رویکرد جرم‌شناختی به جعل هویت برای ارتکاب کلاهبرداری

در بانکداری نوین*

□ حسین میرمحمدصادقی[۱]
□ افشین آذری متین[۲]

چکیده

جعل هویت نوعی تقلب است و فناوری اطلاعات، ارتکاب این جرم را تسهیل کرده است. جعل هویت در محیط سایبر، سوءاستفاده از ناتوانی رایانه در شناسایی بدون خطای کاربر رایانه است. یکی از شیوه‌ها استفاده از رمز عبور برای ورود به سامانه‌های بانکی است. چون رایانه تنها می‌تواند رمز عبور صحیح را به عنوان مجوز شناسایی کند، به این دلیل نمی‌تواند کاربر مجاز را از غیر مجاز تشخیص دهد و به این ترتیب مجرمان در واقع هویت را به سرقت نمی‌برند، بلکه

* تاریخ دریافت: ۱۳۹۵/۱۰/۲۰ ـ تاریخ پذیرش: ۱۳۹۶/۲/۲۱.
این مقاله مستخرج از رسالهٔ افشین آذری متین با عنوان *سیاست جنایی ایران در قبال بزه‌های علیه سیستم یکپارچهٔ بانکداری الکترونیکی* است که در دانشکدهٔ حقوق دانشگاه شهید بهشتی در دست تدوین می‌باشد.

۱. استاد دانشگاه شهید بهشتی (drsadeghi128@yahoo.com).
۲. دانشجوی دکتری حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی (نویسندهٔ مسئول) (azarimatin@gmail.com).

از هویت به عنوان ابزاری جهت انجام دیگر فعالیت‌های غیر قانونی استفاده می کنند. به عبارت دیگر، جعل هویت در بانکداری نوین که یکی از کاربردهای فناوری اطلاعات است، دروازهٔ ورود به ارتکاب سایر جرایم خواهد شد. برداشت از حساب‌های بانکی با استفاده از اطلاعاتِ سرقتی یکی از این موارد است که جنبهٔ مالی و اقتصادی دارد.

مشکل اصلی این است که سرقت اطلاعات امنیتیِ کاربران فناوری اطلاعات و به طور خاص کاربران بانکداری نوین به عنوان جرمِ مانع، جرم‌انگاری نشده است و جرم مستقلی نیز تحت عنوان جعل هویت در فضای سایبر نداریم. این امر سبب شده است که تحقیق مستقلی برای علت‌شناسی این جرم انجام نشود. بدین‌ترتیب این تحقیق قصد دارد با برجسته کردن خلأ قانونی موجود، به روش توصیفی و تحلیلی و از طریق شیوه‌های ارتکاب، ویژگی‌های جرم‌شناختیِ جرم جعل هویت را در دو قالب علل وضعیت‌مدار و علل اجتماعی بررسی و روش‌هایی را برای کنترل این جرم ارائه کند.

واژگان کلیدی: بانکداری نوین، نیرنگ‌آمیز، جعل هویت، کلاهبرداری، رمز عبور.

مقدمه

مردم در قالب افتتاح انواع حساب بانکی، نگهداری نقدینگی خود را به بانک‌ها سپرده‌اند. بانک‌ها نیز به عنوان امین مردم وظیفه دارند که سازوکارهای کنترلی و حفاظتی دقیقی را اجرا کنند تا پرداخت پول صرفاً به شخص مورد نظرِ صاحب حساب انجام شود. برداشت پول از حساب‌های سنتی مستلزم حضور ذی‌نفع و احراز هویت او توسط متصدی بانکی است. ابزار برداشت نیز بر حسب نوع حساب بانکی (جاری، پس‌انداز، سرمایه‌گذاری)، دسته‌چک، دفترچهٔ حساب یا گواهی سپرده است. بنابراین اگر شخصی قصد کلاهبرداری از حساب بانکی دیگری را داشته باشد، باید به صورت متقلبانه اقدام به تحصیل ابزار برداشت نماید یا ابزار برداشت فیزیکی را جعل کند و چون بانک تا زمانی که احراز هویت نکند پولی پرداخت نخواهد کرد، کلاهبردار باید خود را به جای ذی‌نفع یا صاحب حساب نیز معرفی کند. تقلب در هویت مستلزم ارائهٔ مدرک هویتی جعلی (شناسنامه یا کارت ملی) به متصدی بانک برای احراز هویت است. در غیر این صورت، امکان برداشت از حساب وجود ندارد. به این عمل، جعل هویت گفته شده و فقط در

مواردی جرم است که طبق مادهٔ ۵۵۵ قانون تعزیرات، شخص خود را در مشاغل دولتی معرفی کند (زراعت، ۱۳۸۳: ۷۲۵). در غیر این صورت، شخصی که در بانک خود را به جای دیگری معرفی کرده است بر اساس مادهٔ ۵۲۵ قانون تعزیرات، به عنوان جاعل اسناد بانکی (میرمحمد صادقی، ۱۳۹۲: ۲۶۷) یا دولتی تحت تعقیب قرار خواهد گرفت.[۱]

اما برداشت پول در بانکداری نوین[۲] که یکی از کاربردهای فناوری اطلاعات است، متفاوت بوده و ابزار برداشت فیزیکی به گذرواژه و کارت بانکی، تغییر ماهیت داده است. در این روش از بانکداری، احراز هویت توسط تجهیزات رایانه‌ای مثل دستگاه‌های خودپرداز یا کارت‌خوان‌های فروشگاهی انجام می‌شود.[۳] بنابراین گذرواژه یا رمز عبورِ عددی و کارت بانکی، جایگزین چک، دفترچهٔ حساب و گواهی سپرده شده است. استفاده از این ابزارها در درگاه‌های بانکی به منزلهٔ تصدیق هویت و مجاز بودن استفاده از آن‌هاست و استفادهٔ غیر مجاز از این ابزارها همان جعل هویت است و چون از این ابزارها برای تبادلات مالی یا انتقال و جابه‌جایی پول الکترونیکی استفاده می‌شود، به سوژه و هدف کلاهبرداران تبدیل شده است.

ضرورت و اهمیت تحقیق از یک‌سو با ماهیت پول الکترونیکی ارتباط دارد؛ چون مالیت دارد، بالاترین آمار جرایم رایانه‌ای را به سوءاستفاده از ابزارهای بانکی اختصاص داده است. همچنین بر خلاف اموال مادی، چون ارزش آن محدود نبوده و خسارات وارده گسترده و کلان است (زیبر، ۱۳۸۳: ۲۰)، به عنوان جرم اقتصادی تلقی خواهد شد

---

۱. اختیار کردن اسم یا عنوان مجعول از مصادیق تمثیلی متقلبانه است که قانون‌گذار در مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ برشمرده است. همچنین قانون تخلفات، جرایم و مجازات‌های مربوط به اسناد سجلّی و شناسنامه مصوب ۱۳۷۰ برای استفاده از شناسنامهٔ دیگری، دریافت شناسنامهٔ موهوم و جعل هویت، مجازات‌هایی را پیش‌بینی کرده است (خالقی و صالح‌آبادی، ۱۳۹۴: ش۱۰۴/۱۰۶ـ۱۰۸).

۲. اصطلاح بانکداری نوین، دو عنوان بانکداری الکترونیکی (ارائهٔ خدمات در تمام ساعات شبانه‌روز و روزهای هفته = ۲۴×۷) و بانکداری مجازی (ارائهٔ خدمات بدون شعبهٔ بانکی) را در بر می‌گیرد (مبینی دهکردی و رسولی‌نژاد، ۱۳۹۰: ۱۹۶).

۳. طبق مادهٔ ۵ دستورالعمل رعایت مقررات مبارزه با پول‌شویی در حوزهٔ نظام‌های پرداخت بانکداری الکترونیکی، تطبیق هویت ارباب رجوع با اقلام اطلاعاتیِ شناسایی مشتری در مراجعات غیر حضوری از طریق ابزارهای شناسایی است.

(جعفری، ۱۳۹۳: ۲۳). به همین دلیل، جعل هویت به منظور کلاهبرداری با کارت‌های اعتباری و بدلی، در یازدهمین کنگرهٔ سازمان ملل متحد دربارهٔ پیشگیری از جرایم اقتصادی نیز مورد توجه قرار گرفته است.[۱] از سوی دیگر، در فضای سایبر جرم مستقلی با عنوان جعل هویت نداریم.[۲] به تعبیر «دورکیم»، رواج ارتکاب جرم می‌تواند هشداری به جامعه باشد، مبنی بر اینکه اخلاق، باورها و ارزش‌های اجتماعی، اقتصادی، سیاسی و فرهنگی موجود در جامعه دگرگون شده است. بنابراین لازم است که قانون‌گذار نیز به نوبهٔ خود در جرم‌انگاری و جرم‌زدایی، تحولات صورت‌گرفته را در نظر گیرد (نجفی ابرندآبادی، ۸۴ـ۱۳۸۳: ۳۵). همچنین طبق نظر «بائر»، سبک بودن یا نداشتن ضمانت اجرا در جرایم اقتصادی، یکی از عوامل ارتکاب بزهکاری اقتصادی است (همو، ۸۵ـ۱۳۸۴: ۱۴۷۳). به علاوه در رابطه با این موضوع، تحقیقات مشابهی انجام شده که بیشتر به مفهوم‌شناسی سرقت هویت و بررسی آن پرداخته است. در برخی پژوهش‌های دیگر، با جرایم سنتی مشابه (طبیبی و خدادادی، ۱۳۹۳: ش۸۷/۱۰) مقایسه شده است، ولی به صورت اختصاصی در بانکداری نوین تحلیل و بررسی نشده است و از این جهت، موضوعی نو و جدید است.

اما هدف از این تحقیق، بررسی جرم‌شناختی شیوه‌های فریب‌کارانهٔ فنی و غیر فنیِ انسانی است که بزهکاران برای تحصیل ابزارهای تصدیق هویت در بانکداری نوین و فریب رایانه استفاده کرده‌اند تا کلاهبرداری کنند. به دلیل عدم دسترسی به پرونده‌های قضایی، روش‌های تحصیل ابزارهای هویتی در بانکداری نوین با استفاده از منابع روزنامه‌ای و وبگاه‌های معتبر استخراج شده است. این شیوه‌ها نسبت به سایر روش‌های کلاهبرداری نوآورانه است و چون بیشتر شگردهای استفاده‌شده، نیاز به مواجههٔ مستقیم با بزه‌دیده ندارد، برای بزهکار پرهزینه نیست. به همین دلیل، بررسی تحلیلی عللِ

۱. مرکز اطلاعات سازمان ملل متحد در تهران به نشانی <www.unodc.org> و <www.unis.univerna.org>.

۲. قانون فدرالِ سرقت هویت مصوب ۱۹۹۸ ایالات متحدهٔ آمریکا این عمل را جرم تلقی کرده است <www.flc.gov.bcp/cloin/pubs/creditlidtheft/htm=low>. همچنین دریافت غیر مجاز اطلاعات خصوصی دیگران، از جمله اطلاعات مربوط به حساب بانکی مانند گذرواژه علاوه بر اینکه می‌تواند مقدمهٔ کلاهبرداری رایانه‌ای باشد، همزمان می‌تواند جزء جرایم علیه حریم خصوصی افراد باشد. ولی به دلیل اینکه تاکنون لایحهٔ حریم خصوصی تصویب نشده است، مستند قانونی ندارد (فضلی و باطنی، ۱۳۸۸: ش۱۹۴/۲۲). نظریهٔ مشورتی اداره کل حقوقی قوهٔ قضاییه به شمارهٔ ۶۵۶/۹۳/۷ مورخ ۹۳/۳/۲۴ نیز صِرف به دست آوردن رمز ورودی را جرم ندانسته است.

ارتکاب سرقت هویت با هدف کلاهبرداری در بانکداری نوین، با کلاهبـرداری سـنتی متفاوت شده است و نیاز به تحلیل علت‌شناختی مستقلی دارد؛ زیرا شـرایط و اوضـاع و احوال متفاوتی برای ارتکاب داشته و از نوع قانون‌گذاری و علل شخصی ـ محیطی متفاوتی نیز نسبت به بزهکار برخوردار است و به همین ترتیب، روش‌هـای پیـشگیرانه نیـز کـاملاً متمایز است. بر این اساس، پژوهش حاضر قصد پاسخ به سؤالات زیر را دارد:

۱. ماهیت جعل هویت رایانه‌ای چیست و چه گونه‌هایی در بانکداری نوین دارد؟

۲. شیوه‌های ارتکاب با کدام یـک از نظریـات جـرم‌شناسـی تطـابق دارد و راهکـار پیشگیرانهٔ کاربردی مبتنی بر روش‌های ارتکاب چیست؟

ساختار تحقیق نیز بر اساس نظریهٔ چندعاملی «کوراکیس» در تبیین جرایم اقتصادی، در دو قسمت طراحی شده است. به عقیدهٔ کوراکیس، بزهکاری ناشی از ترکیب عواملی نظیر شهرنشینی، توسعهٔ صنعت و فنـاوری و شخـصیت بزهکـار اسـت (نجفی ابرندآبادی، ۸۵ـ۱۳۸۴: ۱۴۷۳). بدین‌ترتیب قـسمت اول بـه دلیـل اینکـه فعالیـت بانـک‌هـا در شـهرها متمرکز شده است، به نقش توسعهٔ صـنعت و فنـاوری نـوین و شـهری شـدن ایـن جـرم پرداخته است، به طوری کـه ابزارهـای بانکـداری نـوین را بـه وسـیله‌ای مجرمانـه بـرای دستیابی به سودهای نامشروع و ارتکاب جرم به ویژه جرایم اقتصادی تبدیل کرده است. روش‌های استفاده‌شده در این قسمت با نظریات جرم‌شناسـی عمـل مجرمانـه (تجربـی) تبیین شده، جنبـهٔ علـت‌شـناختی نـدارد و شـگردهای بزهکـاری را بـر اسـاس شـرایط و موقعیت بزه‌دیده و سبک ارائهٔ خدمات بانکداری نوین توضیح خواهـد داد. بـه عبـارت دیگر در بررسی‌های به عمل‌آمده، چـون مـسئلهٔ تقـصیرزدایی از مجـرم مطـرح نیـست و معادلات مجرم، بزهکاری را به بزه‌دیده منتقـل کـرده اسـت، عمـل مباشـر جـرم کـه بـا سبُک و سنگین کردن عملش تصمیم‌گیـری کـرده اسـت، از طریـق مطالعـات میـدانی بررسی خواهد شد. در قسمت دوم، نظریات جامعه‌شناسی جنایی در رابطه با روش‌هـای ارتکابیِ سرقت هویت منتهی به کلاهبرداری در بانکداری نوین نقد و ارزیـابی خواهـد شد. این نظریات جنبهٔ علت‌شناسی دارد و با تمرکز بر نوع آلت ارتکاب جرم در جـرایم اقتـصادی، رابطـهٔ بـین توسـل بـه دروغ فریبنـدهٔ غیـر زبـانی در جـرایم نیرنـگ‌آمیـز و کلاهبرداری در بانکداری نوین را روشن خواهد ساخت. بدین‌ترتیب در این دو قالـب،

روش‌های ارتکاب توضیح داده شده، با نظریات جرم‌شناسی مرتبط می‌گردد و به مناسبت راه حل‌های پیشگیرانه کاربردی ارائه خواهد شد.

۱. عوامل وضعی سرقت هویت برای ارتکاب کلاهبرداری در بانکداری نوین

بانک جهانی از وجود ۲۹/۱ شعبهٔ بانک در ایران به ازای هر یکصد هزار نفر خبر داده است. این تعداد شعبه، بالاتر از استانداردهای جهانی است و نشان‌دهندهٔ عدم توسعهٔ بانکداری الکترونیک در کشور است (*روزنامهٔ خراسان*، ۱۳۹۳/۷/۸: ش۱۴/۱۸۷۹۸). در عین حال، آمارهای بانک مرکزی حکایت از آن دارد که در شبکهٔ بانکی کشور تا پایان شهریور ۱۳۹۵، حدود ۳۵۰ میلیون کارت بانکی صادر شده و جمع تراکنش‌ها بالغ بر ۴۵۰ میلیون است (آمار منتشرشده در وبگاه بانک مرکزی به نشانی: <www.cbi.ir>). از این آمار، ۴۵۰ هزار کارت و ۵ میلیون تراکنش مربوط به شرکت دولتی پست‌بانک است. این شرکت، وظیفهٔ ایجاد و گسترش خدمات پست مالی در مناطق روستایی را بر عهده دارد.[۱] مقایسهٔ این آمارها نشان‌دهندهٔ ماهیت شهری بانکداری الکترونیک است و از این لحاظ به رشتهٔ جامعه‌شناسی شهری مرتبط است.[۲] زیرا بانکداری الکترونیک از نظر اقتصادی به عنوان یکی از کارکردهای پایهٔ شهری مطرح است[۳] و در جامعه‌شناسی شهری

۱. برای کسب اطلاعات بیشتر ر.ک: بند ۴ مادهٔ ۴ قانون تشکیل شرکت پست جمهوری اسلامی ایران مصوب ۱۳۶۶، تبصرهٔ ۳ ماده واحدهٔ قانون تأسیس شرکت دولتی پست‌بانک مصوب ۱۳۷۴ و مادهٔ ۳ اساسنامهٔ شرکت دولتی پست‌بانک مصوب ۱۳۷۵/۲/۳۰ هیئت وزیران.

۲. موضوعات جامعه‌شناسی شهری (urban sociology)، بسیار گسترده و متنوع است و به مباحثی چون: قشربندی اجتماعی، گروه‌های کوچک، سازمان‌های رسمی، توسعهٔ اقتصادی و... پرداخته است. به همین جهت، جامعه‌شناسی شهری در مباحث خود یا علوم دیگر مانند انسان‌شناسی، اقتصاد، جغرافیا، اقتصاد سیاسی و... تداخل یافته است (شارع‌پور، ۱۳۸۷: ۱۱).

۳. بر اساس مفهوم پایهٔ اقتصادی، دو نوع فعالیت (کارکرد) برای شهرها وجود دارد: اول، کارکرد پایه‌ای (اساسی) است که برای رشد شهرها ضروری است. این گونه فعالیت‌ها شامل کارخانه، تجارت کالاها یا تأمین خدمات است و دوم کارکرد شهرساز است که از نوع خدمات‌رسانی به شهر است؛ مانند خواروبارفروشی، رستوران و...، و پاسخ‌گوی نیازهای ساکنان داخل شهر است. با توجه به تعریف و ویژگی‌هایی که از بانکداری الکترونیک ارائه شده، از نوع کارکردهای پایه (اساسی) به حساب آمده است (صدیق سروستانی، ۱۳۹۱: ۹۵).

به مباحث توسعهٔ اقتصادی نیز پرداخته شده است. از نظر مکتب شیکاگو[۱] نیز شهر نوعی نظم اجتماعی و اقتصادی مدرن ناشی از کاپیتالیسم صنعتی است که ریشه در بوم‌شناسی شهری دارد (شارع‌پور، ۱۳۸۹: ۱۳۵). ریشه‌های نظری بوم‌شناسی شهری[۲] به نظریهٔ دورکیم[۳] و اثر معروف او یعنی تقسیم کار اجتماعی مرتبط است (دورکیم، ۱۳۸۱: ۶۳). بوم‌شناسی شهری که به بررسی رفتار یک فرد شهرنشین در قالب محیط شهری پرداخته است،[۴] سبب شد که پایه‌گذاران مکتب شیکاگو، جامعه‌شناسی شهری جرایم شهری[۵] را وارد حوزهٔ مطالعات اجتماعی نمایند. بزهکاری اقتصادی و مالی نوعی از جرایم شهری است؛[۶]

۱. به طور معمول هنگامی که به مکتب شیکاگو اشاره می‌شود، منظور مجموعه‌ای از تحقیقات و نوشته‌های علوم اجتماعی است که بین سال‌های ۱۹۱۵ و ۱۹۴۰ توسط اساتید و دانشجویان دانشگاه شیکاگو انجام شده است (کولن، ۱۳۹۴: ۱۰).

۲. بوم‌شناسی شهری (urban ecology) و بوم‌شناسی انسانی (human ecology) از ره‌آوردهای مکتب شیکاگو است. در بوم‌شناسی شهری، نحوهٔ استفاده از زمین در نواحی مختلف شهری مشخص خواهد شد و در بوم‌شناسی انسانی به نحوهٔ انطباق انسان با محیط شهری پرداخته شده است (شارع‌پور، ۱۳۸۹: ۱۳۴).

۳. دورکیم معتقد است که هر وقت تعداد زیادی انسان در یک محل تجمع یابند، لازم است که تقسیم کار پیچیده‌ای صورت گیرد. به نظر او جامعه، افراد مختلفِ دارای تخصص را در یک کل منسجم کرده است و همین انسجام، منتهی به همبستگی سازمان‌یافته شده است؛ زیرا به سبب وجود یک تقسیم کار پیچیده، هر یک از اعضای جامعه به دیگری وابسته است و این وابستگیِ هر یک از اعضا به کل (یعنی همبستگی سازمان‌یافته) عامل اصلی اتحاد اعضاست. بر این اساس، دورکیم بر این نظر تأکید داشت که چنانچه تقسیم کار اجتماعی منظم نباشد، بزهکاری در محیط‌های شهری جدید رو به فزونی خواهد گذاشت (نجفی ابرندآبادی، ۱۳۸۳: ۳۱).

۴. ساختار جامعهٔ شهری منجر به ارتکاب جرایمی شده که نمی‌توان نظیر آن را در نقاط دیگر دید. فعالیت‌های شهری بر خلاف روستاها، به روزانه و شبانه، صنعت و خدمات و... تقسیم شده است. به علاوه شهرها دارای نقاط کور زیادی بوده و مستعد جرایم بیشتری نسبت به سایر نقاط هستند. اندازهٔ محیط‌های شهری و ناشناس بودن مردم برای همدیگر، از جمله وسایل دسته‌بندی‌های مختلف میان مردم در شهرهاست. از دید جرم‌شناسی، شهرنشینی منجر به ایجاد فرصت‌های بیشتری برای ارتکاب جرم شده و فقدان یا ضعف کنترل‌های غیر رسمی اجتماعی، زمینه را برای فعالیت‌های مجرمانه فراهم ساخته است (السان، ۱۳۸۷: ۹/۹).

۵. جرایم شهری، آن بخش از ناهنجاری‌ها، کجروی‌ها و قانون‌شکنی‌های اجتماعی تعریف شده است که در نتیجهٔ پیدایش شهرنشینی و تشدید مشکلات ناشی از آن در چارچوب نظام شهری و به عنوان مانعی در جهت تأمین انتظام و تعادل شهری پدیدار گردیده است (موسوی، ۱۳۷۸: ش۱/۱۱).

۶. از جملهٔ نظریات جامعه‌شناسی جنایی که به تأثیر انواع محیط بر بزهکاری پرداخته است، قانون اشباع و فوق اشباع جنایی است که بی‌ارتباط با جرایم شهری نیست. در این قانون بر اساس معیار جغرافیایی، نرخ بزهکاری روستایی با شهری مقایسه و مشاهده شده است که بزهکاری اقتصادی و مالی، یک پدیدهٔ شهری است (نجفی ابرندآبادی، ۱۳۸۳: ۲۲۸۴).

از این رو سیاست جنایی مقابله بـا جـرایم اقتـصادی و جرایمـی کـه از طریـق ابزارهـای بانکداری الکترونیک رخ خواهد داد، باید «شـهرمحور» بـوده و بـا مقتـضیات شـهری تطابق داشته باشد.[1]

ویژگی شهرمحور بودن بـا نقـش عوامـل وضـعی در ارتکـاب جـرم کلاهبـرداری از طریق سرقت هویت، با ابزارهای بانکداری نوین در ارتباط است؛ چون رابطهٔ بین فقـر و بی‌کاری با بزهکاری مطرح نیست، به نقش شخصیت بزهکار در گذر اندیـشه بـه فعـل نیز بی‌اعتناست و به بررسی ساختار اجتماع و محیط پیرامونی که شخص در آن زنـدگی می‌کند، خواهد پرداخت. به همین دلیل، کلاهبرداری از این طریـق، بـا نظریـهٔ فرصـت تبیین خواهد شد. فرصت‌های ارتکاب جرم گاهی مربوط به افراد و گاهی مربوط به اشیا و اموال است (محمدنسل، ۱۳۸۶: ش۳۰۴/۳). رشد فناوری در صـنعت بانکـداری از جملـهٔ فرصت‌های بزهکاری است که باعث تحـول فعالیـت‌هـای روزانـهٔ مـردم و ایجـاد سـیبل جاذبه‌دار گردیده و عدم حفاظت و مراقبت از سیبل را جـرم‌زا کـرده اسـت (فیـشر و لـب، ۱۳۹۳: ۲۰۹/۱). به همین دلیل، ویژگی شهرمحور بودن، با دو نظریهٔ مـشهور بـه انتخـاب عقلانی: «نظریهٔ فعالیت روزانه» و «نظریهٔ شیوه و سبک زندگی» مرتبط است (صـفاری و کونانی، ۱۳۹۲: ۱۱۳). در نظریه‌های مشهور به گزینهٔ عقلانی، انسان مجرم بـه عنـوان یـک انسان مقتصد، محاسبه‌گر و معقول ترسیم و مطالعـه شـده اسـت. مجـرم در ایـن نظریـه کسی است که هزینـه‌هـای ارتکـاب جـرم را سـنجیده و سـپس انتخـاب خواهـد کـرد. انتخاب بزهکار بر اساس موقعیت، سن، شغل و هویت اجتماعی بزه‌دیده شکل می‌گیرد (ویلیامز و دیگران، ۱۳۸۳: ۲۴۲). بدین‌ترتیب این دو نظریه بر اساس شیوه‌هـای جعـل هویـت در بانکداری نوین مورد بررسی قرار خواهد گرفت.

۱ـ۱. نظریهٔ فعالیت روزانه

از جمله شیوه‌هایی که در بانکـداری نـوین از دیـدگاه بـزه‌دیـدگان قابـل بررسـی اسـت، روش‌های غیر فنیِ دسترسی به گذرواژه به شیوهٔ انواع مهندسی اجتماعی مبتنی بر انسان

۱. در سیاست جنایی سازمان ملل متحد، زیست‌بوم انسانی مورد توجـه واقـع گردیـده و در بیانیـهٔ اسـتانبول دربارهٔ سکونتگاه‌های انسانی ۱۹۹۶، به توسعهٔ اقتـصادی و اجتمـاعی شـهرهای بـزرگ و کوچـک توجـه شده است (عامری سیاهوئی، ۱۳۸۷: ۱۳۴).

است. در این شیوه، بزه‌دیده به عنوان عامل شتاب‌دهنده و اثرگذار در ارتکاب جرم مطرح است و در شکل‌گیری و عملی نمودن اندیشهٔ مجرمانه، موجب تسریع در حرکت فرایند جنایی خواهد شد. در نظریهٔ فعالیت روزانهٔ مطرح‌شده، تحولات اقتصادی که از طریق رشد فناوری و صنعت به وجود آمده، سبب تحول فعالیت‌های روزانهٔ مردم شده است. از جملهٔ این تحولات، ارائهٔ خدمات بانکی بدون مراجعه به شعب بانک است. دستگاه‌های خودپرداز، کارت‌خوان‌های فروشگاهی[1] یا درگاه‌های اینترنتی بانک از طریق کارت بانکی یا رمز عبور (گذرواژه) خدمات مالی ارائه می‌کنند. یکی از شیوه‌هایی که در بانکداری نوین، بزه‌دیده به عنوان علت ارتکاب جرم مطرح است، شیوهٔ مهندسی اجتماعی است. در شیوهٔ مهندسی اجتماعی مبتنی بر انسان از بی‌احتیاطی یا اطمینان بیش از حد انسان‌ها برای جمع‌آوری اطلاعات حساس استفاده شده است. با این توضیح، شیوه‌هایی که بر اساس این نظریه رخ داده، بررسی خواهد شد.

در روش خالی کردن حساب از طریق جستجو در زباله‌های بانکی، رئیس پلیس فتای تهران از دستگیری جوانی با مدرک کارشناسی خبر داد. وی کسانی را که در بانک اقدام به افتتاح حساب و دریافت کارت بانکی می‌کردند، شناسایی و تعقیب می‌کرد. هنگامی که این مشتریان برای تعویض رمز کارت خود به دستگاه خودپرداز مراجعه می‌کردند و پاکت حاوی رمز اولیهٔ کارت را باز کرده و به سطل زباله می‌انداختند، او این کاغذ را برداشته و با استفاده از اطلاعات درج‌شده (شامل رمز اول و دوم کارت) اقدام به برداشت اینترنتی می‌نمود.

در موردی دیگر، برادرزن با استفاده از رمز اینترنتی داماد اقدام به برداشت غیر مجاز

---

۱. درگاه‌های حضوری بانکی عبارت‌اند از:

الف) دستگاه خودپرداز (ATM = Automated Teller Machin) با شناسایی مشتریان از طریق کارت بانکی، به آن‌ها امکان دریافت وجه از حساب، انتقال پول به سایر حساب‌ها، پرداخت قبوض، خرید شارژ و بررسی گردش حسابشان را بدون نیاز به تحویل‌دار بانک ممکن خواهد ساخت.

ب) پایانهٔ فروش (POS = Point of Sale) یا کارت‌خوان فروشگاهی دستگاهی است که با پذیرش کارت بانکی، امکانی را فراهم خواهد کرد که وجه به صورت الکترونیکی از حساب دارندهٔ کارت به حساب فروشنده منتقل شود و معمولاً در فروشگاه‌ها و مراکز تجاری کاربرد دارد.

و خرید اینترنتی کرده بود. در این رابطه رئیس پلیس فتای استان خراسان رضوی هشدار داد که در خریدهای آنلاین، تحت هیچ شرایطی از رمزهای اینترنتی در حضور دیگران استفاده نشود و در صورت اجبار، بلافاصله رمز تغییر داده شود.

روش دیگر، پرسه‌زنی در کنار دستگاه‌های خودپرداز بانک‌ها با نیت کمک به افراد مسن و بی‌سواد است. در پروندهٔ نیکوکار قلابی، رئیس پلیس فتای استان فارس اعلام کرد که نیکوکار قلابی پس از جلب رضایت مراجعان و اخذ عابربانک به همراه رمز کارت، در یک فرصت مناسب اقدام به فعال‌سازی رمز دوم حساب (رمز اینترنتی) کرده و پس از ترک محل، کل حساب قربانیان خود را خالی نموده است.

در روش دیگر، ادارهٔ نظام‌های پرداخت بانک مرکزی، نسبت به روش فیشینگ تلفنی هشدار داد و اعلام نمود که افرادی طی تماس تلفنی با برخی از مشتریان بانک، خود را به عنوان نمایندهٔ بانک در امور فناوری اطلاعات و خدمات الکترونیک معرفی کرده و به شیوه‌های گوناگون، مبادرت به اخذ اطلاعاتی نظیر رمز اول و دوم حساب بانکی و کلاهبرداری نموده‌اند.

۱ـ۲. نظریهٔ سبک زندگی

بانکداری نوین، شیوهٔ دریافت خدمات مالی به مردم را تغییر داده و این شیوه‌ها، زندگی مالی مردم را از حالت بسته و محتاطانه خارج کرده و در معرض دید عموم قرار داده و بدین‌ترتیب احتمال بزه‌دیدگی را افزایش داده است. نظریهٔ شیوه و سبک زندگی نیز نوع فعالیت‌های روزانه در زمینه‌های مختلف شغلی، تفریحی را هدف قرار داده و بیان داشته که هر چه شیوهٔ زندگی بازتر باشد، شانس بزه‌دیدگی نیز بیشتر است (والک لیت، ۱۳۸۶: ۷۱). بدین‌ترتیب دو روش رایج مطابق نظریهٔ فوق توضیح داده خواهد شد.

برای مثال، روش ساده‌ای که در شعبهٔ ۸۰۲ بازپرسی مجتمع قضایی شهید قدوسی مشهد رسیدگی شده، «بدل‌اندازی با کارت‌های سوخته» نام گرفته است. در این روش، مرتکب با پرسه‌زنی در اطراف دستگاه‌های خودپرداز، قربانیان خود را که بیشتر افراد سالخورده و کم‌سواد بودند شناسایی می‌کرد و قربانیان که تصور داشتند این شخص نیز مثل خودشان قصد دریافت خدمات از دستگاه خودپرداز را دارد از او

تقاضای کمک می‌کردند. طبق اعلام رئیس پلیس آگاهی خراسان رضوی، در مواردی مرتکب به این بهانه که قصد دارد مثلاً مبلغ ۵۰ هزار تومان به حساب بانکی فردی بی‌بضاعت واریز کند، اما کارت بانکی خود را به همراه ندارد، این مبلغ را نقدی به قربانی پرداخت می‌کرد و چون قربانیان قادر به استفاده از کارت خود نبودند، استفاده از کارت را به مرتکب واگذار می‌کردند. این شخص نیز هنگام استفاده از کارت، مبالغ زیادی را به حساب‌های دیگر انتقال می‌داد یا با دسترسی به رمز کارت که از صاحب آن می‌پرسید، به بهانهٔ اینکه دستگاه خودپرداز خراب است و باید به خودپرداز دیگری مراجعه شود، در یک لحظه کارت بانکی را با کارت‌های خالی و سوختهٔ مسروقه تعویض و سپس استفاده می‌کرد. در این پرونده، ادارهٔ جعل و کلاهبرداری پلیس آگاهی خراسان رضوی اعلام کرد که متهم ۳۳ ساله که از وی ۲۳ عدد کارت مسروقه کشف شده است و تا کنون ۳۰ شاکی دارد، با این روش ۲۰۰ میلیون تومان تحصیل کرده است. به طوری که ملاحظه می‌گردد، در این شیوه اگر بزه‌دیدگانْ سیستم پیامکیِ حساب بانکی خود را فعال کرده بودند، بلافاصله متوجه انتقال گردیده و مانع بزه‌دیدگی می‌شدند.

۲. عوامل اجتماعی سرقت هویت برای ارتکاب کلاهبرداری در بانکداری نوین

جعل هویت در بانکداری نوین، جنبهٔ فنی و تخصصی دارد و یکی از اشکال تقلب علیه سیستم پردازش خودکار داده‌هاست. ابزار مورد استفاده نیرنگ و تزویر است. این روش رفتار شخص را در وضعیت عدم تعادل قرار داده که بر خلاف عدالت است. وقتی از این حالت عدم تعادل مشخص سوءاستفاده شود، یعنی فریب مؤثر واقع شده و تحصیل مال صورت پذیرفته است. در این صورت بزهکار توانسته به یک هدف ضد ارزش که همان منافع اقتصادی نامشروع است دست یابد، ارزش نقض‌شده امنیت اقتصادی و مورد حمایت حقوق جزاست. معیار جرم‌انگاری آن نیز جلوگیری از ضرر است. به‌همین دلیل این جرم اقتصادی و مبتنی بر تزویر است. در مقابل، استفادهٔ منصفانه و

متعادل از زرنگی که مفهومی مقبول و خنثی است، جرم نیست، ولی نیرنگ به عنوان وسیله‌ای که باعث نقض یک ارزش مورد حمایت حقوق جزا شده است، وسیلهٔ مجرمانه بوده و محکوم است. بدین سبب حقوق جزا به حقوق وسایل نیز تعبیر شده است.

ماهیت کلاهبرداری با روش جعل هویت مبتنی بر دروغ است؛ چون اطلاعات شفاهی و غیر شفاهیِ غلط ارائه می‌شود تا دیگری فریب بخورد و اطلاعات امنیتی حساب یا کارت بانکی خود را افشا نماید. این اقدام نوعی خشونت انحرافی (گسن، ۱۳۸۹: ۲۵) به‌حساب آمده و دروغی فریبنده است که باعث خواهد شد کاربران بانکداری الکترونیک متوجه حملهٔ مزورانه و نیات واقعی طرف مقابل نشوند و چون به گفته‌های دروغ اعتماد کرده و در نتیجه دفاعی برای حفاظت از اطلاعات بانکی خود پیش‌بینی نکرده‌اند، به همین خاطر جزء دروغ‌های حمله و دفاع از نوع منفعت‌محور است. در حقیقت دروغ‌گو در قالب یک فعالیت روان‌شناختی ارتباطی جلب اطمینان کرده و رفتار مخاطب را هدایت خواهد کرد. در حالی که اگر اطلاعات درست بود نتایج متفاوتی به دنبال داشت و مخاطب در مسیر مورد نظر کلاهبردار که همان کسب منافع است، قرار نمی‌گرفت. بنابراین این نوع دروغ خودخواهانه است؛ چون برای کسب منافع صورت گرفته است. بر اساس روان‌شناسی اجتماعی نیز این دروغ‌گویان ماهرند و از قدرت کنترل کامل هیجانات و توان بالای کنترل رفتارهای کلامی و غیر کلامی برخوردارند.

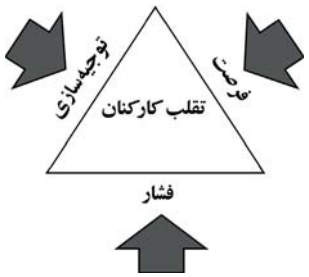
عمل دروغ‌گویی یک اقدام تعاملی و دوسویه است و برای رسیدن به هدف تحصیل مال همانند یک مجموعهٔ ساختاری از عناصر است. یکی از عناصر ساختاری، شرایط و اوضاع و احوال دروغ است که در دو سطح ایجاد خواهد شد؛ سطح اول مربوط به جایی است که ایدهٔ توسل به دروغ شکل گرفته و به آن اوضاع و احوال ایجادکننده گفته‌اند. این شرایط به القای اندیشهٔ توسل به دروغ در وجدان فرد کمک خواهد کرد. در رابطه با کلاهبرداری در بانکداری نوین، شرایط ایجادکننده توسعهٔ نوآوری‌های فنی مانند توسعهٔ پرداخت و دریافت پول با کارت بانکی است که موجب شکل‌گیری شرایط ایجادکنندهٔ دروغ گردیده و ارتکاب جرم کلاهبرداری را با نظریهٔ فرصت تبیین

کرده است؛ زیرا در وضعیت کنونی، استفاده از فناوری‌های نوین اطلاعاتی با توسعه و رشد قابل توجهِ فرصت‌های کلاهبرداری قابل توجیه است.

اما باید خاطرنشان ساخت که اگر این اوضاع و احوال، اثر افزایشی بر برخی از اشکال دروغ داشته باشد، همه مرتکب آن نمی‌شوند. بی‌تردید شخصیت مرتکب در اینجا بی‌تأثیر نیست. در هر حالت، شرایط و اوضاع و احوال باید گذر از اندیشه به فعل را اجازه دهد. اینجاست که نوع دومِ اوضاع و احوال یعنی شرایط محقق‌کننده ظاهر خواهد شد (همان: ۱۴۳ـ۱۴۷). شکل‌گیری این نگرش در ذهن همان چیزی است که دیوید متزا آن را فنون خنثی‌سازی نامیده است. فنون خنثی‌سازی نوعی توجیه‌سازی آگاهانهٔ اعمال مجرمانه است (همان: ۱۰۵). با این مقدمه به تحلیل و بررسی سایر روش‌های جعل هویت در بانکداری نوین پرداخته خواهد شد. توضیح این روش‌ها بر پایهٔ نظریات جرم‌شناسی علت‌شناسی است که بر خلاف نظریات عقلانی‌محور به علل شخصی و محیطی پرداخته خواهد شد و ساختار شکل‌گیری دروغ و چگونگی کاربرد آن در بانکداری نوین را نشان خواهد داد.

۲ـ۱. نظریهٔ مثلث تقلب

مثلث تقلب مجموعه‌ای از عوامل مشترک برای متقلبان درون‌سازمانی در تمام سطوحِ مؤسسات خدمات مالی است که دارای عناوین خیانت در امانت یا اختلاس است.



دونالد کرسی[1] برای ارتکاب جرم اختلاس، فرایندی را با سه مرحله بیان داشته که به مثلث تقلب[2] معروف شده است؛ فشار به مشکلات مالی مربوط می‌شود که آن‌ها را

1. Donald Cressy.
2. Fraud Triangle.

آشفته کرده است. فرصت، زمانی به وجود می‌آید که یک کارمند ضعفی را در کنترل‌های ضد تقلب سازمان کشف کند و گمان کند که در دام نخواهد افتاد و توجیه‌سازی یک فرایند روانی است که بر اساس آن، فردی که مرتکب تقلب شده است، خود را متقاعد خواهد کرد که کار نادرستی انجام نداده است؛ مثلاً وجوه را دوباره به جای اول خود برخواهد گرداند یا او لیاقت وجوه سرقت‌شده را داشته، چون بانک با عدم ترفیع او در حقش اجحاف کرده است (گلدمن، ۱۳۹۲: ۴۵ـ۴۶). این نظریه در رابطه با جعل هویت توسط کارکنان بانک نیز مصداق دارد و در بانکداری نوین از طریق دسترسی غیر مجاز به تجهیزات رایانه‌ای صورت می‌گیرد. در زیر نمونه‌هایی توضیح داده خواهد شد.

در بانکداری نوین، یکی از دستکاری‌های رایانه‌ای از طریق درگاه تحویلداری است[۱] که از نوع دستکاری اطلاعات ورودی است. این نوع فریبکاری با استفاده از داده‌ها[۲] توسط کارمندان بانک انجام‌شدنی است؛ برای معرفی نمونه‌ای از جعل هویت و دستکاری اطلاعات توسط کارمندان، می‌توان به پروندهٔ یک کارمند بانک دولتی در شعبهٔ ۷۰۳ دادسرای عمومی و انقلاب مشهد اشاره کرد که با ۲۰ سال سابقهٔ کاری، تحویلدار یک شعبهٔ محلی بوده است. در تحقیقات قضایی مشخص شد که این کارمند با استفاده از رمز کاربری برخی همکارانش و بدون اطلاع آن‌ها، وارد سیستم بانکی شده و پس از شناسایی حساب‌های مشتریان خوش‌حساب اقدام به برداشت و انتقال میلیون‌ها تومان به حساب خود و دیگر حساب‌های مورد نظرش نموده است.[۳]

مثال دیگر به کارمندی دیگر در یک بانک دولتی مربوط است که با سوءاستفاده از

۱. درگاه تحویلداری به آن بخش از امور بانکی اطلاق می‌شود که کار دریافت و پرداخت وجوه نقدی یا امور مربوط به انتقالات وجوه از حساب‌ها را به عهده دارد. این قسمت که رابطهٔ مستقیم با مشتریان بانک دارد، صندوق نامیده می‌شود (ادارهٔ آموزش و مدیریت بانک ملی ایران، ۱۳۸۲: ۴۸).

۲. بر اساس گزارش *روزنامهٔ خراسان* از دادسرای جرایم رایانه‌ای تهران، صاحب یک شرکت خصوصی اقدام به اخراج حسابدار شرکت کرد، ولی رمزهای اینترنتی حساب بانکی شرکت را تغییر نداد. کارمند اخراجی که به رمزهای حساب دسترسی داشت، اقدام به برداشت و انتقال مبلغ ۲۰ میلیون تومان از حساب شرکت کرد.

3. Data diddling.

سیستم چکاوک[1] اقدام به برداشت بیش از ۱۲ میلیارد ریال از حساب مشتریان کرده بود. رئیس پلیس فتای استان تهران خبر داد که از طریق بررسی سیستم رایانه‌ای کارمند یک بانک دولتی مشخص شد که وی بدون اطلاع مسئولان بانک و با سوءاستفاده از موقعیت خود، رمزهای عبور را در سیستم خود ذخیره نموده و بدین طریق اقدام به نقد کردن چک‌های فاقد موجودی کرده است.

تغییر دوره‌ای پست، توزیع وظیفه بین چند نفر و حفاظت از کلمات عبور، از جمله تدابیر درون‌محیطی برای پیشگیری از این جرم است (ابراهیمی و صادق‌نژاد نائینی، ۱۳۹۲: ش۱۶۶/۵).

۲ـ۲. نظریهٔ عمومی فشار رابرت اگنو

نظریهٔ عمومی فشار، از رویکرد اجتماعی ـ روان‌شناختی پیروی می‌کند و پیوند بین منابع فشار، احساسات منفی ناشی از فشار و رفتار مجرمانهٔ فردی را بررسی می‌کند. به بیان دیگر، رابرت اگنو مفهوم فشار را فراتر از رویکرد مرتون بسط داد و به جای تأکید صرف بر فشارهای اقتصادیِ مدّنظر مرتون، چندین منبع فشار را معرفی کرد که ممکن است منجر به حالات یا احساسات منفی به ویژه خشم شده و در نهایت منجر به رفتارهای ضد اجتماعی گردد. نظریهٔ عمومی فشار، قابل تعمیم برای کلیهٔ افراد طبقات ضعیف، متوسط و ثروتمند است و از این جهت نیز نسبت به نظریهٔ مرتون عمومیت دارد. اما نکتهٔ مشترک در هر دو نظریه، نوآوری مجرمانه برای دستیابی به اهداف مادی است (نجفی ابرندآبادی و صادق‌نژاد نائینی، ۱۳۹۲: ش۶۲/۱۳) که برخی شیوه‌های جعل هویت از این طریق را قابل تحلیل کرده است و در ذیل خواهد آمد.

در روشی که در کشور آلمان اتفاق افتاد و مرتکبان در ۱۶ ژانویهٔ ۱۹۸۶ به وسیلهٔ

---

۱. سامانهٔ چکاوک، مسئولیت تبادل تصاویر و اطلاعات چک را بر عهده دارد. کل فرایند به این صورت است که مشتری، چک را به بانک خود تحویل داده تا شعبهٔ تحویل‌گیرندهٔ چک پس از اسکن چک، تصویر چک را به همراه اطلاعاتی نظیر شمارهٔ حساب و نام ذی‌نفع به بانک بدهکار ارسال کند. شعبهٔ پرداخت‌کننده پس از کنترل اطلاعات و کنترل موجودی حساب مشتری، چک را در صورت کفایت حساب پاس کرده و در غیر این صورت در سامانه، اعلام عدم کفایت موجودی خواهد کرد. بانک بستانکار نیز بر اساس نتیجهٔ اعلام‌شده توسط بانک بدهکار، وجه مورد نظر را به حساب مشتری واریز خواهد نمود.

دوربین مخفی شناسایی و دستگیر شدند، آنان یک عدد کارت خالی را در محل قرارگیری کارت دستگاه خودپرداز وارد نموده و جایگاهی را نیز برای وارد کردن کارت به دستگاه خودپرداز متصل کردند تا مشتری کارت خود را در این قسمت وارد نماید. بدیهی است که چون کارت خالی قبلاً به قسمت کارت‌خوان دستگاه خودپرداز وارد شده بود، مشتریان با ورود رمز کارت خود با خطای رمز مواجه می‌شدند و طبق برنامهٔ امنیتیِ دستگاه‌های خودپرداز، با ورود سه بار رمز به صورت اشتباه، کارت خالی توسط دستگاه ضبط می‌گردید. مشتریان نیز به تصور ضبط کارتشان توسط دستگاه، محل را ترک می‌کردند. در این لحظه مرتکبان کارت را از محل قرارگیری آن برمی‌داشتند[۱] و برای فهمیدن رمز مشتری نیز صفحه‌کلید دستگاه خودپرداز را از قبل به روغن آغشته می‌کردند و بدین‌ترتیب کلیدهای مورد استفاده مشخص می‌شد که با آزمایش ۴ رقم استفاده‌شده، شمارهٔ صحیح را پیدا می‌کردند.[۲] مرتکبان از این طریق، حدود ۸۰۰۰ مارک آلمان به دست آورده بودند (زیبر، ۱۳۸۳: ۳۲).

در پروندهٔ دستبرد ۳۶۰ میلیون تومانی به ۱۳۷ کارت اعتباری، فرمانده انتظامی خراسان رضوی اعلام کرد که روش به کاررفته، استفاده از دستگاه «اسکیمر»[۳] بوده است. در این پرونده، متهم ۲۹ ساله اقدام به خرید یک دستگاه اسکیمر به همراه

۱. یکی دیگر از روش‌های به دست آوردن کارت، ریختن چسب مایع در محل کارت دستگاه خودپرداز است که پس از ناامید شدن صاحب کارت از دریافت آن و ترک محل، سارقان کارت را برداشته و استفاده خواهند کرد.

۲. از جملهٔ روش‌های تحصیل گذرواژه، قرار دادن صفحه کلید بدلی شبیه صفحه کلید اصلی روی دستگاه خودپرداز است، به گونه‌ای که کاربر متوجه نخواهد شد که یک صفحه کلید اضافی روی شماره‌های اصلی قرار گرفته است. بدین‌ترتیب کاراکترهای گذرواژه کپی خواهد شد. نصب و استتار دوربین کوچک بالای دستگاه خودپرداز یا ایستادن کنار کاربر به منظور دیدن و خواندن کلمهٔ عبور، از جملهٔ روش‌های غیر فنیِ دسترسی به گذرواژه به شیوهٔ انواع مهندسی اجتماعی مبتنی بر انسان است.

۳. به کپی غیر قانونی علائم نوار مغناطیسی بانکی روی کارت دیگر، اسکیمینگ (Skimming) گویند. اسکیمرها دستگاه‌های کوچکی هستند که در محل ورودی دستگاه خودپرداز بانک‌ها، خودپردازهای تقلبی و یا روی دستگاه کارت‌خوان فروشگاهی نصب می‌شوند. اسکیمینگ از این واقعیت پیروی کرده که قسمت مغناطیسی لبهٔ بیشتر کارت‌های عابربانک را می‌توان کپی کرد و یا تغییر داد. دانش لازم برای دستکاری قسمت مغناطیسی تا حد زیادی از طریق مطالعهٔ استانداردهای بین‌المللی همگانی مربوط به کارت‌های عابربانک به دست آمده است (زیبر، ۱۳۸۳: ۳۰).

کارت خام بانکی نموده و با بازگشایی مغازهٔ کلی‌فروشیِ محصولات آرایشی بهداشتی و نصب اسکیمر روی دستگاه کارت‌خوان فروشگاهی، تعداد زیادی کارت بانکی را کپی کرده بود. رئیس پلیس فتای استان تهران نیز در مهرماه ۱۳۹۴ از پرونده‌ای مشابه خبر داد که سرقت نامرئی ۷۰۰ میلیون تومانی از ۴۱ نفر نام گرفت. در این پرونده، رمز مشتریان به بهانهٔ کوتاه بودن سیم دستگاه کارت‌خوان پرسیده شده بود.

بدین‌ترتیب منابع فشار مادی و غیر مادی به فرد اجازه خواهد داد تا برای دستیابی به اهداف مادی به عنوان نوآور از وسایل مجرمانه استفاده کند که جنبهٔ نیرنگ‌آمیز داشته و خلاقانه است. برای اینکه سرقت هویت با این روش رخ ندهد، استفاده‌کنندگان از کارت‌خوان‌های فروشگاهی نباید رمز عبور خود را به صاحب فروشگاه اعلام کنند و خودشان شخصاً رمز را وارد کنند. همچنین کاربران در هنگام استفاده از دستگاه‌های خودپرداز باید از واقعی بودن و تعلق داشتن خودپرداز به یک بانک، مطمئن شوند و در موقع استفاده از خودپرداز بررسی کنند که دستگاه اضافه در قسمت دریافت کارت نصب نشده باشد.

۲ـ۳. نظریه‌های یادگیری اجتماعی

نظریه‌های یادگیری اجتماعی نظیر معاشرت‌های ترجیحی ساترلند، نظریهٔ فراگیری اجتماعی آلبرت بندورا و نظریهٔ خنثی‌سازی ماتزا، جرم را محصول یادگیری هنجارها، ارزش‌ها و رفتارهای مرتبط با فعالیت جنایی می‌دانند. این یادگیری شامل فراگیری دانش مرتبط با فنون ارتکاب جرم و رهایی اخلاقی به وسیلهٔ کشف توجیهات منطقیِ مناسب برای رفتارهای مجرمانه است. بر اساس این نظریات، چون برخی روش‌های جعل هویتْ فنی است، به صورت اکتسابی باید فرا گرفته شود. این فراگیری شامل رفتار جزایی و فنون ارتکاب است و از طریق ارتباط معمولی با گروه‌های صمیمی انتقال می‌یابد. چون آثار منفی رفتار به منظور بازدارندگی مجرم در محیط ارتکاب ضعیف است، در طول زندگی فرد حفظ خواهد شد. آنچه در نهایت باعث بدل شدن این تجربهٔ آموزشی به جرم خواهد شد، ایجاد ارزش‌های پنهانی موازی است. انکار مسئولیت و آسیب به قربانی از جملهٔ این موارد است که باعث خواهد شد مجرم وجدان اخلاقی

خود را پاک کرده و احساس گناه نکند (دالال و شارما، ۱۳۸۸: ۴۳۵ـ۴۴۰).

از جمله روش‌های فنی جعل هویت، مهندسی اجتماعی مبتنی بر رایانه است.[۱] ابزار استفاده‌شده رایانه است، صفحات جعلی یا فیشینگ[۲] یا رمزگیری، از این دست مهندسی اجتماعی است که سبب افشای کلمهٔ عبور یا گذرواژهٔ کاربر می‌شود و پس از آن نفوذگر خواهد توانست به عنوان کاربر مجاز و از طریق درگاه‌های بانکی، اقدام به کلاهبرداری نماید. سرپرست ادارهٔ پیشگیری مرکز تشخیص و پیشگیری پلیس فتا نیز اعلام نمود که ۶۰ درصد جرایم سایبری در حوزهٔ جرایم مالی و از طریق سرقت اطلاعات کارت‌های بانکی رخ داده است و روش ارتکاب، توسل به انتشار تبلیغ تخفیف‌های باورنکردنی،[۳] حراج کالاها یا فروش کالا از طریق فروشگاه‌های اینترنتی است؛ به طوری که با این روش، افراد متقاضی خرید را به سمت صفحات جعلی درگاه‌های بانکی هدایت می‌نمایند و آنگاه اطلاعات بانکی خریدار به راحتی در اختیار فیشرها قرار خواهد گرفت. این روش که از شایع‌ترین روش‌های دسترسی به گذرواژه است، این امکان را برای مجرمان فراهم می‌سازد که بتوانند دامنهٔ ارتکاب جرم را از لحاظ کمی[۴] و کیفی ارتقا ببخشند؛ چون درگاه‌های جعلی بسیار شبیه درگاه‌های

۱. اعتماد طبیعی انسان، اصلی‌ترین و ابتدایی‌ترین روش برای هر حملهٔ مهندسی اجتماعی است و مهندسان اجتماعی به این حقیقت امید دارند که مردم نسبت به اطلاعات باارزش خود اطلاع ندارند و نسبت به محافظت از آن بی‌مبالات هستند. مهندسی اجتماعی هنری است که در آن فرد متقاعد خواهد شد که اطلاعات محرمانهٔ خود را آشکار می‌سازد.

۲. فیشینگ (phishing) کنایه از ماهی‌گیری و بر پایهٔ بی‌احتیاطی و فریب افراد است که برای دسترسی به رمزهای عبور شخصی کاربران استفاده شده است. در این حالت، صفحه‌ای مشابه درگاه پرداخت برخط یکی از بانک‌ها ساخته شده و هنگامی که کاربر وارد درگاه جعلی شود و اطلاعات خود را وارد کند، اطلاعات وی از طریق درگاه جعلی برای نفوذگر ارسال و سرقت خواهد شد.

۳. تبلیغاتی مثل شارژ شگفت‌انگیز و ارزان تلفن همراه از این جمله است؛ یعنی با خرید مبلغی مشخص، فرد می‌تواند به صورت نامحدود تا یک هفته یا یک ماه با تلفن همراه صحبت کند و پیامک ارسال نماید.

۴. به گزارش خبرگزاری فارس، رئیس پلیس فضای تولید و تبادل اطلاعاتِ فرماندهی انتظامی استان اصفهان اعلام کرد که در پی شناسایی وبگاهی جعلی توسط پلیس فتای استان در زمینهٔ فروش تلفن همراه، اطلاعات حساب بیش از ۱۸۰ کاربر اینترنتی که قصد خرید گوشی تلفن همراه داشتند، به سرقت رفته است.

پرداخت بانک‌ها هستند[۱] و باعث فریب کاربران و در اختیار قرار دادن اطلاعات حساب بانکی آن‌ها خواهند شد. از طرف دیگر، بر خلاف کلاهبرداری‌های سنتی که تحصیل مال محدود به موجودی بزه‌دیده است، مجرمان رایانه‌ای قادرند با ایجاد مبالغ و موجودی‌های واهی و غیر واقعی از مقدار حساب‌های موجود نیز فراتر روند و با روش اصطلاحاً برش کالباسی،[۲] خسارت‌های قابل توجهی وارد نمایند (زیبر، ۱۳۸۳: ۷۲).

برای مثال، در پروندهٔ پسری دیپلمه که به حساب بانکی ۴ هزار نفر ایرانی دسترسی پیدا کرده بود، فرمانده انتظامی استان مرکزی اعلام کرد که این شخص در مدت ۳ سال و با طراحی ۱۵ درگاه جعلی توانسته اقدام به برداشت غیر مجازِ ۴ میلیارد و ۲۰۰ میلیون ریال از کاربران بانکی نماید.[۳] در موردی دیگر، فرمانده انتظامی میاندوآب اعلام کرد که هکری ۲۰ ساله با راه‌اندازی درگاه جعلی و سرقت اطلاعات کارت بانکی ۴۰۰ نفر از نقاط مختلف کشور، توانسته یک میلیارد و ۵۰ میلیون ریال از حساب بانکی آن‌ها در مدت ۲ ماه برداشت کند.

فریب از طریق پیامک، یکی دیگر از روش‌های فیشینگ است که ادارهٔ نظام‌های پرداخت بانک مرکزی نیز نسبت به آن چنین هشدار داده است: «فریب پیامک‌های برنده شدن در قرعه‌کشی را نخورید»؛[۴] بدین‌ترتیب که مشترکان تلفن همراه از طریق دریافت پیامکِ اعطای جوایز چند ۱۰ میلیون تومانی، تشویق به وارد کردن اطلاعات حساب بانکی خود نظیر شمارهٔ کارت، رمز اینترنتی و... در درگاه‌های بانکی جعلی می‌شوند و از این طریق اقدام به برداشت از حساب آن‌ها می‌گردد. در این مورد می‌توان به برداشت غیر مجاز از حساب بانکی ۱۰۵۸ نفر توسط جوانی ۲۴ ساله اشاره کرد. بر اساس

---

۱. پلیس فتا در پیام‌های هشداردهنده، راه‌های به دام نیفتادن در صفحات فیشینگ بانکی را اعلام کرد. یک راه تشخیص وبگاه‌های فیشینگ در قسمت URL وبگاه کاملاً واضح است و کاربران باید حتماً دقت کنند که در کنار آدرس وبگاه، عبارت https ذکر شده باشد. همچنین وجود نماد قفل در کنار صفحات آدرس اینترنتی ضرورت دارد. راه دوم برای اطمینان از اصالت نماد الکترونیک، مراجعه به وبگاه www.enamad.ir است.

۲. Salami: ریزه‌ریزه یا خردخرد

۳. در وبگاهی که این شخص طراحی کرده بود، کاربران برای خرید یک محصول با قیمت بسیار پایین در حدود ۱۰ هزار ریال به سمت درگاه جعلی بانک هدایت می‌شدند.

۴. خبر مندرج در وبگاه بانک مرکزی به نشانی <www.cbi.ir> در تاریخ ۱۳۹۳/۵/۱۳.

گزارش رئیس پلیس فتای استان، این شخص با ارسال پیامک به اشخاص اعلام می‌کرد که در قرعه‌کشی تصادفی وبگاه، یک دستگاه گوشی اپل برنده شده‌اید و برای دریافت جایزه باید به درگاه <www.rahyab24.com> مراجعه و اطلاعات حساب بانکی خود را وارد کنید. فرد مزبور، با این روش از سال ۹۱ تا ۹۳ اقدام به کلاهبرداری از حساب ۱۰۵۸ شهروند نموده بود. در تحلیل بزه‌دیده‌شناسی این نوع جعل هویت باید گفت کسانی که بزه‌دیده واقع شده‌اند، حالت زودباوری و ساده‌لوحی داشته‌اند، به دنبال سرمایه‌گذاری و کار پرمنفعت بوده‌اند یا طمع کرده‌اند و به همین دلیل مورد سوءاستفادهٔ کلاهبرداران قرار گرفته‌اند (گسن، ۱۳۸۹: ۱۰۰). بنابراین روش پیشگیری، اطمینان از اصالت درگاه بانکی و داشتن نماد اعتماد الکترونیکی برای فروشگاه‌های خرید کالاست.

روش فنی دیگرِ جعل هویت، شنود از طریق انتشار یا نصب نرم‌افزار رخنه‌گر است؛ برای مثال، در فارمینگ[1] کاربر یک رایانامهٔ به ظاهر صحیح را باز خواهد کرد ولی در حقیقت یک کلیدخوان[2] را روی سیستم خود نصب می‌کند. این کلیدخوان یک نرم‌افزار است که کلیدهای فشرده‌شده توسط کاربر را در جایی ثبت و ذخیره و آنگاه در موقعیتی مناسب برای نفوذگر ارسال می‌کند. اطلاعات ارسالی ممکن است حاوی اطلاعات ارزشمندی همچون نام کاربری و رمز عبور کاربر باشد.[3] نمونه‌ای از این نوع سوءاستفاده، پروندهٔ «سرقت اطلاعات در چت‌روم» مطرح در شعبهٔ جرایم رایانه‌ای دادسرای مشهد است. در این پرونده، پسری ۲۷ ساله با حضور در فضای مجازی و چت‌روم‌ها، ابتدا با طعمه‌های خود طرح دوستی می‌ریخت و در لابه‌لای فایل‌های مبادله‌ای، فایل مخربی را برای قربانی خود ارسال می‌کرد که به محض باز کردن توسط مخاطب، اطلاعات بانکی‌اش به سرقت می‌رفت. به همین ترتیب، در پروندهٔ دیگری که در این شعبه رسیدگی شد، دو نوجوان ۱۵ و ۱۷ ساله در فیس‌بوک اقدام به تبلیغ نرم‌افزار

1. Pharming.

2. Keylogger.

۳. سازمان بین‌المللی پلیس جنایی (اینترپل) اعلام کرده است که باگ یا حفرهٔ امنیتی «سیمدا» از جدیدترین بدافزارهایی است که در صورت نفوذ به یک رایانه، جزئیات اطلاعات شخصی و محرمانهٔ فرد به ویژه رمزهای بانکی و سایر اطلاعات مالی وی را به سرعت شناسایی کرده و به سرقت خواهد برد.

هک بازیِ «کلش آف کلنز» نموده بودند. این نرم‌افزار طوری طراحی شده بود که در لابه‌لای نصب فایل‌های هک بازی، یک نرم‌افزار کلیدخوان را نیز نصب می‌کرد. بنابراین هر کس نرم‌افزار ارائه‌شده را دانلود و نصب می‌کرد، هر اقدامی که با صفحه‌کلید خود انجام می‌داد ـ از جمله وارد کردن رمزهای عبور حساب بانکی بدون استفاده از «صفحه‌کلید مجازی»ـ، در رایانه‌اش ذخیره می‌شد و در هنگام اتصال رایانه به اینترنت، تمام اطلاعات ذخیره‌شده به رایانامهٔ تعریف‌شدهٔ دو نوجوان هکر ارسال می‌گردید. این دو نوجوان بدین‌وسیله موفق به سرقت اطلاعات بانکی و در نهایت برداشت از حساب بیش از ۱۵۰ نفر از کاربران فضای مجازی شده بودند.[۱] بنابراین استفاده از صفحه‌کلید مجازیِ تعبیه‌شده در درگاه‌های بانکی، مهم‌ترین روش پیشگیری از جعل هویت با این روش است.

تحصیل گذرواژه یا رمز عبور از طریق نصب غیر مجاز نرم‌افزار کلیدخوان نیز انجام شده است. در پروندهٔ «استفاده از نرم‌افزار جاسوسی برای دستبرد به حساب بانکی دانشجویان»، رئیس پلیس فضای تولید و تبادل اطلاعات خراسان رضوی از دستگیری جوانی ۲۵ ساله در یک عملیات ضربتی خبر داد که با نصب نرم‌افزار جاسوسیِ کلیدخوان روی رایانهٔ دانشجویان، به اطلاعات محرمانهٔ حساب‌های بانکی تعدادی از آن‌ها دسترسی پیدا کرده و با این روش، مبالغ زیادی از حساب ۱۸ دانشجو برداشت کرده بود. در پروندهٔ «باند سارقان اینترنتی زاهدان» نیز متهم اصلی و همدستانش با سوءاستفاده از غفلت متصدیان کافی‌نت‌های زابل و زاهدان، نرم افزار جاسوسیِ

---

۱. این روش از طریق تلفن همراه و با ارسال پیامک نیز انجام‌شدنی است. رئیس پلیس فتای استان کرمان هشدار داد که این پیامک یک بدافزار از نوع تروجان و حاوی یک لینک است. زمانی که کاربر روی لینک کلیک کند یک نرم‌افزار به صورت خودکار روی تلفن همراه دانلود شده و در صورتی که این نرم‌افزار نصب شود، پیامی برای کاربر نمایش داده خواهد شد که به اجبار باید آن را تأیید کند. با تأیید این پیام، تروجان مورد نظر به سرورهای فرماندهی و کنترل هکرها متصل شده، در مرحلهٔ بعد، تروجانْ تلفن همراه قربانی را برای یافتن هر گونه نرم افزار بانکی جستجو کرده و به محض یافتن نرم‌افزار بانکی، موجودی حساب بانکی کاربر را به حساب دیگری منتقل خواهد کرد. حتی زمانی که حساب کاربر تخلیه شده و بانک نتیجهٔ تراکنش را در قالب یک پیامک برای کاربر ارسال کند، تروجان این پیامک را قبل از رسیدن به کاربر به سرورهای فرماندهی و کنترل خود ارسال کرده و پاک خواهد کرد و به این ترتیب سیستم پیامکی بانک را نیز دور می‌زند.

کلیدخوان را بر روی سیستم‌های رایانه‌ای کافی‌نت نصب کرده بودند. طبق اظهار رئیس پلیس فضای تولید و تبادل اطلاعات فرماندهی انتظامی سیستان و بلوچستان، باند مزبور اقدام به برداشت غیر مجاز از حساب ۶۰۰ نفر از کسانی نموده بود که برای ثبت‌نام آزمون کارشناسی ارشد مراجعه کرده بودند.[۱] تغییر دوره‌ای کوتاه‌مدت رمز عبور یا داشتن رمز عبور متغیر که زمان اعتبار مشخصی دارد، مناسب‌ترین روش‌ها برای پیشگیری است.

روش فنی دیگر، استراق سمع یا شنود غیر مجاز است. در سال ۱۹۸۲ یک کارمند شرکت مخابرات در ژاپن توانست ارتباطات برخط بانک را شنود کند. وی سپس اطلاعات کارت بانکی خود را رمزگشایی نمود و با استفاده از یک کارت آزمایشی جعلی نوعی کارت ویژه به دست آورد (زیبر، ۱۳۸۳: ۳۰).

شیوهٔ دریافت امواج از طریق درگاه‌های حضوری نیز امکان‌پذیر است. دستگاه خودپرداز و پایانهٔ فروش مانند هر رایانه‌ای امواج الکترومغناطیسی ساطع می‌کند که به آن نشت الکترونیکی[۲] گفته می‌شود. به محض فشردن هر یک از کلیدهای صفحه‌کلید، امواج از طریق سیستم‌های حامل جریان الکترونیکی در محیط اطراف منتشر می‌شود که به وسیلهٔ تجهیزات خاصی قابل شنود و آشکارسازی[۳] است. چون صفحهٔ نمایشگر کاربر برای نفوذگر قابل رؤیت نیست، پیش‌بینی رمز عبور یا کد عبور متنی یک تدبیر امنیتی ضد شنود است.

نتیجه‌گیری

جعل هویت و کلاهبرداری در بانکداری نوین با جرایم حوزهٔ حقوق کیفری اقتصادی

۱. بنا به گزارش *روزنامهٔ خراسان* از دادسرای جرایم رایانه‌ای تهران، یکی از روش‌های جالب سرقت هویت از طریق «وای فایِ» بدون رمز است. در این روش، بزهکار اقدام به خرید اینترنت پرسرعت کرده و هیچ رمزی برای آن قرار نمی‌دهد تا افراد فاقد اینترنت شخصی، از این شبکهٔ رایگان برای ورود به سامانه‌های بانکداری الکترونیک استفاده کنند. آنگاه اطلاعات مربوط به رمز و حساب بانکی آن‌ها در اختیار این شخص قرار می‌گیرد و سپس وی با این اطلاعات، اقدام به خالی کردن حساب کاربران می‌نماید.

2. Electronic emanation.

۳. برای اینکه اطلاعات کاربر از طریق سیم‌های رابط درگاه‌های حضوری شنود نشود، به روکش ضد مغناطیسی مجهز شده است.

و به طور خاص حقوق کیفری بانکی در ارتباط است و به همین دلیل به عنوان جرم مبتنی بر تزویر با دو مشخصهٔ دروغ و غضب شناخته شده است. تزویر عبارت است از شیوه یا روش ماهرانه‌ای که برای سوءاستفاده و فریب به کار برده شده و غضب نیز انگیزهٔ جرایم مبتنی بر تزویر و تصاحب و دارا شدن ناحق اموال است. دروغ این امتیاز را دارد که چون دروغ‌گو متوسل به خشونت نمی‌شود، طرف مقابل متوجه نشده و در نتیجه دفاع نخواهد کرد یا خیلی دیر متوسل به دفاع خواهد شد. بنابراین دروغ در جریان مبارزه، نوعی صرفه‌جویی در قدرت و زور است (گسن، ۱۳۸۹: ۲۱ـ۲۵). انگیزهٔ محرکِ مرتکبان این نوع جرایم، اغلب حرص و آز است که با نظریهٔ روان‌شناختیِ شخصیت جنایی ژان پیناتل و مؤلفهٔ خودمحوربینی تطابق دارد؛ زیرا به فرد اجازه خواهد داد که منافع خود را نسبت به منافع دیگران در اولویت قرار دهد و در جریان گذر از اندیشه به عمل از فنون خنثی‌سازی استفاده کند (نجفی ابرندآبادی، ۸۵ـ۱۳۸۴: ۲۳۳۶).

اما بر خلاف تحلیل‌های جرم‌شناختی، عده‌ای از جرم‌شناسانْ ارتکاب این جرم را که بیشتر جنبهٔ شهری دارد، با نظریهٔ فرصت تبیین کرده‌اند (گسن، ۱۳۸۹: ۱۰۰)؛ زیرا معتقدند که گونه‌های مختلف کلاهبرداری، با گسترش استفاده از فناوری‌های نوین اطلاعات و ارتباطات در ارتباط است.

ویژگی شهرمحور بودن با نظراتی مانند الگوی جرم، فرصت بزهکاری، پنجره‌های شکسته، پیشگیری محیطی و مکتب جغرافیای جنایی مرتبط گردیده است. این نظرات برای شناسایی کانون‌های جرم‌زا و نیل به کنترل و پیشگیری مکانی بزهکاری ارائه شده است (صفاری و کونانی، ۱۳۹۲: ۱۱۳). بر این اساس، جرایمی که در حوزهٔ بانکداری نوین رخ می‌دهد، با نظریهٔ سیاست جنایی ریسک‌مدار تطابق دارد. نظریهٔ سیاست جنایی ریسک‌مدار، نظریه‌ای اجتماعی است که ایجاد و مدیریت ریسک‌ها را در جامعهٔ مدرن تشریح کرده است. این اصطلاح، نخستین‌بار به وسیلهٔ اولریش بک به کار گرفته شد (بک، ۱۳۸۸: ۱۰). در جامعهٔ ریسک‌مدار، ریسک‌های مدرن محصول فعالیت بشری‌اند که مصنوعی‌اند و چون محصول فعالیت بشرند، سنجش میزان ریسکی که ایجاد شده یا خواهد شد، امکان‌پذیر است (پاک‌نهاد، ۱۳۸۸: ۶۰ـ۶۱) و از آنجا که جامعه در کل نمی‌تواند این خطرات از جمله خطر جرم را به کلی ریشه‌کن کند و به جامعه‌ای عاری

از جرم تبدیل شود، باید با مدیریت متناسب با وضعیت و درجهٔ خطر بزهکاری، آن را در حد تحمل‌پذیر برای اعضا و امنیت خود کاهش دهد. مطابق این نظریه، بیمهٔ سپرده‌های بانکی[1] و توجه به عامل‌های وضعی ـ فنی بزهکاری به منظور کاهش فراوانی خطر ارتکاب جرم به عنوان یکی از ره‌آوردهای «جرم‌شناسی نو» در بانکداری نوین، مورد توجه واقع شده است (نجفی ابرندآبادی، ۱۳۸۸: ۷۳۰)؛ مانند نصب دوربین مداربسته روی دستگاه‌های خودپرداز؛ محدودیت سقف برداشت و انتقال وجه از طریق درگاه‌های حضوری و غیر حضوری؛ رعایت استانداردهای امنیتی[2] برای صدور کارت‌های اعتباری و....

در باب فرضیات ارائه‌شده در تحقیق نیز دو ایراد وارد است که به شرح ذیل پاسخ داده خواهد شد:

ایراد اول اینکه چون در جرایم علیه اموال، مال موضوع جرم است و پول الکترونیکی مال است و موضوع جرم قرار دارد؛ چرا این جرم اقتصادی است و جزء جرایم علیه اموال نیست؟ در پاسخ باید گفت که موضوع جرم در جرایم اقتصادی متغیر است و مال فراتر از موضوع جرم و اخص از جرایم مالی است و اگر جرایم اقتصادی با امنیت اقتصادی مرتبط گردد، فقط رفتارهایی که باعث خدشه به نظام اقتصادی شده است، داخل در جرم اقتصادی نبوده و اموال نیز موضوع جرایم اقتصادی است. البته ممکن است به استناد مادهٔ ۳۶ قانون مجازات اسلامی ۱۳۹۲ استدلال شود که کلاهبرداری در صورتی جرم اقتصادی است که در سطح کلان باشد. اما در مقابل باید گفت که چون رسالت حقوق کیفری اقتصادی مضاعف است و هم در مقام حفاظت از منافع خصوصی و هم منافع عمومی و جمعی دولت است، در نتیجه شامل جرایم مالی نیز خواهد شد.

۱. با توجه به اهمیت این موضوع و لزوم ایجاد نهادی برای ضمانت سپرده‌های مردم، مجلس شورای اسلامی در مادهٔ ۹۵ قانون برنامهٔ پنجسالهٔ پنجم توسعهٔ جمهوری اسلامی ایران، بانک مرکزی را مکلف نمود که نسبت به ایجاد صندوق ضمانت سپرده‌ها اقدام نماید.

۲. در اصول ۴ تا ۱۰ مدیریت ریسک در بانکداری الکترونیک از دیدگاه کمیتهٔ نظارت بر بانکداری بال که توسط بانک مرکزی منتشر شده است، بر کنترل‌های امنیتی تأکید شده است (برگرفته از سایت بانک مرکزی به نشانی <www.cbi.ir>).

دومین ایراد در رابطه با عمل دروغ‌گویی است. دروغ که تحریف و دستکاری واقعیات است، از نظر ساختاری به صورت شفاهی و کتبی است. چگونه ممکن است که استفادهٔ غیر مجاز از دستگاه کپی کارت، جستجو در زباله‌های بانکی برای به دست آوردن گذرواژهٔ حساب بانکی، تحصیل مخفیانهٔ گذرواژه یا استفادهٔ غیر مجاز از کلمهٔ عبور کارمند دیگر، در زمرهٔ جرایم تزویرآمیز و مبتنی بر دروغ باشد؟ در پاسخ باید گفت که اگر معتقد باشیم خشونت یا نیرنگ در مرکز همهٔ نظام‌های کیفریِ طبیعی و اکتسابی وجود دارد و دارای دو خصیصهٔ اساسی مشترکِ «وضعیت نابرابر خاص بین بزهکار و بزه‌دیدهٔ او» و «استفادهٔ سوء از این وضعیت به ضرر بزه‌دیده» است، کلیهٔ شیوه‌های متقلبانه را که موجب شکل‌گیری یک وضعیت نابرابر خاص بین کلاهبردار و بزه‌دیدهٔ او شده، در بر گرفته و منحصر به شیوهٔ کلامی نخواهد شد.

پیشنهاد

یکی از روش‌های ارتکاب جرم کلاهبرداری در بانکداری نوین از طریق جعل هویت است. در هر دو نوع سنتی و رایانه‌ای، روش ارتکاب در عنصر قانونی آمده است، اما از یک طرف، روش ارتکاب به عنوان جرمی مستقل فاقد عنوان مجرمانه است و چون کلاهبرداری جرمی مقید است، در صورتی که نتیجهٔ مجرمانه حاصل نشود، به غیر از شنود غیر مجاز[1] و فارمینگ[2] که دارای جرم‌انگاری مستقلی است، در سایر موارد، نفس عمل انجام‌شده جرم نیست و از موارد تعدد جرم به حساب نخواهد آمد. در صورتی که در نظام‌های حقوقی آمریکا یا ترکیه استفادهٔ غیر مجاز از ابزارهای هویتی دیگری جرم است (شکربیگی و مرادی کرتویجی، ۱۳۹۵: ۱۱۴). اگر در حقوق کیفری ایران نیز این عمل جرم‌انگاری شود، هزینهٔ ارتکاب جرم را بالا خواهد برد و بر اساس نظریات جرم‌شناسی‌های عمل مجرمانه (تجربی)، چون مجرم، ارتکاب جرم را با اراده انتخاب کرده و قربانی جامعه و محیط نیست، باعث انصراف و بازدارندگی خواهد شد. نظریهٔ کنترل اجتماعی نای نیز تهدید به مجازات را باعث همنوایی فرد با جامعه دانسته است.

---

۱. مادهٔ ۷۳۰ قانون مجازات اسلامی.

۲. بند الف مادهٔ ۷۵۳ قانون مجازات اسلامی (انتشار نرم‌افزار مجرمانه).

از طرف دیگر، جاعلان هویت که مسلط به اصول و ضوابط بانکداری نوین هستند، فقط در صورتی که بیش از دو بار جرایم رایانه‌ای را تکرار کرده باشند، امکان محروم کردن آن‌ها از دسترسی به اینترنت و بانکداری نوین وجود دارد.[1] خلأ قانونی دیگری که اینجا وجود دارد این است که ارتکاب دو بار یا بیشتر جرایم رایانه‌ای نشان از حالت خطرناک دارد و شخص را مشمول مدیریت انسان‌مدار ریسک جرم قرار خواهد داد (رضوانی، ۱۳۹۵: ۲۳). این محرومیت نباید منحصر به جرایم رایانه‌ای باشد؛ زیرا در بسیاری از مواردی که رایانه به عنوان وسیلهٔ جرم استفاده شده است، بزهکار مشمول قوانین جرایم سنتی قرار خواهد گرفت و این محرومیت قابل اعمال نیست. این محرومیت از نظر تعدد جرم نیز قابل بررسی است؛ تعدد جرم نمود خطرناکی است (همان: ۱۱۹). رقم سیاه این جرایم بالاست. ممکن است جاعلان هویت در زمان دستگیری، کلاهبرداری‌های متعددی انجام داده باشند که بابت آن‌ها محاکمه نشده‌اند، ولی این نشانه‌ای است که بزهکار بر جرم خود پافشاری و اصرار ورزیده است و در حال تبدیل شدن به یک مجرم حرفه‌ای است. دو معیار تکرار و تعدد جرم از جملهٔ مواردی است که می‌تواند جنبهٔ طرد و خنثی‌کنندگی مجازات را تقویت کند؛ چون طبق نظر دورکیم، جرم پدیده‌ای معمولی و به‌هنجار است، کارکرد اجتماعی داشته و موتور تحولات جامعه است؛ بنابراین وجود آن برای جامعه ضروری بوده و جامعهٔ عاری از جرم نداریم، به ویژه که صنعت بانکداری در حال گسترش بوده و شیوه‌های جدید سرقت هویت نیز مرتباً خلق و تولید خواهد شد. بدین ترتیب بر اساس نظریهٔ مدیریت خطر جرم باید با روش‌هایی نرخ بزهکاری را کنترل کرد؛ یعنی هر چه متهم شناسنامهٔ کیفری بیشتری داشته باشد، در معرض ارتکاب جرم است و باید مدیریت و کنترل شود.

همچنین سیستم بانکی برای اینکه مشتریان بیشتری جذب کرده، به سود حداکثری برسد، بر اساس مدل نظام اقتصادی لیبرال عمل کرده است؛ یعنی به محض احراز اهلیت قانونی، ابزارهای الکترونیکی را اختصاص خواهد داد و حتی به افرادی که به دلیل کم‌سوادی، بی‌سوادی یا کِبَر سن، امکان یادگیری صحیحِ استفاده از ابزارها را

۱. مادهٔ ۷۵۵ قانون مجازات اسلامی.

ندارند، خدمات الکترونیک ارائه خواهد داد. در حالی که این افراد و برخی افراد دیگر، مکرراً از طریق ابزارهای برداشت الکترونیکی مورد بزه‌دیدگی قرار گرفته و در بازه‌های زمانی کوتاه‌مدت از بانک، تقاضای ابطال کارت، مسدود شدن حساب و... را داشته‌اند. این افراد که به عنوان بزه‌دیدهٔ بالقوه هستند، قبل از اینکه ابزار برداشت الکترونیک را دریافت کنند، مستلزم دریافت آموزشِ نحوهٔ به کارگیری ابزارهای الکترونیک و آشنایی با روش‌های مورد استفادهٔ کلاهبرداری هستند؛ هرچند سایر استفاده‌کنندگان از خدمات بانکداری الکترونیک نیز از این نوع آموزش‌ها به عنوان تدابیر پیشگیرانهٔ اجتماعی بی‌نیاز نیستند و لازم است که بانک‌ها به صرف الزام مشتریان به رعایت تدابیر حفاظتی اکتفا ننمایند[1] و در صورتی که آموزش‌های به کار گرفته‌شده مؤثر واقع نشود، صرفاً ابزارهای برداشت سنتی را در اختیار آن‌ها قرار دهند. به علاوه اقداماتی مثل نصب دوربین مداربسته روی دستگاه‌های خودپرداز یا تعبیهٔ ابزارهای هویتی بیومتریک مانند اثر انگشت که بزه‌دیده‌محور است، اگر پیش‌بینی و تقویت شود، می‌تواند مانع تحقق کلاهبرداری گردد یا محدودهٔ آن را کم کند. تدابیر مبتنی بر حمایت از بزه‌دیده یا همان پیشگیری وضعی، سیاست جنایی نظریات عقلانی‌محور است[2] که باعث کاهش فرصت‌های مجرمانه خواهد شد.

۱. بند ۱ از فصل چهارم طرح شبکهٔ خدمات کارت مصوب ۱۳۷۷/۲/۲۸ شورای عالی بانک‌ها (والی‌نژاد، ۱۳۸۸: ۸۷۰/۲).

۲. نظریهٔ انتخاب عقلانی، نظریهٔ فعالیت روزانه و نظریهٔ سبک زندگی (کوهن و فلسون) و نظریهٔ پیشگیری وضعی ـ فنی از جرم (کلارک) از این جمله است (نجفی ابرندآبادی، ۱۳۸۸: ۷۴۳).

کتاب‌شناسی

۱. ابراهیمی، شهرام و مجید صادق‌نژاد نائینی، «تحلیل جرم‌شناختی جرایم اقتصادی»، *فصلنامهٔ پژوهش حقوق کیفری*، سال دوم، شمارهٔ ۵، زمستان ۱۳۹۲ ش.
۲. ادارهٔ آموزش و مدیریت بانک ملی ایران، *بانکداری داخلی (۱) (تجهیز منابع)*، ۱۳۸۲ ش.
۳. السان، مصطفی، «پیشگیری چندنهادی از جرایم شهری»، *فصلنامهٔ مطالعات پیشگیری از جرم*، سال سوم، شمارهٔ ۹، ۱۳۸۷ ش.
۴. بک، اولریش، *جامعهٔ در مخاطرهٔ جهانی*، ترجمهٔ محمدرضا مهدی‌زاده، تهران، کویر، ۱۳۸۸ ش.
۵. پاک‌نهاد، امیر، *سیاست جنایی ریسک‌مدار*، تهران، میزان، ۱۳۸۸ ش.
۶. جعفری، امین، *حقوق کیفری کسب و کار*، تهران، شهر دانش، ۱۳۹۵ ش.
۷. خالقی، ابوالفتح و زهرا صالح‌آبادی، «مطالعهٔ سرقت هویت در حقوق فدرال آمریکا با نگاهی اجمالی به حقوق ایران»، *دو فصلنامهٔ حقوق تطبیقی*، دورهٔ دوم، شمارهٔ ۱۰۴، زمستان ۱۳۹۴ ش.
۸. دالال، ا. اس. و راقاو شارما، «نیم‌نگاهی به ذهن هکرها: آیا نظریه‌های جرم‌شناسی می‌توانند هک کردن را تبیین کنند؟»، ترجمهٔ احسان زررخ، *روزنامهٔ رسمی کشور* (مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات)، ۱۳۸۸ ش.
۹. دورکیم، امیل، *دربارهٔ تقسیم کار اجتماعی*، ترجمهٔ باقر پرهام، تهران، نشر مرکز، ۱۳۸۱ ش.
۱۰. رضوانی، سودابه، *تحولات مفهوم خطرناکی در جرم‌شناسی و آثار آن در حقوق کیفری*، رسالهٔ دکتری دانشگاه شهید بهشتی، ۱۳۹۵ ش.
۱۱. زراعت، عباس، *قانون مجازات اسلامی در نظم حقوق کنونی*، تهران، ققنوس، ۱۳۸۳ ش.
۱۲. زیبر، اولریش، *جرایم رایانه‌ای*، ترجمهٔ محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، تهران، کتابخانهٔ گنج دانش، ۱۳۸۳ ش.
۱۳. شارع‌پور، محمود، *جامعه‌شناسی شهری*، تهران، سمت، ۱۳۸۹ ش.
۱۴. شکربیگی، علیرضا و معین مرادی کرتویجی، *قوانین کیفری ترکیه*، تهران، مجد، ۱۳۹۵ ش.
۱۵. صدیق سروستانی، رحمت‌الله، *جامعه‌شناسی شهری*، تهران، علمی، ۱۳۹۱ ش.
۱۶. صفاری، علی و سلمان کونانی، *درآمدی بر جغرافیای شهری*، تهران، مجد، ۱۳۹۲ ش.
۱۷. طبیبی، مرتضی و انیس خدادادی، «سرقت هویت»، *مجلهٔ فقه و حقوق اسلامی*، شمارهٔ ۱۰، ۱۳۹۳ ش.
۱۸. عامری سیاهوئی، حمیدرضا، *زیست‌بوم انسانی در اسناد سازمان ملل متحد*، تهران، مجد، ۱۳۸۷ ش.
۱۹. فضلی، مهدی و ابراهیم باطنی، «مقابلهٔ کیفری با پیام‌های ناخواسته (رویکرد جهانی، بایسته‌سنجی ملی)»، *فصلنامهٔ حقوق اسلامی*، شمارهٔ ۲۲، ۱۳۸۸ ش.
۲۰. فیشر، بونی اس. و استیون پی. لب، *دانشنامهٔ بزه‌دیده‌شناسی و پیشگیری از جرم*، ترجمهٔ اساتید حقوق کیفری و جرم‌شناسی سراسر کشور، زیر نظر علی‌حسین نجفی ابرندآبادی، تهران، میزان، ۱۳۹۳ ش.
۲۱. کولن، آلن، *مکتب شیکاگو*، ترجمهٔ میرروح‌الله صدیق، تهران، مجد، ۱۳۹۴ ش.
۲۲. گسن، رمون، *جرم‌شناسی بزهکاری اقتصادی (نظریهٔ عمومی تزویر)*، برگردان شهرام ابراهیمی، تهران، میزان، ۱۳۸۹ ش.
۲۳. گلدمن، پیتر، *تقلب در بانک‌ها و مؤسسات مالی*، ترجمهٔ ناصر مکارم، تهران، پژوهشکدهٔ پولی و بانکی، ۱۳۹۲ ش.

۲۴. مبینی دهکردی، علی و احسان رسولی‌نژاد، *شکل‌دهی به فضای نوین بانکداری؛ رویکرد دانش‌بنیان*، تهران، نور علم، ۱۳۹۰ ش.
۲۵. محمدنسل، غلامرضا، «اصول و مبانی نظریهٔ فرصت»، *فصلنامهٔ حقوق*، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، دورهٔ سی و هفتم، شمارهٔ ۳، ۱۳۸۶ ش.
۲۶. موسوی، سیدیعقوب، «تبیین تئوریکی و جامعه‌شناختی جرایم شهری»، *فصلنامهٔ دانش انتظامی*، شمارهٔ ۱، ۱۳۷۸ ش.
۲۷. میرمحمدصادقی، حسین، *جرایم علیه امنیت و آسایش عمومی*، چاپ بیست و دوم، تهران، میزان، ۱۳۹۲ش.
۲۸. نجفی ابرندآبادی، علی‌حسین، *تقریرات درس جامعه‌شناسی جنایی ـ جامعه‌شناسی جرم*، دورهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی، نیمسال دوم ۸۴ـ۱۳۸۳، قابل دسترسی در <lawtest.ir>.
۲۹. همو، *تقریرات درس جرم‌شناسی (درآمدی بر جرم‌شناسی بزهکاری اقتصادی) و حقوق کیفری اقتصادی*، دورهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی، نیمسال نخست ۸۵ـ۱۳۸۴، قابل دسترسی در <lawtest.ir>.
۳۰. همو، «کیفرشناسی نو ـ جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار»، *تازه‌های علوم جنایی (مجموعه مقالات)*، تهران، میزان، ۱۳۸۸ ش.
۳۱. نجفی ابرندآبادی، علی‌حسین و مجید صادق‌نژاد نائینی، «نظریهٔ عمومی فشار و جرایم شرکتی»، *مجلهٔ تحقیقات حقوقی*، دانشکدهٔ حقوق دانشگاه شهید بهشتی، شمارهٔ ۱۳، ۱۳۹۲ ش.
۳۲. والک لیت، ساندرا، *شناخت جرم‌شناسی*، ترجمهٔ حمیدرضا ملک‌محمدی، تهران، میزان، ۱۳۸۶ ش.
۳۳. والی‌نژاد، مرتضی، *مجموعهٔ قوانین و مقررات ناظر بر بانک‌ها و مؤسسه‌های اعتباری*، تهران، پژوهشکدهٔ پولی و بانکی، ۱۳۸۸ ش.
۳۴. ویلیامز، فرانک پی. و دیگران، *نظریه‌های جرم‌شناسی*، ترجمهٔ حمیدرضا ملک‌محمدی، تهران، میزان، ۱۳۸۳ ش.