-- Journal of Criminal Law Research------
Spring 2025, 13 (50), 143-180
Jclr.atu.ac.ir
DOI: 10.22054/jclr.2025.84663.2744

ATU PRESS

Original Research
Received: 02/Mar/2025 *** Accepted: 06/Sep/2025
ISSN: 2345-3575
eISSN: 2476-6224

The Australian Criminal Justice System's Approach to the Criminalization of Identity Theft

Meysam Abbasi Lahroudi* Ph.D. student of Jurisprudence and Criminal Law, Tehran University of Shahid Motahari, Tehran, Iran

Mohammad Rasaei Assistant Professor, Department of Jurisprudence and Criminal Law, Tehran University of Shahid Motahari, Tehran, Iran

Mohammad Bahrami Khoshkar Associate Professor, Department of Jurisprudence and Private Law, Tehran University of Shahid Motahari, Tehran, Iran

Seyyed Abolghasem Naghibi Professor, Department of Jurisprudence and Private Law, Tehran University of Shahid Motahari, Tehran, Iran

Abstract

Identity theft has become a prominent issue in both media and public discourse and is recognized as one of the fastest-growing crimes globally. It is a national and international concern and often plays a central role in transnational crimes. Typically committed for the

* Corresponding Author: meysamabbasi004@gmail.com
How to Cite: Abbasi Lahroudi, M. , Rasaei, M. , Bahrami Khoshkar, M. and Naghibi, A. (2025). The Australian Criminal Justice System's Approach to the Criminalization of Identity Theft. *Journal of Criminal Law Research*, 13 (50), 143 - 180. doi: 10.22054/jclr.2025.84663.2744

purpose of fraud, identity theft involves an individual using another person's identity without their knowledge, posing a major challenge in the digital age. While identity-related crimes are not new, the digital era's increased access to and reliance on personal information has significantly facilitated their rise and ease of execution.

Perpetrators commonly use stolen personal information to withdraw money from bank accounts, open new accounts, or access services such as healthcare under the victim's identity. One of the most alarming aspects of identity theft is the broad spectrum of potential victims—including governments, companies, and individuals across all ages, genders, educational backgrounds, and income levels. The consequences can be severe, ranging from financial loss and psychological harm to a damaged credit rating, false criminal records, and extensive time and effort required to restore one's financial and legal standing.

In Australia, identity crime has recently emerged as a pressing issue within the criminal justice system, imposing significant costs on the national economy and often serving as a facilitator for more serious offences such as terrorism and human trafficking. In response, Australian authorities have undertaken considerable efforts to study identity crime and develop relevant laws at both federal and state levels.

This article represents the first study in our country to examine Australian laws on identity crime. By focusing on the criminalization of identity theft, the research contributes to broader criminal law scholarship. Analyzing the current legal frameworks used to prosecute identity crimes is essential for developing effective deterrents and

guiding law enforcement responses. Employing a descriptive-analytical method and relying on library resources, this study explains the concept of identity theft, explores the principles underpinning its criminalization, critically reviews Australian statutes, highlights the key features of different legal approaches, and identifies fundamental differences across jurisdictions.

The study's findings indicate that, despite increasing concern about the damaging consequences of identity theft, Australian jurisdictions have not yet fully criminalized the offence. Instead, the legal focus remains on preventing broader social harm through predicate offences—such as possessing or trading identity information—that lack clear mental elements tied to the accused's intent. These offences are not only overly broad in scope but also rest on a problematic theoretical foundation centered around the mere possession of information. This breadth shifts the responsibility of defining criminal boundaries from legislators to law enforcement, which risks undermining core principles of fairness and justice in criminal law. Consequently, secondary offences may overshadow the primary crimes they are meant to support.

Systematic efforts are needed to clearly define prohibited activities and avoid vague or misleading terminology. There must be a careful balance between protecting society and avoiding over-criminalization. To that end, lawmakers should provide clear, rational justifications for criminalizing specific behaviors. A standardized legal definition of identity crimes—something international bodies have yet to achieve—is crucial. Such a definition should incorporate the essential elements of identity crimes, including acquisition, production,

transfer, possession, and use of identity information. Establishing this foundation is vital for understanding identity theft and formulating effective prevention, prosecution, and compensation strategies.

Keywords: Criminal justice system, Australia, Criminalization, Identity theft, Identity crimes.

مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۱۲/۱۲ ** تاریخ پذیرش: ۱۴۰۴/۰۶/۱۵

ISSN: ۲۳۴۵-۳۵۷۵

eISSN: ۲۴۷۶-۶۲۲۴

-- فصلنامه علمی پژوهش حقوق کیفری ---------

دوره ۱۳، شماره ۵۰، بهار ۱٤۰٤، ۱٤۳-۱۸۰

Jclr.atu.ac.ir

DOI: 10.22054/jclr.2025.84663.2744

رویکرد نظام کیفری استرالیا به جرم‌انگاری سرقت هویت

میثم عباسی لاهرودی* دانشجوی دکتری فقه و حقوق جزا، دانشگاه شهید مطهری واحد تهران، تهران، ایران

محمد رسایی استادیار گروه فقه و حقوق جزا، دانشگاه شهید مطهری واحد تهران، تهران، ایران

محمد بهرامی خوشکار دانشیار گروه فقه و حقوق خصوصی، دانشگاه شهید مطهری واحد تهران، تهران، ایران

سید ابوالقاسم نقیبی استاد گروه فقه و حقوق خصوصی، دانشگاه شهید مطهری واحد تهران، تهران، ایران

چکیده

امروزه موضوع سرقت هویت مورد توجه رسانه‌ها و افکار عمومی قرار گرفته و به عنوان یکی از سریع‌ترین جرایم در حال رشد در سطح جهانی شناخته می‌شود. این مسئله در سطح داخلی و بین‌المللی حائز اهمیت است و می‌تواند عنصری محوری در جرائم فراملی باشد. در این پدیده‌ی مجرمانه که عمدتاً به منظور کلاهبرداری انجام می‌شود، فردی هویت متعلق به غیر را بدون آگاهی او مورد استفاده قرار می‌دهد و این موضوع به چالشی بزرگ برای جوامع عصر دیجیتال تبدیل شده است؛ قربانیان این جرم، خسارات مالی و روانی فاجعه‌باری را تجربه می‌کنند و پیامدهای آن برای جامعه بسیار گسترده است. از این رو، در سال‌های اخیر، حوزه‌های قضایی استرالیا نیاز به تصویب جرایمی تحت عنوان جرایم هویتی را احساس کرده‌اند. این مطالعه با روش توصیفی-تحلیلی و بهره‌گیری از منابع کتابخانه‌ای، ضمن تبیین مفهوم سرقت هویت و مبانی جرم‌انگاری آن، به بررسی و نقد جرایم مقرر در حقوق استرالیا می‌پردازد. یافته‌های پژوهش حاضر نشان می‌دهد که قانونگذاران استرالیا هنوز سرقت هویت را به طور دقیق جرم‌انگاری نکرده‌اند بلکه بیشتر به پیشگیری از آسیب‌های اجتماعی و خساراتی که ممکن است در نتیجه‌ی سوءاستفاده از اطلاعات شناسایی حاصل شود، توجه داشته‌اند. درک جرایم هویتی و بازنگری قوانین برای مقابله مؤثر با آن، پیام اصلی این مطالعه است.

کلیدواژه‌ها: نظام کیفری، استرالیا، جرم‌انگاری، سرقت هویت، جرائم مرتبط با هویت.

* نویسنده مسئول: meysamabbasi004@gmail.com

مقدمه

در حال حاضر، افراد نه با نام یا چهره‌شان بلکه به تدریج با انباشته‌ای از اسناد و یا ابزارهای تشخیص هویت معرفی می‌شوند. «هویت بر جنبه‌های مختلف زندگی از جمله پیوندهای خانوادگی، روابط اجتماعی، کار، تحرک، نحوه‌ی انجام معاملات، دسترسی به حقوق شهروندی و سوابق پزشکی افراد تأثیر می‌گذارد» (Ahmed, 2020: 12). به طور کلی، هویت به فرایند ارائه‌ی اطلاعات درباره‌ی یک شخص یا شیء اشاره دارد و به دلیل نقشی که در تمایز افراد یا اشیاء از یکدیگر ایفا می‌کند، از اهمیت زیادی برخوردار است. گرچه معنای هویت در نگاه اول ساده و بدیهی به نظر می‌رسد اما در واقع گزاره‌ای پیچیده است که سال‌ها توسط فیلسوفان، روان‌شناسان، حقوقدانان و جامعه‌شناسان به طور عمیق مورد بحث قرار گرفته است.

در مفهوم آکادمیک، جایشانکار اذعان دارد که هویت را می‌توان از سه جنبه‌ی شخصی، اجتماعی و قانونی دسته‌بندی کرد؛ هویت شخصی به «تجربیات خاص یک فرد برای درک خود» اشاره دارد در حالی که هویت اجتماعی به نحوه‌ی دیدگاه دیگر اعضای جامعه نسبت به فرد اطلاق می‌شود و معنای هویت قانونی، به رسمیت شناختن یک شخص یا نهاد از سوی قانون و اعطای حقوق و تکالیف به اوست (Jaishankar, 2008: 10). در دنیای امروز، داشتن این نوع هویت ضروری است؛ زیرا بدون یک هویت قانونی معتبر، پیگیری حقوق یا دسترسی به خدمات عمومی و خصوصی به راحتی امکان‌پذیر نیست. هویت‌ها به ویژه هویت‌های قانونی به دلیل مزایای بی‌شماری که به دارندگان خود ارائه می‌دهند، هدفی برای مجرمان قرار گرفته تا از این امتیازات بهره‌برداری کنند. توسعه‌ی اینترنت با «جوامع مجازی» و «تعاملات بدون چهره» ایجاب می‌کند که از این دارایی ارزشمند حفاظت شود.

جرایم مرتبط با هویت پدیده‌ی جدیدی نیست اما بدون شک، دسترسی به اطلاعات و وابستگی به آن در عصر دیجیتال موجب رونق این نوع جرایم شده و ارتکاب آن را نسبت به گذشته آسان‌تر نموده است. در این جرایم، مرتکب از اطلاعات شخصی افراد برای برداشت از حساب‌های بانکی، افتتاح حساب‌های جدید، دریافت خدمات پزشکی از بیمه‌ی

سلامت قربانی و غیره استفاده می‌کند (Ahmed, 2019: 155). یکی از خطرناک‌ترین جنبه‌های سرقت هویت، طیف وسیعی از قربانیان شامل دولت‌ها، شرکت‌ها و افراد با هر سن، جنسیت، تحصیلات، درآمد و موارد مشابه است (Lawson, 2011: 113-114). این پدیده می‌تواند تأثیرات مالی، روانی و غیره برای قربانیان به همراه داشته باشد؛ به طوری که باعث آسیب به رتبه‌ی اعتباری فرد، ایجاد سابقه‌ی کیفری به نام قربانی و صرف زمان و تلاش بسیار برای بازیابی سوابق معاملات یا تاریخچه اعتباری شود. موارد فوق نشان می‌دهند که سرقت هویت در عصر اطلاعات، یک مسئله‌ی چالش‌برانگیز بوده و نیاز به پیگرد قانونی دارد. اخیراً نظام کیفری استرالیا نیز با معضل جرایم هویتی مواجه گردیده است؛ این امر قربانیان را تحت تأثیر قرار داده، هزینه‌های قابل توجهی برای اقتصاد استرالیا به وجود آورده و اغلب جرایم جدی‌تر مانند تروریسم و قاچاق انسان را تسهیل می‌کند (MCLOC, 2008: 9). در این راستا، استرالیا تلاش بسیاری برای مطالعه‌ی تأثیرات جرم هویتی و تدوین قوانین ملی و ایالتی انجام داده است.[۱]

به طور کلی، مطالعه‌ی قوانین مرتبط با جرایم هویتی از اهمیت خاصی برخوردار بوده و در کشور ما این اولین نوشتاری است که به بررسی قوانین استرالیا در این زمینه می‌پردازد. همچنین، پژوهش حاضر با تمرکز بر جرم‌انگاری سرقت هویت به مطالعات حقوق کیفری کمک می‌کند؛ زیرا تحلیل قوانینی که امروزه برای تعقیب جرایم هویتی اعمال می‌شود، یک مؤلفه‌ی اساسی در توسعه‌ی بازدارنده‌های مناسب و پاسخ مجریان قانون به این جرایم است. در این مطالعه، مفهوم سرقت هویت و مبانی جرم‌انگاری آن مورد بحث واقع شده، سپس قوانین کیفری استرالیا برای مقابله با آن مورد ارزیابی قرار گرفته است. پژوهش حاضر نشان می‌دهد که جرایم حقوق استرالیا از نوع ناقص بوده و در نهایت، به بررسی انتقادی این جرایم می‌پردازد که بر نحوه‌ی جرم‌انگاری تخلفات مرتبط با هویت و مجازات‌های قانونی متمرکز است.

---

۱. برای نمونه، می‌توان به قوانین زیر اشاره نمود:

Criminal Law Consolidation (Identity Theft) Amendment Act 2003 (SA); Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 (NSW).

۱. مفهوم و ماهیت سرقت هویت

تاکنون تعریف جامع و مشترکی از سرقت هویت که مورد توافق اکثر حقوقدانان باشد ارائه نشده است. حتی اصطلاحی که برای توصیف این پدیده به کار می‌رود یکسان نیست؛ به عنوان مثال، در ایالات متحده «سرقت هویت» انواع جرایم هویتی را دربرمی‌گیرد[۱] در حالی که در بریتانیا و استرالیا به ترتیب از عباراتی مانند «کلاهبرداری هویت» و «جرم هویتی» برای تعریف این‌گونه جرایم استفاده می‌شود (Zulhuda & Mohamed, 2015: 171). از لحاظ تاریخی، همان‌طور که وانگ و هوانگ اشاره داشته اند، اصطلاح «سرقت هویت» برای توصیف جرایم علیه افراد و «کلاهبرداری هویت» در وصف جرایم علیه نهادهای جمعی مانند دولت و مؤسسات مالی استفاده می‌شود. اخیراً، گفته می‌شود که «سرقت هویت» برای تمایز عمل به دست آوردن و «کلاهبرداری هویت» برای سوءاستفاده از اطلاعات شناسایی به کار می‌رود (Wang & Huang, 2011: 5).

پیشینه‌ی سرقت هویت به سال ۱۹۶۴ برمی‌گردد (Komakula & Jagadeeshwar, 2021: 104)، هرچند عبارت چندان جالبی نیست. مسئله‌ی اصلی در اینجا ناتوانی قانونگذاران در توصیف صحیح رفتارهایی است که قصد جرم‌انگاری آن را داشته اند. مفهوم سرقت هویت به طور گسترده در بحث‌های مربوط به این جرایم مطرح شده است.[۲] به هر حال، این تشبیه نادرست است؛ زیرا سرقت هویت در واقع، قربانی را از هویت خود محروم نمی‌کند. به عبارت دیگر، واژه‌ی «سرقت» به‌خودی‌خود به «بردن مال متعلق به غیر به قصد سلب مالکیت واقعی او» اشاره دارد در حالی که آسیب ناشی از سرقت هویت بیشتر به دلیل استفاده از هویت مسروقه است تا خود عمل سرقت. بنابراین، اصطلاح «سرقت»

---

۱. ایالات متحده‌ی آمریکا اولین کشوری است که در سال ۱۹۹۸ به موجب قانون فدرال به این رفتار، وصف مجرمانه مستقل بخشیده است (سلیمان دهکردی و حیدریان، ۱۳۹۸: ۶۳). به موجب ماده‌ی ۱۰۲۸ (الف)(۷) از جلد ۱۸ مجموعه قوانین ایالات متحده، سرقت هویت بدین صورت تعریف شده است: «انتقال، تملک یا استفاده‌ی آگاهانه و بدون مجوز قانونی از ابزار شناسایی دیگری به قصد ارتکاب یا معاونت، تحریک یا ارتباط داشتن با هرگونه فعالیت غیرقانونی که به منزله‌ی نقض قانون فدرال باشد یا به موجب هر کدام از قوانین قابل اجرای ایالتی یا محلی جرم محسوب شود».

۲ Identity Theft and Assumption Deterrence Act 1998 (US Legislation); Criminal Law Consolidation (Identity Theft) Amendment Act 2003 (SA).

می‌تواند باعث سردرگمی میان متهمان، دادستان‌ها و قضات شود؛ به ویژه زمانی که جرم در چندین حوزه‌ی قضایی رخ دهد و حال آنکه طبق معیارهای دادرسی عادلانه، به‌کارگیری اصطلاحات دقیق ضروری است تا متهمان بتوانند در برابر اتهامات از خود دفاع کنند (Ahmed, 2020: 49).

سازمان همکاری اقتصادی و توسعه[1]به عنوان یک مرجع بین‌المللی، نحوه‌ی ارتکاب سرقت هویت را این‌گونه شرح می‌دهد: «سرقت هویت زمانی تحقق می‌یابد که مرتکب به تحصیل، انتقال، تصرف و یا استفاده‌ی غیرمجاز از اطلاعات شناسایی اشخاص حقیقی یا حقوقی مبادرت نماید؛ بدین منظور که کلاهبرداری یا جرایم دیگری را مرتکب شده و یا اقدامی مرتبط با این اهداف انجام دهد» (OECD, 2008: 3). همچنین، توافق‌نامه‌ی شورای دولت‌های استرالیا در آوریل ۲۰۰۷ پیرامون استراتژی امنیت هویت ملی[2]شامل تعاریفی است که توسط مرکز تحقیقات پلیس استرالیا[3]بیان شده است. به موجب این توافق‌نامه:

«**جرم هویت**» یک اصطلاح عمومی برای توصیف فعالیت‌ها یا جرایمی است که در آن مرتکب از هویت‌های ساختگی، دستکاری شده یا مسروقه/ اتخاذشده برای تسهیل ارتکاب جرم استفاده می‌کند.

«**کلاهبرداری هویت**» به معنای کسب پول، کالا، خدمات یا سایر مزایا و همچنین اجتناب از تعهدات با هویت‌های جعلی، دستکاری‌شده یا مسروقه/ اتخاذشده است.

«**سرقت هویت**» عبارت است از سرقت یا اتخاذ هویت «قبل از موجودیت» (یا بخش مهمی از آن)، با یا بدون رضایت قربانی و صرف نظر از اینکه آن شخص در قید حیات باشد یا نباشد (COAG, 2007: 2-3; ACPR, 2006: 15).

---

1. Organization for Economic Co-operation and Development (OECD).

۲. The April 2007 Council of Australian Governments (COAG) Agreement to a National Identity Security Strategy (NISS).

۳. Australasian Centre for Policing Research (ACPR).

به طور کلی، تعاریف فوق حاوی عناصر کلیدی مشترک است که عبارتند از: موضوع سرقت هویت (داده یا اطلاعات هویتی[۱])، رفتار مجرمانه (کسب داده، استفاده یا دستکاری آن و غیره)، عنصر روانی (قصد به دست آوردن، استفاده از اطلاعات و...) و بالأخره، نداشتن اجازه از بزه‌دیده. چهار عنصر یادشده برای پیشنهاد هر متن قانونی کیفری و تعریف ساختار آن ضروری به نظر می‌رسد (Gercke, 2011: 31).

فنون مختلفی برای کسب اطلاعات هویتی وجود دارد که از شیوه‌های بسیار ساده تا پیچیده، متغیر است. در روش دیجیتال، مجرمان از تاکتیک‌های مختلفی استفاده می‌کنند؛ از جمله:

- **فیشینگ:** «یک سازکار جنایی که از ترکیب مهندسی اجتماعی و فریب‌های فنی برای سرقت اطلاعات و اعتبارنامه‌های مالی مصرف‌کنندگان استفاده می‌کند» (Jaishankar, 2008: 11).

- **اسکیمینگ:** «کپی‌برداری از اطلاعات نوار مغناطیسی کارت‌های اعتباری حین خرید کالا یا برداشت وجه از دستگاه‌های خودپرداز» (Wang & Huang, 2011: 8).

- **هک:** «استفاده غیرمجاز از رایانه و داده‌های سیستم» یا به عبارت دیگر، «تغییر عملکرد برنامه‌ها و نرم‌افزارهای کامپیوتری به منظور دستیابی به هدفی خارج از هدف اصلی سازنده» (Kumar & Agarwal, 2018: 2253).

- **نرم‌افزارهای مخرب:** «هر نوع نرم‌افزاری که برای مختل کردن عملکرد عادی سیستم، جمع‌آوری اطلاعات حساس یا دسترسی به سیستم‌های رایانه‌ای به کار می‌رود» (Jain & Bajaj, 2014: 931).

---

۱. به طور کلی، اطلاعاتی که توسط قوانین ملی حمایت می‌شود و معمولاً هدف مجرمان هویتی قرار می‌گیرد، سه دسته است:

۱) نام، نشانی، تاریخ تولد، وضعیت تأهل، گواهی فوت، کارت شناسایی، گذرنامه یا اسناد مهاجرتی، گواهینامه‌ی رانندگی، شماره‌ی تأمین اجتماعی، شماره‌ی بیمه‌ی سلامت، اثر انگشت، صدانگاشته، تصویر شبکیه یا عنبیه و نمونه‌ی DNA؛

۲) شماره کارت اعتباری یا نقدی، شماره حساب مؤسسات مالی، امضای مکتوب و مانند آن؛

۳) رمز عبور رایانامه یا مرورگرهای وب، نشانی Mac یا IP، امضای الکترونیکی یا دیجیتال و نام کاربری (Martins de Almeida, 2011: 65).

همچنین، روش‌های غیر دیجیتال شامل مواردی مانند تغییر نشانی پستی که به مجرمان امکان می‌دهد به مدارک ارسالی از این طریق دسترسی پیدا کنند، سرقت کیف پول و گذرنامه، زباله‌گردی، استفاده از اطلاعات موجود در دسترس عموم که در کتاب‌ها یا روزنامه‌ها و مواردی از این قبیل موجود است و حملات خودی‌ها مانند رشوه دادن به کارکنان برای دستیابی به اطلاعات هویتی بزه‌دیدگان است (Gercke, 2011: 15-16).

در مجموع، ماهیت جرایم هویتی بسته به نحوه‌ی استفاده‌ی مجرمان متفاوت است که می‌تواند به مقاصد مالی و غیرمالی مربوط باشد؛ به عنوان مثال، مرکز بین‌المللی بازنگری قوانین و سیاست عدالت کیفری[1] دریافته است که مجرمان هویتی از اطلاعات شناسایی اشخاص در فعالیت‌های غیرقانونی زیر استفاده می‌کنند:

۱) فروش اطلاعات به سایر مجرمان برای ارتکاب جرایم هویتی؛

۲) دسترسی و استفاده از کارت‌های اعتباری یا نقدی قربانیان و تصاحب حساب‌های بانکی آن‌ها؛

۳) افتتاح حساب‌های مالی جدید و اخذ وام به نام قربانی؛

۴) دریافت گذرنامه یا سایر مدارک شناسایی، بهره‌برداری از مزایا و خدمات دولتی به نام قربانی؛

۵) پنهان کردن هویت خود در سفرهای غیرقانونی، قاچاق مواد مخدر، پول‌شویی، تروریسم و غیره؛

۶) گمراه کردن و فریب مجریان قانون با سوق دادن آن‌ها به سوی افراد بی‌گناه (ICCLR, 2011: 6-7).

۲. تأملی بر مبانی جرم‌انگاری سرقت هویت

جرم‌انگاری در هر نظام حقوقی بر پایه اصول و مبانی فکری خاص آن نظام شکل می‌گیرد که دولت‌ها با بهره‌گیری از آن به تعیین رفتارهای مجاز و ممنوع می‌پردازند. از شیوه‌های حفظ و حمایت از اهداف، منافع و ارزش‌های حاکم توسط دولت‌ها توسل به حقوق کیفری

---

۱. International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR)

و ضمانت اجراهای آن است. اینک پیرامون مسئله‌ی سرقت هویت، این سؤال مطرح می‌شود که چه دلایلی مداخله‌ی کیفری در این حوزه را توجیه می‌کند و در ادامه، به بررسی آن خواهیم پرداخت.

نظریه‌ی حقوق فطری: بر اساس این نظریه، تمامی انسان‌ها دارای حقوق اساسی هستند که برتر از خواست و اراده‌ی دولت‌هاست (کاتوزیان، ۱۴۰۰: ۳۸/۱). از جمله‌ی این حقوق می‌توان به حق حیات و حق بهره‌مندی از زندگی خصوصی اشاره نمود. از این دیدگاه، انسان اولاً و بالذات آزاد و رها خلق شده است لذا همین آزادی و رهایی اولیه اقتضا دارد که اولاً، فرد بتواند از آگاهی و اطلاع دیگران درباره‌ی جنبه‌های مختلف زندگی خود جلوگیری کند و اجازه ندهد دیگران به کاوش در اطلاعات شخصی او بپردازند. ثانیاً، در صورت تمایل بتواند از مداخله‌ی سایرین در زندگی خصوصی خود ممانعت به عمل آورد (صالح‌آبادی، ۱۳۹۱: ۶۹). بر این اساس، هر نوع مداخله در زندگی افراد از جمله دسترسی به اطلاعات و استفاده‌ی غیرمجاز از هویت دیگران به عنوان نقض حقوق طبیعی آن‌ها تلقی می‌شود.

نظریه‌ی 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: ۴۱۱/۱-۴۱۲). حقوق نیز اخلاق را هدف و راهنمای خود در قاعده‌گذاری می‌داند. از آنجا که حمایت از افراد و حریم خصوصی‌شان از سوی اخلاق مورد تأکید قرار گرفته است (صالح‌آبادی، ۱۳۹۱: ۷۰)، اقدام فردی که بدون کسب اجازه به حریم دیگری وارد می‌شود و به اطلاعات او دسترسی پیدا می‌کند، از منظر اخلاقی ناپسند و قبیح است لذا تدوین چارچوب‌های قانونی مبتنی بر اصول اخلاقی به منظور حفاظت از حریم خصوصی اطلاعات شهروندان و حفظ کرامت آنان امری ضروری به شمار می‌آید.

نظریه‌ی قرارداد اجتماعی: بر اساس این نظریه 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 قراردادها تحت عنوان

قرارداد اجتماعی است که قدرتی فرافردی (حکومت) در جامعه ایجاد می‌کند (روسو، ۱۳۶۶: ۱۸). یکی از مواردی که در این قرارداد بر آن توافق می‌شود، ضرورت حمایت 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 در نظر می‌گیرند، آزاد بودن از هرگونه نظارت و مداخله‌ی دیگران در جنبه‌های مختلف زندگی از جمله اطلاعات شخصی آن‌هاست. استناد به نظریه‌ی قرارداد اجتماعی، این زمینه را فراهم می‌سازد که نه تنها وقوف دیگران بر اطلاعات شخصی بلکه هر نوع استفاده‌ی مادی از آن نیز قابل منع باشد لذا حکومت باید قوانینی را تصویب و اجرا کند که به حفظ حقوق و حریم خصوصی افراد، هویت و هر آنچه به آن‌ها مربوط می‌شود، بپردازد (صالح‌آبادی، ۱۳۹۱: ۷۲-۷۱).

حمایت از شأن، منزلت و کرامت انسانی: کرامت انسانی بنیان بسیاری از حقوق، امتیازات و تکالیف به شمار می‌آید که در آموزه‌های دینی و اسناد بین‌المللی بر اهمیت آن تأکید شده و به معنای احترام به فرد است. این موضوع نه تنها یک حق بلکه ویژگی ذاتی انسان به شمار می‌آید که بر پایه‌ی دو خصوصیت عقل و اختیار او استوار است. به طور کلی، سرقت هویت می‌تواند به مشکلات جدی در ایجاد یا حفظ اعتبار، اشتغال، مسکن، بیمه، گواهینامه‌ی رانندگی، گذرنامه و دیگر اسناد 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، به ویژه هنگامی که قربانیان به دلیل جرایمی که هرگز مرتکب نشده‌اند، بازداشت می‌شوند (Lawson, 2011: 123). علاوه بر این، دسترسی به اطلاعات شخصی به عاملی برای نقض آزادی و استقلال انسان‌ها، استفاده‌ی ابزاری و سلطه بر آن‌ها تبدیل شده است لذا قانونگذار باید با جرم‌انگاری این پدیده از شأن، منزلت، آزادی و استقلال افراد حمایت به عمل آورد.

بدون شک، ماهیت شدید و رنج‌آور مداخله‌ی حقوق کیفری و پیامدهای زیانبار واکنش‌های متنوع آن نسبت به جرم از یک‌سو و تمایل فزاینده‌ی قدرت عمومی به گسترش

اختیارات خود از سوی دیگر، ضرورت وجود نظریه‌ی جرم‌انگاری را ایجاب می‌کند (محمودی جانکی، ۱۳۹۳: ۸۴). نظریه‌ی جرم‌انگاری در نظام‌های حقوقی گوناگون عمدتاً بر پایه‌ی اصل ضرر[1]استوار است؛ طبق این اصل، رفتارهایی که به جامعه و افراد آن آسیب می‌زند باید توسط مقنن 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 فوق‌الذکر و خسارات هنگفتی که از سرقت هویت حاصل می‌شود، هر آنچه موجب سوءاستفاده از هویت افراد گردد، باید ممنوع شود و برای آن‌ها مجازات تعیین شود.

۳. پیشینه‌ی قوانین مرتبط با سرقت هویت در استرالیا

جرایم هویتی در قوانین موضوعه در سطح فدرال و سراسر ایالت‌های استرالیا به چشم می‌خورد. ایالت استرالیای جنوبی در این زمینه پیشگام بوده و در سال ۲۰۰۳ نخستین مقررات را وضع نمود[2]که نمایانگر یکی از سه مدل‌های تقنینی متمایز در این قاره است. مدل دوم، چهار سال بعد در کوئینزلند ایجاد شد.[3]مقررات مشابهی بین سال‌های ۲۰۰۹ تا ۲۰۱۱ در نیوساوت‌ولز،[4] ویکتوریا،[5] استرالیای غربی[6] و سطح فدرال[7] بر اساس مدل کوئینزلند مصوب گردید که سومین مدل قانونی را معرفی می‌کند. در تاریخ ۱۰ اکتبر ۲۰۱۲، لایحه‌ای به پارلمان مشترک‌المنافع ارائه شد که پیشنهاد وضع جرایم هویتی جدید

1. The Harm principle.

۲ Criminal Law Consolidation (Identity Theft) Amendment Act 2003 (SA).

۳ Criminal Code and Civil Liability Amendment Act 2007 (Qld).

۴ Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 (NSW).

۵ Crimes Amendment (Identity Crime) Act 2009 (Vic).

۶ Criminal Code Amendment (Identity Crime) Act 2010 (WA).

۷ Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011.

را مطرح نمود.[۱]این لایحه در ۲۸ نوامبر ۲۰۱۲ مورد تأیید قرار گرفت و مفاد آن از روز بعد به اجرا درآمد.[۲]

دو عامل به پیشبرد وضع قوانین مرتبط با جرایم هویتی در دولت استرالیا کمک کرد که به افزایش تخلفات هویتی در سطح داخلی و همچنین، به عنوان بخشی از تروریسم و جرایم فرامرزی مربوط می‌شد.[۳]طبق برآورد مؤسسه‌ی جرم‌شناسی استرالیا[۴]یک چهارم از کلاهبرداری‌های گزارش‌شده به پلیس فدرال استرالیا مبتنی بر هویت‌های جعلی بود که این آمار، شیوع تقلب هویتی در مقایسه با سایر جرایم را نشان می‌داد (AIC, 2002: 3). همچنین، آمار تحقیقاتی سازمان صنعت اوراق بهادار آسیا و اقیانوسیه[۵]در سال ۲۰۰۳ نشان داد که در سال‌های ۲۰۰۲ - ۲۰۰۱ تقلب هویتی منجر به خسارتی معادل ۱,۱ میلیارد دلار برای کسب‌وکارهای بزرگ شده است (Cuganesan & Lacey, 2003: 55).

در دو دهه‌ی گذشته، نگرانی‌هایی پیرامون جرایم هویتی در استرالیا وجود داشته است. کمیته‌ی ویژه‌ی مقامات حقوق کیفری[۶]متذکر شد که این مسئله برای جامعه‌ی استرالیا اعم از افراد، نهادهای دولتی و خصوصی، سازمان‌های اجرای قانون و مؤسسات مالی بسیار حائز

---

۱ Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Bill 2012 (Cth).

۲ Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Act 2012 (Cth) s 2(1).

۳. این دو عامل در نشریات وابسته به مراکز تحقیقاتی پارلمان کوئینزلند (Dixon, 2005: 1-2)، نیوساوت‌ولز (Lozusic, 2003: 1-2) و ویکتوریا (Higgins, 2009: 2) گزارش شده است. در برخی تحقیقات، شیوع تخلفات هویتی به عوامل متعددی نسبت داده شده است؛ از جمله افزایش سرعت انتقال اطلاعات، جهانی شدن، استفاده‌ی بیشتر از ارتباطات راه دور برای انجام معاملات غیرحضوری به جای تعاملات سنتی رو در رو، سهولت جعل اسناد با روش‌های پیشرفته، جمع‌آوری و انتشار گسترده‌ی داده‌ها توسط بخش خصوصی و سایر سازمان‌ها که امکان دسترسی آسان به اطلاعات شخصی را فراهم می‌کند (Lozusic, 2003: 11-13).

۴Australian Institute of Criminology (AIC).

۵Securities Industry Research Centre of Asia-Pacific (SIRCA).

۶Model Criminal Law Officers' Committee (MCLOC);

این کمیته در سال ۱۹۹۰ با هدف توسعه یک قانون جزای ملی در حوزه‌های مختلف استرالیا و به طور کلی، مشاوره در مسائل حقوق کیفری توسط کمیته‌ی دائمی دادستان‌های کل تأسیس شد.

اهمیت است. از این رو، کمیته‌ی دائمی دادستان‌های کل[۱] در ژوئیه ۲۰۰۴ به MCLOC دستور داد تا به بررسی موضوع سرقت هویت بپردازد. پس از یک دوره رایزنی کلی، کمیته‌ی ویژه‌ی مقامات حقوق کیفری گزارش نهایی خود را در مارس ۲۰۰۸ ارائه نمود که در آن به تصویب سه جرم تحت عناوین «معامله‌ی اطلاعات شناسایی»، «نگهداری اطلاعات شناسایی با قصد ارتکاب یا تسهیل ارتکاب یک جرم قابل تعقیب» و «نگهداری تجهیزات تولید اطلاعات شناسایی در شرایط خاص» توصیه گردید (MCLOC, 2008: para 6). این کمیته همچنین به برخی «تأثیرات نامشهود» از جمله دسترسی به اسناد مهاجرتی، مزایای بیمه‌ی تأمین اجتماعی، کسب مدارک وابستگی حرفه‌ای و ارتکاب جرایم هویتی توسط گروه‌های سازمان‌یافته برای تسهیل فعالیت‌هایی مانند قاچاق انسان و تروریسم اشاره کرد (MCLOC, 2008: para 2.4). متعاقب گزارش مزبور، این سه رفتار در قوانین فدرال و ایالتی هرچند به طور غیر جامع جرم‌انگاری شد.[۲]

بدین ترتیب، مدل سوم که به آن اشاره گردید، منعکس‌کننده‌ی جرایم پیشنهادی MCLOC است.[۳] مقررات استرالیای جنوبی با وجود جرم «اخذ هویت جعلی» که به این حوزه قضایی تعلق دارد، متمایز می‌گردد.[۴] همچنین در این ایالت، جرم سوءاستفاده از اطلاعات شناسایی[۵] و مجموعه‌ای از جرایم مرتبط با تولید، نگهداری و توزیع «مواد

---

۱ Standing Committee of Attorneys-General (SCAG);

این کمیته متشکل از دادستان کل استرالیا، وزیر امور داخلی، دادستان‌های کل ایالت‌ها و وزیر دادگستری نیوزیلند است که به تسهیل همکاری در اهداف مشترک می‌پردازد.

۲. پژوهشگران قبل از تصویب قوانین جدید، تعدادی از جرایم موجود در دولت مشترک‌المنافع و ایالت‌ها را شناسایی کردند که تا حدی به سوءاستفاده‌ی هویتی مربوط می‌شد. فهرستی گسترده هرچند غیر جامع از این جرایم در گزارش نهایی MCLOC ارائه شد (MCLOC: paras 5.4-5.5) که شامل سرقت، جعل و همچنین برخی جرایم سایبری بود اما در پوشش آن خلأهایی وجود داشت؛ چراکه نیاز به اثبات عمل مجرمانه‌ی دیگری داشتند و در جرایم خاص هویتی قابل اعمال نبودند. از این رو، MCLOC این سه جرم را مورد تأکید قرار داد (ibid: para 6).

۳ Criminal Code Act 1995 (Cth) ss 372.1, 372.2 and 372.3; Crimes Act 1900 (NSW) ss 192J-92L; Crimes Act 1958 (Vic) ss 192B-92D; Criminal Code Act Compilation Act 1913 (WA) ss 490-92.

۴ Criminal Law Consolidation Act 1935 (SA) s 144B.

۵ ibid s 144C.

ممنوعه»[۱]تعریف شده که از نظر محتوا تشابهاتی با جرایم موجود در سایر حوزه‌های قضایی دارند. ایالت کوئینزلند در ابتدا یک ماده‌ی قانونی تصویب کرد که به طور خاص رفتارهایی مانند معامله و نگهداری اطلاعات شناسایی را مجازات می‌کرد[۲]اما بعد جرم داشتن تجهیزات را نیز به لیست خود اضافه نمود.[۳]

٤. بررسی جرایم مرتبط با هویت

به دلیل وجود تفاوت‌های جزئی در حوزه‌های قضایی مختلف، توصیف جرایم استرالیا دشوار است اما همان‌طور که استیل بیان می‌کند، «توافق اساسی در تعاریف اصلی و نوع رفتارهای ممنوعه وجود دارد» (Steel, 2010: 509). این مطالعه چارچوبی مناسب برای تحلیل و ارزیابی دقیق‌تر جرایم ارائه می‌دهد.

۱-٤. اتخاذ هویت جعلی

در ایالت استرالیای جنوبی، اخذ هویت جعلی با قصد ارتکاب یا تسهیل ارتکاب یک جرم جدی،[۴]جرم محسوب می‌شود. همچنین، ادعای نادرست مبنی بر داشتن مدارک یا حق انجام وظیفه در یک مقام خاص با همین نیت جرم است.[۵]گرچه این مقرره جرم را به معنای عام «تظاهر دروغین» توصیف می‌کند[۶]اما مفهوم «فریبکاری» را به رفتارهای مورد اشاره محدود می‌نماید.[۷]

---

۱ ibid s 144D.

۲ Criminal Code Act 1899 (Qld) s 408D (1).

۳ ibid s 408D (1A).

۴. «جرم جدی» به معنای جرم قابل تعقیب قضایی یا جرمی است که به موجب مقررات خاص وضع شده است (Criminal Law Consolidation Act 1935 (SA) s 144A).

۵ Criminal Law Consolidation Act 1935 (SA) s 144B.

۶ ibid s 144B (3).

۷ ibid s 144B (1).

یک فرد زمانی هویت جعلی به خود می‌گیرد که وانمود کند شخص دیگری است، چه آن شخص در قید حیات باشد یا نباشد، واقعی، ساختگی، حقیقی یا حقوقی باشد[۱] و رضایت بزه‌دیده او را از مسئولیت معاف نمی‌کند.[۲] بنابراین، رفتار لازم برای جرم تظاهر به دروغ ممکن است متضمن سرقت هویت باشد اما محدود به آن نیست. این جرم به نحوی مبتنی بر تقلب هویت است؛ اگر اطلاعاتی که مورد سوءاستفاده واقع شده مربوط به یک فرد زنده باشد، قطعاً سرقت هویت به وقوع پیوسته و ضرورت وجود نیت پنهان به عنوان یکی از عناصر اصلی مشهود است.

۲-٤. معامله‌ی اطلاعات شناسایی

موضوع این جرم، «اطلاعات شناسایی شخصی» است که تعریف آن در حوزه‌های قضایی استرالیا شباهت‌های زیادی را نشان می‌دهد و به طور کلی، عبارت است از اطلاعاتی که به تنهایی و یا در ترکیب با اطلاعات دیگر برای شناسایی یک فرد استفاده می‌شود، اعم از اینکه شخص موردنظر زنده، مرده یا خیالی باشد.[۳] هر تعریف طیفی از اطلاعات دیجیتال و غیر دیجیتال را دربرمی‌گیرد که نمایانگر انواع ابزارهای تشخیص هویت است؛[۴] به عنوان مثال، تعریف ایالت نیوساوت‌ولز در این مورد شامل نام، نشانی، تاریخ تولد و همچنین، داده‌های بیومتریک، صدانگاشته و امضای دیجیتال است.

---

۱ ibid s 144A.

۲ ibid s 144B (2).

۳ Criminal Code Act 1995 (Cth) s 370.1; Crimes Act 1900 (NSW) s 192I; Criminal Code Act 1899 (Qld) s 408D (7); Criminal Law Consolidation Act 1935 (SA) s 144A; Crimes Act 1958 (Vic) s 192A; Criminal Code Act Compilation Act 1913 (WA) s 489.

۴. استیل به نکته‌ی قابل توجهی اشاره دارد که این تعاریف فراتر از اطلاعات خصوصی، شامل اطلاعات در دسترس عموم نیز می‌شود؛ نام، نشانی، وضعیت تأهل، تاریخ و محل تولد به ویژه در مورد سلبریتی‌ها و افرادی که در شبکه‌های اجتماعی فعالیت دارند، به راحتی در اینترنت قابل دسترسی است و آگاهی از آن‌ها هیچ منع قانونی ندارد (Steel, 2010: 510). به هر حال، چه اطلاعات در دسترس عموم باشد و یا با توافق به دست آمده باشد، از جدیت آسیب‌های احتمالی ناشی از سوءاستفاده هویتی نمی‌کاهد.

استرالیای غربی در این زمینه، دو مفهوم «اطلاعات شناسایی» و «مواد شناسایی» را به کار می‌برد؛ مفهوم اول فقط حاوی نمونه‌هایی از اطلاعات است که شامل گواهینامه‌ی رانندگی، گذرنامه و کارت‌های اعتباری یا نقدی نمی‌شود بلکه به اطلاعات ذخیره شده در آن می‌پردازد. اصطلاح «مواد شناسایی» به طور گسترده به اطلاعات شناسایی و سوابق حاوی این اطلاعات اشاره می‌کند.[۱] با این حال، در استرالیای جنوبی، اطلاعات شناسایی شخصی به‌گونه‌ای تعریف شده که گواهینامه‌ی رانندگی،[۲] گذرنامه،[۳] کارت‌های اعتباری یا نقدی[۴] و هر آنچه به طور معمول برای شناسایی اشخاص استفاده می‌شود[۵] را دربرمی‌گیرد و مفهوم «مواد ممنوعه»[۶] نیز حاوی اطلاعات هویتی و اقلام شناسایی است که به فرد امکان می‌دهد هویت جعلی به خود بگیرد یا حق مالکیت دیگری بر مال یا اطلاعات را تصاحب نماید.[۷] در نیوساوت‌ولز[۸] و قوانین مشترک‌المنافع[۹] نیز اصطلاح «اطلاعات شناسایی» به طور مشخص شامل گواهینامه‌ی رانندگی، گذرنامه و کارت اعتباری یا نقدی می‌شود.

تعریف موجود در ویکتوریا با عبارت «اطلاعاتی مانند» آغاز می‌شود[۱۰] که گواهینامه‌ی رانندگی،[۱۱] گذرنامه[۱۲] و کارت اعتباری یا نقدی[۱۳] را دربرمی‌گیرد. این رویکرد نشان می‌دهد که سایر اسناد هویتی نیز در تعریف اطلاعات شناسایی گنجانده شده است.

---

۱ Criminal Code Act Compilation Act 1913 (WA) s 489.

۲ Criminal Law Consolidation Act 1935 (SA) s 144A para a (ii) of definition.

۳ ibid para a (iii) of definition.

۴ ibid para a (vi) of definition.

۵ ibid para a (vii) of definition.

۶ Prohibited Material.

۷ Criminal Law Consolidation Act 1935 (SA) s 144A.

۸ Crimes Act 1900 (NSW) s 192I paras (c) (d) and (g) of definition.

۹ Criminal Code Act 1995 (Cth) s 370.1 paras (c) (d) and (g) of definition.

۱۰ Crimes Act 1958 (Vic) s 192A.

۱۱ ibid para (d) of the definition.

۱۲ ibid para (e) of the definition.

۱۳ ibid para (h) of the definition.

همچنین، مقررات مشترک‌المنافع و ایالت ویکتوریا شامل مفهومی به نام «مدارک شناسایی» است؛ این مفهوم به مدارک یا اقلام حاوی اطلاعات شناسایی اشاره دارد که می‌تواند برای مقاصدی مانند جعل هویت مورد استفاده قرار گیرد.[۱]مشابه این وضعیت در کوئینزلند نیز دیده می‌شود که تعریف موجود شامل نمونه‌هایی از اطلاعات شناسایی یک فرد است.[۲]با این حال، مقررات کوئینزلند مفهومی مانند مواد یا مدارک شناسایی را ندارند.

مفهوم «معامله» به عنوان رفتار مجرمانه، به طور مشخص در دولت مشترک‌المنافع،[۳] ایالت‌های نیوساوت‌ولز[۴]و کوئینزلند[۵]به کار رفته است. واژه‌ی «معامله» در لغت به معنای تجارت یا دادوستد (شخص یا کالا) است. در قلمرو مشترک‌المنافع[۶]و ایالت نیوساوت‌ولز[۷] این اصطلاح به‌گونه‌ای تعریف شده که شامل تولید، تأمین یا استفاده از اطلاعات شناسایی است، در حالی که کوئینزلند آن را به تأمین یا استفاده محدود می‌کند.[۸]دیگر حوزه‌های قضایی استرالیا واژه‌ی «معامله» را به کار نمی‌برند اما هر یک رفتارهای مشابهی را ممنوع کرده‌اند. در ویکتوریا این جرم به عنوان تهیه، تأمین و استفاده از اطلاعات شناسایی شناخته می‌شود[۹]اما استرالیای غربی، این اعمال را در رابطه با مواد شناسایی جرم‌انگاری نموده است.[۱۰]در استرالیای جنوبی، رفتارهای مجرمانه شامل استفاده،[۱۱]تولید،[۱۲]فروش، عرضه

---

۱ ibid s 192A.

۲ Criminal Code Act 1899 (Qld) s 408D.

۳ Criminal Code Act 1995 (Cth) s 372.1.

۴ Crimes Act 1900 (NSW) s 192J.

۵ Criminal Code Act 1899 (Qld) s 408D.

۶ Criminal Code Act 1995 (Cth) s 370.1.

۷ Crimes Act 1900 (NSW) s 192I.

۸ Criminal Code Act 1899 (Qld) s 408D (7).

۹ Crimes Act 1958 (Vic) s 192B.

۱۰ Criminal Code Act Compilation Act 1913 (WA) s 490.

۱۱ Criminal Law Consolidation Act 1935 (SA) s 144C.

۱۲ ibid s 144D (1)(a).

برای فروش، دادن و پیشنهاد[۱]است که استفاده محدود به اطلاعات شناسایی شخصی است اما سایر جرایم به مواد ممنوعه مربوط می‌شوند.

ضرورت وجود نیت پنهان (سوءنیت خاص)، خصیصه‌ی جرایم معامله‌ی اطلاعاتی است، همان‌طور که در سایر جرایم نیز مشاهده می‌شود. در تمام حوزه‌های قضایی به‌جز استرالیای جنوبی، این قصد با یک جرم قابل تعقیب مرتبط است.[۲]اصلاحات اخیر در قانون مشترک‌المنافع آن را به «جرایم قابل تعقیب خارجی» توسعه می‌دهد[۳]که هدف از این تعمیم، بر اساس یادداشت‌های توضیحی لایحه، «تقویت نظام کنونی در برابر جرایم هویتی با هدف شناسایی افراد مستقر در استرالیا است که در جرایم هویتی بین‌المللی فعالیت می‌کنند».[۴]در استرالیای جنوبی، سوءاستفاده از اطلاعات باید با قصد ارتکاب یا تسهیل ارتکاب یک جرم جدی صورت گیرد.[۵]همچنین، در این حوزه تفاوت اصلی در جرایم مرتبط با مواد ممنوعه شامل تولید و تأمین اطلاعات شناسایی است که نیازمند اثبات قصد ارتکاب یا تسهیل ارتکاب هر نوع جرم، مستلزم کیفرخواست یا دادرسی اختصاری است[۶] و این در تضاد با جرایم معاملاتی در سایر حوزه‌ها است. در ادامه، به دو ویژگی خاص از قوانین استرالیا در سطح فدرال و ایالتی اشاره می‌شود که بررسی دقیق‌تری از نقش نیت پنهان در این دسته جرایم ارائه می‌دهد.

---

۱ ibid s 144D (2).

۲ Criminal Code Act 1995 (Cth) s 372.1(1)(c)(i); Crimes Act 1900 (NSW) s 192J; Criminal Code Act 1899 (Qld) s 408D (1); Crimes Act 1958 (Vic) s 192B (1)(b); Criminal Code Act Compilation Act 1913 (WA) s 490 (1).

۳. «جرم قابل تعقیب خارجی»، جرمی است که بر اساس قوانین یک کشور خارجی یا حوزه‌ی قضایی درون آن کشور، چنانچه در استرالیا ارتکاب یابد، معادل یک جرم قابل تعقیب فدرال خواهد بود (Criminal Code Act 1995 (Cth) s 370.2)؛ به عنوان مثال، اگر شهروند استرالیا اطلاعات شناسایی را به قصد ارتکاب کلاهبرداری در انگلستان معامله کند، رفتار او مشمول مقررات اصلاحی می‌شود.

۴ Explanatory Memorandum, Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Bill 2012 (Cth): 37.

۵ Criminal Law Consolidation Act 1935 (SA) s 144C (1).

۶ ibid s 144A.

ویژگی اول به جرم مشترک‌المنافع مربوط می‌شود که نیاز به اثبات نیت میانی دارد. در این حوزه‌ی قضایی، فردی که اطلاعات شناسایی را در اختیار دارد، باید قصد استفاده از آن را برای تظاهر یا معرفی خود به‌جای دیگری، خواه زنده، مرده یا موهوم داشته باشد[۱] و این تحریف هویتی به منظور ارتکاب یا تسهیل ارتکاب یک جرم مشترک‌المنافع یا جرم قابل تعقیب خارجی صورت گیرد.[۲] سایر حوزه‌ها اثبات چنین قصدی را لازم نمی‌دانند بلکه رفتارهای فیزیکی ممنوعه را به طور مستقیم با نیت ارتکاب یا تسهیل ارتکاب یک جرم مقصود مرتبط می‌سازند. استیل معتقد است که ضرورت وجود نیت میانی ایجاب می‌کند جرم تا حدی بر تقلب هویت استوار باشد (Steel, 2010: 511).

ویژگی دوم به طور خاص در ویکتوریا مطرح می‌شود. تعریف جرم در این حوزه، صراحتاً مقرر می‌دارد که «مرتکب باید از این موضوع آگاه باشد یا احتمال دهد اطلاعاتی که در اختیار دارد، اطلاعات شناسایی شخصی است».[۳] این ماده هرگونه تردید در مورد لزوم اثبات عنصر معنوی در ارتباط با عنصر مادی جرم را از بین می‌برد. در حوزه‌های قضایی استرالیا، زمانی که یک مقرره‌ی قانونی در مورد لزوم اثبات عنصر روانی ساکت است، فرض قوی بر وجود آن است.[۴] بنابراین، با توجه به ماهیت این جرایم و مجازات آن، دادگاه‌ها باید این پیش‌فرض را در نظر بگیرند که این موضوع مورد تأیید استیل نیز است (Steel, 2010: 519).

۳-٤. جرایم داشتن و نگهداری اطلاعات شناسایی و ابزار تولید آن

یک ویژگی مشترک در سراسر حوزه‌های قضایی، جرایم داشتن و نگهداری است که نیاز به اثبات نیت پنهان دارد و در دولت مشترک‌المنافع، نیت میانی از سوی مرتکب نیز الزامی

---

۱ Criminal Code Act 1995 (Cth) s 372.1(1)(b).

۲ ibid ss 372.1 (1)(b) and (c).

۳ Crimes Act 1958 (Vic) s 192B (1)(a).

۴ He Kaw Teh v The Queen (1985) 157 CLR 523 (HCA).

است. هر حوزه‌ی قضایی، داشتن و نگهداری اطلاعات شناسایی[۱] و تجهیزات تولید آن[۲] را ممنوع می‌کند. در استرالیای غربی، این جرم فراتر از اطلاعات شناسایی، هر نوع رکورد حاوی اطلاعات و در استرالیای جنوبی، هر آنچه تسهیل‌کننده‌ی جعل هویت باشد را دربرمی‌گیرد.

دامنه‌ی جرم «تجهیزات» در حوزه‌های قضایی استرالیا متفاوت است. در نیوساوت‌ولز، این جرم شامل تجهیزات، مواد یا سایر اشیائی است که قابلیت استفاده برای تهیه‌ی مدارک یا اقلام شناسایی را دارند[۳] لذا داشتن هر چیزی با چنین قابلیتی جرم تلقی می‌شود. بنابراین، داشتن یک تکه کاغذ می‌تواند منجر به مسئولیت کیفری گردد که این موضوع باید بخشی از بررسی‌های انتقادی این جرایم باشد. در استرالیای غربی نیز عبارت تجهیزات شناسایی به «هر آنچه که قادر به استفاده، تولید، تأمین یا نگهداری مواد شناسایی باشد» تعریف شده است.[۴]

در دولت مشترک‌المنافع،[۵] ایالت‌های استرالیای جنوبی[۶] و کوئینزلند،[۷] این جرم منحصراً شامل تجهیزات است اما معنای آن بستگی به تشخیص مقام قضایی دارد که این موضوع سبب عدم قطعیت در دامنه‌ی جرم می‌شود. برخلاف استرالیای غربی، مقررات ویکتوریا محدود به تجهیزاتی شده که قادر به استفاده، تهیه، تأمین یا نگهداری مدارک شناسایی

---

۱ Criminal Code Act 1995 (Cth) s 372.2; Crimes Act 1900 (NSW) s 192K; Criminal Code Act 1899 (Qld) s 408D (1); Criminal Law Consolidation Act 1935 (SA) s 144D (1)(b); Crimes Act 1958 (Vic) s 192C; Criminal Code Act Compilation Act 1913 (WA) s 491.

۲ Criminal Code Act 1995 (Cth) s 372.3; Crimes Act 1900 (NSW) s 192L; Criminal Code Act 1899 (Qld) s 408D (1A); Criminal Law Consolidation Act 1935 (SA) s 144D (3); Crimes Act 1958 (Vic) s 192D; Criminal Code Act Compilation Act 1913 (WA) s 492.

۳ Crimes Act 1900 (NSW) s 192L (a).

۴ Criminal Code Act Compilation Act 1913 (WA) s 492 (1).

۵ Criminal Code Act 1995 (Cth) s 372.3.

۶ Criminal Law Consolidation Act 1935 (SA) s 144D (3).

۷ Criminal Code Act 1899 (Qld) s 408D (1A).

باشد.[۱] با این حال، در قوانین مشترک‌المنافع به قابلیت عملکردی تجهیزات پرداخته نشده است.[۲]

٤-٤. جرایم الحاقی مشترک‌المنافع

قانون اصلاحات جرایم (مواد مخدر جدی، جرایم هویتی و سایر تخلفات) مصوب ۲۰۱۲ (مشترک‌المنافع) جرم خاصی برای معامله ایجاد کرد[۳] که اگر از طریق سرویس حمل‌ونقل انجام شود، قابل پیگرد قانونی است.[۴] این اصطلاح به‌گونه‌ای تعریف شده که شامل خدمات اینترنتی یا مخابراتی نیز می‌شود. قانون مزبور همچنین معامله‌ی اطلاعات شناسایی را که از طریق سرویس حمل‌ونقل به دست آمده جرم می‌داند.[۵] هر دو جرم برای ارتکاب نیاز به نیات میانی و نهایی دارند. اگر ثابت شود فردی در زمینه‌ی اطلاعات شناسایی فعالیت کرده یا آن را به دست آورده، فرض بر آن است که از خدمات حمل‌ونقل استفاده شده، مگر خلاف آن اثبات شود.[۶]

---

۱ Crimes Act 1958 (Vic) s 192D.

۲. بر اساس یادداشت‌های توضیحی لایحه، پارلمان مشترک‌المنافع معتقد بود که این جرم مقدماتی است لذا کارایی عملی تجهیزات موضوعیت نداشته و تنها نیت فرد مهم است. در نتیجه، مجرم نمی‌تواند با ادعای اینکه تجهیزات در اختیار او قادر به تولید مدارک شناسایی نبوده، از پیگرد قانونی فرار کند. همچنین، پارلمان اذعان داشت که حذف این الزام، دامنه‌ی جرم را گسترش می‌دهد؛ به گونه‌ای که مسئولیت را بر قصد مجرمانه تحمیل می‌کند، حتی اگر وقوع جرم غایی امکان‌پذیر نباشد (Explanatory Memorandum, Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2010 (Cth): 9).

۳. دلیل اتخاذ چنین رویکردی این بود که اولاً، گروه‌های سازمان‌یافته از اینترنت و سایر فناوری‌های ارتباطی مدرن برای جمع‌آوری و سوءاستفاده از اطلاعات شناسایی بهره‌برداری می‌کردند. ثانیاً، مرتکبان جرایم سازمان‌یافته و جدی به منظور پنهان کردن هویت خود و ارتکاب جرایمی مانند قاچاق مواد مخدر و پول‌شویی، در سفرهای هوایی از هویت جعلی استفاده می‌کردند (Explanatory Memorandum, Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Bill 2012 (Cth): 37).

۴ Criminal Code Act 1995 (Cth) s 372.1A (1).

۵ Ibid s 372.1A (3).

۶ ibid s 372.1A (5).

در مواد ۳۷۶,۲ تا ۳۷۶,۴ جرایم مرتبط با هویت جعلی در سفرهای هوایی ذکر شده که متفاوت از سایر جرایم استرالیا است. به طور خلاصه، این جرایم عبارتند از:

۱) به‌کارگیری اطلاعات شناسایی جعلی، بدون توجه به اینکه اطلاعات مزبور برای شناسایی مسافر پرواز استفاده شود؛[۱]

۲) خرید بلیت پرواز از طریق سرویس حمل‌ونقل با اطلاعات شناسایی جعلی، صرف‌نظر از اینکه اطلاعات برای شناسایی مسافر پرواز استفاده خواهد شد؛[۲]

۳) سفر هوایی با بلیتی که از طریق سرویس حمل‌ونقل با اطلاعات شناسایی جعلی به دست آمده است؛[۳]

۴) خرید بلیت پرواز با اطلاعات شناسایی جعلی، بدون توجه به اینکه اطلاعات برای شناسایی مسافر پرواز استفاده شود؛[۴]

۵) سفر هوایی با بلیت حاوی اطلاعات جعلی که منجر به شناسایی فرد به عنوان مسافر پرواز می‌گردد.[۵]

۵. تحلیل قوانین کیفری استرالیا

در این بخش پس از ارائه‌ی توضیحات اولیه، به ارزیابی انتقادی جرایم پرداخته می‌شود که بر نحوه‌ی جرم‌انگاری تخلفات هویتی و مجازات‌های قانونی متمرکز است. همچنین، این مطالعه به بررسی مفهوم گواهی قربانی می‌پردازد که از مشخصه‌های مقررات قانونی است؛ زیرا به افرادی که اطلاعات شخصی‌شان مورد سوءاستفاده قرار گرفته، نوعی حمایت ارائه می‌دهد و اهمیت این نوع تسهیلات در بحث جرم‌انگاری به وضوح مشخص است.

۱-۵. جرم‌انگاری در زمینه‌ی تخلفات مرتبط با هویت

---

۱ ibid s 376.2 (1).

۲ Ibid s 376.3 (1).

۳ ibid s 376.3 (2).

۴ ibid s 376.4 (1).

۵ ibid s 376.4 (2).

اگرچه عناصر متشکله‌ی برخی جرایم مانند «معامله‌ی اطلاعات شناسایی» و «اتخاذ هویت جعلی» می‌تواند شامل اقداماتی نظیر سرقت هویت باشد اما اثبات این جرایم مستلزم ارائه‌ی شواهدی فراتر از به‌کارگیری اطلاعات شناسایی قربانی برای تصاحب هویت او است؛ به عنوان مثال، مجرمی که با در اختیار داشتن اطلاعات شناسایی یک فرد خود را به‌جای او وانمود می‌کند، ممکن است این عمل سرقت هویت از ارکان جرم محسوب شود اما به‌خودی‌خود جرم نیست. این رفتار تنها در صورتی به وقوع می‌پیوندد که با قصد ارتکاب یک جرم قابل تعقیب همراه باشد. بدون شک، وجود عناصر اضافی بیانگر این است که قانونگذاران از هدف اصلی خود مبنی بر جرم‌انگاری سرقت هویت فاصله گرفته و پیشگیری از آسیب‌های احتمالی ناشی از سوءرفتارهای هویتی را مدنظر قرار داده‌اند. از این رو، آن‌ها به تصویب برخی جرایم پرداختند که عمدتاً به صورت ناقص[1] تعریف شده است (Alleyne, 2014: 134).

هر بحث انتقادی باید بر نوع، ماهیت تخلف و آسیب ناشی از این جرایم تمرکز داشته باشد. یک توجیه عمومی برای پذیرش جرایم «ناتمام» در حقوق کیفری این است که به عنوان یک اقدام پیشگیرانه طراحی شده‌اند تا از بروز فعالیت‌های زیانبار جلوگیری شود. تأکید اشورث بر این نکته که اقدامات بالقوه‌ی عامل، مؤلفه‌ی اصلی جرم‌انگاری است می‌تواند مؤید این مطلب باشد که هدف وضع‌کنندگان چنین جرایمی پیشگیری از آسیب بوده، همان‌طور که هوساک به عنوان «آسیب نهایی» به آن اشاره می‌کند (Husak, 2008: 160). با این حال، نگرانی موجود به فاصله میان آسیب نهایی و ارکان تشکیل‌دهنده‌ی جرم مربوط می‌شود که پاکر در این باره می‌نویسد: «یکی از چالش‌های حساس در تدوین قوانین کیفری، یافتن نقطه‌ای است که از آسیب نهایی مورد انتظار

---

۱. همان‌طور که هوساک اشاره می‌کند، حوزه‌های قضایی استرالیا فراتر از جرایم کلاسیک مانند شروع به جرم، توطئه و تحریک، جرایم ناقص دیگری را تصویب کرده‌اند (Husak, 2008: 161). اشورث در این زمینه بیان می‌کند: «بسیاری از جرایم به‌گونه‌ای تعریف شده که نیازی به ایجاد آسیب واقعی ندارند. رفتاری که فرد را به دلیل ارتکاب عمل خاصی «با قصد انجام X» مجازات می‌کند، در واقع به‌صورت ناقص تعریف شده و بسیاری از ویژگی‌های جرائم ناقص را دارد. جرایم نگهداری نیز ماهیتاً ناقص است که در آن، صرف نگهداری شیء یا ماده مهم نیست بلکه هر آنچه دارنده ممکن است با آن انجام دهد، دلیل اصلی جرم‌انگاری است» (Ashworth, 2006: 444).

فاصله‌ی زیادی دارد و می‌توان مداخله‌ی پیشگیرانه‌ای انجام داد. گرچه شناسایی افراد خطرناک قبل از رسیدن به مرحله‌ی حاد امری مطلوب به نظر می‌رسد؛ اما در واقع، گسترش دامنه‌ی قوانین کیفری به منظور مداخله‌ی زودهنگام، کار پرخطری است» (Packer, 1968: 270).

هوساک نیز بر چهار اصل محدودکننده در ارتباط با جرم‌انگاری آسیب‌های غیرمستقیم تأکید دارد که این جرایم تنها در صورتی توجیه‌پذیر است که اولاً، به منظور کاهش خطرات ناشی از آسیب طراحی شده باشد. ثانیاً، جرم‌انگاری به طور واقعی احتمال وقوع آسیب نهایی را کاهش دهد. ثالثاً، آسیب نهایی ناشی از رفتارهایی باشد که دولت مجاز به جرم‌انگاری آن است. رابعاً، یک جرم در صورتی بیش از حد جامع محسوب می‌شود که بدون افزایش احتمال وقوع آسیب نهایی قابلیت ارتکاب داشته باشد (Husak, 2008: 161-168).

برای درک آسیب یا خطرات احتمالی، لازم است به نقش‌های مختلفی که این جرایم ایفا می‌کنند اشاره گردد. در ابتدا بیان شد که سوءاستفاده از اطلاعات شناسایی می‌تواند منجر به آسیب‌های مختلفی گردد و برخی جرایم ثانویه را در پی داشته باشد؛ برای نمونه، ممکن است فردی با ادعای نادرست به عنوان دارنده‌ی حساب بانکی، وجوهی را از طریق برداشت از حساب و یا وام مسکن به دست آورد. در این موارد، سوءاستفاده از اطلاعات به عنوان ابزاری برای کلاهبرداری عمل می‌کند که می‌توان آن را «نقش تسهیل‌کننده‌ی آسیب مستقیم» نامید. در مقابل، «نقش تسهیل‌کننده‌ی آسیب غیرمستقیم» به شرایطی اشاره دارد که در آن، افراد مرتبط با جرم سازمان‌یافته از هویت‌های جعلی استفاده می‌کنند تا در نهایت به تسهیل اقداماتی مانند تروریسم و قاچاق انسان بپردازند. در این صورت، سوءرفتار هویتی از ارکان تخلف نهایی محسوب نمی‌شود بلکه وقوع آن را تسهیل می‌کند. نقش سوم به این واقعیت مربوط می‌شود که سوءاستفاده از اطلاعات ممکن است برای پنهان کردن هویت واقعی مرتکب و انتساب جرم به غیر صورت گیرد. نتیجه‌ی اجتناب‌ناپذیر این روش، تأخیر در شناسایی مجرم و طولانی کردن فرآیند اجرای قانون است که خطر آسیب به قربانی هم کاملاً مشهود است.

داف معیارهای قانونی شروع به جرم را که مستلزم انجام اقداماتی فراتر از «آمادگی صرف» است اتخاذ می‌کند. با این حال، او معتقد نیست که رفتار مقدماتی صرف هرگز نباید جرم‌انگاری شود (Duff, 2005: 44-45). به طور قطع، جرم اتخاذ هویت جعلی در استرالیای جنوبی مستلزم اقداماتی فراتر از تملک صرف است و بر حسب شرایط، چنین رفتارهایی ممکن است بیش از «آمادگی صرف» در نظر گرفته شوند. همین امر می‌تواند در مورد استفاده از اطلاعات شناسایی شخصی تحت عنوان معامله نیز رخ دهد که به میزان ارتباط اعمال انجام شده با هر جرم احتمالی بعدی بستگی دارد. با وجود این، در مواردی که مداخله‌ی انسانی برای ایجاد آسیب ضروری است (مانند جرایم داشتن و نگهداری)، جرم‌انگاری سوءرفتارهای اولیه می‌تواند از نظر اخلاقی مشکل‌ساز باشد. فرض اینکه عامل یا حتی شخص دیگری برای ایجاد پیامد زیانبار مداخله کند، به معنای نادیده گرفتن اصل خودمختاری است؛ زیرا افراد تنها به خاطر اعمال خود مسئول شناخته می‌شوند (Duff, 2005: 63).

افزون بر اینکه مشروعیت اخلاقی این جرایم مورد تردید است، در آن نمونه‌هایی از دوگانگی مشاهده می‌شود. لیدر الیوت نیز در بررسی‌های خود پیرامون وجود جرایم ناقص در استرالیا به این مطلب اذعان دارد که یک جرم ناقص، خود ممکن است به عنوان هدفی برای ارتکاب جرایم ثانویه در نظر گرفته شود. ماده‌ی ۳۷۲,۲ از قانون مشترک‌المنافع در این زمینه قابل توجه است؛ این ماده نگهداری اطلاعات را که به ظاهر عملی بی‌ضرر است، چنانچه با قصد ارتکاب جرم مندرج در ماده‌ی ۳۷۲,۱ انجام شود، مجازات می‌کند. جرم مذکور نیز «معامله‌ی» اطلاعات را با نیت ارتکاب یک جرم مشترک‌المنافع محکوم می‌کند. این محقق در بررسی انتقادی خود خاطرنشان کرد که تحمیل مسئولیت کیفری برای شروع به ارتکاب هر یک از این جرایم ناقص ممنوع است. لیدر الیوت مفهوم جرایم مقدماتی را به عنوان معیاری برای نقد جرایم هویتی استرالیا به کار گرفته است که در این راستا به جرم خاص توطئه در سطح مشترک‌المنافع[1] اشاره دارد و برخی نکات در مجازات‌های قابل اجرا

---

1. Criminal Code Act 1995 (Cth) s 11.5.

را مطرح می‌کند که نباید از مجازات جرم مقصود فراتر رود (Leader-Elliott, 2011: 82-96).

استیل متذکر می‌شود که جرایم داشتن و نگهداری بیشتر مبتنی بر فعل و انفعالات ذهنی است و عینیت خارجی ندارد. به عبارت دیگر، اطلاعات شناسایی شخصی و ابزار تولید آن به‌خودی‌خود خطرناک نیستند؛ این اطلاعات ممکن است به روش‌های متعددی به کار رود و به دیگران ارائه شود، یا مدارک شناسایی با استفاده از تجهیزاتی تولید شوند که به عنوان رفتار اجتماعی مفید یا حداقل بی‌ضرر در نظر گرفته شوند و چنین رفتارهایی به‌خودی‌خود جرم نیست. با این حال، در چند دهه‌ی گذشته، تحقیقات زیادی درباره‌ی جرایم هویتی منتشر گردیده که اطلاعات و تجهیزات شناسایی برای مقاصد مجرمانه نیز مورد استفاده قرار می‌گیرند. از این رو، وجود قصد باطنی در این جرایم از اهمیت چندانی برخوردار است که رفتار مرتکب را مجرمانه جلوه می‌دهد (Steel, 2010: 525-526).

اگر محتوای قانون به‌طور دقیق منعکس می‌شد، می‌توان گفت که قوانین استرالیای جنوبی در راستای مقابله با «سرقت هویت» نسبت به سایر حوزه‌های قضایی کارآمدتر بود. با این حال، اصطلاح سرقت هویت در مقررات موجود تعریف نشد و سایر حوزه‌های قضایی نیز به جای اصطلاح «سرقت هویت» از اصطلاحات گسترده‌تری مانند «جرم هویت» در استرالیای غربی و ویکتوریا و «جرایم هویت» در قوانین فدرال و نیوساوت‌ولز بهره می‌برند. با توجه به آنچه گفته شد، سرقت هویت در هیچ یک از حوزه‌های قضایی به طور خاص جرم‌انگاری نشده که این موضوع مورد تأیید برخی محققان نیز است، هرچند آن‌ها تعاریف متفاوتی از سرقت هویت ارائه داده‌اند؛ برای نمونه، استیل که سرقت هویت را به «کسب و نگهداری اطلاعات شناسایی» توصیف می‌کند، معتقد است قوانین موجود در صدد توصیف یا ممنوع کردن این رفتار مجرمانه نیست (Steel, 2010: 504-510). همچنین، سالیوان که سرقت هویت را «سوءاستفاده از هویت معاملاتی متعلق به غیر در معامله» و کلاهبرداری هویت را «استفاده از هر نوع اطلاعات شناسایی دیگر برای مقاصد متقلبانه» می‌نامد، بر این باور است که در قوانین استرالیا سرقت یا کلاهبرداری هویت جرم‌انگاری نشده است (Sullivan, 2011: 114-118). بنابراین، میان عناوین قانونی به

کار رفته و جرایم موجود نوعی ناهماهنگی وجود دارد در حالی که قوانین باید به زبانی روشن و صریح نوشته شوند تا برای عموم مردم و مجریان قانون قابل درک باشند و تفسیرهای متفاوتی از آن نشود. این امر به افزایش اعتماد عمومی به نظام حقوقی و کارآمدی قانون کمک می‌کند تا از نارضایتی عمومی جلوگیری شود.

۲-۵. مجازات‌های قانونی

مقررات جزایی استرالیا از دو جنبه قابل نقد هستند: جنبه‌ی اول به تفاوت حداکثر مجازات‌های قانونی در حوزه‌های قضایی مربوط می‌شود. حداکثر مجازات جرم «معامله» در ایالت‌ها متفاوت است و از سه سال در کوئینزلند[۱] تا ده سال در نیوساوت‌ولز[۲] متغیر است. در استرالیای غربی، کیفر این جرم بیش از هفت سال یا مدت محکومیت به شروع به جرم قابل تعقیب است.[۳] این جرم در ویکتوریا[۴] و سطح ملی[۵] با حداکثر پنج سال حبس قابل مجازات است در حالی که در استرالیای جنوبی، کیفر جرم فریب[۶] و سوءاستفاده از اطلاعات شناسایی[۷] به میزان شروع به ارتکاب جرم جدی مقصود است.

جرایم داشتن و نگهداری در مشترک‌المنافع،[۸] ایالت‌های کوئینزلند[۹] و ویکتوریا[۱۰] و همچنین، جرم در اختیار داشتن تجهیزات در نیوساوت‌ولز، مجازات قانونی حداکثر سه سال حبس دارند.[۱۱] با این حال، در نیوساوت‌ولز، نگهداری اطلاعات شناسایی مجازات

---

۱ Criminal Code Act 1899 (Qld) s 408D (1).

۲ Crimes Act 1900 (NSW) s 192J.

۳ Criminal Code Act Compilation Act 1913 (WA) s 490.

۴ Crimes Act 1958 (Vic) s 192B (1).

۵ Criminal Code Act 1995 (Cth) ss 372.1 (1) and 372.1A (1).

۶ Criminal Law Consolidation Act 1935 (SA) s 144B (3).

۷ ibid s 144C (1).

۸ Criminal Code Act 1995 (Cth) ss 372.2 (1) and 372.3 (1).

۹ Criminal Code Act 1899 (Qld) ss 408D (1) and 408D (1A).

۱۰ Crimes Act 1958 (Vic) ss 192C (1) and 192D (1).

۱۱ Crimes Act 1900 (NSW) s 192L.

حداکثر هفت سال حبس در پی خواهد داشت.[۱] در استرالیای غربی، مجازات جرایم داشتن و نگهداری در صورت محاکمه با کیفرخواست، حداکثر پنج سال حبس و در صورت محکومیت اجمالی، بیست‌وچهار ماه حبس و بیست‌وچهار هزار دلار جزای نقدی است.[۲] در استرالیای جنوبی، مرتکب جرایم مرتبط با مواد ممنوعه به حداکثر سه سال حبس محکوم خواهد شد.[۳] با وجود این، جرایم مربوط به سفرهای هوایی در سطح فدرال مجازات حداکثر یک سال حبس را به همراه دارند.[۴] بدون شک، تفاوت‌های موجود نشان می‌دهند که تعیین مجازات‌ها بیشتر تحت تأثیر عوامل سیاسی محلی است تا یک رویکرد ملی منطقی (Steel, 2010: 529) و حال آنکه با وجود قوانین ملی و امکان ارتکاب جرایم فرامرزی، انتظار می‌رفت هماهنگی بیشتری در این زمینه وجود داشته باشد. در مجموع، جرایم مشترک‌المنافع نسبت به جرایم ایالتی مجازات‌های کمتری دارند لذا نیاز بیشتری به بازنگری مقررات جزایی احساس می‌شود.

کمیته‌ی ویژه مقامات حقوق کیفری نیز تأکید نموده که جرایم مربوطه ماهیتی مقدماتی دارند لذا بهتر بود مجازات‌های کمتری تعیین می‌شد. با این حال، اعمال مجازات شدید برای جرم «معامله» به منظور ایجاد تعادل میان جنبه‌های مقدماتی جرم و همچنین، جدیت و تأثیرات اجتماعی آن صورت گرفت (MCLOC, 2008: 35).

مسئله‌ی عدم تناسب مجازات بین جرایم ناقص و غایی، نقطه‌ی ارجاع دیگری برای نقد و بررسی است. لیدر الیوت به طور جامع به این موضوع پرداخته است که به‌طور کلی، کیفر جرایم ناقص از مجازات جرم مقصود فراتر نمی‌رود؛ او متذکر می‌شود که در برخی موارد ممکن است مجازات یک جرم قابل تعقیب حداقل دوازده ماه حبس باشد و در نتیجه، مجرم هویتی مجازات بیشتری را نسبت به زمانی که به جرم اصلی متهم شده، متحمل گردد. او ادامه می‌دهد که احتمالاً عکس این وضعیت نیز صادق است؛ به طوری که جرم

---

۱ ibid s 192K.

۲ Criminal Code Act Compilation Act 1913 (WA) ss 491 (1) and 492 (2).

۳ Criminal Law Consolidation Act 1935 (SA) s 144D.

۴ Criminal Code Act 1995 (Cth) ss 376.2 (1), 376.3 (1), 376.3 (2), 376.4 (1) and 376.4 (2).

قابل تعقیب مجازات شدیدتری نسبت به حداکثر مجازات‌های قانونی جرم ناقص داشته باشد و این ناهماهنگی‌ها به راحتی قابل دفاع نیست. با این حال، همان‌طور که لیدر الیوت بیان می کند، احتمالاً یکی از دلایل توجیه چنین مقرراتی این است که قصد ارتکاب تقلب هویت به عنوان یک عامل تشدیدکننده‌ی مجازات برای جرایم با کیفر کمتر از سه یا پنج سال حبس در نظر گرفته شده است (Leader-Elliott, 2011: 92). اشاره‌ی او به تقلب از این واقعیت ناشی می‌شود که در جرایم مشترک‌المنافع، اثبات نیت میانی برای اتخاذ هویت جعلی ضروری است.

استیل پیرامون گستره‌ی این جرایم و تعمیم آن به جرایم قابل تعقیب، تأکید می کند که این موضوع منجر به جرم‌انگاری افراطی می‌شود. از دیدگاه او علاوه بر جرایم قابل تعقیب موجود در قوانین کیفری، برخی مقررات نظارتی نیز وجود دارد که نقض آن‌ها جرم محسوب می‌شود (Steel, 2010: 527). این وضعیت در استرالیای جنوبی تشدید می‌شود که در برخی موارد، رفتارهای اصلی تنها به جرایم قابل تعقیب محدود نمی‌شود بلکه شامل طیف وسیعی از جرایم می گردد.

۳-۵. صدور گواهی خاص بزه‌دیده

به طور معمول، انتظار می‌رود که بحث از مجازات، پایان بررسی یک قانون کیفری باشد. با این حال، یکی از ویژگی‌های خاص قوانین استرالیا در زمینه جرایم هویتی، امکان صدور گواهی برای افرادی است که به دلیل سوءاستفاده از اطلاعات شخصی آسیب دیده‌اند. این گواهی به عنوان مجازات و یا جبران خسارت محسوب نمی‌شود بلکه هدف آن، کمک به بزه‌دیدگان در کاهش برخی پیامدهای ناشی از آسیب‌دیدگی این جرایم از جمله آسیب به اعتبار فرد، ایجاد سابقه‌ی کیفری به نام بزه‌دیده و صرف زمان و تلاش بسیار برای بازیابی سوابق معاملات یا تاریخچه اعتباری است که کمیته‌ی ویژه‌ی مقامات حقوق کیفری بر این موضوع تأکید داشته است. در این شرایط، دریافت گواهی برای بزه‌دیده‌ی جرم هویتی مفید به نظر می‌رسد تا در واقع نشان دهد معاملات و رفتارهای مجرمانه توسط شخص دیگری که خود را به جای بزه‌دیده معرفی کرده انجام شده است. گواهی ممکن است

شامل جزئیات تخلف، نام بزه‌دیده و هر موضوع دیگری باشد که دادگاه آن را مرتبط می‌داند (MCLOC, 2008: 42–43).

کمیته‌ی ویژه‌ی مقامات حقوق کیفری در ارائه‌ی این توصیه، از رویکرد ایالت‌های استرالیای جنوبی[۱] و کوئینزلند[۲] پیروی کرد که این پیشنهاد از سوی دولت فدرال،[۳] ایالت‌های استرالیای غربی،[۴] ویکتوریا[۵] و نیوساوت‌ولز[۶] پذیرفته شد. اگرچه مقررات مربوط به گواهی در حوزه‌های مختلف برای هدفی مشترک وضع شده است اما در نحوه‌ی تعریف «بزه‌دیده» و تأثیر رضایت او، زمان و شرایط صدور گواهی، نهادهای صادرکننده، محتوا و مدت اعتبار گواهی تفاوت‌هایی وجود دارد. در این زمینه نیازی به مطالعه‌ی تطبیقی جامع نیست بلکه کافی است به طور مختصر بر مفهوم بزه‌دیده و تأثیر رضایت او تمرکز کنیم. بررسی مقررات حوزه‌های قضایی مختلف نشان می‌دهد که مواضع متضادی در هر دو جنبه وجود دارد؛ برای نمونه، در استرالیای جنوبی، بزه‌دیده‌ی مورد حمایت قانون به فردی اطلاق می‌گردد که از اطلاعات هویتی او بدون مجوز قانونی برای ارتکاب جرم، سوءاستفاده شده است.[۷] با وجود این، در حوزه‌ی قضایی مشترک‌المنافع، هر فردی که از وقوع جرم متحمل ضرر و زیان گردد، بزه‌دیده شناخته می‌شود و صرف‌نظر از اینکه به موضوع رضایت داشته باشد یا خیر، حق دریافت گواهی را دارد.[۸] بنابراین، مقرره‌ی فدرال در تلاش برای تضمین چنین نتیجه‌ای، فراتر از حد لازم عمل می‌کند و حتی فردی که به ارتکاب جرم رضایت می‌دهد نیز از حمایت برخوردار است.

نتیجه

۱ Criminal Law (Sentencing) Act 1988 (SA) s 54.

۲ Criminal Code Act 1899 (Qld) s 408D (3)-(6).

۳ Criminal Code Act 1995 (Cth) division 375.

۴ Criminal Code Act Compilation Act 1913 (WA) s 494 (2).

۵ Sentencing Act 1991 (Vic) ss 89E-89H.

۶ Criminal Procedure Act 1986 (NSW) s 309A.

۷ Criminal Law (Sentencing) Act 1988 (SA) s 54(3).

۸ Criminal Code Act 1995 (Cth) s 375.1.

با وجود گسترش نگرانی‌ها درباره‌ی پیامدهای زیانبار ناشی از سوءرفتارهای هویتی، حوزه‌های قضایی استرالیا هنوز سرقت هویت را به طور دقیق جرم‌انگاری نکرده‌اند بلکه بیشتر به پیشگیری از آسیب‌های اجتماعی و خساراتی که ممکن است در نتیجه‌ی سوءاستفاده از اطلاعات شناسایی حاصل شود، توجه داشته‌اند. آن‌ها برخی جرایم مقدماتی نظیر نگهداری یا معامله‌ی اطلاعات هویتی را تصویب کرده‌اند که هیچ عنصر ذهنی مرتبط با اعمال متهم را ارائه نمی‌دهد. نه تنها دامنه‌ی این جرایم بسیار وسیع بلکه مبنای نظری آن‌ها نیز نامناسب و حول مفهوم در اختیار داشتن اطلاعات است.

در این راستا، با مطالعه‌ی جرایم معامله‌ی اطلاعاتی در استرالیا می‌توان گفت که تملک در این زمینه به معنای کنترل فیزیکی و قصد کنترل نیست بلکه به آگاهی از اطلاعات اشاره دارد. همین ملاحظات نشان می‌دهند در اختیار داشتن اطلاعات در جرم سرقت هویت مستلزم آن است که متهم از ماهیت آن مطلع باشد چنانکه این تفسیر در جرایم حقوق ویکتوریا نیز پذیرفته شده است؛ اما یک اشکال عمده وجود دارد که اصولاً حاکمیت قانون ایجاب می‌کند تا حد امکان، اصطلاحات قانونی دارای معنای واحدی باشند، نه اینکه برای افراد یا در زمینه‌های مختلف معانی متفاوتی داشته باشد. تملک یک مفهوم پیچیده است که در برخی حوزه‌ها نیاز به تأمل دارد.

از طرفی، وسعت دامنه‌ی این جرایم موجب می‌شود که تعیین مرزهای جرم از اختیار قانونگذار خارج شده و بر عهده‌ی نهادهای اجرای قانون قرار گیرد. چنین رویکردی اصول بنیادین یک نظام حقوقی عادلانه و منصفانه را تخریب می‌کند و می‌تواند منجر به تضعیف قانون کیفری ماهوی شود؛ به طوری که جرایم اصلی تابع این جرایم فرعی باشند. بنابراین، لازم است تلاش‌های نظام‌مند در توصیف دقیق فعالیت‌های ممنوعه صورت گیرد و از به کار بردن اصطلاحات نادرست اجتناب گردد. نگرانی‌های واقعی در حفظ محدودیت‌های معقول بر استفاده از قدرت قهری دولت برای وضع جرایم کیفری، تعهد به حداقل‌گرایی و پرهیز از جرم‌انگاری افراطی، همگی نیاز به یک معیار منطقی برای تصویب این نوع جرایم را مطرح می‌کنند. بنابراین، مقنن باید دلایلی منطقی را برای جرم‌انگاری این رفتارهای ناقص ارائه دهد. در این راستا، پیشنهاد می‌شود که ابتدا یک تعریف استاندارد

برای توصیف و پیگرد جرایم هویتی وجود داشته باشد. نهادهای بین‌المللی به این مسأله پرداخته‌اند اما توافقی در این زمینه حاصل نشده است. همچنین، معیارهای مدنظر قانونگذار باید مؤلفه‌های اصلی جرایم هویتی (کسب، تولید، انتقال، تملک و استفاده) را دربرگیرد. این امر به درک سرقت هویت و ارزیابی راه‌حل‌ها برای پیشگیری، تعقیب و جبران خسارت ناشی از آن کمک می‌کند.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID

Meysam Abbasi Lahroudi https://orcid.org/0000-0002-1037-0334
Mohammad Rasaei https://orcid.org/0009-0003-6655-7506
Mohammad Bahrami Khoshkar https://orcid.org/0000-0001-7834-6480
Seyyed Abolghasem Naghibi https://orcid.org/0000-0001-7761-7832

منابع

فارسی

برهانی، محسن (۱۳۸۸). «سیاست کیفری ایران در قبال روسپیگری»، *فصلنامه‌ی مطالعات راهبردی زنان*، دوره‌ی ۱۲، شماره‌ی ۴۵، ۷-۴۲.

روسو، ژان ژاک (۱۳۶۶). قرارداد اجتماعی یا اصول حقوق سیاسی، چاپ سوم، ترجمه‌ی منوچهر کیا، تهران، گنجینه.

سلیمان دهکردی، الهام و حیدریان، ارشیاناز (۱۳۹۸). «تبیین سرقت هویت در نظام کیفری ایران»، *پژوهشنامه‌ی حقوق فارس*، دوره‌ی ۲، شماره‌ی ۲، ۶۳-۸۵.

صالح‌آبادی، زهرا (۱۳۹۱). جرایم علیه هویت با تأکید بر فضای سایبر، پایان‌نامه‌ی کارشناسی ارشد، دانشکده‌ی حقوق دانشگاه قم.

کاتوزیان، ناصر (۱۴۰۰). فلسفه‌ی حقوق، جلد اول، چاپ دوم، تهران، گنج دانش.

محمودی جانکی، فیروز (۱۳۹۳). «جرم‌انگاری حق‌مدار؛ با تأکید بر نظریه‌ی آلمانی مصالح حقوقی»، *فصلنامه‌ی پژوهش حقوق کیفری*، دوره‌ی ۳، شماره‌ی ۹، ۸۳-۱۱۰.

References

Ahmed, S. M. S. (2019). Identity Crime in the Digital Age: Malaysian and Mauritanian Legal Frameworks. International Journal of Law, Government and Communication, 4(15), 154-165. DOI: 10.35631/ijlgc.4150016

Ahmed, Syed R. (2020). Preventing Identity Crime: Identity Theft and Identity Fraud: An Identity Crime Model and Legislative Analysis with Recommendations for Preventing Identity Crime. Leiden; Boston: Brill Nijhoff.

Alleyne, O. (2014). Criminalising Identity Theft: A Comparative Study of Barbados, England and Australia. Thesis submitted for the degree of Doctor of Philosophy. University of Leicester.

Ashworth, A. (2006). Principles of Criminal Law. 5th edn. Oxford; New York: Oxford University Press.

Australasian Centre for Policing Research (ACPR) (2006). Standardisation of Definitions of Identity Crime Terms: A Step towards Consistency. Report Series No. 145.3, Commonwealth of Australia.

Australian Institute of Criminology (AIC). (2002). Identity Fraud. Newsletter, Summer/Autumn, No. 17.

Council of Australian Governments (COAG). (2007). An Agreement to a National Identity Security Strategy. Australia Government.

Cuganesan, S., & Lacey, D. (2003). Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent. Securities Industry Research

Centre of Asia-Pacific (SIRCA). Sydney: Standards Australia International & Business Excellence Australia.

Dixon, N. (2005). Identity Fraud. Research Brief No 2005/03, Queensland Parliamentary Library.

Duff, R.A. (2005). 'Criminalizing Endangerment' in R.A. Duff, & S.P. Green (eds), Defining Crimes: Essays on the Special Part of the Criminal Law. Oxford; New York: Oxford University Press.

Gercke, M. (2011). Legal Approaches to Criminalize Identity Theft. In United Nations Office on Drugs and Crime (UNODC), Handbook on Identity-related Crime. New York: United Nations.

Higgins, C. (2009). Crimes Amendment (Identity Crime) Bill 2009. Research Brief No 1, Victoria Parliamentary Library Research Service.

Husak, D. (2008). Overcriminalization: The Limits of the Criminal Law. Oxford; New York: Oxford University Press.

International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR). (2011). Responding to Victims of Identity Crime: A Manual for Law Enforcement Agents, Prosecutors and Policy-Makers. available at: http://www.icclr.law. ubc.ca.

Jain, M., & Bajaj, P. (2014). Techniques in Detection and Analyzing Malware Executables: A Review. IJCSMC, 3(5), 930-935.

Jaishankar, K. (2008). Identity related Crime in the Cyberspace: Examining Phishing and its impact. International Journal of Cyber Criminology, 2(1), 10–15.

Komakula, S., & Jagadeeshwar, M. (2021). Identity Theft in Cyber Security: Literature Survey. Strad Research, 8(9), 104 – 109. DOI: 10.37896/sr8.9/014

Kumar, S., & Agarwal, D. (2018). Hacking Attacks, Methods, Techniques and Their Protection Measures. IJSART, 4(4), 2253-2257.

Lawson, P. (2011). Identity-related Crime Victim Issues: A Discussion Paper. In United Nations Office on Drugs and Crime (UNODC), Handbook on Identity-related Crime. New York: United Nations.

Leader-Elliott, I. (2011). Framing Preparatory Inchoate Offences in the Criminal Code: The Identity Crime Debacle. Criminal Law Journal, Vol. 35, 80-97. University of Adelaide Law School Research Paper No. 2011-012.

Lozusic, R. (2003). Fraud and Identity Theft. Briefing Paper No 8/03, NSW Parliamentary Library Research Service.

Martins de Almeida, G. (2011). Typology and Criminalization Approaches to Identity-related Crime: Compendium of Examples of Relevant Legislation. In United Nations Office on Drugs and Crime (UNODC), Handbook on Identity-related Crime. New York: United Nations.

Model Criminal Law Officers' Committee (MCLOC). (2008). Final Report: Identity Crime. Commonwealth of Australia.

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.

Packer, H.L. (1968). The Limits of the Criminal Sanction. California: Stanford University Press.

Steel, A. (2010). The True Identity of Australian Identity Theft Offences: A Measured Response or an Unjustified Status Offence? University of New South Wales Law Journal, 33(2), 503-531.

Sullivan, C. (2011). Digital Identity: An Emergent Legal Concept. South Australia: University of Adelaide Press.

Wang, SY. K., & Huang, W. (2011). The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet. Internet

Journal of Criminology. available at: http:// www.internetjournalofcriminology.com

Zulhuda, S., & Mohamed, S. M. O. (2015). The Shari'ah Approach to Criminalise Identity Theft. Pertanika J. Soc. Sci. & Hum, 23 (S), 169-182.

Persian References Translated into English

Borhani, Mohsen (2009). "Iran's Criminal Policy Against Prostitution", Quarterly Journal of Strategic Women's Studies, Volume 12, Issue 45, 7-42. [In Persia]

Rousseau, Jean-Jacques (1987). The Social Contract or Principles of Political Law, Third Edition, Translated by Manouchehr Kia, Tehran: Ganjineh. [In Persia]

Soliman Dehkordi, Elham and Heydarian, Arshianaz (2019). "Explaining Identity Theft in the Iranian Penal System", Persian Law Research Journal, Volume 2, Issue 2, 63-85. [In Persia]

Salehabadi, Zahra (2013). Crimes against Identity with Emphasis on Cyber Environment, Master's Thesis, Faculty of Law, University of Qom. [In Persia]

Katouzian, Naser (2021). Philosophy of Law, Volume 1, Second Edition, Tehran: Ganj Danesh. [In Persia]

Mahmoudi Janaki, Firouz (2015). "Right-Orientation in Criminalization; With Emphasis on the German Theory of Legal Interests", Journal of Criminal Law Research, Volume 3, Number 9, 83-110. [In Persia]

استناد به این مقاله: عباسی لاهرودی، میثم، رسایی، محمد، بهرامی خوشکار، محمد و نقیبی، سید ابوالقاسم . (۱۴۰۴). رویکرد نظام کیفری استرالیا به جرم‌انگاری سرقت هویت. *پژوهش حقوق کیفری*، (۵۰) ۱۳، ۱۴۳-۱۸۰.

Doi: 10.22054/jclr.2025.84663.2744