مطالعات حقوق کیفری و جرم‌شناسی

دورهٔ ۴۹، شمارهٔ ۲، پاییز و زمستان ۱۳۹۸
صفحات ۴۴۹ تا ۴۶۸

قربانیان سرقت هویت در فضای سایبر
با تأکید بر نظام کیفری آمریکا

علی غلامی *

دانشیار دانشکده معارف اسلامی و حقوق دانشگاه امام صادق (ع)

علی ابراهیم‌نیا

دانش‌آموختهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه امام صادق (ع)

(تاریخ دریافت: ۱۳۹۸/۸/۱۱ - تاریخ تصویب: ۱۳۹۸/۱۲/۵)

چکیده

سرقت هویت در فضای سایبر پدیده‌ای مجرمانه است که به‌واسطهٔ گسترش فضای مجازی در کشورهای مختلف، از جمله ایران، بیش از پیش پدیدار گشته است؛ اما به خاطر ضعف قانونی و تکنیکی ناظر به مهار آن، موجب خسارات مختلفی برای کشور شده است. سرقت هویت در فضای سایبر همچون سرقت هویت در فضای حقیقی، قربانیانی را به همراه دارد که هر یک به‌نوعی درگیر خسارات می‌شوند؛ اما تعداد قربانیان و همچنین نوع و میزان خسارت در هر کدام متفاوت است. اما خسارات این جرم و مجراهای جبران آن چیست و نقش قربانیان و موانع شناسایی آن‌ها کدام است؟ در مقام پاسخ به این سؤال، در این نوشتار با روش توصیفی به تعریف قربانیان و خسارات مستقیم و غیرمستقیم واردشده بر آن‌ها پرداخته و با روش تحلیلی، موانع شناسایی قربانیان، مجراهای جبران خسارات و نقش قربانیان و طرف‌های دیگر درگیر را با رویکردی تطبیقی و با توجه به تجربهٔ نظام کیفری ایالات متحدهٔ آمریکا در برخورد با این جرم، تبیین می‌کنیم.

واژگان کلیدی

سرقت هویت، فضای سایبر، قربانیان سرقت هویت، جبران خسارت

* 1355gholami@gmail.com

مقدمه

سرقت هویت، عمل خلافکارانهٔ ناشی از به‌دست‌آوردن و استفاده از هویت فردی به‌صورت غیرقانونی است. این عمل می‌تواند بدون کمک وسایل فنی و همچنین به‌صورت آنلاین، با استفاده از فناوری اینترنت انجام شود. به‌طور کلی، جرائم توصیف‌شده به‌عنوان سرقت هویت شامل سه مرحلهٔ متفاوت است:

الف) در مرحلهٔ اول، مجرم اطلاعات مربوط به هویت را به دست می‌آورد. این بخش از جرم می‌تواند به عنوان مثال با استفاده از نرم‌افزارهای مخرب یا حملات فیشینگ[1] انجام شود؛

ب) مرحلهٔ دوم با استفاده از اصالت جدید محقق می‌شود. بسیاری از متخلفین از اطلاعات هویتی به‌دست‌آمده برای مخفی‌کردن اطلاعات واقعی خود استفاده می‌کنند؛

ج) مرحلهٔ سوم استفاده از اطلاعات مربوط به هویت در اعمال خلافکارانه است. اغلب، دسترسی به اطلاعات هویت، افراد را برای ارتکاب بیشتر جرائم توانا می‌سازد. بنابراین متخلفان بر روی خود اطلاعات تمرکز نمی‌کنند؛ بلکه بر روی توانایی استفاده از آن‌ها در اَعمال خلافکارانه تمرکز می‌کنند؛ مثال ملموس برای این تخلفات، تحریف اسناد هویتی با جعل کارت اعتباری است.

به هر ترتیب، تفاوت نگرش و دیدگاه به این جرم موجب شده است تا روندهای مختلف قضایی به این موضوع پیش‌گرفته شود و روش‌های پیشگیری، تعقیب و مجازات مختلفی در این مسیر به کار گرفته شود.

«تاکنون اجماع بین‌المللی برای تعریف جرم رایانه‌ای شکل نگرفته و در تعریف آن الگوی یکسانی مورد تبعیت قرار نگرفته است. این امر از یک طرف ناشی از سطح غیریکسان تکنولوژی رایانه‌ای و گسترش جرائم رایانه‌ای در کشورهای مختلف و از سوی دیگر ناشی از نظرات و دیدگاه‌های متفاوتی است که مبنای تعاریف جرم رایانه‌ای را شکل می‌دهد» (باستانی، ۱۳۹۰: ۲۹).

عملاً می‌توان گفت که یافتن تعریف واحد برای این جرم دشوار است؛ چراکه به‌واسطهٔ عدم اجماع تعاریف متعددی می‌توان یافت (طبیبی و خدادادی، ۱۳۹۴: ۸۰-۷۷). در عین حال «سازمان همکاری و توسعهٔ اقتصادی به‌عنوان یک مرجع بین‌المللی، اولین تعریف از جرم رایانه‌ای را ارائه نمود. مطابق تعریف این سازمان، سوءاستفاده از رایانه شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش اتوماتیک در انتقال داده‌هاست» (شیرزاد، ۱۳۸۸: ۳۳-۳۲).

---

۱. فیشینگ، اصطلاحی بود که در سال ۱۹۹۶ توسط هکرهای آمریکایی که قصد حمله به حساب‌های کاربران «آمریکا آنلاین (**AOL**)» را داشتند، ابداع شد. این هکرها با به‌دست‌آوردن مخفیانهٔ رمز حساب‌های کاربران، از آن‌ها سوءاستفاده می‌کردند. در واقع، فیشینگ روشی است که با ایجاد طعمه برای کاربران، آن‌ها را به دام می‌اندازد؛ به این معنی که در شکل ایمیل‌های ارسالی از شرکت‌ها و وبگاه‌های قانونی و معتبر و دیگر روش‌ها، اطلاعات افراد را بدون ایجاد هرگونه ظن و اتهام به سرقت می‌بردند.

صرف‌نظر از تعاریف مختلفی که نسبت به سرقت هویت در فضای سایبر ارائه شده است، تعریف ذیل به‌عنوان تعریف مختار ملاک عمل قرار می‌گیرد: «سرقت هویت زمانی رخ می‌دهد که فرد یا گروهی اقدام به کسب، انتقال، تصرف و یا استفادهٔ غیرمجاز از اطلاعات شخصی فرد یا افراد حقوقی یا حقیقی کند؛ با این هدف که کلاهبرداری و یا جرم دیگری را مرتکب شود و یا اقدامی ناظر به این اهداف انجام دهد» (OECD, 2009, Online Identity Theft) .

این تعریف کلی شامل هر دو نوع سرقت هویت می‌گردد؛ یعنی سرقت هویت چه در فضای سایبر و چه در فضای واقعی، تعریفی واحد دارد و تنها تفاوت آن‌ها در وسیلهٔ ارتکابی آن است که تأثیری در تعریف آن نخواهد داشت؛ اما اثرات مختلفی از جرم در دو فضا ناشی می‌شود. نکتهٔ مهم آنکه ارائهٔ تعریفی مجزا برای این جرم در فضای سایبر ثمرهٔ خاصی نخواهد داشت؛ چراکه تفاوتی مبنایی میان هدف و تعریف این جرم در فضای مجازی و فضای واقعی وجود ندارد. تنها تفاوت مهم، آثار و نوع ارتکاب آن است که بدان اشاره خواهد شد.

همان طور که در تعریف دیده می‌شود، دو شرط اساسی برای اطلاق جرم سرقت هویت لازم است. اول اینکه دسترسی به اطلاعات یا استفاده و تصرف از آن‌ها باید به‌نحوی غیرمجاز صورت گیرد. بدین ترتیب اگر فرد اطلاعات شخصی فردی دیگر را با اجازهٔ قانونی، مورد تصرف یا انتقال قرار دهد، مرتکب سرقت هویت نشده است؛ اما اگر فرد صرفاً مجاز به انجام جزئی از یک کار باشد و در جزء دیگر جواز نداشته باشد، قطعاً در زمرهٔ سارقین هویت قرار می‌گیرد؛ مثلا اگر فرد اجازهٔ انتقال اطلاعات را داشته باشد، اما مجاز به تصرف در آن‌ها نباشد، به عنوان سارق هویت قابل پیگرد خواهد بود.

دوم اینکه هدف از هر یک از چهار عمل آتی باید انجام فعلی مجرمانه باشد یا باید ارتباطی حداقلی با عملی تبهکارانه داشته باشد. بنابراین در صورتی که این اقدام مرتکب برای هدفی مفید یا لازم باشد، سرقت هویت نام نخواهد گرفت؛ به عنوان مثال، اگر فردی برای نجات بخش عظیمی از اطلاعات سازمانی امنیتی، اقدام به تصرف اطلاعاتِ شخصیِ مسئول آن قسمتی که کشته شده است، نماید، به‌عنوان سارق هویت تحت پیگرد قرار نخواهد گرفت.

نکتهٔ شایان توجه دیگری که در این تعریف بدان اشاره شده است، تفکیک میان چهار عمل مختلفی است که در خصوص دستیابی به اطلاعات یا تصرف در آن بیان شده است.

الف) کسب اطلاعات زمانی رخ می‌دهد که فرد صرفاً اطلاعات مدنظر خود را در اختیار می‌گیرد و نکتهٔ جالب اینجاست که صرفاً کسب اطلاعات و دراختیارگرفتن آن‌ها به‌عنوان عملی مجرمانه مطرح شده است؛ چراکه تنها دراختیارداشتن اطلاعات شخصی افراد یا هویت الکترونیکی

آن‌ها، راه را برای ارتکاب جرائم دیگر هموار می‌سازد و همین لازمهٔ جرم‌انگاری آن را فراهم می‌آورد.

ب) انتقال اطلاعات شخصی افراد، چه از طریق اینترنت و چه از طریق وسایل الکترونیکی در زمرهٔ افعال مجرمانه قرار می‌گیرد. انتقال اطلاعات هویتی افراد لزوماً به این معنا نیست که فرد به آن اطلاعات دسترسی داشته باشد یا امکان تصرف در آن را داشته باشد؛ بلکه صرف اینکه آن اطلاعات را به دیگری انتقال دهد، کافی است؛ برای مثال ممکن است مرتکب به مجموعهٔ اطلاعات هویتی فردی دست پیدا کند ولی به‌واسطهٔ وجود سیستمی امنیتی در آن مجموعه قادر به تصرف و مشاهدهٔ آن نباشد؛ بدین‌ترتیب آن را برای رمزگشایی و بررسی به دیگری منتقل می‌کند.

ج) تصرف به این معنی است که فرد، اطلاعات هویتی فرد دیگری را دچار تغییر و خدشه کند یا بدون ایجاد تغییر در اصل اطلاعات، کاری کند که قابل‌ردیابی و مشاهده برای افراد خاصی شود؛ مثلاً ممکن است مرتکب به نام کاربری و رمز قربانی دست پیدا کند و با ورود به حساب کاربری او و تغییر رمزش، اقدام به انجام اموری کاملاً متعارض با خواسته‌ها و شخصیت قربانی کند. مثال دیگر مربوط به حالتی است که فرد به نام کاربری و رمز حساب قربانی در یک شرکت، دست پیدا کند ولی بدون هیچ‌گونه تغییر و خدشه در آن، با اضافه‌کردن یک افزونه، عملکرد و فعالیت‌های او را به‌شکلی زنده و از راه دور بررسی کند.

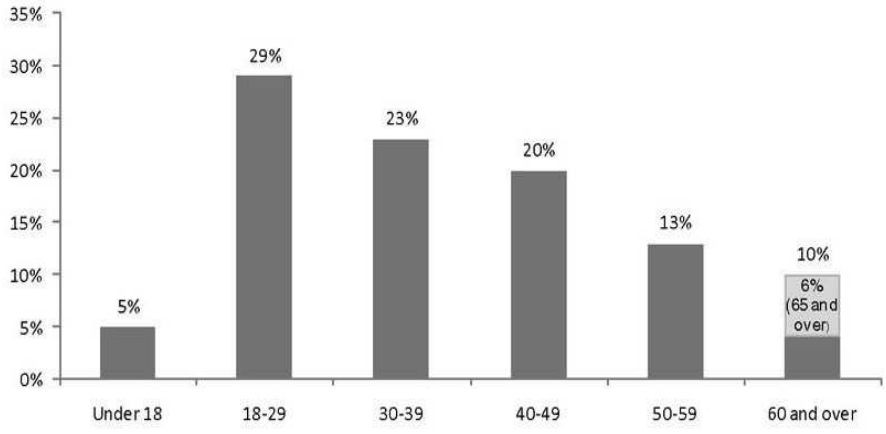
د) استفاده زمانی است که سارق با استفاده از روش‌های مخصوص به خود، به اطلاعات فرد دست پیدا کند و بدون اطلاع او اقدام به بهره‌گیری از آن برای افعال مختلف کند. این مورد جزء شایع‌ترین انواع سرقت هویت است که فرد با داشتن هویت الکترونیکی قربانی می‌تواند به نمایندگی از او هر جرمی را مرتکب شود. حتی ممکن است اقداماتی صورت دهد که در قانون جرم شناخته نشده است؛ اما قطعاً مضر خواهد بود و جنبهٔ تبهکارانه خواهد داشت.

با توجه به مقدمات پیش‌گفته و مشخص‌شدن تعریف جرم سرقت هویت در فضای سایبر، در این مقاله ابتدا به تعریف قربانی سرقت هویت در فضای سایبر پرداخته خواهد شد و پس از آن خسارات ناشی از این جرم بر قربانیان تبیین می‌گردد. در ادامه مسئولیت قربانیان در ایجاد خسارات و سپس موانع شناسایی قربانیان سرقت هویت در فضای سایبر بررسی می‌شود. مجراهای جبران خسارات ناشی از سرقت هویت در فضای سایبر، محور بعدی مقاله است و در نهایت نیز نقش قربانیان و طرف‌های دیگر درگیر در جرم اشاره خواهد شد.

۱. تعریف قربانی سرقت هویت در فضای سایبر

بحث قربانیان سرقت هویت در وهلهٔ اول، محدود به کسانی می‌شود که به‌نحوی از انحاء، اطلاعات آنان به سرقت رفته و از آن سوءاستفاده شده است و در نتیجه متحمل خساراتی شده‌اند. با توجه به تحقیقی که در سال ۲۰۰۳ توسط گروه پیشگیری از کلاهبرداری در کانادا صورت گرفته، آثار سرقت هویت صرف‌نظر از مدرک و میزان درآمد افراد، همهٔ سنین را تحت‌الشعاع قرار داده است و عملاً گسترهٔ قربانیان در کانادا بسیار وسیع است (BWGCBMMF, 2004: 4). در ماه می سال ۲۰۰۶، بیش از ۲۰,۰۰۰ دادخواست و شکایت ناظر به فیشینگ در کانادا طرح شد که نسبت به سال قبل از آن، رشد ۳۴درصدی در این کشور داشته است.

در ایالات متحده آمریکا نیز طبق گزارش بخش حمایت از مصرف‌کنندگان کمیسیون تجارت فدرال، در سال ۲۰۰۷، یافته‌ای مشابهِ یافته‌های آماری در کانادا به دست آمده است (US FTC, 2007a). همان طور که در نمودار زیر مشاهده می‌شود، از میان قربانیانی که سن خود را ارائه داده‌اند، افراد بین ۱۸ تا ۲۹ سال به‌عنوان اکثریت مطرح هستند و بیش‌ترین سرقت هویت در فضای سایبر نسبت به این افراد واقع شده است. این اکثریت معادل ۲۹درصد است و گروه بعدی قربانیان، افراد بین ۳۰ تا ۳۹ سال هستند که ۲۳درصد کل قربانیان این جرم را تشکیل می‌دهند.



تصویر شمارهٔ ۱- میزان شکایات مربوط به سرقت هویت در فضای سایبر به‌نسبت سن افراد

نکته آنکه این آمار از میان افرادی به دست آمده است که مسئلهٔ سرقت هویت ناظر به خود را به کمیسیون تجارت بین‌الملل گزارش داده‌اند و سن خود را نیز بیان کرده‌اند. به بیان دیگر، این نمودار بیانگر آمار مربوط به ۹۴درصد افرادی است که گزارش وقوع جرم در خصوص آنان به

دست کمیسیون تجارت فدرال رسیده است (US FTC, 2007a, Report on consumer Fraud and Identity Theft Complaint Data).

مشاهده می‌شود که نقصان جامعهٔ آماری، موجب می‌شود که تصویر کاملی از خسارت واردشده به قربانیان سرقت هویت وجود نداشته باشد و همین موضوع موجب پیچیده‌شدن مفهوم قربانی در این جرم می‌شود. نکتهٔ دیگر آنکه هیچ‌گاه این‌گونه شکایات مشخص نمی‌سازد که آیا مؤسسات و نهادهای تجاری نیز جزء قربانیان بوده‌اند یا خیر. مثلاً ممکن است یک سارق سایبری با استفاده از حساب بانکی یکی از مشتریان بانک و با استفاده از نام و علامت تجاری آن بانک خاص، پول فرد دیگری را سرقت کند و در واقع با این عمل، آن بانک را نیز قربانی سرقت هویت و کلاهبرداری‌های بعدی سازد؛ زیرا تا زمانی که سارق هویت یافت نشود، بانک مسئول پرداخت خسارت به فرد ثالث است و ممکن است به‌اجبار برای حفظ اعتبار و موقعیت اقتصادی خود، هزینه‌های دیگری نیز متحمل گردد.

در حقوق ایران نیز به علت صریح‌نبودن تعریف سرقت هویت، نمی‌توان به‌طور قطع مدعی شد که سرقت هویت دربرگیرندهٔ چه دسته‌ای از قربانیان است. قوانینی همچون قانون تجارت الکترونیکی و قانون جرائم رایانه‌ای، هیچ‌کدام به صراحت، عنوان سرقت هویت را مطرح نکرده‌اند؛ اما باید گفت که در بعضی از مقررات که عملاً فراتر از جرائم رایانه‌ای محسوب می‌شوند، اشاراتی به جرائم مرتبط شده است که می‌توان سرقت هویت در فضای سایبر را به‌نوعی به آنان نزدیک دانست.

برای مثال در «قانون تخلفات، جرائم و مجازات‌های مربوط به اسناد سجلی و شناسنامه» که در سال ۱۳۷۰ به تصویب مجمع تشخیص مصلحت نظام رسید، هرگونه سوءاستفاده از شناسنامهٔ دیگری یا دریافت شناسنامهٔ موهوم، جرم‌انگاری شده است یا در مادهٔ ۳۷ قانون گذرنامه مصوب ۱۳۵۲ به‌صراحت ذکر شده است که هر کس برای دریافت گذرنامه یا اسناد در حکم گذرنامه به نام خود یا دیگری اسناد و مدارک خلاف واقع یا متعلق به غیر را عالماً و عامداً به مراجع مربوط تسلیم کند، به حبس تأدیبی از دو ماه تا شش ماه محکوم می‌شود و در صورتی که عمل او منجر به صدور گذرنامه شود، به حبس از دو ماه تا دو سال محکوم خواهد شد.

مصادیق دیگری که می‌توان در قوانین ایران به‌طور مستقیم یا غیرمستقیم به جرم سرقت هویت در فضای مجازی مرتبط دانست، عبارت است از: مادهٔ ۶۱ قانون خدمت وظیفه عمومی مصوب ۱۳۶۳ ناظر به استفاده از شناسنامهٔ دیگری برای رهایی از خدمت وظیفهٔ عمومی؛ مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری دربارهٔ اختیارکردن اسم یا عنوان مجعول؛ مادهٔ ۶۶ قانون انتخابات سال ۱۳۷۸ راجع به دخالت در امر انتخابات با سمت مجعول؛ مادهٔ ۶۶

قانون تجارت الکترونیک ناظر به استفاده از علائم تجاری دیگران (صادقی، ۱۳۸۸: ۶۹)؛ مادهٔ ۵۳۸ قانون مجازات اسلامی در خصوص جعل گواهی پزشکی؛ مادهٔ ۵۴۱ قانون مجازات اسلامی ناظر به جعل یا سرقت هویت کارت ورود به جلسهٔ آزمون و در نهایت مادهٔ ۱۲ قانون جرائم رایانه‌ای که به‌طور خاص به ربودن و برش‌دادن اشاره کرده است (خالقی و صالح‌آبادی، ۱۳۹۴: ۱۱۱-۱۰۵).

البته عمدهٔ این قوانین ناظر به کلاهبرداری‌ها و سرقت‌های هویتی غیراینترنتی و آفلاین است و همین امر ضعف موجود در بررسی عواقب جرم سرقت هویت در فضای مجازی را مبرهن می‌سازد. هم‌اکنون بسیاری از امور اداری از طریق اینترنت صورت می‌پذیرد و استفاده از اسناد هویتی در فضای مجازی الزامی است و حتی در برخی موارد، دریافت اطلاعات هویتی اینترنتی الزامی است؛ همچون دریافت اطلاعات هویتی سجام که در امور مالی استفاده می‌شود.

قطعاً این موضوع موجب ضعف جدی در ارائهٔ آمار قربانیان سرقت هویت اینترنتی می‌شود و بررسی خسارات تحمیل‌شده بر قربانیان در ایران را با دشواری همراه می‌سازد.

۲. خسارات ناشی از سرقت هویت در فضای سایبر بر قربانیان

همان طور که قبلاً اشاره شد، سرقت هویت به‌عنوان جرمی مستقل در تمامی کشورهای عضو سازمان همکاری و توسعه اقتصادی، مطرح نیست. به‌علاوه، عمدهٔ آمار ارائه‌شدهٔ ناظر به این جرم، از ضعف‌های متعددی، همچون دربرگرفتن جرائم مختلف و یکسان‌نبودن نتیجه‌های حاصل‌شده و... (UN IEG, 2007: 62) رنج می‌برد. مضاف بر اینکه اطلاعات به‌دست‌آمده، هر کدام مربوط به یک کشور می‌شود و مربوط به اقتصاد، مصرف‌کنندگان و تجارت همان کشور است.

۲-۱. خسارات مستقیم وارده بر قربانیان

در ایالات متحدهٔ آمریکا با توجه به آمار گارتنر در سال ۲۰۰۷، متوسط خسارت مالی ناشی از سرقت هویت برای هر پرونده در این کشور در سال ۲۰۰۶، معادل ۲۵۷ دلار آمریکایی بوده است؛ یعنی چیزی معادل دو برابر این خسارات در سال ۲۰۰۵.[1] به علاوه طبق گزارش‌ها، در این مدت، میزان کلاهبرداری‌های مربوط به ایجاد ۳,۲۵۷ حساب جدید، دو برابر شده است. طبق گزارش کلی سال ۲۰۰۷، سرقت هویت، چیزی حدود ۴۹,۳ میلیارد دلار در سال به صنایع و مصرف‌کنندگان این کشور خسارت وارد می‌سازد.[2] با توجه به گزارش امنیت قانونی و صنایع

1. https://www.gartner.com/ newsroom/id/501912, آخرین بازدید اردیبهشت ۹۶

2. www. javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/, آخرین بازدید بهمن ۹۵

انگلستان، در ایالات متحدهٔ آمریکا، مصرف‌کنندگان در سال ۲۰۰۵، چیزی معادل ۲,۴ میلیون دلار در پی کلاهبرداری‌های حاصل از حمله‌های فیشینگ، خسارت دیده‌اند (BT, 2006: 9).

با توجه به مطالعات مؤسسهٔ امنیت رایانه‌ای و اف بی آی بر روی بیش از ۶۰۰ کمپانی فناوری اطلاعات در آمریکا در سال ۲۰۰۶[1] مشخص شده است که رخنه‌های امنیتی تا حدود ۱۸درصد کاهش یافته است؛ به این معنی که خسارات مالی مستقیم وارده بر این شرکت‌ها به‌طور متوسط از ۲۰۳۶۰۶ دلار به ۱۶۷۷۱۳ دلار کاهش یافته است. البته این مقدار از سوانح امنیتی نیز بسیار قابل توجه است، چراکه در مجموع معادل ۵۲ میلیارد دلار به شرکت‌های فناوری اطلاعات آمریکا خسارت وارد آورده است.

این میزان از تفاوت در آمار، این سؤال را مطرح می‌سازد که چرا اطلاعات موجود ناظر به خسارات مستقیم وارده بر قربانیان تا این میزان متفاوت و متعارض است. در پاسخ باید گفت که شاید این تفاوت در نتیجه تلاش شرکت‌های تجاری برای کم جلوه دادن میزان خسارات وارده به مشتریان خود باشد. چراکه کم بودن میزان خسارات نشان کارآمدی یک شرکت می‌باشد و این همان چیزی است که هر شرکتی سعی در به‌دست آوردن آن دارد. علاوه بر این، میزان و مقیاس خسارات بدون بررسی بازخورد مشتریان و گزارش‌گیری از آنان غیرممکن است. بنابراین به نظر می‌رسد که به‌دست آوردن الگویی قطعی برای تشخیص و سنجش خسارات مستقیم وارده بر افراد و مشتریان کاری بسیار صعب و دشوار باشد.

۲-۲. خسارات غیرمستقیم وارده بر قربانیان

خساراتی که به نحوی غیرمستقیم بر قربانیان وارد می‌آید، می‌تواند اشکال و انواع متعددی داشته باشد. البته هیچ‌گونه گزارش و یا آماری در مورد میزان و گستره خسارات غیرمستقیم وارده بر قربانیان سرقت هویت در فضای سایبر وجود ندارد، در عین حال کمیسیون تجارت فدرال ایالات متحده آمریکا و CIFAS[2] دستورالعمل‌هایی در رابطه با این موضوع تهیه کرده‌اند.

طبق گزارش کمیسیون تجارت بین‌الملل در سال ۲۰۰۶، ۱۶ درصد از قربانیان سرقت هویت در استفاده از کارت‌های اعتباری خود دچار مشکل بودند و یا قادر به دریافت کارت‌های اعتباری جدید نبودند؛ ۱۰ درصد از این افراد دچار مشکلاتی ناظر به چک‌های بانکی‌شان شدند و از داشتن چک محروم گردیدند؛ حدود ۳۷ درصد از افرادی که هدف سرقت هویت قرار گرفته بودند،

1. http://solutions.journaldunet.com/0607/060726-etude-securite-csi-fbi.shtml, آخرین بازدید آذر ۹۷

۲. سرویس پیشگیری از کلاهبرداری تجاری. (Credit Industry Fraud Avoidance Service)

حداقل یکی از مشکلات مذکور در بالا را تجربه کرده‌اند و ۲۱ درصد این افراد رنج چند مورد از موارد فوق را تحمل نمودند (US FTC, 2007b: 42).

علاوه بر این، ۳۳ درصد افرادی که یک یا چند مورد از این مشکلات را تجربه کرده بودند، ابراز داشته‌اند که فقط چیزی حدود ۴۰ ساعت برای رفع آن‌ها وقت صرف کرده‌اند که این خود موجب نقصان‌های متنوعی در منافع اکتسابی آنان در زندگی شده است. طبق گزارش CIFAS (www.cifas.org.uk/identity_fraud_is_theft_serious.asp، آخرین بازدید بهمن ۹۵) ، افرادی که درگیر سرقت هویت در فضای سایبر می‌شوند، بین ۳ تا ۴۸ ساعت باید برای پاک کردن نام خود و برطرف نمودن مشکلات ایجادشده در نتیجه سرقت صورت‌گرفته، صرف کنند. CIFAS همچنین این نکته را بیان می‌دارد که اگر فرد صاحب هویت، قربانی یک سرقت هویت کامل و اصطلاحاً ربایش کامل گردد، آنگاه شاید نیاز پیدا کند که با ۲۰ یا ۳۰ سازمان و ارگان مختلف درگیر شود و این خود موجب طولانی‌تر شدن روند اداری لازم برای او و صرف وقتی معادل ۲۰۰ ساعت یا بیشتر می‌شود که با این توصیف باید مبلغی قریب به ۸۰۰۰ پوند صرف این امر کند.

بسیاری از قربانیان سرقت هویت به‌واسطهٔ اطلاعات غلطی که از آنان به جا مانده است و یا سوءاستفاده‌هایی که از هویت آنان صورت گرفته است، دچار مشکلاتی همچون از دست دادن شغل، وام، اتومبیل، تحصیلات، خانه و بسیاری دیگر از منافع و تسهیلات دیگر می‌شوند. حتی بعضی از آنان به خاطر این سوابق دستگیر می‌شوند. قربانیان هزینه‌های دیگری همچون هزینه‌های دادرسی و یا مخارجی که برای پیشبرد سیر اداری خود باید پرداخت کنند، متحمل می‌شوند. علاوه بر تمام این موارد آن‌ها از صدمهٔ روحی نیز رنج می‌برند و روندی بسیار طولانی را برای بهبود وضعیت و بازگرداندن شهرت و اعتبار شخصی خود طی خواهند کرد که لزوماً این روند نتیجه نمی‌دهد و گاهی فرد برای همیشه سرافکنده باقی می‌ماند. این بخش از خسارات بعضاً غیرقابل جبران است و صدمهٔ وارده به شخص به‌راحتی قابل تخمین نیست و نتیجهٔ حاصل از آن در ابعاد مختلف زندگی او بروز خواهد یافت و ممکن است به‌واسطهٔ این لطمه به شهرت و اعتبار او، دوستان و خانواده و یا امتیازات زندگی خود را نیز از دست بدهد و همهٔ این موارد به‌نحوی تصاعدی به صدمه‌های روحی او اضافه خواهد کرد.

۳. نقش و مسئولیت قربانیان در ایجاد خسارات

سرقت هویت عمدتاً در نتیجهٔ قصور شخصی، تجاری یا حکومتی روی می‌دهد. اشخاص معمولاً به‌واسطهٔ بی‌پروا بودن در استفاده از امکانات الکترونیکی و اعتماد بیش از حد به ایمیل‌ها، وبگاه‌ها و یا هر چیزی در دنیای مجازی، امکان وقوع سرقت هویت از خویش را افزایش می‌دهند. در

فضای تجارت نیز، شرکت‌ها و مدیران با عدم رعایت موازین مربوط به ورود به فضای سایبری و یا بی‌مبالاتی در اجرای تدابیر لازم برای اجتناب از خطرات احتمالی، راه را برای سارقان هویت باز می‌کنند. حکومت نیز در صورت عدم ایجاد زیرساخت‌های لازم برای پیشگیری از این‌گونه موارد می‌تواند به نوعی مرتکب قصور شود. ایجاد ایمیل‌های امن و یا ایجاد علامت‌ها و نشانگرهای اعتباری خاص برای شرکت‌های تجاری و تبلیغاتی و بانک‌ها، می‌تواند مواردی باشد که توسط حکومت برای جلوگیری از سرقت هویت ایجاد و یا مدیریت می‌شود.

علاوه بر این، مواردی نیز وجود دارد که نمی‌توان شخص حقیقی یا حقوقی خاصی را به عنوان مسئول شناسایی کرد. به علت پیچیدگی‌های متنوعی که در جرم سرقت هویت در فضای سایبر وجود دارد، شناسایی فرد یا نهادی که مسئول این جرم بوده است، دشوار است؛ خصوصاً اینکه در فضای سایبر، آثار جرم سرقت هویت و فیشینگ مشهود نیست و عملاً غیرقابل‌پیگرد است و حتی شناسایی عاملی که موجب وقوع سرقت هویت شده است، دشوار است.

نحوهٔ وقوع سرقت هویت در تعیین نوع مسئولیت قربانی و ایجاد آن مؤثر است. مثلاً ممکن است شرکت‌های تجاری به‌واسطهٔ عدم رعایت موازین امنیتی کافی، قربانی این جرم شوند و اطلاعاتی که از مشتریان دارند، به‌واسطهٔ این سهل‌انگاری به سرقت رود. در این صورت این شرکت‌ها هم متحمل خسارات مستقیم می‌شوند و هم خسارات غیرمستقیم. به بیان دیگر هم باید مسئولیت این خسارات را متحمل شوند و هم جریمه‌های مربوط به خسارات وارده به مشتریان را پرداخت کنند و علاوه بر این، غالباً همه یا بیشتر مشتریان خود را از دست خواهند داد.

مسئلهٔ مسئولیت هم در حوزهٔ تقنین و هم در حوزهٔ فعالیت‌های تجاری محل سؤال و ابهام است. طبق دستورالعمل تجارت الکترونیک در سال ۱۹۹۹، محدودیت‌های ناظر به مسئولیت ناشی از استفادهٔ فریبکارانه یا غیرمجاز از سیستم‌های پرداختی، ابزاری بسیار قدرتمند برای افزایش اعتماد مصرف‌کنندگان می‌باشد و گسترش استفادهٔ آنان از فضای تجارت الکترونیک باید مدنظر قرار گیرد (OECD, 1999, section V).

همچنین در عهدنامهٔ مربوط به سرقت هویت، فیشینگ و اعتماد مصرف‌کننده در سال ۲۰۰۷ : (TACD's Resolution, 8th recommendation: www.tacd.org/cgibin/db.cgi?page=view& config= admin/ docs.cfg&id= 306. آخرین بازدید مهر ۹۸) آمده است که مسئولیت خسارات مالی ناشی از سرقت هویت یا فیشینگ، بر عهدهٔ شرکت‌ها و ارائه‌دهندگان خدمات است نه مشتریان، مگر اینکه به هر نحوی اثبات شود که مشتریان مقصر بوده‌اند.

در بیشتر کشورها، مسئولیت شرکت‌های تجاری، ناظر به فراهم آوردن تدابیر امنیتی مناسب و یا افشای تمام رخنه‌های محتمل نسبت به شرکت است. چنین تکالیفی چه به صورت مسئولیت

مدنی و چه به صورت قراردادی، به‌عنوان راهکاری مناسب برای پیشگیری از به دام افتادن مشتریان در سرقت هویت حائز اهمیت خواهد بود.

در بیشتر کشورهای عضو سازمان توسعه و تجارت اقتصادی سقفی برای مسئولیت مربوط به هزینه‌های تحمیل‌شده توسط سارقین هویت گذارده شده است. برای مثال در ایالات متحده آمریکا، مسئولیت مصرف‌کننده برای پرداخت‌های اعتباری غیرمجاز، محدود به حداکثر ۵۰ دلار آمریکایی است (OECD Report on Consumer Protections for payments Cardholders, DSTI/CP (2001)3/FINAL, (OECD, 2001).). در تبادلات مالی الکترونیک غیرمجاز نیز، میزان مسئولیت محدود شده است. در بعضی کشورها، علاوه بر تمام قوانین و مقررات، در حوزهٔ صنعت نیز مشتریان را از مسئولیت مبرا دانسته‌اند.

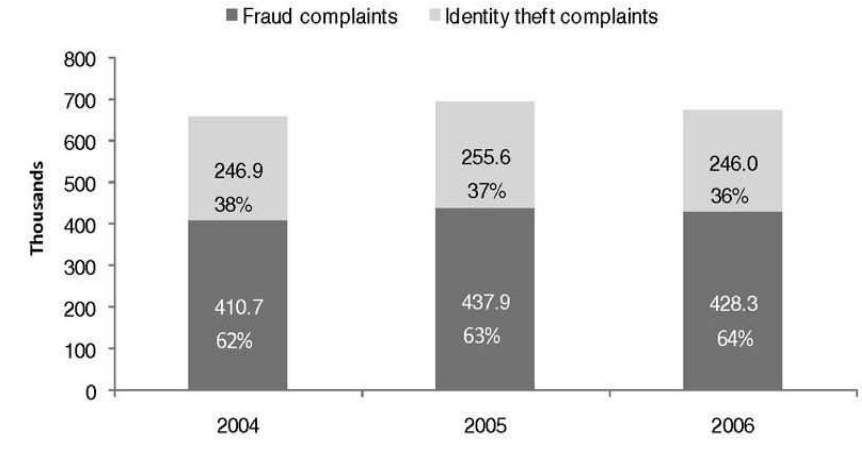
۴. موانع شناسایی قربانیان سرقت هویت در فضای سایبر

بررسی تعداد و میزان وقوع جرم سرقت هویت چه در فضای سایبر و چه در فضای حقیقی بسیار دشوار است، چراکه اولاً مصادیق معدودی از موارد آن شناسایی می‌شود و از این میان نیز تعداد کمی به مرحلهٔ شکایت می‌رسد؛ چراکه امید و امکان قانونی لازم برای به‌دست آوردن حقوق ازدست‌رفته در بسیاری از موارد کم است، ولی با این حال آماری نسبی در مورد میزان وقوع این جرم در فضای سایبر وجود دارد که عمدهٔ آن‌ها بر پایهٔ قربانیانی است که به مراجع قانونی مراجعه کرده‌اند.

۴-۱. اطلاعات سرقت هویت ناظر به بعضی از گونه‌های خاص کلاهبرداری

اطلاعات موجود ناظر به اشکال مختلف سرقت هویت، چندان بیانگر خود جرم و عواقب آن نیست و آمارهایی که ارائه می‌شود اگر صرفاً ناظر به نوع خاصی از این جرم و یا کلاهبرداری حاصل از آن باشد، نخواهد توانست تصویری کامل از عموم جرم سرقت هویت و آثار آن به حقوق‌دانان ارائه نماید. این نکته نیز باید مورد توجه قرار گیرد که این آمار، هر کدام نسبت به همان کشور مورد مطالعه قابل بررسی است و نمی‌تواند به سایر کشورها تسری داده شود.

با توجه به گزارش کمیسیون تجارت فدرال در ایالات متحده آمریکا، در سال ۲۰۰۶ برای ششمین سال پیاپی، جرم سرقت هویت به عنوان اولین مورد در میان دعاوی رسیده از مشتریان اینترنتی مطرح شده است.



تصویر شماره ۲– آمار شکایات رسیده در سال‌های ۲۰۰۴ تا ۲۰۰۶

این آمار بر اساس شکایات واصله است و شامل شکایات ناظر به تماس‌های تبلیغاتی نیست (USFTC , 2007a,) گزارش شکایات ناظر به سرقت هویت و کلاهبرداری از مصرف‌کنندگان).

آمار ارائه‌شدهٔ پیش‌گفته نشان می‌دهد که اطلاعات ناظر به شکایات را می‌توان در دو بخش طبقه‌بندی کرد؛ شکایات مربوط به سرقت هویت و شکایات مربوط به کلاهبرداری. شکایات مربوط به کلاهبرداری نیز تقسیم می‌شود به کلاهبرداری‌های اینترنتی و کلاهبرداری غیر آن. اما شکایات مربوط به سرقت هویت که ناظر به سوءاستفاده از اطلاعات شخصی افراد است، هیچ‌گونه تقسیم‌بندی ندارد، فارغ از اینکه از اینترنت صورت گرفته باشد یا از غیر آن.

یکی از بزرگ‌ترین معضلات در ایران، نبود اطلاعات آماری کافی ناظر به قربانیان جرائم رایانه‌ای است. اطلاعات موجود فعلی به صورت کلی صرفاً میزان رشد پرونده‌های واصله به نهادهای قضایی را نشان می‌دهد؛ برای مثال رئیس پلیس فتا در استان خراسان در گزارشی بیان می‌دارد که کشفیات جرائم سایبری در نوروز سال ۱۳۹۸ نسبت به مدت مشابه در سال ۱۳۹۷ با بیش از ۳۱۵ درصد رشد همراه بوده است (هدف کلاهبرداران سایبری سرقت اطلاعات حساب قربانیان؛ در: www.cyberpolice.ir/news/141726/، آخرین بازدید مهر ۹۸).

در گزارشی دیگر رئیس پلیس فتای کشور ابراز داشت که حدود ۶۵ درصد از جرائم رایانه‌ای کشور را جرم فیشینگ تشکیل می‌دهد و چون فیشینگ یکی از اصلی‌ترین طبقه‌بندی‌های سرقت هویت در فضای سایبر است، می‌توان میزان جدیت و حساسیت این نوع از جرائم رایانه‌ای را متوجه شد (۶۵ درصد کل جرائم سایبری کشور در حوزهٔ جرائم فیشنگ رخ می‌دهد؛ در: www.cyberpolice.ir/news/145945/65، آخرین بازدید مهر ۹۸).

تقریباً هر ساله با گزارشاتی ناظر به افزایش سرقت هویت و جرائم مرتبط به آن در ایران روبرو می‌شویم (افزایش ۲۰ درصدی جرایم در حوزهٔ کلاهبرداری اینترنتی؛ در: www.cyberpolice.ir/podcast/114121/، آخرین بازدید مهر ۹۸) اما ضعف در ارائهٔ آمار دقیق در این مسئله موجب تضعیف مطالعهٔ وضعیت قربانیان این جرم می‌شود.

از این رو عموماً هنگام تطبیق آمارهای داخلی با کشورهای دیگر، اطلاعات چندانی از این جرم در ایران قابل ارائه نیست، که البته بخشی از آن به‌خاطر پراکنده بودن قوانین قابل اعمال در این جرم و طبعاً گسترهٔ بالای پرونده‌هاست.

۴-۲. واگرایی در اطلاعات عمومی و خصوصی

مشکل دیگری که بر سر راه ایجاد تعریفی مناسب از قربانی سرقت هویت و آمار دقیق آن در فضای سایبر ایجاد شده است، تفاوت عمده و قابل‌توجهی است که میان اطلاعات جمع‌آوری شده توسط مقامات عمومی و اطلاعات به‌دست آمده توسط نهادهای خصوصی وجود دارد. مقامات عمومی و دولتی بر اساس اهداف عمومی و گستردهٔ خود اقدام به جمع‌آوری این اطلاعات می‌کنند، در حالی که نهادهای خصوصی اهداف آماری خود را صرفاً محدود به منویات نهاد و یا کار و تجارت خود می‌نمایند.

از سوی دیگر، شرکت‌های خصوصی نیز برای حفظ اعتبار و ارزش خود، حاضر نیستند سخن از خسارات مالی وارده بر خود، به میان آورند. این در حالی است که میزان سرقت هویت در فضای آنلاین و سایبر، در نهادها و سازمان‌های خصوصی هر لحظه در حال گسترش است.

طبق گزارش کمیسیون تجارت فدرال ناظر به سرقت هویت در سال ۲۰۰۳، در سال ۲۰۰۲ حدود ۱۰ میلیون شهروند آمریکایی به انحاء مختلف از این جرم متأثر شده‌اند (US FTC, 2003: 4). در گزارش همین کمیسیون در سال ۲۰۰۶ مشخص شده است که حدود ۸,۳ میلیون نفر آمریکایی متوجه شده‌اند که در سال قبل آن، یعنی سال ۲۰۰۵ قربانی سرقت هویت در فضای سایبر بوده‌اند ولی مطلع نبوده‌اند (US FTC, 2007b: 4).

در سال ۲۰۰۷ گزارشی ناظر به جرم کلاهبرداری از هویت ارائه شد، مبنی بر اینکه در یک سال، کاهشی ۱۲ درصدی در کلاهبرداری در این زمینه مشاهده شده است (www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-sstudy ، آخرین بازدید بهمن ۹۷). این گزارش بعدها به‌شدت در معرض انتقادات مختلف قرار گرفت. منتقدین بر این باور بودند که هدف از این گزارش صرفاً نشان‌دادن ثبات در بازار و موفق جلوه‌دادن تجارت در حفاظت از حقوق مشتریان بوده است. بعدها شرکت امنیتی مکافی این آمار را عمیقاً نقد کرد. این شرکت

مدعی بود که آن آمار (۱۲درصد) به‌شدت پایین آورده شده است (McAfee, 2007: 11). با مقایسهٔ این آمار با مواردی همچون گزارش گارتنر (http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html، آخرین بازدید بهمن ۹۶) .مشخص می‌شود که میزان قربانیان در این دو نمونه بسیار متعارض است؛ چراکه در گزارش گارتنر، قربانیان سرقت هویت در سال ۲۰۰۷، حدود ۱۵میلیون نفر اعلام شده‌اند.

علاوه بر تمام این تعارض‌های آماری، بعضی از مؤسسات و نهادهای تجاری و بازرگانی ابراز کردند که تابه‌حال هیچ‌یک از مشتریان آنان دچار این معضل نشده‌اند و همگی از فیشینگ و سرقت هویت و چنین کلاهبرداری‌هایی مصون بوده‌اند.

۵. مجراهای جبران خسارات ناشی از سرقت هویت در فضای سایبر

لزوم جبران خسارت برای قربانیان، جایگاهی اساسی خصوصاً در کشورهای توسعه‌یافته دارد؛ زیرا قربانیان چنین جرمی معمولاً مشتریان بنگاه‌ها و مراکز مالی یا خدماتی‌اند که بانک‌های اطلاعاتی آنان مورد هجمه قرار گرفته است. ازاین‌رو، شرکت‌ها و مؤسسات موظف‌اند تا در صورت وقوع این حملات و سوانح سایبری، جهت جبران خسارت مشتریان خود اقدام یا حداقل تسهیل‌گری کنند.

آنگاه که مشتریان خود به‌واسطهٔ سهل‌انگاری یا اشتباهات شخصی و...، موجبات سرقت هویت را فراهم می‌آورند، لازم است به آنان در احیای هویت سایبری‌شان کمک شود؛ چراکه مخدوش‌شدن هویت فرد، امنیت او را از جهات مختلف در معرض خطر قرار می‌دهد و حمایت‌نکردن از این قربانیان ممکن است محملی برای افزایش خسارات شود.

در ایالات متحده آمریکا، روندی نسبتاً جامع برای مقابله با سرقت هویت و ارائهٔ ابزارهای جبران‌کنندهٔ لازم برای قربانیان در نظر گرفته شده است. بسیاری از قوانین فدرال موجود در ایالات متحده، انتخاب‌های متنوعی را در اختیار قربانی قرار می‌دهد تا بتواند از خسارات ناشی از سرقت هویت اجتناب کند یا سارقان هویت را به صحنهٔ مصالحه بکشاند. این ابزارها به‌عنوان مشوّقی برای مشتریان و مصرف‌کنندگان برای ارائهٔ گزارش تجربهٔ سرقت هویت خود به کمیسیون تجارت فدرال، نقش‌آفرینی می‌کنند و نهادهای قانون‌گذار می‌توانند با استفاده از این گزارش‌ها به راهکارهای مناسب برای پیشگیری از سرقت هویت‌های بعدی دست یابند یا مسیرهای خطرناک تجاری را مسدود سازند.

علاوه بر این در آمریکا، آژانس‌ها و سازمان‌هایی هستند که به قربانیان سرقت هویت و مشتریان، این امکان را می‌دهند تا با اِعمال سیستمی تحت عنوان «هشدار کلاهبرداری» بر اطلاعات

هویتی آنان، در مدت ۹۰ روز، هرگونه استفاده یا سوءاستفاده از اطلاعات آنان را کشف کنند (15 U.S. Code § 1681c-1 - Identity theft prevention; fraud alerts and active duty alerts (a) (1).) و بعد از این مدت در صورت پیدانشدن موردی خاص، مشتریان می‌توانند برای دریافت وام و شغل یا خرید خانه و ماشین اقدام کنند. اما اگر در این مدت مورد مشکوکی ناظر به سوءاستفاده از هویت آنان یافت شود، این سازمان‌ها علاوه بر فراهم‌آوردن امکان ارائهٔ دادخواست در دادگاه، این سیستم هشداردهندهٔ هویتی را تا ۷ سال بر اطلاعات هویتی آن فرد اعمال خواهند کرد. علاوه بر این، مشتریان این امکان را خواهند داشت تا یک رونوشت از گزارش مالی مربوط به هویت خود از سازمان‌های مزبور دریافت کنند تا در صورت مشاهدهٔ هرگونه اعمال کلاهبردارانه، آن حساب‌ها را مسدود سازند و راه را به روی سارقین هویت ببندند.

در ایالات متحده، همچنین به مشتریان توصیه می‌شود تا گزارش‌ها و تبادلات مالی را از شرکت‌هایی که توسط سارقین هویت در هنگام جرم مورد استفاده قرار گرفته‌اند، دریافت کنند. مشتریان از این طریق قادر خواهند بود تا راه‌هایی را که مجرمین برای ایجاد خدشه در سابقهٔ هویتی قربانیان استفاده کرده‌اند، شناسایی کنند (US IDTTF, 2007, vol ii: 75). البته این امر برای بزه‌دیده جنبهٔ پیشگیرانه ندارد و صرفاً جهت بررسی میزان خسارت وارده و چگونگی شروع برای جبران آن مفید خواهد بود. از سوی دیگر، مقامات قضایی در آمریکا به قربانیان توصیه می‌کنند تا بلافاصله بعد از قربانی واقع‌شدن در این جرم، اقدام به مسدودکردن حساب‌هایی که مورد سوءاستفاده قرار گرفته است، نمایند و طلبکاران خود را از این واقعه و مخدوش‌بودن آن حساب‌ها مطلع سازند(US IDTTF, 2007, vol ii: 76) .

۶. نقش قربانیان و طرف‌های دیگر درگیر در جرم

در سرقت هویت اطراف مختلف وارد عمل می‌شوند که هر کدام از آنان می‌توانند نقش مؤثری در کاهش یا افزایش سرقت هویت داشته باشند. مطالعهٔ هر کدام از گروه‌ها و طرف‌هایی که در سرقت هویت نقش دارند، موجب می‌شود تا بتوان به الگویی مناسب برای تعیین تکالیف و وظایف قانونی برای هر یک و تبیین حقوق آنان نائل شد. علاوه بر این، می‌توان از این طریق راهی برای کاهش خطر سرقت هویت پیدا کرد.

افراد می‌توانند برای جلوگیری از وقوع سرقت هویت، از کارت‌های اعتباری یا اطلاعات خود در رایانه‌ها و گوشی‌ها بیشتر محافظت کنند. بسیاری از مشتریانی که در فضای سایبر، تبادل اطلاعات و خرید می‌کنند، اهمیت چندانی به نحوهٔ تحقق این تبادلات یا خریدها نمی‌دهند یا از خطرات آن مطلع نیستند؛ مثلاً در خریدهای بانکی توصیه می‌شود که در هنگام ورود اطلاعات

کارت‌های اعتباری و رمز آن، از صفحه‌کلید رایانه یا گوشی همراه استفاده نشود. همیشه در این مواقع، صفحه‌کلیدی مجازی و مطمئن در اختیار خریداران قرار داده می‌شود و آن‌ها می‌توانند با استفاده از آن احتمال لورفتن اطلاعات خود را از بین ببرند؛ چراکه بعضی بدافزارها صرفاً به بررسی کلیدهای استفاده‌شده در صفحه‌کلید می‌پردازد و اگر فرد از صفحه‌کلید خود در هنگام خرید یا ورود اطلاعات مهم استفاده کند، عملاً با دستان خود اطلاعات شخصی خود را لو داده است؛ لذا شاید بتوان گفت که بی‌احتیاطی او عامل اصلی این جرم می‌شود.

افزون بر این، افراد می‌توانند برای اطلاع سریع از هرگونه رفتار مشکوک ناظر به حساب بانکی خود، به‌صورت مداوم از آن خبر گرفته و بر گردش و موجودی حساب خود دائماً نظارت کنند. همچنین افراد در بسیاری از امور سایبری خود باید رمزها و اطلاعات امنیتی خود را هر چند وقت یک بار تغییر دهند و راه را برای کسانی که از طریق مهندسی اجتماعی سعی در به‌دست آوردن آن اطلاعات دارند، ببندند. در مقابل، کسانی که از مشتریان کالا یا مبلغی را دریافت می‌کنند، موظف هستند تا از وجود فرد اصلی در پسِ هویت ارائه‌شده اطمینان حاصل کنند. به همین دلیل لازم است تا علامت‌ها و نشانه‌های امنیتیِ خاصی مربوط به شخص دارندهٔ حساب یا عنوان هویتی طراحی کنند؛ به‌صورتی که صرفاً خود شخص بتواند از آن استفاده کند. از سوی دیگر، شرکت‌های مسئول باید تدابیر و استانداردهای خاصی برای هرگونه احتمال استفاده از هویت توسط دیگران، اعمال کنند. البته تدابیری که هر یک از طرفین برای جلوگیری از به‌دام‌افتادن در این جرم می‌اندیشند، بستگی عمیقی به مسئولیت مدنی یا کیفری آنان دارد که بعد از وقوع جرم گریبان‌گیرشان می‌شود.

سوءاستفاده از کارت‌های الکترونیک و حساب‌های بانکی و حساب‌های کاربری افراد در اینترنت، پدیده‌هایی‌اند که در دههٔ اخیر شدت گرفته‌اند و قواعد و قوانین نیز متناسب با آن‌ها دچار تحولاتی شده‌اند. قواعد ناظر به مسئولیت افراد در این جرم، با استفاده از قوانین یا قراردادهای فی‌مابین تعیین می‌شود. به‌طور خلاصه، طبق قوانین فدرال ایالات متحده آمریکا، مشتریان و مصرف‌کنندگان حداکثر تا میزان ۵۰ دلار مسئول شناخته می‌شوند و اگر میزان کلاهبرداری از این مقدار افزون‌تر رود، نمی‌توان آنان را مسئول شمرد. جالب اینجاست که عمدهٔ کلاهبرداری‌های حاصل از سرقت هویت، رقمی بالاتر از ۵۰ دلار دارد و عملاً هیچ مسئولیتی بر مصرف‌کنندگان بار نمی‌شود. همچنین رقابت‌های اقتصادی میان شرکت‌های تجاری موجب شده است تا مسئولیت مشتریان و مصرف‌کنندگان حتی کمتر از این مقدار شود. البته شرایطی نیز برای جلوگیری از سوءاستفاده از این امتیاز قرار داده شده است؛ مثلاً دارندگان کارت‌های اعتباری موظند تا حداکثر در زمانی معین که توسط شرکت‌ها مشخص می‌شود، گزارش کلاهبرداری یا سرقت هویت خود را

به اطلاع مقامات مسئول برسانند که در این صورت هیچ‌گونه هزینه و مسئولیت مدنی بر آنان بار نمی‌شود. در واقع این نوع از مسئولیت علاوه بر برداشتن بار هزینه و خسارت از دوش مشتریان و کاربران موجب خواهد شد تا آنان به‌طور مداوم به چک‌کردن حساب خود بپردازند.

در نقطهٔ مقابل، باید ملاحظه‌ای دیگر را نیز مدنظر قرار داد و آن اینکه در فضای مجازی، مشتری و خریدار و مصرف‌کنندگانی که از خدمات اینترنتی و آنلاین استفاده می‌کنند، باید میزان ریسکش را پیش‌بینی کنند. به این معنی که آنان باید برای مبادلات خود اطمینان کافی به منبعی که از آن خرید می‌کنند، داشته باشند. این خریدار است که باید دقت‌نظر و توجه کافی در خرید خود به خرج دهد و در موارد مشکوک از خریدکردن پرهیز کند. خصوصاً در خریدهایی که شامل تبادل مقادیر فراوانی از کالا و پول است؛ برای مثال وقتی شخصی می‌خواهد گلی را به‌نحو اینترنتی بخرد، شاید آن‌چنان برایش مهم نباشد که فروشنده و متصدی حمل‌ونقل، دو شرکت یا گروه مختلف باشند؛ اما وقتی فردی می‌خواهد طلا یا جواهرات را به‌صورت آنلاین بخرد، باید دقت‌نظرهای لازم را انجام دهد و در صورت مشاهدهٔ هرگونه تفاوت در ارائه‌دهندهٔ کالا و متصدی حمل آن، باید از آن دوری کند وگرنه در صورت خرید و متحمل‌شدن خسارت، خودش مسئول بی‌احتیاطی خواهد بود.

شرکت‌های طراحی‌کنندهٔ کارت‌های اعتباری، سایت‌های خرید اینترنتی، درگاه‌های پرداخت، حساب‌های کاربری، سیستم‌های امنیتی آنلاین و دیگر طراحانی که به‌نحوی در روند امنیتی کاربران اینترنتی دخیل‌اند، باید تدابیر لازم را برای استحکام حدود امنیتی محصولات خود انجام دهند و هرگونه ضعف کارایی از سیستم‌های امنیتی آنان موجب ایجاد مسئولیت برای آنان می‌شود.

در مجموع باید گفت که زمان انجام امور بانکی در فضای سایبر، نمی‌توان گفت که صرفاً فرد فروشنده یا فقط وسیلهٔ واسط الکترونیکی، به‌عنوان طرف فاعل شناخته می‌شود؛ بلکه هر کدام متناسب با میزان دقت‌نظر یا بی‌احتیاطی خود در شرایط مختلف مسئول شناخته می‌شوند و نمی‌توان به‌طور مطلق، یکی از عوامل را به‌عنوان مسئول در نظر گرفت؛ بلکه شرایط هر سرقت هویت و عوامل مختلف آن در تعیین مسئولیت افراد مؤثر است.

نتیجه‌گیری

نکتهٔ منحصربه‌فرد دربارهٔ سرقت هویت در فضای سایبر این است که بسیاری از قربانیان سرقت هویت نه‌تنها از منشأ سرقت و دزدی اطلاعات هویتی خود اطلاعی ندارند، بلکه مدت‌های مدیدی پس از وقوع سرقت و کلاهبرداری‌های بعد از آن، متوجه موضوع و خسارت می‌شوند و آنجاست که نه‌تنها یافتن عامل سرقت تقریباً غیرممکن است، بلکه حتی خسارات وارده نیز به‌راحتی

جبران‌پذیر نیست؛ ازاین‌رو لازم است نکات کلیدی ذیل به عنوان پیشنهاد برای بهبود وضعیت ناظر به سرقت هویت در فضای سایبر مطرح شود:

الف) آمار موجود در خصوص سرقت هویت در آمریکا نشان‌دهندهٔ گسترش و افزایش ارتکاب این جرم در این کشور است. افزایش میزان قربانیان نیز در این آمار نشان از خطر شدید و حساسیت این موضوع است. همچنین بر اساس اعلام پلیس فتا، آماری مشابه در ایران نیز وجود دارد که با گسترش شبکه‌های ارتباطی و اینترنتی، در حال افزایش است؛ خصوصاً اینکه در ایران میزان آگاهی دربارهٔ این خطر بسیار کمتر است و روش‌های جلوگیری و پیشگیری از سرقت هویت نیز چندان به کار نرفته است. علاوه بر این، در قانون نیز به‌طور خاص و صریح از موضوع سرقت هویت بحث نشده است و همین موجب شده است که صرفاً شاخه‌های متعدد ناشی از سرقت هویت یا انواع خاصی از عملیات‌های مخرب سایبری که هم‌نوع و هم‌شکل با سرقت هویت در فضای سایبر است، به‌عنوان جرائم رایانه‌ای مطرح گردد که این خود آسیبی است که توسط قانون به شهروندان وارد می‌آید. مطرح‌کردن صریح این جرم در قانون به‌عنوان جرمی خاص می‌تواند بسیاری از سردرگمی‌های قانونی ناظر به این مسئله را حل کند و علاوه بر آن موجب آگاهی مردم و ترسی ناخودآگاه در دل مرتکبین شود؛ زیرا در حال حاضر آنان می‌توانند به اشکال و بهانه‌های مختلف و صرفاً به‌واسطهٔ تصریح‌نشدن قانونی در این خصوص، از اتهام فرار کنند.

ب) در همین زمینه، کنوانسیون بوداپست که به‌عنوان منبع اصلی قانون مبارزه با جرائم رایانه‌ای ایران مطرح شده است، تأکید فراوانی بر لزوم همکاری بین‌المللی برای مبارزهٔ کیفری با این‌گونه از جرائم دارد. طبق این کنوانسیون، کشورهای عضو باید در کنار وضع قوانینی لازم‌الاجرا برای حمایت از محرمانه‌بودن، صحت و در دسترس‌بودن اطلاعات، تدابیری نیز برای فراهم‌آوردن امکان کشف، تعقیب، تحقیق و مبارزهٔ مؤثر با جرائم رایانه‌ای اتخاذ کنند. این تدابیر نه‌تنها باید در سطح ملی بلکه در سطح فراملی و بین‌المللی نیز فراهم آید. این کار باید از طریق همکاری با شرکت‌های بین‌المللی صورت گیرد و لزوم همکاری بین‌المللی در زمینهٔ سرقت هویت در فضای سایبر، امری انکارناپذیر است؛ چراکه می‌توان گفت تقریباً همه جرائم سایبری به‌عنوان جرائم بدون مرز شناخته می‌شود و اگر همکاری و تعامل بین‌المللی در مبارزه با این جرائم وجود نداشته باشد، مبارزه به نتیجه‌ای مؤثر منتهی نمی‌گردد.

ج) برای مقابله با جرم سرقت هویت که به‌صراحت در قوانین موجود ذکر نشده است و رو به افزایش است، نیاز به ایجاد قانونی مؤثر در این حوزه احساس می‌شود؛ خصوصاً اینکه کنوانسیون بوداپست به‌نحوی بسیار کلی، اقدام به جرم‌انگاری اقدامات علیه امنیت اطلاعات کرده است؛ در حالی که جرم سرقت هویت در فضای سایبر، به‌واسطهٔ داشتن جوانب و زوایای پنهان بسیار،

نیازمند برخوردی دقیق‌تر و جامع‌تر است که بدون ایجاد موادی خاص متناظر با آن، این برخورد غیرممکن می‌نماید. بنابراین نباید اتکا به قانون بوداپست را به‌عنوان یگانه گزینهٔ موجود در نظر گرفت و ضروری است متناسب با آمار موجود در ایران به تصمیم‌گیری قانونی مناسب دراین‌باره رسید.

د) به نظر می‌رسد باید قوانین ناظر به سرقت هویت با رویکردی پیشگیرانه طراحی شود تا بتوان مانع از شروع به جرم شد. هرچند این مسئله نیاز به داشتن فناوری لازم برای شناسایی به‌موقع این جرم دارد، این نکته بسیار اساسی است که در وضع قوانین اولاً باید تمام احتمالات و خطرات لازم را در نظر گرفت؛ کما اینکه با ذکرنشدن سرقت هویت در قانون، فضا برای بسیاری از خطرات و جرائم ارتکابی باز شده است و ثانیاً نباید منتظر فناوری برای همگام‌شدن با مقابله با جرم شد. این مسئله را باید به خاطر داشت که همیشه مجرمین حداقل یک قدم از پلیس و مأموران قانون جلوتر هستند؛ ولی قانون باید چندین مرحله از مرتکبین جلوتر باشد و این به معنای آماده‌کردن بستر قانونی لازم برای برخورد با مرتکبین و باقی‌نگذاشتن راه فرار یا توجیه برای آنان است.

و) نکتهٔ آخر اینکه مسروق‌عنه جزو مظلوم‌ترین قربانیان حاصل از جرائم رایانه‌ای است. لزوم فراهم‌نمودن شرایط قانونی و تکنیکی لازم برای بازگرداندن هویت، اعتبار و مال ازدست‌رفته او روشن است. ازاین‌رو، به نظر می‌رسد که قانون‌گذار باید برای تضمین این حقوق و آبروی ازدست‌رفته، برای نهادهایی که به‌نوعی با هویت مسروق‌عنه در ارتباط هستند، الزاماتی وضع کند که وی را به صحنهٔ جامعه بازگردانند.

منابع

الف) فارسی

۱. باستانی، برومند (۱۳۹۰)، **جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری**، چ ۳، تهران: انتشارات بهنامی.

۲. خالقی، ابوالفتح؛ صالح‌آبادی، زهرا (۱۳۹۴)، «مطالعه سرقت هویت در حقوق فدرال آمریکا با نگاهی اجمالی به حقوق ایران»، حقوق تطبیقی، پاییز و زمستان، ش ۱۰۴، صص ۱۱۴ – ۸۷.

۳. شیرزاد، کامران (۱۳۸۸)، **جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین الملل**، چ ۱، تهران: انتشارات بهینه فراگیر.

۴. صادقی، حسین (۱۳۸۸)، **مسئولیت مدنی در ارتباطات الکترونیک**، چ ۱، تهران: نشر میزان.

۵. طبیبی، مرتضی؛ خدادادی، انیس (۱۳۹۴)، «سرقت هویت»، مجله علمی پژوهشی فقه و حقوق اسلامی، بهار و تابستان، ش ۱۰، صص۹۶ – ۷۵.

۶. هدف کلاهبرداران سایبری سرقت اطلاعات حساب قربانیان، در: آخرین بازدید مهر ۹۸
www.cyberpolice.ir/news/141726/
۷. ۶۵ درصد کل جرائم سایبری کشور در حوزهٔ جرائم فیشنگ، در:آخرین بازدید مهر ۹۸
www.cyberpolice.ir/news/145945/
۸. آخرین بازدید مهر ۹۸
www.cyberpolice.ir/news/146064/
۹. افزایش ۲۰ درصدی جرایم در حوزهٔ کلاهبرداری اینترنتی، در: آخرین بازدید مهر ۹۸.
www.cyberpolice.ir/podcast/114121/

ب) غیرفارسی

10. BT, BT (British Telecom), CPP, Get Safe Online, Lloyds TSB, Metropolitan Police, Yahoo! (UK) (2006), Security Report, February 2006.
11. BWGCBMMF, (Bi-national Working Group on Cross-Border Mass Marketing Fraud) (2004), Report on Identity Theft, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, October 2004.
12. FTC (Federal Trade Commission) (US) (2006a), Identity Theft Task Force Seeks Public Comment, press release, 26 December 2006.
13. FTC (Federal Trade Commission) and DOJ (Department of Justice) (US) (2007a), Combating Identity Theft: A Strategic Plan, US President's Task Force on Identity Theft, 23 April 2007.
14. FTC (Federal Trade Commission) (US) (2007b), Report on Consumer Fraud and Identity Theft Complaint Data.
15. Javelin Strategy and Research (2007), 2007 Identity Fraud Survey Report - Identity Fraud Is Dropping, Continued Vigilance Necessary, Consumer Version, February 2007.
16. McAfee Avert Labs (2007), Identity Theft, White Paper, January 2007.
17. OECD, (Organization for Economic Co-operation and Development) (1999), Guidelines for Consumer Protection in the context of Electronic Commerce, section V, OECD, Paris.
18. OECD (2001), Report on Consumer Protections for payments Cardholders, DSTI/CP (2001)3/FINAL, OECD, Paris.
19. TACD (Trans-Atlantic Consumer Dialogue) (2007), Resolution on Identity Theft, Phishing and Consumer Confidence, 22 February 2007.
20. UN IEG, (United Nations Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity) (2007), Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, E/CN.15/2007/8, 2 April 2007.
21. US FTC, FTC (Federal Trade Commission) (US) (2003), 2003 Identity Theft Survey Report, prepared by Synovate, September 2003.
22. US IDTTF, (Identity Theft Task Force) (US) (2007), Combating Identity Theft: A Strategic Plan, 23 April 2007, vol ii.
23. OECD (2009), (Organization for Economic Co-operation and Development), Online Identity Theft, OECD, Paris.
24. https://www.gartner.com/ newsroom/id/501912, آخرین بازدید اردیبهشت ۹۶
25. Www. javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/, آخرین بازدید بهمن ۹۵
26. http://solutions.journaldunet.com/0607/060726-etude-securite-csi-fbi.shtml, آخرین بازدید آذر ۹۷
27. www.cifas.org.uk/identity_fraud_is_theft_serious.asp, آخرین بازدید بهمن ۹۵
28. TACD's Resolution, 8th recommendation: www.tacd.org/cgibin/db.cgi?page=view& config= admin/ docs.cfg&id= 306, آخرین بازدید مهر ۹۸