فصلنامه رهیافت پیشگیری/ دورهٔ اول، شمارهٔ دوم، تابستان ۱۳۹۷
Prevention Approach Quarterly
Vol. 1, No.2, (Summer 2018)

تاریخ دریافت: ۱۳۹۷/۰۴/۲۴
تاریخ پذیرش: ۱۳۹۷/۰۵/۱۵

نقش بانک‌ها در پیشگیری از جرایم بانکداری الکترونیکی

نسترن ارزانیان[۱] و مرضیه دیرباز[۲]

چکیده

زمینه و هدف: با روی کارآمدن فضای سایبر و پیشرفت فناوری‌های نوظهور، جهان با ساحتی برای تعاملات الکترونیکی و دخالت کمتر عناصر انسانی مواجه شد. فضای سایبر عرصه‌های مختلفی را با تغییرات شگرفی رو به رو ساخت، که یکی از این عرصه‌های پیشگام، صنعت بانکداری است. مسلم است که در پَس خدمات شایان بانک‌ها در چارچوب منحصر به فرد سیستم بانکداری الکترونیکی، صنعت بانکداری با تهدیدات و مخاطرات نوظهوری نیز مواجه است. ناامنی فضای اینترنت و نظام بانکداری الکترونیکی، از مهمترین مخاطرات مطرح در این حوزه به شمار می‌آید. شایان توجه است که استفاده از تدابیر پیشگیرانه، یکی از راه‌های برقراری امنیت و انتظام جوامع است.

روش شناسی: پژوهش حاضر با تکیه بر نظرات حقوقی، داده‌ها و آموزه‌های علمی گردآوری شده از میان کتاب‌ها، مقالات، پایان نامه‌ها و پایگاه‌های اینترنتی صورت پذیرفته است. افزون بر این، نوع پژوهش فرارو، به صورت کاربردی و شیوه نگارش آن توصیفی است. در این میان به قوانین جمهوری اسلامی ایران و اسناد بین‌المللی نیز توجه ویژه شده است.

یافته‌ها و نتایج: در عصر دوم اینترنت و روی کارآمدن فناوری نوظهور بلاک‌چین، کارآیی پیشگیری وضعی از جرم درگرو بهره‌جویی از فناوری‌های نوین و گرایش به سوی به کارگیری تدابیر پیشگیرانهٔ فنی است، زیرا در دنیای هوشمندی اشیاء که بانکداری الکترونیکی در بستر آن فرصت بروز می‌یابد، ماهیت محیط سایبر به گونه‌ای است که بانک‌ها را ناگزیر از اتخاذ تدابیر پیشگیرانهٔ فنی می‌سازد.

کلیدواژه‌ها: بانکداری الکترونیکی، امنیت، جرایم سایبری، پیشگیری از جرم.

❑ **استناد:** ارزانیان، نسترن؛ دیرباز، مرضیه (تابستان، ۱۳۹۷). **نقش بانک‌ها در پیشگیری از جرایم بانکداری الکترونیکی**. *فصلنامه رهیافت پیشگیری، ۱(۲)*، ۱۲۱-۱۳۸.

۱. دانشجوی کارشناسی ارشد حقوق حمل و نقل دانشگاه علوم قضایی و خدمات اداری. (نویسنده مسئول). رایانامه: arzanian72@gmail.com
۲. دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه کاشان. . رایانامه: marziyedirbaz@gmail.com

مقدمه

فناوری‌های نوظهور ارتباطی، پیش از پیدایش فناوری‌های ذخیره و پردازش اطلاعات وجود داشته‌اند. اما، تولید رایانه و ورود آن به بازار، مولد انقلابی در ساحت فناوری‌های اطلاعات شد. تجارت، یکی از عرصه‌هایی است که فناوری نوین اطلاعاتی در آن رسوخ بیشتری داشته است. استفاده از ابزارهای الکترونیکی، معاملات تجاری الکترونیکی را به‌وجود آورد که در مقایسه با تجارت سنتی، افزایش چشمگیری داشته‌اند. در روش‌های تجارت سنتی، مذاکرات و معاملات، کم رنگ و بازرگانان از پیشگامان استفاده از ابزار نوظهور بودند. تجارت الکترونیکی[1]، مبادلات تجاری عاری از تماس یا تعاملات مستقیم فیزیکی در بستر ابزار الکترونیکی را دربر می‌گیرد. به‌طور مثال می‌توان به مواردی چون مبادلهٔ الکترونیکی کالا و خدمات و انتقال فوری داده‌های دیجیتالی اشاره کرد.

مهمترین مرحلهٔ مولد تجارت الکترونیکی، وجود سیستم پرداخت الکترونیکی است (حبیب‌زاده، ۱۳۹۰، ص ۱۰۳). بنابراین یکی از ابزارهای کارآمد تشکیل و جریان شگرف تجارت الکترونیکی، صنعت بانکداری در قالب ابزار الکترونیکی[2] است، که به بانکداری الکترونیکی شهرت دارد. شایان توجه است که در گذشته نزدیک، مردم از گذر نظام بانکداری سنتی[3] تراکنش‌های بانکی مورد نیاز خود را، انجام و رهگیری می‌کردند (مشرف‌جوادی و همکاران، ۱۳۸۹، ص ۲۶). منظور از بانکداری سنتی، رسانیدن خدمات بانکی در شعب، با بهره‌گیری از ابزار کاغذ و قلم، در قالب عملیات فیزیکی و عوامل سراسر انسانی است. در پی پیدایش و گسترش استفاده از وسایل و ابزارهای اطلاعاتی نوظهور، نظام بانکداری سنتی، کارآمدی خود را اندکی از دست داد. زیرا بانکداری الکترونیکی، بدون توجه به موقعیت جغرافیایی بر امکان‌سنجی، داد و ستدهای تجاری مشتریان سخت در تلاش است (ویج و همکاران[4]، ۲۰۱۴، ص ۶۶). مسلم است که در پَسِ خدمات شایان بانک‌ها در چارچوب منحصر به فرد سیستم بانکداری الکترونیکی، صنعت بانکداری با تهدیدات و مخاطرات نوظهوری نیز مواجه است. به علاوه این شیوه نوظهور بانکداری، فرصت‌های تازه‌ای را

1. Electronic Commerce
2. Electronic Banking
3. Traditional Banking
4. Vij Jyoti & Kavita Vij &Vinod Vij

در اختیار مجرمان قرار داده و منجر به تولد جرایم سایبری شده است. از این رو، مهمترین مسئله مطرح در این سیستم، حفظ امنیت شهروندان و جلوگیری از بزه‌دیدگی آنان است.

به باور دورکیم، بزهکاری پدیده‌ای عادی و بهنجار در جامعه و اجتناب‌ناپذیر است (حاجی ده‌آبادی، ۱۳۹۴، ص ۲۵). اما، این پدیده عادی و خطر طبیعی باید با عاملی به نام امنیت اداره و کنترل شود. امروزه، امنیت به امر ارزشمندی تبدیل شده که بشر مصمم به تأمین آن است. مدیریت خطر جرم در جوامع مختلف، به دو شیوه کیفری و غیرکیفری صورت می‌گیرد. ابزار اصلی مدیریت غیرکیفری ریسک جرم، پیشگیری است. ایران نیز در دو دهه گذشته، زیرساخت‌های جدیدی را افزایش داده که با شیوه‌های نوین به کنترل بزهکاری می‌پردازند. این زیرساخت‌ها، به سمت اهدافی مانند پیشگیری، امنیت، کاهش ریسک و کاهش ترس که با اهداف سنتی تعقیب و مجازات متفاوت هستند، میل کرده‌اند.

نوشتار پیش‌رو، بر آن است تا نقش بانک‌ها را در تأمین امنیت مشتریان و همچنین پیشگیری از جرایم بانکداری الکترونیکی مورد بررسی قرار دهد. با بررسی پیشینه پژوهش‌های انجام شده درخصوص موضوع پژوهش به چند مورد اشاره می‌شود: حسین زاده شهری و قدک‌فروشان (۱۳۹۱) در پژوهش خود به بررسی ریسک‌های موجود در نظام بانکداری الکترونیکی پرداختند و هریک از آن‌ها را براساس شاخص‌های موجود اولویت بندی نمودند. پس از آن به این نتیجه رسیدند که بانک‌ها باید ارزیابی مناسبی از ریسک‌های قانونی مرتبط با خدمات بانکداری الکترونیکی داشته باشند. بنابراین پیشنهاداتی را در این باره مطرح کرده‌اند. همچنین یافته‌های پژوهش مشرف‌جوادی، بهزادفر و قوچی‌فرد (۱۳۸۹) نشان می‌دهد که مسئله امنیت و حریم خصوصی، از مهمترین موانع توسعه بانکداری الکترونیکی هستند. از نتایج پژوهش حبیب‌زاده و میرمجیدی هشجین (۱۳۹۰) می‌توان به این نکته اشاره کرد که بانکداری الکترونیکی، موجب تسهیل ارتکاب جرم پولشویی شده و روش‌های جدیدی را جهت ارتکاب این جرم پدید آورده است. براین اساس پژوهش حاضر نویسنده با بررسی نظام بانکداری در فضای سایبر، گونه‌های پیشگیری از جرایم در این بستر را مورد ارزیابی و راهکارهای پیشگیرانه‌ای را ارائه می‌دهد.

بانکداری الکترونیکی: با گسترش افق‌های فکری در ارتباط با کسب‌وکار- به ویژه کسب و کار از

طریق الکترونیکی که همراه با ارائه سرویس و خدمات الکترونیکی بود-، بانک‌ها به خاطر ماهیت خاص خود، به کاربران کارآمدتر و به روزتری در استفاده از فناوری آنلاین تبدیل شدند (صنایعی، شاهین و سلیمیان، ۱۳۹۲، ص ۲). بدین ترتیب، سیستم بانکداری الکترونیکی به صنعت بانکداری راه یافت. بانکداری الکترونیکی عبارت است از به‌کارگیری فناوری‌های پیشرفتهٔ نرم‌افزاری و سخت‌افزاری، در قالب شبکه‌های رایانه‌ای و کانال‌های الکترونیکی مستقیم، که خدمات بانکی سنتی و جدید را به مردم ارائه می‌دهند (فلاح تفتی، ۱۳۹۰، ص ۷). به بیان دیگر، بانکداری الکترونیکی به سرویس‌دهی الکترونیکی بانکی در میان مشتریان و بانک می‌پردازد. در بانکداری الکترونیکی، مفاهیمی همچون چک الکترونیکی، امضای دیجیتالی، پول الکترونیکی و بلیط الکترونیکی که از طریق کانال‌های اینترنتی در دسترس همگان هستند مطرح می‌شوند (اکبری اصل، ۱۳۸۶، ص ۲۷).

نخستین پرداخت الکترونیکی در جهان، در سال ۱۹۱۸ میلادی، از طریق تلگراف و نسبت به انتقال وجه توسط بانک فدرال رزرو آمریکا[1] انجام گرفت. در سال ۱۹۵۹ میلادی نیز، با تبدیل سیستم سرویس‌دهی بانک‌ها از شکل سنتی به نظام مدرن، نوع جدیدی از خدمات به نام کارت‌های اعتباری، از سوی بانکی آمریکایی فراهم شد (ملکی و اکبری، ۱۳۸۹، ص ۱۵) و در نهایت، خدمات بانکداری آنلاین، برای اولین بار در اوایل دهه ۱۹۸۰ میلادی در جهان ارائه شدند (شاه‌محمود و کلارک[2]، ۲۰۰۹، ص ۳).

سابقه بانک‌داری الکترونیکی در ایران، به سال ۱۳۵۰ خورشیدی نخستین استفاده از دستگاه‌های خودپرداز، باز می‌گردد. در نخستین سال‌های دهه ۱۳۷۰خورشیدی، بانک تجارت ایران، برای اولین بار موفق به صدور کارت بانکی شد. در همین راستا، گام‌های مهمی نیز در مسیر بهره‌گیری از بانکداری الکترونیکی از رهگذر طرح جامع اتوماسیون بانکی برداشته شد. این طرح در سال ۱۳۷۲ خورشیدی، توسط مجمع عمومی بانک‌ها تصویب شده و در پی آن، شرکت ملی انفورماتیک[3] تأسیس شد (کشته‌گر، ۱۳۹۰، ص ۵۳). بر اساس همین مصوبه، مسئولیت و پیشبرد طرح بر عهده

---

۱. بانک‌فدرال رزرو (Federal Reserve Bank)، بانک مرکزی ایالات متحده امریکاست که در سال ۱۹۱۳ میلادی و با هدف نظارت بر عملیات بانکی در این کشور تأسیس شده است.

2. ShahMahmood & Clarke

۳. برای اطلاعات بیشتر در این زمینه، بنگرید به:http://www.nicholding.net

مشاور اجرایی ریاست کل بانک مرکزی قرار گرفته بود. طرح مزبور، با درنظر داشتن نیازهای اطلاعاتی بانک و ساختار گردش اطلاعات، مدل متمرکز اطلاعات را در بانک‌ها شناسایی کرد. ایجاد زمینه لازم برای کاهش مبادلات نقدی و نقل و انتقال پول، صرفه‌جویی در وقت کارکنان و مشتریان بانک‌ها، کاهش نقل و انتقال فیزیکی مدارک در شعب، کاهش سفرهای شهری، قطع وابستگی جغرافیایی مشتریان به شعب خاص، گسترش ارائه خدمات بانکی به خارج از ساعات کار رسمی بانک، یکپارچگی اطلاعات بانک و اجتناب از ذخیره چندباره و زاید اطلاعات، از جمله اهدافی هستند که طرح جامع، در پی دستیابی به آنها بود (حسین زاده شهری و قدک فروشان، ۱۳۹۱، ص ۵۶).

امنیت مشتریان: حق بر امنیت، یکی از حقوق بنیادین بشر است که در ماده ۹ میثاق بین المللی حقوق مدنی و سیاسی (مصوب سال ۱۹۶۶ میلادی)[1] نیز، به رسمیت شناخته شده است. واژه امنیت، در لغت به معنای در امان بودن، ایمنی، آرامش و آسودگی آمده است (عمید، ۱۳۸۶، ص ۱۵۶). به بیان دیگر، وجود احساس اعتماد و اطمینان نسبت به یک موضوع را امنیت گویند. از نظر سیاسی، دولت‌ها متولی امنیت هستند و این حق، دولت‌مردان را مکلف می‌کند تا امنیت جانی، مالی و حیثیتی شهروندان را تضمین کنند (نجفی ابرندآبادی، ۱۳۹۱، ص ۱۱۰). میان احساس ناامنی و احساس ترس از جرم، یک رابطهٔ مستقیم وجود دارد. با عنایت به این موضوع احساس ترس و ناامنی، زمانی به‌وجود می‌آید که افراد، با تصور وجود عوامل تهدیدکننده در جامعه، وقوع جرم در آینده و بزه‌دیدگی خود را احتمال بدهند (طاهری، ۱۳۹۲، ص ۹۱). افزون بر آن تمامی افراد در اجتماع در معرض بزه‌دیده شدن هستند. ترس از جرم و بدگمانی نسبت به امنیت، در حوزه‌های مختلفی، ساختار جامعه را به هم می‌ریزد و خود مولد شرایطی است، که خود آن شرایط ایجادی، سبب تحقق جرایم و از بین رفتن آرامش آحاد مردم خواهد شد (گسن، ۱۳۸۵، ص ۲۰۳). همچنین، برخی از افراد ممکن است با احساس ناامنی و ترس از بزه‌دیده شدن بیشتری مواجه باشند. این امر می‌تواند از وضعیت‌ها و موقعیت‌های ویژه‌ای که طیفی از افراد با آن رو به رو هستند، سرچشمه بگیرد. به‌طور مثال اشخاصی که با نظام بانکداری الکترونیکی تعامل دارند و در عملیات روزانه خود پیوسته از آن بهره‌مند هستند،

1. International Covenant on Civil and Political Rights

بیش از دیگران از ترس و بی‌قراری ناشی از نبود امنیت در فضای سایبر رنج می‌برند.

امنیت در نظام بانکداری الکترونیکی: امنیت یکی از پیش نیازهای اولیه و ضروری در سیستم بانکداری الکترونیکی است، زیرا با ورود فناوری نوین اینترنتی به حرفهٔ بانکداری، باید زیرساخت‌ها و بستر مورد نیاز برای مقبولیت و اطمینان مشتریان نیز فراهم شود. به‌طور حتم بیشترین فعالیت صنعت بانکداری بر بنیان اطلاعات شخصی و حساس مشتریان است. بنابراین حفاظت از اطلاعات شخصی و حریم خصوصی مشتریان، امری ضروری است. رعایت نکردن تدابیر پیشگیرانه و بی‌توجهی بانک‌ها و مشتریان به مقررات وضع شده از سوی قانون‌گذار در فضای سایبر، درصد تولید جرایم و رویارویی مشتریان با خطرات احتمالی شده و عملیات حفاظت از دسترسی غیرمجاز به اطلاعات شخصی مشتریان و حتی بانک‌ها، در تمامی سطوح از خدمات‌رسانی صنعت بانکداری الکترونیکی را با دشواری مزمنی رو به رو ساخته است. صنعت بانکداری الکترونیکی، با وجود تمام ویژگی‌های مثبت و قابلیت‌های شگرف خود، در برابر تهدیدات و خطرات آسیب‌پذیر است. این نظام، در کنار جرایم سنتی، فرصت‌های جدیدی را در اختیار مجرمان قرار داده و موج جدیدی از جرایم نوظهور را، با عنوان جرایم سایبری[1]، به‌وجود آورده است (حبیب‌زاده و میرمجیدی هشجین، ۱۳۹۰، ص ۲۴). جرایم سایبری، جرایمی هستند که در فضای مجازی و هوشمندانه اینترنت ارتکاب یافته و مکمل جرایم رایانه‌ای قلمداد شده‌اند. این طیف از جرایم را می‌توان به دو بخش کلی تقسیم کرد: جرایمی که در آنها رایانه فقط ابزاری برای تولید محتوای مجرمانه مورد استفاده کاربران متخلف قرار می‌گیرد[2]؛ و جرایمی که در فضای سایبر با محتوای داده‌های رایانه‌ای در ارتباط هستند[3] (حبیب‌زاده، ۱۳۹۳، ص ۵). در تقسیم‌بندی دیگری، جرایم سایبری به چهار گروه کلی تقسیم شده‌اند (رضوی، ۱۳۸۶، ص ۱۲۳): ۱) اینترنت به عنوان ابزاری برای ارتکاب جرایم سنتی مورد استفاده کاربران مجرم فضای سایبر قرار می‌گیرد و ماهیتاً موضوعیت ندارد. برای مثال، کلاهبرداری اینترنتی، از حساب کاربران محقق می‌شود. ۲) جرایمی که علیه محرمانگی داده‌ها

1. Cyber-Crimes
2. Computer-related crimes
3. Content-related crimes

صورت می‌گیرند. برای نمونه، دسترسی غیرمجاز به یک داده محتوا، در این دسته جای می‌گیرد. ۳) جرایم علیه صحت و تمامیت داده‌ها، رتبه سوم از این تقسیم‌بندی را از آن خود کرده است. برای مثال، می‌توان به ممانعت از دستیابی اشخاص مجاز، به داده‌ها با تغییر رمز ورود اشاره کرد و ۴) جرایمی مانند انتشار محتویات غیراخلاقی یا انتشار فحشای سایبری که با محتوای داده‌ها عجین هستند. برای پیشگیری از تولید جرایم سایبری در حوزه بانکداری الکترونیکی، امنیت باید در چهار بخش اعم از، اتصالات ارتباطی، رایانه‌ها، پایانه‌ها و کارت‌های بانکی که مؤلفه‌های اصلی تراکنش در نظام بانکداری الکترونیکی هستند، رعایت و تضمین شود. از یک سو، برای برقراری امنیت در محیط سایبر، این اقدامات انجام می‌گیرند: ۱) دشوار ساختن ارتکاب جرایم سایبری، برای مجرمان بالقوه، از رهگذر ایجاد موانع به منظور محدود کردن فعالیت مجرمانه آنها؛ و ۲) دشوار ساختن ارتکاب جرم، با آگاه سازی کاربران این محیط، که همان بزه‌دیدگان بالقوه هستند (خانعلی پور واجارگاه، ۱۳۹۰، ص ۱۲۳)؛ از سوی دیگر، مقنن با جرم‌انگاری جرایم سایبری و پیش‌بینی ضمانت اجرای کیفری برای این دسته از تخلفات، سعی دارد تا به پیشگیری از وقوع این جرایم کمک کند.

جرم‌انگاری جرایم سایبری: برای درک مفهوم جرایم سایبر، درک تعریف سایبر و ویژگی‌های آن ضروری است. در تعریف فضای سایبر می‌توان گفت محیطی اجتماعی و غیرملموس است که در کنار فضای واقعی همواره در حال پیشرفت و فراگیری جهانی است (جهانگرد و رشیدی، ۱۳۸۴، ص ۲۴). از ویژگی‌های مهم این فضا می‌توان به ناشناختگی، سرعت، جهانی بودن، کم هزینه بودن و قابل دسترس بودن اشاره کرد. این ویژگی‌های فضای سایبر سبب گرایش همگان به این فضا و استفاده از آن، جهت پیشبرد اهداف ملت‌ها شده است. جهانی بودن فضای سایبر موجب شده تا هر فردی در هر نقطه جغرافیایی، به روزآمدترین اطلاعات دست پیدا کند (قاجار قیونلو، ۱۳۹۱، ص ۲۱۲). همچنین سرعت و قابل دسترس بودن فضای سایبر سبب دسترسی آسان به اطلاعات مورد نیاز شده است. به شکلی که هر فرد در هر نقطه از جهان و در هر زمان در چند ثانیه به جمع آوری و تبادل اطلاعات می‌پردازد (فضلی، ۱۳۸۹، ص ۷۲). با توجه به ویژگی‌های یادشده افراد برای مقاصد مختلف از فضای سایبر بهره می‌برند. سرعت و در دسترس بودن فضای سایبر در بانکداری نیز مورد توجه قرار گرفته است. با این

وجود عده‌ای در پیشبرد مقاصد سوء همچون کلاهبرداری، سرقت الکترونیکی و دیگر جرایم بانکداری الکترونیکی از این فضای منحصر به فرد استفاده می‌کنند.

با تغییر جامعه و پیشرفت آن، شکل جرایم نیز تغییر می‌کند. در گذشته که فضای سایبر وارد زندگی بشریت نشده بود، جرایم مالی تنها به شکل سنتی ارتکاب می‌یافتند. امروزه با حضور فناوری‌های جدید و فضای سایبر در جامعه، فرصت‌های جدیدی برای ارتکاب جرم به‌وجود آمده است. بنابراین فناوری اطلاعات و وسایل ارتباطاتی، جرایم اطلاعاتی و ارتباطی را در پی دارد. منظور از جرایم جدید هم جرایم سنتی در اشکال جدید و هم جرایمی بدون سابقه است، که تنها در محیط رایانه‌ای امکان بروز دارد (پیران و محمودی، ۱۳۸۹، ص ۴۹). اینگونه از جرایم اغلب از سوی افراد آگاه به علوم رایانه‌ای ارتکاب می‌یابد که در اغلب موارد از روی تجربه و به شکل عمدی صورت می‌گیرد. بنابراین کمتر می‌توان کسانی که به علوم رایانه‌ای آگاه نیستند را در زمره این دسته از بزهکاران یافت (پیران و محمودی، ۱۳۸۹، ص ۴۹). همچنین برای ارتکاب جرایم سایبری به خصوص جرایم مربوط به بانکداری الکترونیکی به سخت‌افزارها و نرم‌افزارهای ویژه‌ای احتیاج است. در نتیجه می‌توان برای این نوع از جرایم وصف علمی و تخصصی بودن را به کار برد. در همین راستا قوانین متعددی در ایران برای برقراری امنیت و پیشگیری از جرایم بانکداری الکترونیکی، تصویب و اجرا شده است. در این زمینه، می‌توان به موارد پیش‌رو اشاره کرد: ۱) قانون تجارت الکترونیک (مصوب سال ۱۳۸۲)؛ ۲) مواد ۷۲۹، ۷۳۲، ۷۳۳ و ۷۳۹ قانون تعزیرات (قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸)؛ ۳) ماده ۷ قانون مبارزه با پول‌شویی (مصوب سال ۱۳۸۶)؛ ۴) بند ۱۲ ماده ۱۳ لایحهٔ قانونی ادارهٔ امور بانک‌ها (مصوب سال ۱۳۵۸)؛ و ۵) ماده ۱۳ قانون مبارزه با تأمین مالی تروریسم (مصوب سال ۱۳۹۴).

بنابراین هنگامی که بانک‌ها در راستای تأمین امنیت مشتریان اقدامات حفاظتی مناسب را لحاظ نکنند، امکان ارتکاب جرایم متعددی از جمله، دسترسی غیرمجاز به داده‌ها[1]،

---

۱. ماده ۷۲۹ قانون تعزیرات: «هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.

جعل رایانه‌ای[۱]، سرقت و کلاهبرداری رایانه‌ای[۲]، تخریب و اخلال در داده‌های رایانه‌ای و مخابراتی[۳]، جرایم موضوع ماده ۷۵۳ قانون تعزیرات[۴]، تروریسم و تأمین مالی آن[۵]، جرایم کارکنان

---

۱. ماده ۷۳۴ قانون تعزیرات: «هرکس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد: الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانهٔ داده به آنها. ب) تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا واردکردن متقلبانهٔ داده‌ها یا علائم به آنها.»

۲. ماده ۷۴۰ قانون تعزیرات: «هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.» و ماده ۷۴۱ قانون تعزیرات: «هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.»

۳. ماده ۷۳۶ قانون تعزیرات: «هرکس به‌طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.»، ماده ۷۳۷ قانون تعزیررات:« هر کس به‌طور غیرمجاز با اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.» و ماده ۷۳۸ قانون تعزیرات:« هرکس به‌طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذر واژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.»

۴. ماده ۷۵۳ قانون تعزیرات: «هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد: الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معاملهٔ داده‌ها یا نرم افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌رود. ب) فروش یا انتشار یا در دسترس قراردادن گذر واژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند. ج) انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. تبصره ـ چنانچه مرتکب، اعمال یادشده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.»

۵. ماده ۷۵۴ قانون تعزیرات: «در موارد زیر، حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد: الف) هر یک از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها و یا شهرداری‌ها و مؤسسه‌ها و شرکت‌های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به‌طور کلی اعضاء و کارکنان قوای سه گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند. ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد. ج) داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات عمومی باشد. د) جرم به صورت سازمان یافته ارتکاب یافته باشد. ه) جرم در سطح گسترده‌ای ارتکاب یافته باشد.»

بانک‌ها[1]، پولشویی و ساخت پایگاه‌های جعلی برای پرداخت‌های بانکی، فراهم خواهد شد. همچنین به نظر می‌رسد در این میان تولید مفاهیم نوظهوری چون بلاک‌چین، قراردادهای هوشمند و ارز دیجیتالی نیز جهان و به‌ویژه صنعت بانکداری را با شوک و بحران مواجه ساخته است. بلاک‌چین یک فناوری ویژه برای پلتفرم‌های معامله‌گر همتا به همتا است، که از ذخیره‌سازی غیرمتمرکز برای ضبط تمام داده‌ها اعم از مالی و غیرمالی استفاده می‌کند. به عبارتی بلاک‌چین دارای شناسه منحصر به فردی[2] است، که با مواردی مانند امضای دیجیتال[3] برای هر دارنده‌ای شناسایی می‌شود و به مانند یک حساب کاربری عمل می‌کند (ارزانیان، ۱۳۹۶، ص ۲). به عبارت بهتر، فناوری بلاک‌چین دفترعمومی تمام معاملات و تراکنش‌های ارزهای دیجیتالی مانند بیت کوین است، که تاکنون انجام شده است و همواره تراکنش‌های جدید نیز به آن افزوده می شود (ارزانیان، ۱۳۹۶، ص ۳). اعضای شبکه بلاک‌چین، فقط از گذر الگوریتم‌های ریاضی و محاسبات نسبتاً پیچیده، به واسطه راستی آزمایی در بلوک‌ها، اطلاعات مندرجه را تأیید یا رد می‌کنند (نارایانان و بونی‌آو ومیلر[4]، ۲۰۱۶، ص ۲۳). سال‌هاست که از نظریهٔ دهکده جهانی می‌گذرد، جهان در جهت همین مفهوم حرکت کرده و ارتباطات فیزیکی و تعامل انسان با انسان جای خود را به تعامل نماینده‌های الکترونیکی داده است. به نظر می‌رسد با به رسمیت شناختن و مشروعیت بخشی به فناوری جدیدی چون بلاک‌چین بدون هیچ بسترسازی مطمئن و ایمنی، کشورها و نظام حاکمیتی آن‌ها را با بی‌نظمی عجیبی رو به رو می‌سازد. به‌طور مثال حریم خصوصی افراد با خطرات و تهدیدات بسیاری مواجه شده و چه بسا پابرجا نماند. اگر فناوری نوظهور در راستای تخریب داده‌ها و نفوذ دشمنان در فضای سایبری جمهوری اسلامی ایران و ازبین

---

۱. ماده ۱۳ قانون مبارزه با تأمین مالی تروریسم: «تمامی اشخاص و نهادها و دستگاه‌های مشمول قانون مبارزه با پولشویی مصوب ۱۳۸۶/۱۱/۱ موظفند به منظور پیشگیری از تأمین مالی تروریسم اقدامات زیر را انجام دهند: الف) شناسایی مراجعان هنگام ارائه تمام خدمات و انجام عملیات پولی و مالی از قبیل انجام هرگونه دریافت و پرداخت، حواله وجه، صدور و پرداخت چک، ارائه تسهیلات، صدور انواع کارت دریافت و پرداخت، صدور ضمانت‌نامه، خرید و فروش ارز و اوراق گواهی سپرده، اوراق مشارکت، قبول ضمانت و تعهد ضامنان به هر شکل از قبیل امضای سفته، برات و اعتبارات اسنادی و خرید و فروش سهام؛ ب) نگهداری مدارک مربوط به سوابق معاملات و عملیات مالی اعم از فعال و غیرفعال و نیز مدارک مربوط به سوابق شناسایی مراجعان، حداقل به مدت پنج سال بعد از پایان عملیات.»

2. IP

3. Electronic signature

4. Narayanan & Bonneau & Miller.

بردن امنیت، آرامش و اقتدار مرزی کشور همراه باشد، نه تنها ابزاری برای تسریع و سهولت در عملیات و فعالیت‌های مختلف نخواهد بود، بلکه خانمان‌سوز است. مسلم است که هر فناوری جدیدی علاوه بر مؤلفه‌های تقنینی و جرم‌انگاری در مواجهه با تهدیدات و خطرات، نیازمند افزایش دانش و آگاهی‌های فرهنگی جامعه خواهد بود. بنابراین نمی‌توان با چشمانی بسته مشروعیت‌یابی هر مفهومی در نظام تقنینی را دنبال کرد. باوجود اهمیت و ضرورت نقش قانون‌گذار در امنیت حوزهٔ بانکداری الکترونیکی و وضع قوانین متعدد در پیشگیری از جرایم الکترونیکی، تدابیر پیشگیرانه بانک‌ها در تأمین امنیت مشتریان، نقش مهمتر و کلیدی‌تری را ایفا می‌کنند.

روش‌شناسی

تحقیق حاضر به شیوه توصیفی تحلیلی انجام شده است و نگارش آن با تکیه بر نظرات حقوقی، داده‌ها و آموزه‌های علمی گردآوری شده از میان کتاب‌ها، مقالات، پایان‌نامه‌ها و پایگاه‌های اینترنتی صورت پذیرفته است. قوانین ایران و همچنین اسناد بین‌المللی موجود در حوزه جرایم سایبری و پیشگیری از جرم نیز از نظر دور نمانده است. همچنین، داده‌های پژوهش به شیوه کتابخانه‌ای گردآوری شده و نوع پژوهش کاربردی است.

یافته‌ها

پیشگیری از جرایم بانکداری الکترونیکی: پیشگیری از جرم، نه تنها مفهوم شناخته‌شده‌ای در علم جرم‌شناسی است، بلکه از سوی سیاستگذاران و مدیران نیز به عنوان یک تدبیر ضروری برای برقراری نظم، مورد توجه قرار گرفته است. از این رو، یکی از راه‌های تأمین امنیت و نظم در جوامع، استفاده از تدابیر پیشگیرانه است. در مفهوم موسع پیشگیری، به هر اقدامی که پیش از تولید جرم اتخاذ شود، علیه جرم بوده و آن را کاهش دهد، اطلاق خواهد شد. به بیانی دیگر، به مجموعه اقدامات سیاست جنایی، که هدف آنها، محدود کردن امکان وقوع، مجموعه‌ای از جرایم باشد، پیشگیری از جرم می‌گویند (نجفی ابرندآبادی، ۱۳۹۲، ص ۵۰۴). بنابراین هر چیزی که در مبارزه با بزهکاری کارآمد باشد، در قلمرو پیشگیری در مفهوم موسع آن قرار می‌گیرد.

گونه‌های پیشگیری از جرم: پیشگیری از جرم، براساس معیارهای مختلفی قابلیت تقسیم‌بندی دارد. در یک بخش‌بندی کلی، پیشگیری به «کیفری» و «غیرکیفری» تقسیم شده است. پیشگیری در درون نظام عدالت کیفری، شامل همان اقدامات و سیاست‌های مبتنی بر بازپروری و بازدارندگی سنتی است که در چارچوب قانون و به‌وسیلهٔ عوامل نظام عدالت کیفری به اجرا در می‌آیند (سی. ولش و پی. فارینگتون، ۱۳۹۴، ص ۳۰). پیشگیری از جرم در بُعد غیرکیفری، مجموعه‌ای از اقدامات غیر سرکوبگر است که خود به سه نوع «پیشگیری اجتماعی»[1]، «پیشگیری وضعی»[2] و «پیشگیری فنّی»[3] بخش می‌شود.

پیشگیری اجتماعی: پیشگیری اجتماعی، معطوف به علت‌شناسی یا واکاوی علل، عوامل بنیادین وقوع جـرم و شرایط اجتماعی جرم‌زا اسـت (نجفی توانا و شاطری‌پور اصفهانی، ۱۳۹۱، ص ۵۹). این نوع پیشگیری، علت وقوع جرم را در محیط اجتماعی عمومی- مانند نظام اقتصادی، سیاسی یا فرهنگی یک کشور- و محیط اجتماعی شخصی- مانند زیست بوم، خانواده، محل تحصیل یا محیط شغلی- افراد، جستجو می‌کند. به باور برخی، پیشگیری اجتماعی تغییرهایی اصلاح‌گرانه در محیط اجتماعی است که زمینـه‌هـای جلـوگیری از وقوع جـرم را تـا حـدود زیـادی بـه‌صورت پایدار و همیشگی فراهم می‌کند (اصغری و سرمدی واله، ۱۳۹۱، ص ۱۴۴). حکومت با اتخاذ تدابیر پیشگیرانهٔ اجتماعی، در تلاش است تا بسترهای مناسبی را برای نهادینه‌سازی هنجارهای صحیح فراهم سازد و شهروندان خود را از عوامل و شرایط جرم‌زا دور کند. در واقع پیشگیری اجتماعی فردمدار به‌دنبال اقداماتی است که در انواع محیط‌های فردی تأثیر گذارد و در نهایت طی فرآیند جامعه پذیری و اجتماعی شدن، عملکرد مثبتی از خود نشان دهد (علمداری، ۱۳۸۹، ص ۷۸). یکی از روش‌های پیشگیری اجتماعی این‌گونه است که با تکیه بر ظرفیت محیط‌ها، به خصوص محیط‌های اطراف افراد در پی پیشگیری از ارتکاب جرم است. این نوع پیشگیری با استفاده از اقدامات غیرقهرآمیز اجتماعی، فرهنگی و اقتصادی در محیط‌های مختلف در صدد از بین بردن

1. Social Prevention
2. Situational Prevention
3. Technical prevention

عوامل محیطی جرم‌زا و یا کاهش تأثیر آن بر افراد است (نجفی ابرندآبادی، ۱۳۸۳، ص ۵۷۰). به عنوان مثال با ایجاد اشتغال و از بین بردن زمینه‌های فقر مالی و فرهنگی می‌توان از ارتکاب بسیاری از جرایم مالی در حوزه بانکداری الکترونیکی مانع شد. بدین نحو که انگیزه‌های مالی و حتی انتقام‌جویانه که افراد به دلیل فقر نسبت به جامعه دارند، تا حد زیادی از بین برود.

پیشگیری وضعی: پیشگیری وضعی گونه‌ای از پیشگیری در جرم‌شناسی است که مبنای آن وضعیت پیش از بزهکاری است. این نوع از پیشگیری به‌دنبال تغییر وضعیت مشرف به جرم است تا معادله جرم به ضرر مجرم باشد. در واقع می‌خواهد با اقداماتی فرآیند گذار از اندیشه به عمل را قطع کند. لازم به توضیح است هنگامی که مجرم به این نتیجه برسد که اقدام به ارتکاب جرم ضرری بسیار بالاتر از ترک ارتکاب آن دارد، اندیشهٔ ارتکاب را به عمل نمی‌رساند. (نجفی ابرندآبادی، ۱۳۹۱، ص ۵۰۹). این پیشگیری در پی کاهش یا نامساعد جلوه دادن وضعیت‌های پیش‌جنایی است. این نوع پیشگیری بدون توجه به فرآیند شکل‌گیری شخصیت افراد و تنها با تمرکز بر فرصت‌ها درصدد مدیریت اوضاع و احوال پیش از ارتکاب بزهکاری است (صفاری، ۱۳۸۰، ص ۲۹۲). در واقع هدف از آن ایجاد تغییرات در اوضاع و احوال خاصی است که انسان متعارف در آن ممکن است مرتکب جرم شود. ایجاد تغییر در مراحل ارتکاب جرم یعنی جاذبه‌زدایی از آماج جرم و سخت کردن ارتکاب آن است (نجفی ابرندآبادی، ۱۳۹۱، ص ۷۹۳). پیشگیری وضعی به‌دنبال استفاده از ابزارها و معیارهای غیرکیفری برای جلوگیری از گذار مرتکب از اندیشهٔ مجرمانه به فعل مجرمانه است. این امر، به کمک ایجاد تغییر در شرایط و اوضاع و احوال خاصی که در طی آن جرم به‌وجود می‌آید، میسر می‌شود. هدف از این نوع پیشگیری، کاهش فرصت‌های ارتکاب جرم و سوء استفادهٔ بزهکاران از شرایط خاص برای ارتکاب جرم است. در این بُعد از پیشگیری، سیاست پیشگیرانه مبتنی بر کنترل افراد است و حکومت به جای اصلاح، سازوکارهای خود، به کنترل افراد روی می‌آورد (بارانی و افراسیابی، ۱۳۹۱، ص ۷۰۰). پیشگیری وضعی، به دلیل هزینهٔ کمتر و همچنین کنترل، اثربخشی سریع و سهولت بیشتری که در ممانعت از وقوع جرایم دارد، همواره با استقبال بیشتری از سوی دولت‌ها مواجه بوده است.

پیشگیری فنّی: در عصر اینترنت دوم و هوشمندی اشیاء، پیشگیری وضعی برای کارآیی خود از

فناوری‌های نوینی همچون فناوری اطلاعات و ارتباطات -که جایگزین بسیاری از ابزارهای سنتی پیشگیری از جرم شده‌اند-، استفاده می‌کند. به این نوع پیشگیری، پیشگیری فنی از جرم گویند. پیشگیری فنی، هزینه بر است اما، وجود آن در جوامعی که بزهکاران آنها روزآمد شده و با سوء استفاده از پیشرفت علم و فناوری، گونه‌های جدیدی از جرایم را ابداع کرده‌اند، امری حیاتی به نظر می‌رسد. احساس ناامنی در بین مشتریان به ضرر بانک‌ها بوده و منجر به ایجاد خسارات جبران‌ناپذیری می‌شود. از این رو، بانک‌هایی که با سیستم بانکداری الکترونیکی اداره می‌شوند، در راستای تأمین امنیت مشتریان خود، نیازمند اتخاذ اقدامات پیشگیرانه هستند. تدابیر پیشگیرانه فنی، بی‌شک بهترین نوع تدابیر و درخور اهمیتی شایان در این زمینه خواهد بود.

بحث و نتیجه‌گیری

افزایش اختراعات جدید و گسترش فناوری‌های نوین به‌ویژه در زمینهٔ صنعت بانکداری، باعث شده است رویه‌های تقنینی و عملی پیشگیری از جرایم نیز، به سمت تدابیر پیشگیرانهٔ فنی گرایش پیدا کنند. از آنجا که تلاقی سیاست‌های پیشگیرانه با فناوری اطلاعات و ارتباطات امری اجتناب‌ناپذیر است، دولت‌ها و سازمان‌های درگیر با جرایم الکترونیکی از جمله بانک‌ها، بیش از پیش، از تدابیر فنی الکترونیکی برای مصون سازی آماج بالقوهٔ جرم بهره می‌برند. در عصر هوشمندی اشیاء، هیچ چیز فارغ از این فناوری نیست. به علاوه، ماهیت محیط سایبر که بانکداری الکترونیکی در بستر آن فرصت بروز می‌یابد به گونه‌ای است که بانک‌ها را ناگزیر از اتخاذ تدابیر پیشگیرانهٔ فنی می‌سازد. همان‌طور که پیشتر گفته شد، ترس از جرم، ساختار جامعه و اجتماع را بر هم می‌زند و ناامنی، منجر به ایجاد شرایطی می‌شود که آن شرایط، سبب تحقق جرایم و از بین رفتن آرامش اشخاص می‌شوند. بنابراین، اتخاذ تدابیر پیشگیرانه وضعی و فنی از سوی بانک‌ها، می‌تواند منجر به تأمین امنیت مشتریان و آسودگی خاطر تجار در انجام داد و ستدهای الکترونیکی شود. هرچند، به‌کارگیری بعضی از اقدامات و تدابیر پیشگیرانه، مانند سیستم و نرم‌افزارهای نظارتی، ناقض برخی از حقوق شهروندان و حمایت از حریم خصوصی آنان است اما این امر، به دلیل حفظ امنیت مشتریان و حمایت از آنان، قابل توجیه است.

در حال حاضر، بانکداری الکترونیکی با مشکلات زیادی مواجه است؛ از میان این مشکلات می‌توان به مواردی مانند؛ شناسایی ناکافی و دقیق مشتریان و صاحبان حساب الکترونیکی، حملات سایبری و نفوذ به سیستم‌های بانکی توسط هکرها، ناتوانی بانک‌ها در حفظ اطلاعات مشتریان، مدیریت اطلاعات و حساب‌ها، اشتباه در محاسبات، ویروسی شدن سیستم‌ها و مشکلات در پرداخت‌های الکترونیکی، اختلال در سیستم‌های الکترونیکی بانک‌ها و قطع شدن خدمات آنلاین اشاره کرد. ازاین‌رو بانک‌ها باید در مرحله اول، برنامه‌ریزی دقیق و از پیش تعیین شده داشته باشند. خدمات نظام بانکداری الکترونیکی، باید همگام و سازگار با راهبرد مالی بانک‌ها باشد. بانک‌ها باید فهرستی از تمام احتیاجات امنیتی لازم برای ایجاد یک محیط امن برای نظام بانکداری الکترونیکی، تهیه کنند. بانک باید راهبردهایی برای دست‌یابی به مواردی مانند شناسایی و احراز هویت تمام مشتریان و صاحبان حساب‌های الکترونیکی، ایجاد و تقویت مدیریت بحران در رویارویی با حوادث، خطرات مختلف و به‌کارگیری نیروهای متخصص و خبره در این بخش، استفاده از رسانه‌ها برای افزایش آگاهی مردم و جذب مشتریان، ارائه اطلاعات کامل دربارهٔ فراهم‌سازی خدمات و سرویس‌دهی به مشتریان برای آسودگی خاطر آنها و همچنین، رعایت قوانین وضع شده و استانداردها بیابد. امروزه، تلاش برای حفظ و صیانت از اطلاعات شخصی مشتریان و جلوگیری از رویت غیرمجاز، استفاده از روزآمدترین نرم‌افزارها و آنتی ویروس‌های قوی در سیستم‌ها برای جلوگیری از نفوذ هکرها، اهمیت دادن به انتقادات و پیشنهادات مشتریان و استفاده از نظرات آنها، استفاده از شبکه‌های مجازیِ کاوشگرهای الکترونیک[۱]، بازرسی‌های مداوم خودکار رایانه‌ای و استفاده از نرم‌افزار دیوار آتشین[۲]، از ضروری‌ترین لوازم بانکداری الکترونیکی است. افزون بر این موارد عصر هوشمندی اشیاء و هوش مصنوعی، فناوری‌های نوظهوری چون بلاک‌چین و ارز دیجیتالی را به ارمغان آورده است، که پیشتر

---

۱. کاوشگرهای الکترونیک، که به آنها پلیس مجازی نیز می‌گویند، وظیفه احراز هویت‌های مجازی، اعتبارسنجی امضاهای الکترونیکی در فضای سایبر، کنترل دسترسی‌های مجاز به محتوای محرمانه داده‌ها و در مواردی تشخیص مصادیق محرمانه منتشر شده را بر عهده دارند (بهره‌مند و همکاران، ۱۳۹۳، ص ۱۵۷).

۲. استفاده از نرم‌افزار دیوار آتشین، یکی از بهترین روش‌های پیشگیری فنی است. دیوار آتشین، یک سیستم کاملاً حفاظتی است که جریان ترافیک ورودی به شبکه، و در مواردی میان آنها، را کنترل و نظارت می‌کند. وظیفه اصلی این نرم‌افزار، جلوگیری از دسترسی غیرمجاز کاربران خاص به منابع شبکه است.

در ارتباط با تهدیدات و خطراتی احتمالی آن مطالبی بیان شده است.

بنابراین به نظر می‌رسد با روی کارآمدن فناوری بلاک‌چین در نظام بانکداری الکترونیکی، بسترهای جرایم متنوعی چون جعل داده‌ها، سرقت کیف پول دیجیتالی اشخاص، نامشخص بودن هویت کاربران بلاک‌چین گسترانیده شده و این مهم برعهده نظام تقنینی جمهوری اسلامی ایران است، که با بهره‌گیری از جامعه نخبگان و پژوهشگران این حوزه، راهکار مواجه شدن صنایع مختلف به‌ویژه صنعت بانکداری را از پیش، با برنامه‌ای همه‌جانبه و مدون ارائه کنند. همچنین به نظر می‌آید که صنعتی که با خطرات احتمالی فناوری نوظهور بلاک‌چین بیشتر رو به رو خواهد بود، صنعت بانکداری است، زیرا کلیدی‌ترین فرآورده این بستر ناشناخته، ارزهای دیجیتال هستند که ماهیتی مجازی داشته و غایت آن تغییر ذائقهٔ مردم و سوق آنها به سوی داد و ستد در فضای سایبر است. بنابراین بانکداری الکترونیکی باید با توسل به راهبردهای پیشگیرانه از وقوع جرایم سایبری مرتبط با بانکداری جلوگیری کند. در این راستا پیشنهادهای زیر ارائه می‌شود:

- استفاده از رمزنگاری و کلمات عبور یکبار مصرف در سیستم بانکداری الکترونیکی؛
- تهیه توکن‌های امنیتی[1] و استفاده از امضای الکترونیکی؛
- تشکیل کمیته‌های بررسی تخصصی فناوری بلاک‌چین بستر ارزهای دیجیتال توسط نهادهای مرتبط و تدوین برنامه‌ای مدون و پیشگیرانه برای بهبود شرایط فعلی نظام بانکداری و مراقبت‌های لازم برای برقراری امنیت کاربران و پیشگیری همه‌جانبه از تولید جرایم متنوع در حوزهٔ فناوری نوین زنجیره‌های بلوکی یا بلاک‌چین.
- نظارت مداوم و نامحسوس بر کارمندان بانک‌ها و
- تشکیل جلسات مداوم میان مسئولان و کارمندان برای شناسایی نقاط ضعف سیستم و تصمیم‌گیری بهتر در حوزهٔ بانکداری الکترونیکی.

---

۱. توکِن امنیتی (Security Token)، یک سخت‌افزار کوچک است که برای تشخیص هویت کاربران مجاز از سوی سیستم رایانه، در اختیار کاربران قرار می‌گیرد.

فهرست منابع

ارزانیان، نسترن. (۱۳۹۶). *ماهیت بلاک‌چین‌ها با تأکید بر نظام مالیاتی و رگولاتوری در حقوق ایران*، اولین کنگره مقاله نویسی و همایش رگولاتوری بلاک‌چین و رمزارزها، ص ۱-۱۳. قابل بازیابی از: http://regublock.ir

اصغری، عبدالرضا، سرمدی واله، علی. (۱۳۹۱). پیشگیری اجتماعی از جرم در قانون برنامه پنجم توسعه، *آموزه‌های حقوق کیفری، شماره ۴*، صص ۱۴۳-۱۶۶. قابل بازیابی از:
https://www.sid.ir/fa/journal/JournalListPaper.aspx?ID=43058

بارانی، محمد و افراسیابی، علی. (۱۳۹۲). *پیشگیری وضعی از جرم به عنوان رهیافتی معارض یا تعامل‌گر با آموزه‌های حقوق بشر در: دایرةالمعارف علوم جنایی*، زیر نظر: علی‌حسین نجفی ابرندآبادی. چاپ اول، تهران: نشر میزان.

بهره‌مند، حمید، محمدکوره‌پز، حسین و سلیمی، احسان. (۱۳۹۳). راهبردهای وضعی پیشگیری از جرایم سایبری. *آموزه‌های حقوق کیفری، شماره ۷*، صص ۱۴۷-۱۷۶. قابل بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=241594

پیران، صدیقه و محمودی، انسیه. (۱۳۸۹). جرایم سایبر، *مجله مطالعات رسانه‌ای، سال پنجم، شماره ۸*، صص ۷۸-۴۳. قابل بازیابی از: https://www.sid.ir/fa/journal/JournalListPaper.aspx?ID=48865

جلالی فراهانی، امیرحسین و باقری‌اصل، رضا. (۱۳۸۷). پیشگیری از جرایم سایبری راهکاری اصلی برای نهادینه‌سازی *اخلاق سایبری، شماره ۲۴*، صص ۱۰-۱۹. قابل بازیابی از:
https://www.noormags.ir/view/fa/articlepage/29134/10

جهانگرد، نصرالله و رشیدی کمیجان، علیرضا. (۱۳۸۴). *ایجاد توسعهٔ پویا (گزارش نهایی مؤسسه فرصت‌های دیجیتال)*. دبیرخانه شورای عالی اطلاع رسانی. قابل بازیابی از:
www.jgeoqeshm.ir/?_action=export&rf=idc&issue=5084

حاجی ده‌آبادی، محمدعلی. (۱۳۹۴). *جامعه‌شناسی جنایی*. چاپ اول، قم: مرکز بین‌المللی ترجمه و نشر المصطفی.

حبیب‌زاده، طاهر. (۱۳۹۰). *حقوق فناوری اطلاعات مقدمه‌ای بر حقوق تجارت الکترونیک*، جلد اول، چاپ اول، تهران، مرکز پژوهش‌های مجلس شورای اسلامی.

حبیب‌زاده، طاهر. (۱۳۹۳). *نگاهی آکادمیک به رشته حقوق فناوری اطلاعات*، در: وب‌سایت شخصی دکتر طاهر حبیب‌زاده، http://drhabibzadeh.com/pages-56.html، تاریخ بازدید: ۱۳۹۷/۱/۱۷.

حبیب‌زاده، محمدجعفر، میرمجیدی هشجین، سیده سپیده. (۱۳۹۰). نقش بانکداری الکترونیکی در پولشویی و روش‌های مقابله با آن. *پژوهش‌های حقوق تطبیقی، دوره ۱۵، شماره ۱ (۷۱)*، صص ۲۳-۴۲. قابل بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=205569

حسین‌زاده شهری، معصومه، قدک فروشان، مریم. (۱۳۹۱). اولویت‌بندی ریسک‌های بانکداری الکترونیکی از دیدگاه مدیران بانک‌های دولتی و خصوصی، *پژوهش‌های مدیریت منابع سازمانی، دوره ۲، شماره ۴*، صص ۴۵-۶۳. قابل بازیابی از:
https://elmnet.ir/article/1109399-2351/

خانعلی پور واجارگاه، سکینه. (۱۳۹۰). *پیشگیری فنی از جرم*، چاپ اول، تهران، میزان.

رضوی، محمد. (۱۳۸۶). جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها. *دانش انتظامی، دوره ۹، شماره ۱*، صص ۱۲۰-۱۴۰. قابل بازیابی از: https://www.sid.ir/fa/journal/ViewPaper.aspx?id=74998

سی.ولش، براندون، پی.فارینگتون، دیوید. (۱۳۹۴). *پیشگیری از جرم و سیاست عمومی*. (گروهی از پژوهشگران حقوق کیفری و جرم‌شناسی، مترجمان). در: دانشنامهٔ پیشگیری از جرم آکسفورد. چاپ اول، تهران: نشر میزان.

صفاری، علی. (۱۳۸۰). مبانی نظری پیشگیری وضعی، مجله *تحقیقات حقوقی، شماره ۳۳*. قابل بازیابی از:

https://www.sid.ir/fa/journal/ViewPaper.aspx?ID=231912

صنایعی، علی، شاهین، آرش و سلیمیان، حمید. (۱۳۹۲). تحلیل عوامل مؤثر بر پذیرش بانک مجازی به عنوان نسل جدید بانکداری الکترونیک با مطالعه موردی بر شهروندان الکترونیک. *تحقیقات بازاریابی نوین، سال ۳، شماره ۳* (پیاپی ۱۰)، صص ۱-۲۰. قابل بازیابی از: http://ensani.ir/fa/article/327610

طاهری، سمانه. (۱۳۹۲). *سیاست کیفری سخت گیرانه*، چاپ اول، تهران: میزان.

علمداری، علی. (۱۳۸۹). پیشگیری از جرایم سایبری. *مجله مطالعات بین‌المللی پلیس، شماره ۲*، صص ۷۳-۹۱. قابل بازیابی از:http://interpol.jrl.police.ir/content.php

عمید، حسن. (۱۳۸۶). *فرهنگ عمید*، تهران: امیرکبیر.

فضلی، مهدی. (۱۳۸۹). *مسئولیت کیفری در فضای سایبر*. چاپ اول. تهران: انتشارات خرسندی.

فلاح‌تفتی، آتنا. (۱۳۹۰). *بررسی اهمیت ابعاد کیفیت خدمات در بانکداری سنتی و الکترونیک*. پایان‌نامه کارشناسی ارشد دانشگاه یزد.

قاجارقیونلو، سیامک. (۱۳۹۱). *مقدمه حقوق سایبر*. چاپ اول. تهران: انتشارات میزان.

کشته‌گر، محمد. (۱۳۹۰). *بانکداری الکترونیک*. تهران: مؤسسه عالی بانکداری ایران.

گسن، موریس. (۱۳۸۵). *اصول جرم‌شناسی*. (میر روح الله صدیق، مترجم). چاپ اول. تهران: دادگستر.

مشرف‌جوادی، محمدحسین، بهزادفر، فاطمه و قوچی‌فرد، حمزه. (۱۳۸۹). بانکداری الکترونیکی و چارچوب امنیتی آن. *بانک و اقتصاد، شماره ۱۱۲*، صص ۲۴-۲۷. قابل بازیابی از:
https://www.sid.ir/Fa/Journal/ViewPaper.aspx?ID=108985

نجفی ابرندآبادی، علی‌حسین. (۱۳۸۳). *پیشگیری عادلانه از جرم در علوم جنایی*: مجموعه مقالات در تجلیل از استاد محمد آشوری، چاپ نخست، تهران: سمت.

نجفی ابرندآبادی، علی‌حسین. (۱۳۹۱). *تقریرات درس جامعه‌شناسی جنایی*. (مهدی صبوری‌پور، گردآورنده). دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی.

نجفی ابرندآبادی، علی‌حسین. (۱۳۹۲). *تقریرات درس جرم‌شناسی* (از جرم‌شناسی انتقادی تا جرم‌شناسی امنیتی. (سکینه خانعلی‌پور واجارگاه و مهدی قربانی، گردآورنده). دوره دکتری حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی.

نجفی‌توانا، علی و شاطری‌پوراصفهانی، شهید. (۱۳۹۱). پیشگیری اجتماعی از جرم در پرتو تحولات ناشی از جهانی‌شدن فرهنگ. *آموزه‌های حقوق کیفری، شماره ۴*، صص ۸۵-۱۰۸. قابل بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?ID=187335

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Shah Mahmood & Clarke, Steve. (2009). *E-Banking Management*: Issues, Solutions, and Strategies, New York: Information Science Reference.

33. Vij Jyoti & Kavita Vij &Vinod Vij. (2014). *Role of E- Banking in Current Scenario*. International Journal of Technical Research and Applications e-ISSN: 2320-8163, Volume 2. Retrieved from: https://www.ijtra.com/view/role-of-e-banking-in-current-scenario.pdf