalization of Identity Theft", *Criminal Law and Criminology Studies,* 54 (2): 479-498,
DOI: https://doi.org/10.22059/JQCLCS.2025.385559.1956

 Publisher: University of Tehran Press.
https://doi.org/10.22059/JQCLCS.2025.385559.1956

مطالعات حقوق کیفری و جرم شناسی

مجله دانشکده حقوق و علوم سیاسی

https://clcs.ut.ac.ir

شاپا الکترونیکی: ۵۹۰۱-۲۵۸۸

دوره ۵۴، شماره ۲

پاییز و زمستان ۱۴۰۳

مطالعهٔ تطبیقی رویکردهای حاکم بر جرم‌انگاری سرقت هویت

میثم عباسی لاهرودی[۱]✉| محمد رسایی[۲]| محمد بهرامی خوشکار[۳]| سید ابوالقاسم نقیبی[۴]

۱. نویسنده مسئول: دانشجوی دکترای فقه و حقوق جزا، دانشگاه شهید مطهری، تهران، ایران.
رایانامه: meysamabbasi004@gmail.com

۲. استادیار گروه فقه و حقوق جزا، دانشگاه شهید مطهری، تهران، ایران. رایانامه: m.rasaei@motahari.ac.ir

۳. دانشیار گروه فقه و حقوق خصوصی، دانشگاه شهید مطهری، تهران، ایران. رایانامه: m.khoshkar@motahari.ac.ir

۴. استاد گروه فقه و حقوق خصوصی، دانشگاه شهید مطهری، تهران، ایران. رایانامه: da.naghibi@motahari.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۹/۱۵
تاریخ بازنگری:
۱۴۰۳/۱۱/۱۸
تاریخ پذیرش:
۱۴۰۳/۱۲/۰۵
تاریخ انتشار:
۱۴۰۳/۱۲/۱۵

کلیدواژه‌ها:
اطلاعات هویتی،
جرایم مرتبط با هویت،
جرم‌انگاری،
رویکردهای تقنینی،
سرقت هویت.

چکیده

سرقت هویت نوعی فریب و تقلب است که در آن فردی با استفاده از اطلاعات هویتی شخص دیگری، خود را به‌جای آن فرد معرفی می‌کند. این عمل می‌تواند به او این امکان را بدهد که به روش‌های مختلف به منافع مالی دست یابد. فرایند گذار از جوامع صنعتی به جوامع اطلاعاتی، تأثیر شگرفی در توسعهٔ سرقت هویت بر جای گذاشته است. این پدیدهٔ مجرمانه که شامل اشکال و درجات مختلفی است و از استفاده غیرمجاز کارت‌های اعتباری تا تصاحب کامل هویت شخص را در برمی‌گیرد، امروزه به‌عنوان یکی از خطرناک‌ترین جرایم محسوب می‌شود و گاهی اوقات خساراتی غیرقابل‌جبران به همراه دارد. با توجه به اینکه سرقت هویت افراد، چه در دنیای واقعی و چه در فضای مجازی، می‌تواند به ارتکاب اعمال غیرقانونی منجر شود، در برخی کشورها و به‌ویژه در بسیاری از قوانین کیفری ایالت‌های آمریکا این عمل جرم‌انگاری شده است. پژوهش حاضر با روش توصیفی- تحلیلی و با بهره‌گیری از منابع کتابخانه‌ای ضمن تبیین مبانی تحقیق به رویکردهای حاکم بر جرم‌انگاری این پدیده می‌پردازد و در نهایت، پیشنهادهایی برای تدوین قوانین کیفری مناسب در این زمینه ارائه می‌دهد.

استناد: عباسی لاهرودی، میثم؛ رسایی، محمد؛ بهرامی خوشکار، محمد؛ نقیبی، سید ابوالقاسم (۱۴۰۳). مطالعهٔ تطبیقی رویکردهای حاکم بر جرم‌انگاری سرقت هویت، *مطالعات حقوق کیفری و جرم‌شناسی*، ۵۴ (۲)، ۴۹۸-۴۷۹،
DOI: https://doi.org/10.22059/JQCLCS.2025.385559.1956

ناشر: مؤسسه انتشارات دانشگاه تهران.

https://doi.org/10.22059/JQCLCS.2025.385559.1956

۱. مقدمه

«هویت» واژه‌ای مبهم و مجادله‌انگیز است که هریک از صاحب‌نظران در حوزه‌های روش‌شناختی متفاوت در علوم اجتماعی و انسانی، از منظری توجه کرده‌اند. از جمع تعاریف اندیشمندان چنین استنباط می‌شود که منظور از هویت، مجموع صفات و ویژگی‌های اختصاصی است که هر فرد را از سایرین متمایز می‌کند. هر فرد به‌واسطهٔ هویت، حقوق و تکالیفی به دست می‌آورد؛ از جمله حق بر حریم خصوصی، حق بر شرف و آبرو و... که از آن به حقوق شخصیتی یاد می‌شود. بارزترین نقطهٔ شخصیت هر فرد حفاظت از اطلاعات هویتی اوست؛ به نحوی که اگر هویت فرد موضوع یا وسیلهٔ جرم قرار گیرد، گاه به حوادثی منجر می‌شود که جبران‌پذیر نیست و می‌تواند مسیر زندگی عادی شخص را مختل سازد؛ زیرا تحت نظر بودن دائمی فرد و مورد هدف قرار دادن اطلاعات هویتی او ضمن بروز فشار روانی و سلب آسایش اجتماعی متضمن قربانی شدن آزادی فردی و به‌نوعی اعدام هویتی آن فرد است (صالح‌آبادی، ۱۳۹۱: ۱).

اگر به محتوای منتشر شده در رسانه‌ها دقت کنیم، به نظر می‌رسد که بر اساس نتایج تحقیقات انجام شده دربارهٔ ابعاد و خسارات ناشی از سرقت هویت و همچنین تحلیل‌های حقوقی متعدد، سرقت هویت را باید پدیدهٔ قرن بیست‌ویکم تلقی کرد؛ اما واقعیت نشان می‌دهد که این‌گونه نیست. قبل از دهه‌های اخیر، در دههٔ ۱۹۸۰ میلادی خبرگزاری‌ها گزارش‌هایی دربارهٔ سوءاستفاده از اطلاعات هویتی و جنبه‌های مرتبط با سرقت هویت منتشر کرده‌اند؛ از جمله اینکه جعل اسناد در برخی کشورها به مدت بیش از یک قرن جرم تلقی می‌شده است. آنچه تغییر کرده، روش‌ها و ترفندهایی است که مجرمان به کار می‌برند. امروزه با افزایش تراکنش‌های آنلاین، تعامل با رسانه‌های اجتماعی و استفادهٔ عموم از اینترنت به‌عنوان فعالیت‌های رایج روزمره، سبک زندگی جهانی جدیدی پدید آمده است. مجرمان از جمله سارقان هویت با توسعه روش‌های نوآورانه برای ارتکاب جرم، با این سبک زندگی جدید سازگار شده‌اند.

سازمان همکاری اقتصادی و توسعه به‌عنوان یک مرجع بین‌المللی، نحوهٔ ارتکاب سرقت هویت توسط مجرمان را این‌گونه شرح می‌دهد: «سرقت هویت زمانی تحقق می‌یابد که فرد یا گروهی به تحصیل، انتقال، تصرف و یا استفادهٔ غیرمجاز از اطلاعات شخصی فرد یا افراد حقیقی یا حقوقی مبادرت ورزد؛ بدین منظور که کلاهبرداری و یا جرایم دیگری را مرتکب شود و یا اقدامی مرتبط با این اهداف انجام دهد» (OECD, 2008: 3). اخیراً سرقت هویت به‌عنوان یک چالش جدی برای جوامع و همچنین نهادهای قضایی و انتظامی مطرح است که هم از نظر تعداد جرایم و هم از نظر میزان خسارات وارده اهمیت دارد؛ برای مثال در ایالات متحدهٔ آمریکا بر اساس گزارش مرکز شکایات جرایم اینترنتی ادارهٔ تحقیقات فدرال[1]، قربانیان سرقت هویت در سال ۲۰۱۹ بیش از ۱۶۰ میلیون دلار ضرر مالی را تجربه کردند. این افزایش شایان توجهی نسبت به سال ۲۰۱۵ است، زمانی که تلفات قربانیان کمی بیش از ۵۷ میلیون دلار گزارش شد (Alagna, 2020: 6). نکتهٔ شایان توجه این است که تأثیر سرقت هویت تنها به خسارات مالی مستقیم به قربانیان محدود نمی‌شود. آسیب‌هایی که به اعتبار و وجههٔ افراد وارد می‌شود، خساراتی که به مؤسسات مالی و اعتباری تحمیل می‌شود، هزینه‌های مربوط به نظام قضایی و نیروهای انتظامی و همچنین اقدامات پیشگیرانه در برابر این نوع جرایم نیز باید مورد توجه قرار گیرند (Lawson, 2011: 122-128). با توجه به اینکه سرقت هویت افراد، چه در دنیای واقعی و چه در فضای مجازی، می‌تواند زمینه‌ساز رفتارهای غیرقانونی مانند تروریسم، جاسوسی و مهاجرت غیرمجاز شود، در برخی کشورها و به‌ویژه در بسیاری از قوانین کیفری ایالت‌های آمریکا این عمل جرم تلقی شده است (خالقی و صالح‌آبادی، ۱۳۹۴: ۹۲).

1. Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3)

هدف از پژوهش حاضر، ارائهٔ راهبردی در خصوص واکنش کیفری به سرقت هویت و آشنایی هرچه بیشتر با جرایم نوظهوری است که علیه هویت افراد واقع می‌شوند تا بدین طریق بتوانیم گامی در جهت ضرورت تدوین قوانین مناسب به‌منظور حمایت از هویت افراد برداشته باشیم. همان‌گونه که بیان خواهد شد، عبارت «سرقت هویت» برای توصیف حوزه‌ای نسبتاً ناهمگن از جرم‌ها به کار رفته است. با توجه به هر دو جنبهٔ حدود و تأثیر جرایم، بسط و شرح پاسخ کافی به این تهدید چالش‌برانگیز و ضروری است. در مورد سرقت هویت باید اشاره داشت که اگرچه مقالاتی در این زمینه به چاپ رسیده، اما با توجه به نوظهور بودن این جرم تاکنون تحقیقات کاملی صورت نگرفته است و ناشناخته‌های زیادی پیرامون جرایم مرتبط با هویت وجود دارد، از این رو پژوهش حاضر از این نظر که جرم‌انگاری این پدیدهٔ مجرمانه را با رویکردی تطبیقی تجزیه‌وتحلیل می‌کند، واجد جنبه نوآوری است. در تحقیق حاضر با روش توصیفی- تحلیلی ابتدا به تبیین مبانی نظری پژوهش و رویکردهای موجود برای تعریف سرقت هویت پرداخته می‌شود، سپس مروری دربارهٔ استدلال‌های موافق یا مخالف با توسعه رویکردی خاص برای جرم‌انگاری سرقت هویت خواهیم داشت و در پایان، مؤلفه‌های بنیادین و عناصر بالقوه‌ای که برای توسعهٔ رویکرد ملی در زمینهٔ جرم‌انگاری این رفتار لازم است، ارائه خواهد شد.

۲. مبانی کیفری حمایت از هویت

جرم‌انگاری[1] در هر نظام حقوقی بر پایه اصول و مبانی فکری خاص آن نظام شکل می‌گیرد که دولت‌ها با بهره‌گیری از آن‌ها به تعیین رفتارهای مجاز و ممنوع می‌پردازند. از شیوه‌های حفظ و حمایت از اهداف، منافع و ارزش‌های حاکم توسط دولت‌ها توسل به حقوق کیفری و ضمانت اجراهای آن است. اینک در خصوص مسئله سرقت هویت، این سؤال مطرح می‌شود که چه دلایلی حمایت کیفری از هویت اشخاص و مداخلهٔ کیفری در این حوزه را توجیه می‌کند؟ در این زمینه دلایل متعددی وجود دارد که در ادامه، به بررسی آن‌ها خواهیم پرداخت.

۲. ۱. نظریهٔ حقوق فطری

بر اساس نظریهٔ حقوق فطری، تمامی انسان‌ها دارای حقوق اساسی هستند که برتر از خواست و ارادهٔ دولت‌هاست (کاتوزیان، ۱۴۰۰، ج ۱: ۳۸). از جملهٔ این حقوق می‌توان به حق حیات، حق برخورداری از آزادی بیان و حق بهره‌مندی از زندگی خصوصی اشاره کرد. از این دیدگاه باید گفت که انسان اولاً و بالذات آزاد و رها خلق شده است، از این رو همین آزادی و رهایی اولیه اقتضا دارد که اولاً، فرد بتواند از آگاهی و اطلاع دیگران دربارهٔ جنبه‌های مختلف زندگی خصوصی خود جلوگیری کند و اجازه ندهد دیگران به بررسی و کاوش در داده‌ها و اطلاعات این بخش از زندگی او بپردازند؛ ثانیاً، در صورت تمایل بتواند از مداخله سایرین در زندگی شخصی خود ممانعت به عمل آورد (صالح‌آبادی، ۱۳۹۱: ۶۹). بر این اساس، هر نوع مداخله در جنبه‌های مختلف زندگی خصوصی افراد، از جمله دسترسی به اطلاعات شخصی و استفاده از نام و هویت دیگران بدون اطلاع یا رضایت آن‌ها به‌عنوان نقض حقوق طبیعی آن‌ها تلقی می‌شود.

۲. ۲. نظریهٔ اخلاقی

اخلاق شامل مجموعه‌ای از اصول رفتاری است که رعایت آن برای نیل به کمال ضروری بوده و با طبیعت انسان سازگار است (کاتوزیان، ۱۴۰۰، ج ۱: ۴۱۱-۴۱۲). حقوق نیز به مجموعه‌ای از قواعد اطلاق

1. Criminalization

می‌شود که انسان‌ها به‌منظور ایجاد نظم و عدالت در جامعه وضع کرده‌اند و موضوع اصلی آن «رفتار انسان» است. حقوق اخلاق را هدف و راهنمای خود در قاعده‌گذاری می‌داند؛ قاعده حقوقی که از نظر اخلاقی معتبر باشد، به دلیل ایجاد حس رضایت درونی در شهروندان با سهولت بیشتری مورد قبول واقع می‌شود. حمایت از افراد و حریم خصوصی آن‌ها موضوعی است که از سوی اخلاق مورد تأیید و تأکید قرار گرفته و قانونگذار باید با تدوین قواعد رفتاری واضح و مشخص و همچنین، ایجاد ضمانت اجراهای مادی (شامل مجازات کیفری و غیر کیفری) به این موضوع رسیدگی کند (صالح‌آبادی، ۱۳۹۱: ۷۰). بنابراین، اقدام فردی که بدون کسب اجازه به حریم خصوصی دیگری وارد می‌شود و به اطلاعات شخصی او دسترسی پیدا می‌کند، از منظر اخلاقی ناپسند و قبیح است. بر این اساس، بر پایهٔ نظریهٔ اخلاقی، تدوین چارچوب‌های قانونی مبتنی بر اصول اخلاقی به‌منظور حفاظت از حریم خصوصی اطلاعات شهروندان و حفظ کرامت آنان امری ضروری به شمار می‌آید.

۲. ۳. نظریهٔ قرارداد اجتماعی

بر اساس نظریه قرارداد اجتماعی که قوانین اساسی نماد و تجلی آن به شمار می‌روند، زندگی اجتماعی و مدنی انسان‌ها مرزهایی را برای زندگی خصوصی آن‌ها تعیین می‌کند؛ تمایل بی‌پایان بشر به آزادی و نیاز به زندگی جمعی در تضاد با یکدیگر قرار دارند. آنچه این دو را به هم نزدیک می‌کند، مجموعه‌ای از قراردادهاست که قدرتی فرافردی (حکومت) در جامعه ایجاد می‌کند. این قرارداد به نام قرارداد اجتماعی شناخته می‌شود (روسو، ۱۳۶۶: ۱۸). یکی از مواردی که در این قرارداد بر آن توافق می‌شود، ضرورت حمایت و حفاظت از حقوق، آزادی‌ها و خواسته‌های افراد توسط حکومت است و این مابه‌ازای تحمل قدرت فرافردی از سوی افرادی است که اولاً و بالذات آزاد و رها آفریده شده‌اند. یکی از اساسی‌ترین مسائلی که انسان‌ها برای خود به‌عنوان رهایی و آزادی در نظر می‌گیرند، آزاد بودن از هرگونه نظارت و مداخلهٔ دیگران در جنبه‌های خصوصی زندگی‌شان از جمله داده‌ها و اطلاعات مربوط به آن‌هاست.

استناد به نظریه قرارداد اجتماعی این زمینه را فراهم می‌سازد که نه‌تنها وقوف دیگران بر اطلاعات شخصی، بلکه هر نوع استفاده مادی از داده‌های شخصی نیز قابل منع باشد؛ با این توجیه که انتفاع مالی از چنین اموری از مطلوب‌های شخص است، از این رو این امر تنها با رضایت او امکان‌پذیر است، حتی اگر زیان حیثیتی و معنوی به او وارد نیامده باشد. این هدف در زمرهٔ مطلوب‌های مورد حمایت در قرارداد اجتماعی است. بر این اساس، طبق نظریه قرارداد اجتماعی حکومت موظف است قوانینی را تصویب و اجرا کند که به حفظ حقوق افراد و حریم خصوصی آن‌ها، هویت، اسرار و به‌طور کلی هر آنچه به آن‌ها مربوط می‌شود، بپردازد (صالح‌آبادی، ۱۳۹۱: ۷۱-۷۲).

۲. ۴. حمایت از شأن، منزلت و کرامت انسانی

کرامت انسانی بنیان و اساس بسیاری از حقوق، امتیازات و تکالیف انسانی به شمار می‌آید. این واژه از ریشهٔ «ک ر م» به معانی شرافت، حرمت، مقام، رتبه و منزلت اشاره دارد (فراهیدی، ۱۴۰۹ق، ج ۵: ۳۶۸؛ راغب اصفهانی، ۱۴۰۴ق: ۴۲۸). کرامت انسانی به مفهوم عظمت و احترام به فرد است و این موضوع نه‌تنها یک حق، بلکه ویژگی ذاتی انسان به شمار می‌آید که بر پایهٔ دو خصوصیت عقل و اختیار او استوار است.

در آموزه‌های دینی به اهمیت کرامت انسان تأکید شده و امروزه این موضوع در مقدمه منشور سازمان ملل متحد، مادهٔ ۱ اعلامیهٔ جهانی حقوق بشر و بسیاری از اسناد دیگر مورد توجه قرار گرفته است. ریشهٔ اصلی نظریهٔ کرامت ذاتی انسان در تعالیم اخلاقی و حقوقی اسلام، گزارهٔ «وَلَقَدْ كَرَّمْنَا بَنِي‌آدَمَ...: ما آدمیزادگان را گرامی داشتیم...» (اسراء/۷۰) در قرآن کریم است. همچنین در نظام

حقوقی اسلام هر کس که به کرامت انسان تجاوز کند، مسئول مدنی شناخته می‌شود و حتی برخی از موارد هتک حرمت انسان می‌تواند به مسئولیت کیفری منجر شود (ر.ک: نقیبی، ۱۳۹۱: ۵۹-۶۰).

به‌طور کلی، جرایم مرتبط با هویت نه‌تنها به آبرو و حیثیت افراد لطمه وارد می‌کند، بلکه پیامدهای منفی اجتماعی نیز به همراه دارد و سبب ایجاد بدبینی و آسیب‌های مادی و معنوی می‌شود. سرقت هویت می‌تواند به مشکلات جدی در ایجاد یا حفظ اعتبار، اشتغال، مسکن، بیمه درمان، سایر انواع بیمه‌ها، گواهینامه رانندگی، گذرنامه و دیگر اسناد هویت دولتی یا سازمانی منجر شود. همچنین، آسیب‌های وارده بر شهرت و اعتبار می‌تواند مشکلاتی در خروج از کشور ایجاد کند. بدتر از این موارد، خساراتی است که به روابط خانوادگی یا اجتماعی وارد می‌شود، به‌ویژه زمانی که قربانیان به دلیل جرایمی که هرگز مرتکب نشده‌اند، بازداشت می‌شوند (Lawson, 2011: 123). افزون بر این، دسترسی به اطلاعات شخصی و محرمانه به عاملی برای نقض آزادی و استقلال انسان، استفاده ابزاری و سلطه بر آن‌ها تبدیل شده است. ورود به حریم خصوصی افراد، شرافت، حیثیت و تمامیت افراد را نابود ساخته، آزادی و استقلال فردی را مختل می‌سازد. بنابراین، قانونگذار باید با جرم‌انگاری این پدیده از شأن و منزلت، آزادی و استقلال افراد حمایت به عمل آورد.

بدون شک ماهیت شدید و رنج‌آور مداخله حقوق کیفری و پیامدهای زیان‌بار واکنش‌های متنوع آن نسبت به جرم از یک سو و تمایل فزایندهٔ قدرت عمومی به گسترش اختیارات و اقدامات خود از سوی دیگر، ضرورت وجود نظریه جرم‌انگاری را ایجاب می‌کند (محمودی جانکی، ۱۳۹۳: ۸۴). جرم‌انگاری اعلام وصف مجرمانه برای اعمال و رفتارهایی است که از سوی جامعه مستحق مواجهه کیفری هستند و لازم است نظام حاکم مجازات مشخصی را برای مرتکبین این اعمال در نظر بگیرد (وکیلی‌مقدم، ۱۴۰۰: ۲۳۸). نظریه جرم‌انگاری در نظام‌های حقوقی گوناگون عمدتاً بر پایهٔ اصل ضرر[1] استوار است. طبق این اصل، رفتارهایی که به جامعه و افراد آن آسیب می‌زند باید توسط قانونگذار ممنوع شده و برای تخلف از آن‌ها مجازات تعیین گردد. در واقع، با گسترش مفهوم ضرر می‌توان به رفع خلأهای موجود در نظام حقوقی و امکان دفاع از حقوق مردم پرداخت (برهانی، ۱۳۸۸: ۱۸-۱۹). در مجموع، به نظر می‌رسد با توجه به دلایل مذکور که برای حمایت از هویت اشخاص بیان شد و خسارات هنگفتی که از جرایم مرتبط با سرقت هویت حاصل می‌شود، باید هر آنچه موجب سوءاستفاده از هویت افراد یا در تقابل و به ضرر عموم مردم باشد، ممنوع اعلام و برای آن‌ها مجازات تعیین شود.

۳. تعریف سرقت هویت

تعاریف متنوعی از سرقت هویت در نظام‌های قضایی مختلف وجود دارد. حتی اصطلاحی که برای توصیف این پدیده به کار می‌رود، یکسان نیست؛ برای مثال، در ایالات متحدهٔ آمریکا اصطلاح «سرقت هویت» برای در برگرفتن تمام انواع جرایم هویتی به کار می‌رود، در حالی که در بریتانیا و استرالیا به ترتیب از عباراتی مانند «جعل هویت» و «جرم هویت» برای در برگرفتن این‌گونه جرایم استفاده می‌شود (ACPR, 2006: 5).

۳. ۱. تعاریف عمومی

الف) ترکیب «به دست آوردن» و «به‌کارگیری» یک هویت: «سرقت هویت هنگامی رخ می‌دهد که فردی داده‌ها یا مدارک متعلق به دیگری (بزه‌دیده) را به دست می‌آورد و سپس خود را جای بزه‌دیده جا می‌زند» (Mitchison *et al*., 2004: 5). این تعریف حاوی دو مؤلفهٔ مهم است: موضوع (داده‌ها یا مدارک متعلق به دیگری) و دو عملکردی که هر دو برای جرم‌انگاری لازم است: به دست

1. The Harm principle

آوردن داده‌ها و معرفی خود به‌جای بزه‌دیده. در نتیجه، فعل به دست آوردن اطلاعات و یا کسب آن‌ها به‌منظور فروش هیچ‌کدام به‌تنهایی مشمول این تعریف نمی‌شوند.

ب) فعل مستحق مجازات که در آن، هویت هدف یا وسیله باشد: «جرم مرتبط با هویت عبارت است از تمام فعالیت‌های مستحق مجازات که در آن‌ها هویت هدف یا وسیله اصلی باشد». این تعریف متضمن رویکردی نسبتاً کلی است که در آن، موضوع و رفتارهای مجرمانه مشخص نشده است. این تعریف دسته‌بندی سطح بالاتری را ارائه می‌دهد که جرایم مرتبط با هویت گوناگونی همچون سرقت هویت و جعل هویت را در برمی‌گیرد (Koops & Leenes, 2006: 556). نظر به کلی بودن این رویکرد، تعریف مذکور برای تدوین قوانین کیفری مناسب نیست.

ج) جعل یا هرگونه فعالیت غیرقانونی دیگر که در آن «هویت» هدف یا وسیله باشد: «سرقت هویت، جعل یا هرگونه اقدام غیرقانونی دیگری است که در آن از هویت یک شخص موجود، به‌منزلهٔ هدف یا ابزار اصلی و بدون رضایت شخص استفاده می‌شود» (Koops & Leenes, 2006: 556). مفهوم سرقت هویت در این تعریف حاوی دو مؤلفهٔ اصلی است: موضوع (هویت) و رفتار مرتبط (جعل یا هر فعالیت غیرقانونی). در این تعریف برای موضوع و رفتارها به توضیح بیشتری پرداخته نشده است.

د) قبول یک هویت: «سرقت هویت ممکن است برای توصیف سرقت یا اتخاذ هویت «قبل از موجودیت» (یا بخش مهمی از آن)، با یا بدون رضایت و صرف‌نظر از اینکه شخص مربوطه در قید حیات باشد یا نباشد، به کار رود» (ACPR, 2006: 15). این تعریف نیز متشکل از دو مؤلفه است: موضوع (هویت) و رفتار مرتبط (قبول). در مقایسه با تعاریف دیگر، این تعریف موضوع جرم را به‌طور دقیق‌تری ارائه می‌دهد. با این حال، در این تعریف از انتقال یا به‌کارگیری اطلاعات مرتبط با هویت بحث نشده است.

ه) تصاحب هویت موهوم یا نامیدن خود به نام شخص دیگری: «جعل هویت هنگامی اتفاق می‌افتد که کسی یک نام کاملاً موهومی را تصاحب کرده یا نام شخص دیگری را با یا بدون رضایت آن‌ها برداشته باشد» (UK Cabinet Office, 2002: 9). این تعریف شامل دو مؤلفه است: موضوع (هویت موهوم یا واقعی) و رفتار مرتبط (تصاحب/ برداشتن). دربارهٔ موضوع و رفتارها توضیح بیشتری ارائه نشده است. این بند به تصاحب هویت (بسته به اینکه چه تفسیری از واژهٔ تصاحب شود) و به‌کارگیری هویت توجه دارد. بنابراین، بعید است که انتقال یا فروش اطلاعات مرتبط با هویت را نیز در برگیرد. جنبهٔ منحصربه‌فرد این تعریف آن است که به «تصاحب یک نام موهوم» می‌پردازد. ایراد دیگر این است که تمرکز این قبیل اقدامات جزایی، محدود به نام‌ها شده و سایر اطلاعات مرتبط با هویت در این تعریف گنجانده نشده‌اند.

و) تعاریف استفاده‌شده در مطالعات میدانی: در زمینهٔ تحلیل جرایم مرتبط با سرقت هویت، ناهماهنگی مشابهی در مطالعات میدانی وجود دارد؛ برای مثال، مطالعهٔ میدانی «آمار شکایت مشتریان در خصوص جعل و سرقت هویت» که کمیسیون‌های تجارت فدرال ایالات متحده منتشر کرده، حاوی اطلاعات مرتبط با تعریف سرقت هویت است: «جعل کارت اعتباری (۲۵ درصد) رایج‌ترین شکل از سرقت هویت است که تاکنون گزارش شده است». در این مطالعات، «اقدام به کسب اطلاعات مرتبط با هویت (سرقت)» از «ارتکاب جرمی کیفری که با به‌کارگیری این اطلاعات (جعل کارت نقدی) حاصل می‌شود»، تفکیک نشده است (FTC, 2007: 3).

۳. ۲. تعاریف قانونی

جرایم مرتبط با هویت تاکنون توسط دولت‌های معدودی به موجب قوانین خاص جرم‌انگاری شده‌اند. یکی از شناخته‌شده‌ترین رویکردهای تعریف سرقت هویت در ایالات متحدهٔ آمریکا اتخاذ شده است که در ادامه، به توضیح آن می‌پردازیم.

به موجب مادهٔ ۱۰۲۸ (الف)(۷) از جلد ۱۸ مجموعه قوانین ایالات متحده[1]، سرقت هویت بدین صورت تعریف شده است: «انتقال، تملک یا استفاده آگاهانه و بدون مجوز قانونی از ابزار شناسایی شخص دیگر به قصد ارتکاب یا معاونت، تحریک یا ارتباط داشتن با هرگونه فعالیت غیرقانونی که به‌منزلهٔ نقض قانون فدرال باشد یا به موجب هر کدام از قوانین قابل اجرای ایالتی یا محلی جرم محسوب شود». این تعریف نیز متضمن سه مؤلفه است: موضوع (ابزار شناسایی)، رفتار (انتقال، تملک یا استفاده) و قصدی که اقدامات مذکور را با سایر فعالیت‌های مجرمانه مرتبط می‌کند. در صورت انجام هر دو رفتار، همانند سایر جرایم عمدی، این ماده از رویکردی کلی تبعیت می‌کند. بر خلاف مطالعهٔ میدانی «آمار شکایت مشتریان در خصوص جعل و سرقت هویت»، در این ماده الزامی به ارتباط این رفتار با جعل وجود ندارد.

همچنین، به موجب مادهٔ ۱۶۸۱ الف (بند)(۳) از جلد ۱۵ مجموعه قوانین ایالات متحده[2]، کمیسیون تجارت فدرال توصیف دقیق‌تری از سرقت هویت ارائه کرده است:

الف) اصطلاح «سرقت هویت» به معنای ارتکاب جعل یا شروع به آن با استفاده از اطلاعات شناسایی شخصی دیگر بدون مجوز قانونی است؛

ب) اصطلاح «اطلاعات شناسایی» به معنای هرگونه نام یا شماره‌ای است که ممکن است به‌تنهایی یا همراه اطلاعات دیگر، برای شناسایی فردی معین به کار رود، از جمله موارد ذیل:

۱. نام، شمارهٔ تأمین اجتماعی، تاریخ تولد، گواهینامه رانندگی یا کد شناسایی صادره از مقامات ذی‌صلاح ایالتی یا دولتی، شمارهٔ ثبت بیگانگان، شمارهٔ گذرنامهٔ دولتی، شمارهٔ شناسایی کارفرمایان یا مؤدیان مالیاتی؛

۲. داده‌های بیومتریک (زیست‌سنجی) منحصربه‌فرد از قبیل اثر انگشت، صدانگاشته، تصویر شبکیه یا عنبیه، یا سایر علائم فیزیکی منحصربه‌فرد؛

۳. شمارهٔ شناسایی الکترونیکی، نشانی یا کد رهگیری منحصربه‌فرد؛

۴. اطلاعات شناسایی ارتباطاتی یا ابزارهای دسترسی.[3]

این مادهٔ قانونی توصیفی همانند مطالعهٔ میدانی «آمار شکایت مشتریان در خصوص جعل و سرقت هویت» ارائه می‌دهد. از این رو اجرای این ماده در مواردی که مجرم به استفاده از اطلاعات مرتبط با هویت برای انجام سایر جرایم غیر از جعل اقدام می‌کند، با محدودیت مواجه می‌شود. همچنین با اینکه مادهٔ مذکور رفتاری را تعریف می‌کند که متضمن کلمهٔ «سرقت» است، اما صرفاً استفاده از اطلاعات را جرم شناخته است نه به دست آوردن آن را.

---

1. 18 U.S.C. § 1028 (a)(7)

۲. خلاصه‌ای از مفهوم «سرقت هویت» در این ماده آمده است: «ارتکاب جعل با استفاده از اطلاعات هویتی فردی دیگر که می‌توان با جزئیات بیشتر هم تعریف کرد؛ مانند کمیسیون که می‌تواند از طریق مقررات تعیین کند» ((15 U.S.C. 1681 a (q) (3)).

3. Federal Trade Commission, 16 CFR Parts 603, 613, and 614 RIN 3084-AA94 Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act.

۴. رویکردهای حقوقی

جرم‌انگاری جرایم مرتبط با هویت یکی از راهکارهای ممکن برای پاسخ به این پدیده است. در این گفتار، نگاهی کلی به مباحث مربوط به اهمیت جرم‌انگاری و همچنین، رویکردهای ملی و بین‌المللی در خصوص جرم‌انگاری سرقت هویت خواهیم داشت.

۴. ۱. استدلال‌های له و علیه جرم خاص سرقت هویت

اگرچه کشورهای متعددی امکان تعقیب کیفری جنبه‌های معین جرایم مرتبط با سرقت هویت را در قالب قوانین سنتی همچون جعل یا کلاهبرداری فراهم کرده‌اند، اما صرفاً دولت‌های معدودی قوانین ویژه‌ای را برای تعقیب کیفری سرقت هویت به‌عنوان یک جرم مستقل اجرا کرده‌اند.[۱] در نتیجه، ضرورت وجود چنین راه‌حل‌هایی در سطح جهانی مورد توجه قرار نگرفته است. دلیل اصلی تصمیم دولت‌ها برای جرم‌انگاری سرقت هویت، پی بردن به این موضوع است که سوءاستفاده اولیه از هویت می‌تواند به طیفی از جرایم ثانویه منجر شود، از این رو نظام عدالت کیفری را برای پیشگیری از این جرایم در یک مرحله قبل‌تر فعال کرده‌اند (Report of the Secretary-General, 2007: 3).

۴. ۲. قابلیت اجرای قوانین کیفری سنتی

به‌طور کلی، هیچ‌گاه سرقت هویت جرمی مستقل نیست (Briefing Report to Congressional Requesters, 1998: 2). همان‌طور که قبلاً تأکید شد، مفهوم سرقت هویت برای توصیف «ترکیبی از رفتارهای مختلف» به کار رفته است. این رفتارها از سرقت مدارک هویتی تا استفاده از اطلاعات مرتبط با هویت به‌منظور فریب و کلاهبرداری در نوسان است. با تجزیه‌وتحلیل پرونده‌های مربوط به «سرقت هویت» اغلب معلوم می‌شود که صرفاً برخی جرایم سنتی مانند جعل کارت اعتباری را «سرقت هویت» می‌نامند (FTC, 2007: 3). توصیف مجرمانهٔ سرقت و جعل، سنتی دیرینه در بیشتر کشورهاست. بر مبنای مطالعات مذکور، بیشتر جرایم مرتبط با هویت به قصد ارتکاب جعل صورت می‌گیرند که رفتارهای مذکور را به‌طور معمول می‌توان طبق قوانین کیفری سنتی تحت تعقیب قرار داد.

حتی در خصوص رسیدگی به جرایم «سرقت هویت مرتبط با اینترنت» پیش‌بینی مفهومی خاص برای تعقیب این جرایم، ضروری نیست (Gercke, 2007: 13). طی سال‌های اخیر، کشورهای زیادی قوانین خود را برای جرم‌انگاری جرایم مرتبط با رایانه از قبیل جعل رایانه‌ای و دسترسی غیرقانونی به سیستم‌های رایانه‌ای، به‌روز کرده‌اند. با توجه به اینکه بسیاری از جرایم سایبری ابعادی فراملی دارند و با در نظر گرفتن این نکته که استانداردهای حقوقی متفاوت در کشورهای ذی‌ربط می‌تواند تحقیقات قضایی را دچار پیچیدگی کند، در نتیجه برخی سازمان‌های بین‌المللی وظیفه هماهنگ کردن قوانین ملی در سطح جهانی و توسعهٔ همکاری‌های بین‌المللی را بر عهده گرفته‌اند.

یکی از راه‌حل‌های مهم، کنوانسیون جرایم سایبری شورای اروپا مصوب ۲۰۰۱ است؛ این کنوانسیون حاوی مقررات کیفری ماهوی است که رفتارهایی را که بر اساس مبنایی قانونمند، قسمتی از «ترفندهای سرقت هویت مرتبط با اینترنت» از قبیل دسترسی غیرقانونی (مادهٔ ۲) و سوءاستفاده از دستگاه‌ها (مادهٔ ۶) باشند، جرم‌انگاری کرده است. با وجود این، صرف‌نظر از قابلیت اجرای قوانین ماهوی کیفری سنتی، برخی رفتارهایی که در محدودهٔ جرایم مرتبط با هویت انجام گرفته‌اند، مشمول قوانین ماهوی کیفری سنتی و اسناد بین‌المللی از قبیل کنوانسیون جرایم سایبری نشده‌اند. نمونه‌ای از

---

۱. جهت مطالعه بیشتر در این زمینه، ر.ک:
OECD (2008), Scoping Paper on Online Identity Theft, DSTI/CP(2007)3/FINAL, pp. 12-14.

این رفتارها، تبادل و تجارت اطلاعات مرتبط با هویت است. ارتقای قوانین خاص کیفری می‌تواند خلأهای احتمالی از این قبیل را در قوانین داخلی کشورها پر کند (Gercke, 2011: 37).

۴. ۳. جنبه‌های کاربردی مربوط به تحقیقات قضایی

همان‌گونه که ذکر شد، به‌طور کلی سرقت هویت هرگز جرم مستقلی نبوده است. جرم‌انگاری سرقت هویت به مجریان قانون اجازه می‌دهد، رفتارهایی را که از نظر زمانی مقدم بر سایر جرایم هستند نیز تحت تعقیب قرار دهند. چنین قابلیتی می‌تواند از بروز مشکلات در شناسایی مجرمی که اقدامات بعدی را مرتکب می‌شود، جلوگیری کند.

۴. ۴. رویکردهای بین‌المللی

همان‌طور که بیان شد، در حال حاضر ارتقای چارچوب‌های حقوقی برای جرم‌انگاری سرقت هویت فقط در سطح ملی به وقوع پیوسته است. علی‌رغم فقدان استانداردهای حقوق کیفری قابل‌اجرا در سطح جهانی، سازمان‌های بین‌المللی و منطقه‌ای فعالیت‌های خود را در خصوص این موضوعات افزایش داده‌اند.

سازمان ملل متحد؛ مسائل ناشی از جرایم مرتبط با هویت، جایگاه مهمی را در برنامهٔ پیشگیری از جرم و عدالت کیفری سازمان ملل متحد به خود اختصاص داده‌اند. اعلامیهٔ بانکوک در مورد «هم‌افزایی‌ها و پاسخ‌ها: اتحاد راهبردی در پیشگیری از جرم و عدالت کیفری» که قطعنامهٔ مجمع عمومی به شمارهٔ ۶۰/۱۷۷ به تاریخ ۱۶ دسامبر ۲۰۰۵ بر آن صحه گذاشت، بر اهمیت سرنوشت‌ساز مبارزه با جعل سند و جعل هویت به‌منظور کنترل جرایم سازمان‌یافته و تروریسم تأکید کرده است. کشورهای عضو همچنین درخواست «ارتقای همکاری‌های بین‌المللی، از طریق مساعدت فنی برای مبارزه با جعل سند و جعل هویت، به‌ویژه استفاده متقلبانه از اسناد مسافرتی، از طریق ارتقای اقدامات امنیتی و تشویق به تصویب قوانین ملی مناسب» را مطرح کردند.[1]

مطابق قطعنامهٔ ۲۶/۲۰۰۴ شورای اقتصادی و اجتماعی، دفتر جرم و مواد مخدر سازمان ملل متحد (UNODC) مأموریت یافت در زمینهٔ «جعل و سوءاستفاده مجرمانه و تحریف هویت» تحقیق کند که نتیجه آن در اوایل سال ۲۰۰۷ میلادی منتشر شد.[2] رویکرد این تحقیق گسترده‌تر از پژوهشی بود که سازمان همکاری اقتصادی و توسعه (OECD) انجام داد؛ زیرا اولاً، عبارت کلی «جرم مرتبط با هویت» برای در برگرفتن تمام اشکال رفتارهای غیرقانونی مرتبط با هویت از جمله «جعل هویت» و «سرقت هویت» به کار رفت که اغلب دارای روش یکسان و ثابتی نیستند. ثانیاً، در تمام رفتارهای مجرمانه مرتبط با سرقت هویت، ارتکاب جرم به هر دو صورت آنلاین و آفلاین پیش‌بینی شده که به سبب ارتباط آن‌ها با جرایم سازمان‌یافته فراملی و سایر فعالیت‌های مجرمانه تأکید بیشتری بر شیوه‌ها و ترفندهای پیچیده انجام پذیرفته است. ثالثاً، جرایم مرتبط با هویت در ارتباط تنگاتنگ با جرم جعل مورد توجه قرار گرفته که این مسئله در راستای مصوبات شورای اقتصادی و اجتماعی سازمان ملل متحد (ECOSOC) صورت گرفته است (Abdul Manap *et al*., 2015: 293).

گزارش دبیر کل سازمان ملل متحد دربارهٔ رهنمودهایی برای راهبرد ضد تروریسم جهانی، بر اهمیت توسعهٔ ابزارهای مهار سرقت هویت در مبارزه با تروریسم تأکید کرده است.[3] همچنین به

1. Bangkok Declaration, Strategic Alliances in Crime Prevention and :Synergies and Responses Criminal Justice, 2005, paragraph 27.
2. E/CN.15/2007/8 and Add. 1-3.
3. Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy, 27.04.2006, A،60،825, page 13.

چالش‌های مربوط به سرقت هویت و نیاز به واکنش مناسب در این زمینه، در قطعنامه‌های متعدد سازمان ملل متحد اشاره شده است.[۱]

سازمان همکاری اقتصادی و توسعه (OECD)؛ در سال ۱۹۸۳، OECD یک کمیتهٔ تخصصی برای بحث در مورد پدیدهٔ جرایم رایانه‌ای و اصلاح قوانین کیفری ایجاد کرد. این سازمان جرایم مرتبط با رایانه را به‌عنوان رفتارهای غیرقانونی، غیراخلاقی یا غیرمجاز شامل پردازش خودکار داده‌ها و یا انتقال داده‌ها تعریف می‌کند. یکی از توصیه‌های این کمیته در گزارش سال ۱۹۸۵، تأکید بر اهمیت همکاری بین‌المللی برای کاهش و کنترل این نوع فعالیت‌ها به دلیل ماهیت خاص جرایم سایبری بود و به کشورهای عضو توصیه کرد قوانین کیفری خود را برای پوشش جرایم سایبری اصلاح کنند. دستورالعملی برای چنین اهدافی پیشنهاد شد و فهرستی از تخلفات تهیه شد تا سیاست‌ها و قوانین استانداردی را برای مقابله با جرایم مرتبط با رایانه مانند دسترسی و شنود غیرمجاز، کلاهبرداری و جعل رایانه‌ای، آسیب به داده‌ها یا برنامه‌های رایانه‌ای، خرابکاری رایانه‌ای و تکثیر غیرمجاز برنامهٔ رایانه‌ای محافظت شده ارائه دهد (Abdul Manap et al., 2015: 295).

در سال ۱۹۹۹ میلادی، شورای سازمان همکاری اقتصادی و توسعه مجموعه‌ای از رهنمودها را برای محافظت از تجارت الکترونیک تصویب کرد.[۲] با توجه به مشخصه شبه حقوقی این رهنمودها، این متون حاوی راه‌حل‌هایی برای جرم‌انگاری ابعاد خاصی از سرقت هویت نیستند، اما می‌توان آن‌ها را برای توسعه راهبردهایی به‌منظور جلوگیری از سرقت هویت به کار گرفت. در سال ۲۰۰۳ میلادی، این سازمان رهنمودهای دیگری را در خصوص ابعاد فرامرزی جرم جعل ارائه کرد.[۳] این رهنمودها نیز اشارهٔ صریحی به کیفیت جرم‌انگاری سرقت هویت ندارند، ولی می‌توانند برای توسعهٔ چارچوب جامعی برای تحقیقات قضایی و تعقیب این جرایم به کار روند. در سال ۲۰۰۸ میلادی، سازمان همکاری اقتصادی و توسعه «سند ارزیابی سرقت هویت آنلاین»[۴] را منتشر کرد که علاوه بر ارائهٔ تحلیل دقیقی از ترفندهای مختلف سرقت هویت در فضای اینترنت، به ابعاد مربوط به بزه‌دیدگان و کیفیت اجرای قانون می‌پردازد. همچنین در سال ۲۰۰۸ میلادی، OECD اقدام به انتشار «راهنمای سیاستگذاری در زمینهٔ سرقت هویت آنلاین» کرد.[۵] این راهنما نگاهی کلی دربارهٔ راهبردهای متفاوت برای واکنش به سرقت هویت در اینترنت ارائه می‌دهد.

بخش عمده‌ای از تمرکز سازمان همکاری اقتصادی و توسعه در این زمینه بر آموزش و افزایش آگاهی مصرف‌کنندگان، کسب‌وکارها، مقامات دولتی و رسانه‌ها در مورد سرقت هویت در فضای سایبر است تا از قربانی شدن آن‌ها جلوگیری شود و همچنین تلاش‌های دولت را برای مبارزه با چنین فعالیت‌های مجرمانه تسهیل کند. نحوهٔ عملکرد، وقوع و انواع جرایم رایانه‌ای منتشر می‌شود و مصرف‌کنندگان با سرقت هویت در فضای سایبر و روش‌های انجام آن مانند فارمینگ، اسمیشینگ و ویشینگ آشنا می‌شوند (OECD, 2008). نقش دولت در مبارزه با سرقت هویت در فضای سایبر بسیار حیاتی است و وجود یک تعریف مشترک از این موضوع در سیاست‌ها و راهبردهای کشورهای مختلف می‌تواند تأثیر زیادی داشته باشد. این موضوع به این دلیل اهمیت دارد که کشورها به شیوه‌های

---

۱. نمونهٔ این موارد، قطعنامهٔ تقویت پیشگیری از جرم سازمان ملل متحد است که بر «سرقت هویت» به‌مثابهٔ یکی از موضوعات سیاستگذاری نوظهور تأکید کرده که باید از طریق دفتر جرم و مواد مخدر سازمان ملل متحد پیگیری شود. مطابق قطعنامه‌های ۲۶/۲۰۰۴ و ۲۰/۲۰۰۷ مصوب شورای اقتصادی و اجتماعی سازمان ملل متحد، دفتر جرم و مواد مخدر سازمان ملل متحد گروهی از متخصصان را برای تبادل‌نظر در خصوص یافتن بهترین روش برخورد با این مسئله تشکیل داده است.

2. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce.

3 .OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders.

4. Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI،CP(2007)3،FINAL.

5. OECD Policy Guidance on Online Identity Theft.

متفاوتی به آن نگاه می‌کنند؛ برخی آن را به‌عنوان یک جرم می‌شناسند و برخی دیگر به‌عنوان یک مرحلهٔ مقدماتی برای ارتکاب جرایم دیگر در نظر می‌گیرند. این تفاوت در نگرش، یکی از دلایل اصلی متفاوت بودن قوانین مربوطه در کشورهای مختلف است. این تعاریف مختلف ناتوانی در دستیابی به اجماع از مفهوم سرقت هویت در فضای مجازی را نشان می‌دهد (Gercke, 2007: 13). این موضوع باید مورد توجه قرار گیرد تا امکان تهیهٔ پیش‌نویس قوانین جزایی واضح و بدون ابهام فراهم شود.

گستردگی اصطلاحات «سرقت هویت» و «تقلب هویتی» سبب می‌شود که نحوهٔ برخورد با آن‌ها متفاوت باشد. به همین دلیل، گروه کارشناسان بین‌دولتی سازمان ملل در سال ۲۰۰۷ پیشنهاد کرد که از اصطلاح «جرم هویتی» برای پوشش هر دو مورد استفاده شود. با این حال، این خود مشکل دیگری ایجاد می‌کند؛ زیرا در برخی کشورها این رفتارها هنوز جرم محسوب نمی‌شوند. تفاوت دیگر این است که بیشتر تعاریف بر عمل به دست آوردن اطلاعات تأکید دارند که دامنهٔ قوانین کیفری را به جاسوسی داده محدود می‌کند (Gercke, 2007: 13).

اتحادیهٔ اروپا؛ اگرچه اسناد حقوقی متعددی توسط اتحادیهٔ اروپا تهیه شده که به اطلاعات مرتبط با هویت مانند «دستورالعمل اتحادیهٔ اروپا در خصوص حریم خصوصی»[1] و نیز جرم‌انگاری جنبه‌های خاصی از جعل[2] و جرایم مرتبط با اینترنت همچون دسترسی غیرقانونی به سیستم‌های رایانه‌ای می‌پردازد[3]، اما هیچ‌یک از این اقدامات، قوانین و مقررات کیفری ویژهٔ سرقت هویت را شامل نمی‌شوند. با وجود این، پیشتر در سطح اتحادیهٔ اروپا چالش ناشی از فعالیت‌های مجرمانهٔ مرتبط به‌منزلهٔ موضوع درخور توجه در عرصهٔ سیاستگذاری شناخته شده بود. این در حالی است که کمیسیون اروپا پیشنهادی فراتر از آن داده بود که «همکاری نیروهای انتظامی اتحادیهٔ اروپا به شکل بهتری انجام گیرد، مشروط بر آنکه سرقت هویت در تمام کشورهای عضو به‌منزلهٔ جرم شناخته شود». این پیشنهاد فرصتی را برای ایجاد مشاوره‌هایی به‌منظور ارزیابی ضرورت تدوین قوانین خاص در کشورهای عضو هموار کرد و بیش از پیش توجه فضای عمومی اروپا را به پیشگیری و پاسخ مؤثر به سوءاستفاده از هویت برای مقاصد مجرمانه جلب کرد. این کمیسیون (از طریق ادارهٔ کل مربوط به عدالت، آزادی و امنیت) قبلاً در ژوئیهٔ ۲۰۰۷ پژوهشی تطبیقی دربارهٔ تعاریف سرقت هویت که در کشورهای عضو اتحادیهٔ اروپا استفاده شده و تبعات جنایی آن انجام داده است (Abdul Manap *et al.*, 2015: 294).

بیشتر کشورهای اروپایی دارای دو نوع قانون ضد سرقت هویت هستند؛ حفاظت از حریم خصوصی و محافظت در برابر جرایم اقتصادی و مالی. اگرچه تلاش زیادی برای هماهنگ کردن و یکسان‌سازی استانداردهای حفاظت از داده‌ها و حریم خصوصی انجام شده، تفاوت‌هایی به‌ویژه در زمینهٔ چارچوب‌های رویه‌ای و نهادی همچنان وجود دارد. یکی از قوانین مهم حریم خصوصی اتحادیهٔ اروپا، نقض حقوق اساسی حریم خصوصی و همچنین الزامات قانونی رسمی است. نقض حقوق اساسی حریم خصوصی شامل تخلفات ذیل است: ورود، تغییر یا جعل غیرقانونی داده‌ها با هدف آسیب به ذخیره‌سازی داده‌ها. چنین فعالیت‌هایی تحت پوشش جرایم عمومی اطلاعات و سایر قوانین مرتبط با حفظ حریم خصوصی قرار می‌گیرند. افشا، انتشار، به دست آوردن و یا دسترسی غیرقانونی به داده‌ها، فعالیت‌هایی هستند که تحت پوشش بیشتر قوانین، هرچند به درجات مختلف می‌باشند. با افزایش

1. Directive 95،46،EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
2. EU Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, 2001،413،JHA.
3. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

سریع جرایم رایانه‌ای در سطح جهانی، کشورها نیاز به معرفی قوانین جدید یا قوی‌تر برای مقابله با آن‌ها را احساس می‌کنند (Chawki & Abdel Wahab, 2006: 23).

شورای اروپا؛ شورای اروپا از سال ۱۹۴۹ فعالیت می‌کند. این شورا در سال ۱۹۹۰ گزارشی با عنوان «جرایم مرتبط با کامپیوتر»[1] منتشر کرد که حداقل جرایمی را که باید از طریق مداخلهٔ قانونی جرم‌انگاری شوند و همچنین، جرایمی که جرم‌انگاری آن‌ها اختیاری است، فهرست می‌کرد. از آنجا که فضای سایبری بدون مرز است، وجود هنجارها و استانداردهای جهانی برای تأمین امنیت در برابر جرایم این دنیای مجازی ضروری است. کنوانسیون شورای اروپا در مورد جرایم سایبری، گامی مهم در این زمینه به شمار می‌آید. هدف اصلی این کنوانسیون که در سال ۲۰۰۱ در بوداپست مجارستان توسط ایالات متحده و ۲۹ کشور دیگر امضا شد، هماهنگ‌سازی قوانین کیفری داخلی مربوط به فضای سایبری و همچنین رویه‌های تحقیقاتی است. تا اکتبر ۲۰۰۸، در مجموع ۴۵ کشور این کنوانسیون را امضا کرده و ۲۳ کشور اسناد آن را به تصویب رسانده بودند. این کنوانسیون امروزه به‌منزلهٔ سند بین‌المللی مهمی در مبارزه با جرایم سایبری شناخته شده و از طرف سازمان‌های بین‌المللی مختلفی پشتیبانی می‌شود (Abdul Manap *et al*., 2015: 291-292).

کنوانسیون شامل چهار بخش اصلی است که هریک دارای مقررات مربوط به خود است. بخش اول به تعریف اصطلاحات مختلفی مانند سیستم‌ها و داده‌های رایانه‌ای می‌پردازد و بیان می‌کند که کشورهای عضو باید اقداماتی را برای جلوگیری از جرایم مرتبط انجام دهند. در بخش دوم، الزامات و استانداردهای مربوط به رویه‌ها و تحقیقات که کشورهای عضو باید به آن‌ها پایبند باشند، تشریح شده است. بخش سوم دستورالعمل‌هایی را ارائه می‌دهد که همکاری بین‌المللی را از طریق تحقیقات مشترک در مورد جرایم مختلف که در بخش اول تعریف شده، تسهیل می‌کند. بخش پایانی به امضای کنوانسیون، کاربرد سرزمینی آن، اصلاحات و فدرالیسم مربوط می‌شود (Chawki & Abdel Wahab, 2006: 30). از جمله جرایم مهمی که این کنوانسیون به آن‌ها پرداخته و با سرقت هویت در فضای سایبر مرتبط است، می‌توان به دسترسی غیرقانونی (مادهٔ ۲)، شنود غیرقانونی (مادهٔ ۳)، اخلال در داده‌ها و سیستم (مواد ۴و۵)، سوءاستفاده از دستگاه‌ها (مادهٔ ۶) و کلاهبرداری مرتبط با رایانه (مادهٔ ۸) اشاره کرد.

پیش‌نویس کنوانسیون جرایم سایبری نیز به این نکته اشاره می‌کند که همکاری بین‌المللی برای مبارزه با جرایم سایبری ضروری است. فصل سوم این کنوانسیون از کشورهای امضاکننده می‌خواهد که تا حد امکان از طریق توافقات بین‌المللی، معاهدات و قوانین داخلی در رسیدگی به جرایم و ارائهٔ شواهد همکاری کنند.[2] همچنین شامل مقررات دقیقی برای همکاری متقابل در شرایطی است که هیچ توافقنامه‌ای برای همکاری وجود ندارد.[3] بدون شک، چنین رویکرد چندجانبه‌ای بهترین امید را برای مقابله با ماهیت فراگیر سرقت هویت در فضای سایبر ارائه می‌دهد.

در سال ۲۰۰۷ میلادی، شورای اروپا پژوهشی را منتشر کرد که طرق گوناگون جرم‌انگاری سرقت هویت مرتبط با اینترنت در آن بررسی شده بود. این پژوهش نشان داد که علی‌رغم قابلیت اجرای مقررات کیفری کنوانسیون جرایم سایبری در موارد سرقت هویت، مقررات ویژه‌ای وجود ندارد که صرفاً به سرقت هویت بپردازد و قابلیت اعمال در تمام رفتارهای مرتبط را داشته باشد (Gercke, 2007: 30).

1. Recommendation No. R (89)9 on computer related crime and final report of the European committee on crime problems, Strasbourg 1990.
2. Articles 23 and 25 of the Convention on Cybercrime
3. Article 27 of the Convention on Cybercrime

۴. ۵. رویکردهای ملی

همان‌گونه که گفته شد، برخی کشورها مقرراتی را وضع کرده‌اند که فراتر از شیوه‌های سنتی برای جرم‌انگاری کلاهبرداری یا جعل، به‌صراحت بر رفتارهای مرتبط با سرقت هویت متمرکزند.

ایالات متحده؛ در سال ۱۹۹۸ میلادی، کنگرهٔ ایالات متحده با تصویب «قانون منع سرقت و اتخاذ هویت غیرواقعی»[1] جرم‌انگاری ویژه‌ای در زمینهٔ رفتارهای مرتبط با سرقت هویت را در جلد ۱۸ مجموعه قوانین ایالات متحده- مادهٔ ۱۰۲۸ (الف)(۷) عرضه کرد. این قانون مجازات تا ۱۵ سال حبس و حداکثر ۲۵۰۰۰۰ دلار جزای نقدی را برای مرتکب در نظر گرفته و به بزه‌دیده اجازه داده است که متعاقب دعوای کیفری، خسارات ناشی از جرم را نیز مطالبه نماید. این قانون اختیارات لازم برای پیگیری دعاوی و کمک به بزه‌دیدگان را به کمیسیون تجارت فدرال اعطا کرده است (قناد، ۱۳۹۲: ۲۹۷-۲۹۸).

در پی افزایش حرکت‌های سیاسی پس از اتفاقات ۱۱ سپتامبر ۲۰۰۱، کنگرهٔ ایالات متحده تصمیم گرفت قوانین بیشتری را ارائه و در نهایت تصویب کند. در سال ۲۰۰۴ کنگره «قانون تشدید مجازات سرقت هویت»[2] را تصویب کرد (وندرمولن، ۱۳۹۷: ۸۱). به موجب این قانون، هرگونه انتقال، تملک و استفادهٔ غیرمجاز از هویت شخص ثالث به‌منظور ارتکاب جرایمی نظیر سرقت از عواید کارفرما، کلاهبرداری و مهاجرت غیرقانونی علاوه بر مجازات جرم اصلی، با دو سال حبس همراه خواهد بود و چنانچه اقدامات فوق به‌منظور ارتکاب جرایم تروریستی صورت گرفته باشد با پنج سال حبس علاوه بر مجازات اصلی جرم، پاسخ داده خواهد شد.[3] در نهایت، در سال ۲۰۰۸ میلادی «قانون سرقت هویت و جبران خسارت وارده»[4] که تمرکز آن بر رفع خلأهای قانونی موجود بود، توسط کنگره تصویب شد.

این مواد قانونی رویکردی گسترده در زمینهٔ جرم‌انگاری اشکال گوناگون سرقت هویت دارند و با جرم‌انگاری «انتقال» ابزار شناسایی به قصد ارتکاب جرم، امکان تعقیب جرایم مرتبط با مرحلهٔ سوم (فرایند انتقال) را که اغلب در رویکردهای سنتی مغفول می‌مانند، فراهم می‌آورد. حال نظر به اینکه مقررات مذکور بر تعامل مستقیم با داده‌های مرتبط با هویت متمرکز شده است، از این رو عملیات مقدماتی از قبیل ارسال رایانامه‌های فیشینگ و طراحی بدافزارهایی که بتوان از آن‌ها برای «به دست آوردن اطلاعات مرتبط با هویت از رایانه بزه‌دیدگان» استفاده کرد، در مادهٔ ۱۰۲۸ (الف)(۷) و مادهٔ A۱۰۲۸ (الف)(۱)و(۲) تحت پوشش قرار نگرفته است. «قانون سرقت هویت و جبران خسارت وارده» به دنبال رفع خلأهای قانونی نظیر جرم‌انگاری رفتارهای خاصی است که با نرم‌افزارهای جاسوسی و ثبت عملکرد کلیدها مرتبط باشد.

کانادا؛ در سال ۲۰۰۷ میلادی کانادا لایحهٔ قانونی را برای جرایم کیفری خاص مرتبط با سرقت هویت ارائه کرد.[5] این لایحه قانونی شامل دو مادهٔ کلیدی است: نخست، مادهٔ ۴۰۲,۱ که به تعریف اطلاعات مرتبط با هویت می‌پردازد و دوم، مادهٔ ۴۰۲,۲ شامل رفتارهایی است که جرم تلقی شده‌اند.

مادهٔ ۴۰۲,۱ مقرر می‌دارد که در راستای مفاد مواد ۴۰۲,۲ و ۴۰۳، «اطلاعات هویتی» به هر نوع اطلاعاتی از جمله اطلاعات زیست‌شناختی یا فیزیولوژیکی اطلاق می‌شود که اغلب به‌تنهایی یا در ترکیب با سایر اطلاعات به‌منظور شناسایی یک فرد استفاده می‌شود. این اطلاعات می‌تواند شامل مواردی مانند اثر انگشت، صدانگاشته، تصاویر شبکیه و عنبیه، نمونهٔ DNA، نام، نشانی، تاریخ تولد،

1. Identity Theft and Assumption Deterrence Act
2. Identity Theft Penalty Enhancement Act
3. 18 U.S.C. § 1028 A (a) (1), (2)
4. Identity Theft Enforcement and Restitution Act
۵. در اکتبر ۲۰۰۹، لایحهٔ S-4 به‌عنوان اصلاحیه‌ای بر قانون جزایی کانادا (سرقت هویت و سوء رفتار مرتبط با آن) به تصویب رسید. ر.ک: http://www.parl.gc.ca

امضای نوشتاری، امضای الکترونیکی و یا دیجیتال، نام کاربری، شماره (کارت نقدی و اعتباری، حساب مربوط به مؤسسهٔ مالی، گذرنامه، بیمهٔ اجتماعی، بیمهٔ سلامت و گواهینامه رانندگی) یا گذرواژه باشد.

به موجب مادهٔ ۴۰۲,۲:

۱. هر فردی که آگاهانه اطلاعات هویتی دیگران را به دست آورد یا نگهداری کند، اگر شواهد منطقی نشان دهد این اطلاعات به‌منظور استفاده در ارتکاب جرمی قابل‌تعقیب که متضمن کلاهبرداری، فریب یا دروغگویی است، تحصیل شده، مرتکب جرم شده است.

۲. هر فردی که اقدام به انتقال، در دسترس قرار دادن، توزیع، فروش یا عرضهٔ اطلاعات هویتی غیر کند یا این اطلاعات را برای هریک از این مقاصد در تصرف و تملک خود قرار دهد، با علم یا اعتقاد به اینکه این اطلاعات برای ارتکاب جرم قابل‌تعقیبی به کار خواهد رفت که متضمن کلاهبرداری، فریب یا کذب است، یا بی‌توجه بودن به این مسئله، مرتکب جرم شده است.

۳. در ارتباط با بخش‌های فرعی (۱)و(۲) مذکور، جرم قابل‌تعقیب که در هر یک از این بخش‌ها به آن اشاره شده، در یکی از بخش‌های زیر قرار می‌گیرد:

الف) بخش ۵۷ (جعل گذرنامه یا ارائهٔ گذرنامهٔ جعلی)؛

ب) بخش ۵۸ (استفادهٔ متقلبانه از گواهی شهروندی)؛

ج) بخش ۱۳۰ (فریب دادن مأموران انتظامی)؛

د) بخش ۱۳۱ (شهادت دروغ)؛

ه) بخش ۳۴۲ (سرقت، جعل و... کارت اعتباری)؛

و) بخش ۳۶۲ (تظاهر یا اظهارات کذب)؛

ز) بخش ۳۶۶ (جعل اسناد)؛

ح) بخش ۳۶۸ (ارائه، نقل‌وانتقال یا تملک عامدانهٔ مدرک جعلی)؛

ط) بخش ۳۸۰ (کلاهبرداری)؛

ی) بخش ۴۰۳ (جعل هویت).

این لایحهٔ قانونی شامل چندین رویکرد جالب توجه است؛ نخست آنکه در این مواد، مصادیقی برای اطلاعات هویتی ارائه می‌شود، بدون آنکه دامنه شمول مفاد آن محدود شود. به علاوه، این لایحه مجموعه‌ای از جرایم قابل‌تعقیب را معرفی می‌کند. اگرچه این اقدام از یک سو دامنهٔ شمول آن را محدود می‌سازد اما از سوی دیگر، راه‌حل بسیار دقیقی ارائه می‌دهد. در نهایت، این لایحه شامل گسترهٔ وسیعی از جرایم است. لایحهٔ کانادا مشابه رویکردی که ایالات متحده اتخاذ کرده، اعمال تمهیداتی مانند ارسال رایانامه‌های فیشینگ یا طراحی بدافزارها را در برنمی‌گیرد (Gercke, 2011: 42-43).

۵. رویکرد نظام کیفری ایران به جرم‌انگاری سرقت هویت

در نظام حقوقی ایران، قوانین خاصی که به‌طور صریح سرقت هویت را به‌عنوان یک جرم مستقل تلقی نموده باشند، مقرر نشده‌اند. قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای نیز در این مورد صراحتی ندارند، اما برخی مواد قانونی با موضوع مورد بحث مرتبط هستند که در ادامه به آن‌ها اشاره می‌کنیم.

استفاده از اسناد هویتی دیگری: جعل هویت می‌تواند از طریق استفاده از اسناد هویتی دیگری یا جعل در آن صورت پذیرد. اسناد هویتی مدارکی هستند که برای تعیین هویت افراد در جامعه به کار می‌روند؛ چه این مدارک از اسناد سجلی و شناسنامه باشند و یا اسناد دیگری که

می‌توانند در شناسایی استفاده شوند. برای مقابله با هرگونه سوءاستفاده از اسناد سجلی و شناسنامه، قانون خاصی تحت عنوان «قانون تخلفات، جرایم و مجازات‌های مربوط به اسناد سجلی و شناسنامه» در سال ۱۳۷۰ به تصویب مجمع تشخیص مصلحت نظام رسید که برای استفاده از شناسنامهٔ دیگری، دریافت شناسنامه موهوم و جعل هویت مجازات‌هایی را پیش‌بینی کرده است. مادهٔ ۱۰ این قانون نیز به بحث جعل در شناسنامه و اسناد سجلی پرداخته است. مادهٔ ۳۷ قانون گذرنامه مصوب ۱۳۵۱ در این زمینه تسلیم اسناد و مدارک خلاف واقع یا متعلق به غیر از روی علم و عمد به مراجع مربوطه را برای دریافت گذرنامه یا اسناد در حکم گذرنامه به نام خود یا دیگری جرم‌انگاری و برای آن مجازات تعیین کرده است. استفاده از شناسنامه دیگران برای رهایی از خدمت وظیفهٔ عمومی نیز در قانون اصلاح مادهٔ ۶۰ و الحاق دو تبصره به آن و اصلاح مادهٔ ۶۱ قانون خدمت وظیفهٔ عمومی مصوب ۱۳۶۳ و الحاق یک تبصره به آن مصوب ۱۳۶۸ جرم‌انگاری شده است. همچنین رأی دادن با شناسنامهٔ دیگری در مادهٔ ۶۶ قانون انتخابات مصوب ۱۳۷۸ جرم تلقی شده است.

غصب عناوین و مشاغل: بعضاً در روابط اداری و اجتماعی، افرادی خود را صاحب یکی از مناصب مهم نظامی، اداری، سیاسی و قضایی معرفی می‌کنند بدون اینکه دارای آن سمت و عنوان باشند و یا با استفاده از لباس‌های رسمی خود را مأمور نظامی و انتظامی معرفی می‌کنند و بدین طریق منافعی را برای خود یا دیگری به دست می‌آورند. به همین دلیل، قانونگذار به این مسئله توجه داشته و این اقدامات را در فصل هشتم قانون تعزیرات مصوب ۱۳۷۵ ذیل عنوان «غصب عناوین و مشاغل» جرم‌انگاری نموده است. این اقدامات به‌طور معمول با تحصیل غیرقانونی اطلاعات شخصی دیگری یا ابزارهای تشخیص هویت صورت می‌پذیرد. لباس رسمی، نشان، مدال یا سایر امتیازات دولتی و رسمی نشان از هویت دارندهٔ آن دارد. بنابراین، عمل فردی که با کسب اطلاعات شخصی و ابزارهای تشخیص هویت مأمور انتظامی، خود را به‌عنوان مأمور نظامی یا انتظامی معرفی کند سرقت یا جعل هویت است؛ چرا که در واقع هویت آن مأمور را به سرقت برده است (خالقی و صالح‌آبادی، ۱۳۹۴: ۱۰۷).

اختیار اسم یا عنوان مجعول: اختیار اسم یا عنوان مجعول از مصادیق تمثیلی متقلبانه است که قانونگذار در مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری برشمرده است. در سرقت هویت مرتکب به‌طور معمول بعد از سرقت اطلاعات شخصی افراد (به‌خصوص افراد معتبر و خوش‌حساب) خود را به‌جای آن‌ها معرفی نموده و بدین طریق از این اطلاعات در فعالیت‌های غیرقانونی اعم از مالی و غیرمالی استفاده می‌کند. بنابراین، فردی که بعد از سرقت اطلاعات شخصی دیگری و اتخاذ هویت او، دیگران را فریب داده و از این طریق موفق به بردن مال شود، عمل او مشمول کلاهبرداری مادهٔ مزبور خواهد بود. همین‌طور دخالت در امر انتخابات با سمت مجعول و یا به هر نحو غیرقانونی به موجب مادهٔ ۶۶ قانون انتخابات جرم‌انگاری شده است.

استفاده از مهر، علامت، تمبر و...: همان‌طور که اشاره شد، سرقت هویت از طریق سرقت ابزارهای تشخیص هویت و استفاده از آن‌ها در فعالیت‌های غیرقانونی انجام می‌شود. بنابراین، شاید بتوان با تعریفی موسع از ابزارهای تشخیص هویت، مهر، علامت، تمبر و... را نیز نوعی ابزار تشخیص هویت در نظر گرفت؛ چرا که علامت یا مهر مخصوص و مواردی از این قبیل، از هویت شخص حقوقی خاص حکایت دارد. بنابراین، اگر فردی مهر، تمبر و علامت شرکت، اداره، مؤسسه، دانشگاه و... را به دست آورد و از آن در فعالیت‌های غیرقانونی استفاده کند، نوعی سرقت هویت واقع شده است (سلیمان دهکردی و حیدریان، ۱۳۹۸: ۷۸). مادهٔ ۵۲۳ قانون مجازات اسلامی (تعزیرات) به‌طور کلی به کار بردن مهر دیگری بدون اجازهٔ صاحب آن را جعل تلقی کرده است. استفاده از علائم تجاری دیگران در مادهٔ ۶۶ قانون تجارت الکترونیکی مصوب ۱۳۸۲ نیز جرم‌انگاری شده است. همین‌طور عمل فردی که با سرقت مهر مخصوص پزشکی، از آن در سایر فعالیت‌های غیرقانونی استفاده می‌کند نوعی سرقت

هویت است. جعل گواهی پزشکی به اسم طبیب که در مادهٔ ۵۳۸ قانون مجازات اسلامی (تعزیرات) مورد جرم‌انگاری واقع شده، ممکن است از طریق استفاده از مهر پزشک انجام شود.

قلمداد کردن طفل به‌جای طفل دیگر: در جعل هویت اغلب خود فرد اقدام به جعل هویت و معرفی خود به‌جای دیگری می‌کند، ولی می‌توان مواردی را که جعل هویت توسط دیگران صورت می‌پذیرد، یافت. از جملهٔ این‌ها جعل هویت طفل تازه متولدشده است که برای طفل، هویت جدیدی غیر از هویت واقعی او اتخاذ می‌شود. این امر در مادهٔ ۶۳۱ قانون مجازات اسلامی (تعزیرات) مورد جرم‌انگاری واقع شده است.

شرکت در آزمون به‌جای دیگری یا شرکت دادن دیگری به‌جای خود: یکی از مواردی که می‌توان از آن به جعل یا سرقت هویت یاد کرد، شرکت در آزمون به‌جای دیگری است. با توجه به مادهٔ ۵۴۱ قانون مجازات اسلامی (تعزیرات)، می‌توان عمل فردی را که به‌جای داوطلب اصلی در آزمون شرکت می‌کند، جعل یا سرقت هویت دانست؛ چرا که در واقع مرتکب آگاهانه و بدون مجوز قانونی با اتخاذ هویت دیگری خود را به‌عنوان داوطلب معرفی نموده و از این طریق در آزمون شرکت می‌کند. هرچند که این کار با توافق و تبانی مرتکب و داوطلب اصلی انجام می‌گیرد، اما می‌توان عمل فردی را نیز که با تحصیل مدارک شناسایی داوطلب بدون رضایت او در آزمون شرکت می‌کند، مشمول این ماده دانست.

استبدال شخص (غصب هویت دیگری): استبدال شخص یا بدل دیگری واقع شدن نوع خاصی از جعل امضاست؛ بدین نحو که شخصی هویت دیگری را برای اضرار به او غصب می‌کند. امضا کردن ذیل سند به‌جای دیگری، به‌رغم درج امضای واقعی، جعل هویت غیر است. بنابراین، شخصی که به لحاظ هم‌نام بودن با دیگری خودش را به‌جای وی معرفی و با علم به اینکه حواله‌ای متعلق به دیگری است آن را امضا و دریافت می‌کند نیز مرتکب جعل هویت شده است. مادهٔ ۵۲۳ قانون مجازات اسلامی (تعزیرات) استبدال و جانشینی اشخاص را در امضا ولو با اجازهٔ آن‌ها، مجاز ندانسته و آن را به‌عنوان جعل تلقی کرده است.

سرقت هویت در قانون جرایم رایانه‌ای: مادهٔ ۱۲ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ سرقت رایانه‌ای را مورد جرم‌انگاری قرار داده است. رکن مادی این جرم، ربایش داده است که به معنای دست‌اندازی به داده دیگری است و یا با روگرفت (کپی) است یا برش (کات) که این رفتار باید در فضای سایبر انجام گیرد. رفتارهایی که جزء رکن مادی تشکیل‌دهندهٔ سرقت هویت است، استفاده از اطلاعات هویتی دیگری یا انتقال این اطلاعات به دیگری به‌منظور انجام کلاهبرداری یا سایر فعالیت‌های غیرقانونی است. ضمن اینکه به محض کپی یا برش داده دیگری سرقت رایانه‌ای تحقق می‌یابد و نیاز به بهره‌مندی از آن وجود ندارد، ولی در سرقت هویت باید از اطلاعات دیگری سوءاستفاده شود. همچنین سرقت رایانه‌ای اختصاص به فضای سایبر دارد اما سرقت هویت هم در فضای واقعی و هم در فضای سایبر می‌تواند تحقق یابد. بنابراین، سرقت هویت مشمول مقررات سرقت رایانه‌ای نمی‌شود؛ جز اینکه ممکن است در مواردی یکی از شیوه‌های دستیابی به اطلاعات دیگران از طریق ربودن داده صورت پذیرد که در این صورت با توجه به فقدان نص قانونی در خصوص سرقت هویت، عمل این فرد سرقت رایانه‌ای است (سلیمان دهکردی و حیدریان، ۱۳۹۸: ۸۱-۸۲).

در نهایت، می‌توان گفت که هرچند در حقوق ایران عناوین مشابه مانند جعل عناوین و سمت دولتی، سوءاستفاده از اسناد و نشان هویتی، جابه‌جایی هویت اشخاص و استبدال هویت از نظر قانونگذار مغفول نمانده و در قوانین پراکنده جرم‌انگاری شده‌اند، اما به نظر می‌رسد سرقت هویت که بار معنایی خاص دارد، مستلزم جرم‌انگاری مستقل باشد (خالقی و صالح‌آبادی، ۱۳۹۴: ۱۰۵و۱۱۲)؛ زیرا جرایم عامی که بر اساس آن‌ها مرتکب سرقت هویت مجازات می‌شود، هیچ‌یک به رفتار فیزیکی مرتکب

این جرم اشاره‌ای ندارد؛ برای نمونه در سرقت رایانه‌ای مرتکب خود را به‌جای شخص صاحب اطلاعات قلمداد نمی‌کند و تنها به برش و کپی اطلاعات دیگران اکتفا می‌کند. همچنین در کلاهبرداری رایانه‌ای، تنها یکی از نتایج این عمل که کسب سود و منافع مالی است، مورد توجه قرار می‌گیرد و دیگر پیامدهای سرقت هویت از جمله افتتاح حساب بانکی به نام صاحب اطلاعات را شامل نمی‌شود. در سایر جرایم مانند غصب عنوان نیز تفاوت‌های شایان توجهی در رفتار فیزیکی مشاهده می‌شود؛ زیرا در سرقت هویت، هویت فرد به‌طور واقعی غصب نمی‌شود، بلکه تنها اطلاعات هویتی افراد در فعالیت‌های غیرقانونی مورد سوءاستفاده قرار می‌گیرد (سلیمان دهکردی و حیدریان، ۱۳۹۸: ۸۳).

۶. نتیجه و پیشنهادها

سرقت هویت در جوامع وابسته به اطلاعات، مشکل پرهزینه‌ای است اما با اتخاذ تدابیر پیشگیرانه حل‌شدنی است. به سبب تنوع زیاد در شیوه‌های ارتکاب این نوع جرایم، یافتن عنوانی که تمام رفتارهای مختلف را در خود جای دهد، کار دشواری است. از نگرانی‌های اصلی کاربرد «سرقت هویت» این است که در بسیاری از موارد، مجرمان اقدام به برداشتن و انتقال اقلام ملموس و عینی نمی‌کنند، در حالی که این موضوع یکی از الزامات اساسی در بیشتر قوانین سرقت در سطح ملی به شمار می‌آید؛ در واقع، مجرمان هویت را به سرقت نمی‌برند بلکه از آن به‌عنوان ابزاری جهت انجام سایر فعالیت‌های غیرقانونی استفاده می‌کنند. با وجود برخی دیدگاه‌های جزم‌اندیشانه، عبارت «سرقت» واژهٔ دقیقی نیست؛ زیرا در پرونده‌های سرقت، به‌طور معمول مال‌باخته تنها بزه‌دیده این‌گونه جرایم است در حالی که در پرونده‌های سرقت هویت، شخصی که اطلاعات مرتبط با هویتش مورد سوءاستفاده قرار گرفته، لزوماً تنها قربانی این جرم نیست. همچنین استفاده از واژه «جرم» در بسیاری از موارد صرفاً یک چشم‌انداز به شمار می‌آید؛ چون بیشتر دولت‌ها هنوز قانونی در خصوص این نوع جرایم تصویب نکرده‌اند. قانون ایران نیز به تبعیت از کنوانسیون جرایم سایبری، سرقت هویت را پیش‌بینی نکرده است.

به هر حال، این رفتار مضر به دلیل آنکه علیه موضوعات مختلفی از جمله تجارت و اقتصاد الکترونیک سالم و منصفانه، حقوق مصرف‌کننده، حقوق رقابت و شفافیت بازارهای مالی انجام می‌پذیرد و از طرفی، جزو رفتارهای فنی و سیال به شمار می‌آید، از رفتارهای پرخطری است که باید توسط مقنن، جرم تلقی شود. البته بهبود واکنش‌های کیفری نسبت به سرقت هویت نیازمند اتخاذ تصمیمات و بازنگری‌های اساسی است:

۱. در ابتدا ضروری است تعریفی کلی و دقیق از اطلاعات هویتی ارائه شود. پاسخ به این موضوع، به زیرساخت‌های نظام حقوقی هر کشور و سنت‌های حقوقی آن وابسته است. نام‌های کاربری، گذرواژه‌ها و اطلاعات ورود به سیستم ممکن است به‌عنوان عناصر هویتی قانونی یک فرد شناخته نشوند اما نظر به اهمیت استفاده از این داده‌ها برای دسترسی به خدمات دیجیتال، باید در خصوص ضرورت گنجاندن این اطلاعات در تعریف قانونی تصمیم‌گیری شود؛

۲. لازم است رفتارهای مجرمانه دقیقاً مشخص شود که آیا اقداماتی مانند طراحی بدافزارها به‌منظور دستیابی به اطلاعات هویتی یا ارسال ایمیل‌های فیشینگ باید جرم‌انگاری شوند یا خیر؛

۳. برای احتراز از جرم‌انگاری افراطی، این جرم باید به رفتارهایی محدود شود که با جرایم متعددی در ارتباط هستند. رویکرد ایالات متحده و لایحهٔ قانونی کانادا نیز بر این ارتباط تأکید دارند؛

۴. در خصوص مؤلفهٔ روانی مدنظر قانون نیز باید تعیین تکلیف شود. رویکرد ایالات متحده و لایحهٔ قانونی کانادا بر این نکته تأکید دارند که مجرم باید با علم و آگاهی اقدام کرده باشد؛

۵. ضرورت دارد که شرایط قانونی و تکنیکی لازم برای بازگرداندن هویت، اعتبار و مال از دست رفتهٔ قربانی سرقت هویت فراهم شود لذا قانونگذار باید برای تضمین حقوق و آبروی از دست رفته، برای نهادهایی که به‌نوعی با هویت قربانی ارتباط دارند، الزاماتی وضع کند که وی را به صحنهٔ جامعه بازگردانند. البته جرم‌انگاری سرقت هویت تنها یکی از رویکردهای پاسخ به این پدیده است. راهبردهای دیگر به‌ویژه اقدامات پیشگیرانه، آموزش کاربران اینترنت، توسعهٔ روش‌های شناسایی ایمن‌تر و بهبود قوانین حفاظت از داده‌ها به همان اندازه حائز اهمیت هستند.

منابع

الف) فارسی

* قرآن کریم

۱. برهانی، محسن (۱۳۸۸). سیاست کیفری ایران در قبال روسپیگری. *فصلنامهٔ مطالعات راهبردی زنان*، پاییز، (۴۵)، ۷-۴۲.

۲. خالقی، ابوالفتح؛ صالح‌آبادی، زهرا (۱۳۹۴). مطالعهٔ سرقت هویت در حقوق فدرال آمریکا با نگاهی اجمالی به حقوق ایران. *دو فصلنامهٔ حقوق تطبیقی*، پاییز و زمستان، (۲)، ۸۷-۱۱۴.

۳. راغب اصفهانی، حسین بن محمد (۱۴۰۴ق). *المفردات فی غریب القرآن*. چ دوم، بی‌جا: دفتر نشر الکتاب.

۴. روسو، ژان ژاک (۱۳۶۶). *قرارداد اجتماعی یا اصول حقوق سیاسی*. چ سوم، ترجمهٔ منوچهر کیا، تهران: گنجینه.

۵. سلیمان دهکردی، الهام؛ حیدریان، ارشیاناز (۱۳۹۸). تبیین سرقت هویت در نظام کیفری ایران. *پژوهشنامهٔ حقوق فارس*، بهار، (۲)، ۶۳-۸۵.

۶. صالح‌آبادی، زهرا (۱۳۹۱). جرایم علیه هویت با تأکید بر فضای سایبر. *پایان‌نامهٔ کارشناسی ارشد*، دانشگاه قم، دانشکده حقوق.

۷. فراهیدی، خلیل بن احمد (۱۴۰۹ق). *کتاب العین*. چ دوم، قم: دار الهجره.

۸. قناد، فاطمه (۱۳۹۲). پیشگیری از سوءاستفاده‌های هویتی در فضای مجازی. *رهیافت‌های نوین پیشگیری از جرم (مجموعه مقالات پیشگیری از وقوع جرم- معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه)*، ج۲، تهران: روانشناسی و هنر.

۹. کاتوزیان، ناصر (۱۴۰۰). *فلسفهٔ حقوق*. ج۱، چ دوم، تهران: گنج دانش.

۱۰. محمودی جانکی، فیروز (۱۳۹۳). جرم‌انگاری حق‌مدار؛ با تأکید بر نظریهٔ آلمانی مصالح حقوقی. *فصلنامهٔ پژوهش حقوق کیفری، زمستان*، (۹)، ۸۳-۱۱۰.

۱۱. نقیبی، سید ابوالقاسم (۱۳۹۱). مؤلفه‌های کرامت انسان از منظر قرآن کریم. *فصلنامهٔ سراج منیر*، پاییز، (۸)، ۴۶-۶۱.

۱۲. وکیلی‌مقدم، محمدحسین (۱۴۰۰). بایسته‌های جرم‌انگاری در حقوق رقابت و رویکرد نظام‌های حقوقی نسبت به آن. *پژوهشنامهٔ حقوق کیفری*، بهار و تابستان، (۱)، ۲۳۷-۲۵۶.

۱۳. وندرمولن، نیکل اس. (۱۳۹۷). *سرقت هویت مالی*. ترجمهٔ جعفر جمالی، فرهاد عابدینی سعدآباد و الهام سلیمان دهکردی، چ اول، تهران: خرسندی.

ب) انگلیسی

14. Abdul Manap, N., Abdul Rahim, A., & Taji, H. (2015). Cyberspace Identity Theft: An Overview. *Mediterranean Journal of Social Sciences*, 6(4), 290-299.

15. Alagna, V. (2020). *A Comparative Analysis of Identity Theft within America and Australia.* An honors thesis presented to the Department of Criminal Justice, University at Albany.

16. Australasian Centre for Policing Research (ACPR) (2006). *Standardisation of Definitions of Identity Crime Terms: A Step towards Consistency*. Report Series No. 145.3.
17. Chawki, M., & Wahab, M. S. A. (2006). *Identity Theft in Cyberspace: Issues and Solutions*. Lex Electronica, Vol.11, No.1. available at: http:// www.lex-electronica.org.
18. Federal Trade Commission (FTC). (2007). *Consumer Fraud and Identity Theft Complaint Data*, January – December 2006.
19. Gercke, M. (2007). *Internet-related Identity Theft—A Discussion Paper*, Project on Cybercrime, Council of Europe.
20. Gercke, M. (2011). *Legal Approaches to Criminalize Identity Theft.* New York: United Nations Office on Drugs and Crime (UNODC). available at: http://www.unodc.org/Publications/Handbook on Identity- related Crime/ebooke.pdf.
21. Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR.
22. Koops, B-J & Leenes, R. (2006). *or ،Identity Fraud and ,Identity Theft related-Identity* nschutz und DatensicherheitDate ,*Crime*.
23. Lawson, P. (2011). *Identity-related Crime Victim Issues: A Discussion Paper. New York: United Nations Office on Drugs and Crime (UNODC).* available at: http://www.unodc.org/Publications/Handbook on Identity-related Crime/ebooke.pdf.
24. Mitchison, N., Wilikens, M., Breitenbach, L., Urry, R. & Portesi, S. (2004). *Identity Theft–A Discussion Paper*, Technical Report EUR 21098 EN, European Commission– Joint Research Centre.
25. Organization for Economic Co-operation and Development (OECD). (2008). *Scoping Paper on Online Identity Theft.* DSTI/CP(2007)3/FINAL, Directorate for Science, Technology and Industry.
26. Results of the Second Meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, 2007, E/CN.15/2007/8/Add. 3.
27. UK Cabinet Office (2002). *Identity Fraud: A Study*. London.