

محدودیت‌های نظام حقوقی ایران در حمایت از داده‌های شخصی بانکداری برخط؛ مطالعه تطبیقی با الزامات پاسخگویی در مقررات عمومی حفاظت از داده اتحادیه اروپا

ایمان خورشیدوند^۱

تاریخ دریافت: ۱۴۰۴/۱۰/۰۱ تاریخ چاپ: ۱۴۰۵/۰۳/۲۸

چکیده

بانکداری برخط، به‌عنوان یکی از نوآوری‌های مهم در نظام‌های مالی، حجم گسترده‌ای از داده‌های شخصی حساس مشتریان را پردازش می‌کند. محافظت حقوقی از این داده‌ها به دلیل پیچیدگی‌های فناورانه و حقوقی، یکی از دغدغه‌های اساسی محسوب می‌شود. مقاله حاضر با رویکردی تطبیقی چارچوب‌های حقوقی ایران و اتحادیه اروپا (مقررات عمومی حفاظت از داده‌ها - GDPR) را بررسی می‌کند و اصول حاکم بر پردازش داده‌ها، چالش‌ها و خلاءهای قانونی موجود در نظام بانکی ایران را تحلیل می‌کند. همچنین ضمانت‌های اجرایی نقض داده‌های شخصی با تأکید بر رویکرد دو نظام حقوقی مورد بررسی قرار گرفته است. نتایج نشان می‌دهد که ضعف در ساختار قانونی و لزوم تقویت ضمانت اجرای مؤثر، مهم‌ترین موانع حمایت کارآمد از داده‌ها است و توصیه‌هایی برای ارتقاء سیاست‌ها و قوانین مطرح شده است.

واژگان کلیدی

بانکداری برخط، داده‌های شخصی، حمایت حقوقی، مقررات عمومی حفاظت از داده، مسئولیت مدنی

۱. کارشناسی ارشد، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران. iman1995khorshidvand@gmail.com

۱. مقدمه

تحول دیجیتال در نظام بانکی جهان و ایران موجب تغییرات بنیادین در ارائه خدمات مالی شده است. بانکداری برخط به صورت گسترده، آستانه بسیار وسیعی از اطلاعات شخصی مشتریان را در بسترهای فناوری اطلاعات و ارتباطات پردازش می‌کند. از این‌رو، حفظ محرمانگی، امنیت و حقوق شهروندان مرتبط با داده‌های شخصی بسیار حیاتی است. در ایران علی‌رغم تلاش‌هایی برای تصویب قوانین حمایت از داده‌ها، خلأهای قانونی و اجرایی به چشم می‌خورد که می‌تواند به نقض حقوق مشتریان و آسیب‌پذیری نظام بانکی در برابر تهدیدات سایبری می‌انجامد. در مقایسه، اتحادیه اروپا با تصویب GDPR چارچوبی جامع و همه‌جانبه ایجاد کرده که الگوی مناسبی برای ایران به حساب می‌آید. این مقاله با هدف بررسی تطبیقی این دو نظام، تحلیل اصول حقوقی حاکم بر داده‌های شخصی و شناسایی چالش‌ها و شکاف‌های قانونی، تلاش می‌کند راهکارهای ارتقاء حمایت قانونی در فضای بانکداری برخط ایران را پیشنهاد دهد.

۲. بانکداری برخط و داده‌های شخصی

بانکداری الکترونیکی، به عنوان زیرشاخه بانکداری برخط، عبارت است از فراهم آوردن امکانات نرم‌افزاری و سخت‌افزاری برای کارکنان و مشتریان بانک به منظور انجام تراکنش‌ها و خدمات بانکی با سرعت و کارایی بیشتر به صورت غیرحضوری و در هر زمان از شبانه‌روز از طریق کانال‌های ارتباطی امن. به بیان دیگر، بانکداری الکترونیکی متکی بر فناوری‌های پیشرفته شبکه و مخابرات است که امکان تعامل آنلاین بانک و مشتری را با تضمین امنیت داده‌ها و اطلاعات مالی فراهم می‌سازد (زرکلام، ۱۳۹۰، ص ۱۵۳).

در ایران، بانکداری برخط سهم مهمی در ارائه خدمات مالی دارد اما با مشکلات ویژه‌ای مانند ضعف زیرساخت‌های امنیتی، کمبود چارچوب قانونی مدون و محدودیت‌های ناشی از تحریم‌ها روبروست. به‌رغم اینکه بانک‌هایی همچون پاسارگاد توانسته‌اند با بهره‌گیری از فناوری‌های دیجیتال پیشرفته در فهرست برترین بانک‌های جهان قرار گیرند^۱، چالش‌های جدی در زمینه حفاظت از داده‌های شخصی به دلیل نبود قوانین جامع و نظام نظارتی کارآمد همچنان وجود دارد. بنابراین، اهمیت داده‌های شخصی در بانکداری برخط نه تنها به عنوان منبع اصلی برای ارائه خدمات مالی بلکه به عنوان عنصر اساسی در تضمین اعتماد و امنیت مشتریان شناخته می‌شود. بدون مدیریت دقیق داده‌ها و حفاظت قانونی مناسب، ریسک بالای نقض حریم خصوصی و جرایم سایبری می‌تواند رشد و توسعه بانکداری دیجیتال را مختل سازد. این توجه به اهمیت داده‌ها در بانکداری برخط جهانی و وضعیت خاص ایران، حاکی از نیاز جدی به توسعه چارچوب‌های قانونی، ارتقاء فناوری‌های حفاظتی و آموزش مستمر کاربران برای تضمین امنیت داده‌ها و بهینه‌سازی خدمات مالی است.

۳. اصول حاکم بر داده‌های شخصی، چالش‌ها و خلاهای موجود در نظام بانکداری برخط

حریم خصوصی و به تبع آن داده‌های شخصی از اساسی‌ترین و مغتنم‌ترین مفاهیم مربوط به شخصیت اشخاص است و حمایت جدی مقنن را در این عرصه می‌طلبد. قانونگذار ایرانی نیز به زعم خود و در راستای حمایت از داده‌های شخصی اقدام به وضع قوانینی نموده است با این حال قانونی که در این راستا شایان توجه است؛ قانون تجارت الکترونیک است که تلاش‌هایی را در جهت حمایت از داده‌های شخصی نموده اما متأسفانه در این راستا قانون یگانه و مستقلی تا بحال تصویب نگردیده است. البته پیش‌نویس لایحه صیانت از داده‌های شخصی با همکاری وزارت

¹ <https://B2n.ir/eq5348>

ارتباطات و مرکز پژوهشهای مجلس شورای اسلامی تدوین گردیده که هدف اصلی آن، صیانت از حیثیت و کرامت اشخاص است که قواعد و احکام آن شامل؛ تبیین حقوق اشخاص موضوع داده‌ها، به ویژه در تعامل با سایر حق‌های مشروع، ضابطه‌مندی فرآیند پردازش داده‌های شخصی، مسئولیت‌پذیری پردازش، هم‌افزایی امور تنظیمی و نظارتی پردازش و جبران‌پذیری زیان‌ها و آسیب‌های پردازش می‌شود. همچنین مقرر بود چهار لایحه دیگر با عنوان‌های حاکمیت‌های الکترونیکی، مسئولیت‌پذیری در فضای مجازی، لایحه خاص برای تراکنش‌های الکترونیکی و شناسایی الکترونیک در دست اقدام قرار گیرد که تا کنون موردی تصویب نگردیده است.

با وجود بهره‌گیری از ابزار فنی موجود به منظور حمایت از داده‌ها، نظیر فیلتر کردن و رمزنگاری یا رویه‌های داخلی سازمان‌ها و صنایع که بسیار ضروری و حائز اهمیت است، اما به هیچ عنوان کافی نیست و برای حمایت کافی و مؤثر از حریم خصوصی داده‌های شخصی در ارتباطات الکترونیکی وجود قواعد متناسب با چنین حمایتی اجتناب‌ناپذیر هستند (زرکلام، ستار، ۱۳۸۶، ص ۱۷۳).

اصول حاکم بر داده‌های شخصی در بانکداری برخط از مهم‌ترین مباحث حوزه حفاظت از داده‌ها است. این اصول منبعث از مقررات عمومی حفاظت از داده‌ها^۲ اتحادیه اروپا است که الگوی جهانی برای قوانین ملی و سیاست‌های حفاظت داده در بانکداری دیجیتال محسوب می‌شود و موجب حفظ حقوق فردی و ارتقاء امنیت سامانه‌های بانکی می‌گردد. تحلیل این اصول به ویژه در بانکداری برخط اهمیت فراوانی دارد، چرا که بانک‌ها به عنوان متولی داده‌های حساس مشتریان، موظف به حفظ امنیت و حریم خصوصی این داده‌ها هستند. این اصول به شرح ذیل می‌باشند.

۳.۱. قانونمندی و شفافیت^۳

پردازش داده‌ها باید همواره تابع قوانین معتبر باشد و بانک موظف است تمام فرآیندهای جمع‌آوری، پردازش و ذخیره داده‌ها را به صورت شفاف به مشتری اعلام کند. برای مثال، مشتری باید بداند که داده‌های تراکنش‌هایش چگونه استفاده می‌شود و اهداف پردازش مشخص باشد؛ هنگامی که بانک اطلاعات مشتری را برای بازاریابی استفاده کند، لازم است رضایت صریح مشتری اخذ شود. قانونمندی حکم می‌کند که هیچ پردازشی نباید به صورت خودسرانه یا بدون توجه حقوقی معتبر صورت گیرد. بانک‌ها، به عنوان «کنترل‌کنندگان داده»، موظفند برای هر فعالیتی که روی داده‌های شخصی انجام می‌دهند، یک «مبنای قانونی» مشخص و مشروع داشته باشند. در نظام‌های حقوقی پیشرفته، مانند مقررات عمومی حفاظت از داده اتحادیه اروپا، این مبانی به وضوح تعریف شده‌اند. در حوزه بانکداری برخط، پردازش داده‌های مشتری عمدتاً بر سه مبنا استوار است: ۱. ضرورت اجرای قرارداد: زمانی که بانک اطلاعات حساب یا تراکنش را برای انتقال وجه (که درخواست خود مشتری بوده) پردازش می‌کند. ۲. الزامات قانونی: زمانی که بانک طبق مقررات مبارزه با پولشویی موظف به احراز هویت دقیق مشتری و ثبت سوابق است. ۳. رضایت: زمانی که بانک قصد دارد کاری فراتر از خدمات اصلی و الزامات قانونی انجام دهد، مانند تحلیل رفتار مشتری برای ارائه پیشنهادهای بیمه یا ارسال پیامک‌های تبلیغاتی. اصل قانونمندی ایجاب می‌کند که این مبانی قانونی قابل تفکیک باشند. بانک نمی‌تواند ارائه خدمات اصلی (مبنای ۱) را به اخذ رضایت برای بازاریابی (مبنای ۳) منوط کند.

^۲ General Data Protection Regulations (GDPR)

^۳ Lawfulness and Transparency

در کنار قانونمندی، «اصل شفافیت» قرار دارد. شفافیت پلی است که مشتری را به درک این مبانی قانونی می‌رساند. بانک نمی‌تواند صرفاً به داشتن یک مبانی قانونی در اسناد داخلی خود بسنده کند؛ بلکه مکلف است این موارد را به صورت «شفاف، قابل فهم و به سادگی قابل دسترس» به اطلاع مشتری برساند. بر اساس ماده ۵ (بند ۱-الف) و همچنین مواد ۱۲ و ۱۳ همان مقررات، شفافیت مستلزم آن است که در زمان جمع‌آوری داده‌ها، بانک به صراحت موارد زیر را اعلام کند:

- هویت بانک (کنترل‌کننده) و اطلاعات تماس مسئول حفاظت از داده.
- اهداف دقیق پردازش (مثلاً: "احراز هویت"، "ارسال صورتحساب"، "بازاریابی محصولات وابسته").
- مبانی قانونی هر یک از این اهداف (مثلاً: احراز هویت بر مبنای "الزام قانونی" و بازاریابی بر مبنای "رضایت").
- گیرندگان یا دسته‌بندی گیرندگان داده‌ها (مثلاً: شرکت‌های ارزیابی اعتبار، شرکای تجاری برای بازاریابی).
- مدت زمان نگهداری داده‌ها یا معیارهای تعیین آن.

رویه‌های نوین مانند «اعلامیه‌های لایه‌ای» یا «داشبوردهای حریم خصوصی» در اپلیکیشن‌های بانکی، نمونه‌هایی از اجرای صحیح اصل شفافیت هستند که به مشتری امکان می‌دهند به سرعت اطلاعات کلیدی را درک کند و کنترل مؤثری بر داده‌های خود داشته باشد.

۳,۲. محدودیت هدف^۴

بانک تنها می‌تواند داده‌ها را برای اهداف خاص و محدود جمع‌آوری کند و داده‌های جمع‌آوری شده باید صرفاً برای اهداف مشخص، صریح و قانونی استفاده شوند و هیچ گونه استفاده فراتر از هدف اولیه مجاز نیست. بنابر این اصل اطلاعات حساب برای انجام تراکنش‌های بانکی است و داده‌های مشتریان بانک تنها باید برای ارائه خدمات مالی و مدیریت حساب استفاده شود و نباید برای اهداف دیگری مثل فروش به شخص ثالث بدون رضایت مشتری استفاده شود. این ممنوعیت حقوقی بر مبنای اصل "ناسازگاری هدف" استوار است، به این معنی که اگر هدف ثانویه‌ای که بانک دنبال می‌کند، با توقعات منطقی مشتری و با هدف اولیه‌ای که داده‌ها برای آن جمع‌آوری شده‌اند، در تعارض یا ناسازگاری جدی باشد، پردازش داده‌ها غیرقانونی تلقی می‌شود.

در جهان بانکداری برخط، جایی که حجم عظیمی از داده‌های حساس تراکنش‌ها، موقعیت مکانی و الگوهای مصرفی تولید می‌شود، اهمیت این اصل دوچندان می‌گردد. بانک‌ها دائماً وسوسه می‌شوند تا با استفاده از فناوری‌های تحلیل داده‌های بزرگ یا هوش مصنوعی، پروفایل‌های دقیقی از مشتریان بسازند و این داده‌ها را به منبع درآمد ثانویه تبدیل کنند. اما اصل محدودیت هدف، مرز قانونی روشنی بین استفاده مشروع (مثلاً تشخیص کلاهبرداری) و سوءاستفاده (مثلاً بهره‌برداری تجاری غیرمجاز) ترسیم می‌کند.

مقررات عمومی حفاظت از داده اتحادیه اروپا در ماده ۵ (بند ۱-ب)، این اصل را به عنوان یک وظیفه اساسی برای «کنترل‌کنندگان داده» (مانند بانک‌ها) تثبیت کرده است. این مقررات، به منظور حمایت از مشتری، تنها در صورت وجود سه شرط، اجازه پردازش داده‌ها برای هدفی متفاوت از هدف اولیه را می‌دهد:

۱. سازگاری هدف: هدف ثانویه باید به طور منطقی و حقوقی با هدف اصلی سازگار باشد (مثلاً استفاده از داده‌ها برای تهیه گزارش‌های آماری داخلی برای بهبود خدمات).
۲. اقدامات حفاظتی کافی: بانک باید تدابیر فنی و سازمانی لازم (مانند ناشناس‌سازی یا نام مستعار سازی) را برای به حداقل رساندن خطرات حریم خصوصی اتخاذ کند.
۳. تغییر مبانی

⁴ Purpose Limitation

قانونی: اگر هدف ثانویه سازگار نباشد، بانک باید برای پردازش ثانویه، مبنای قانونی جدیدی، مانند رضایت صریح و آگاهانه مشتری، کسب کند یا باید اثبات کند که پردازش برای منافع عمومی یا قانونی ضروری است. به‌کارگیری این اصل، بانک را ملزم می‌کند که «سیستم مدیریت حریم خصوصی» خود را بر اساس طراحی مبتنی بر حریم خصوصی بنا نهد. این بدان معناست که از همان لحظه طراحی یک اپلیکیشن جدید یا یک سرویس بانکداری برخط، باید تمایز میان داده‌هایی که برای تراکنش ضروری هستند و داده‌هایی که برای بازاریابی مفیدند، حفظ شده و داده‌ها صرفاً در حد نیاز و برای هدف مشخص شده پردازش گردند.

۳.۳. دقت^۵ و به‌روزرسانی

این اصل حقوقی که در ماده ۵ (بند ۱-د) مقررات عمومی حفاظت از داده اتحادیه اروپا مورد تأکید قرار گرفته، تضمین می‌کند که تصمیم‌گیری‌های بانک بر اساس اطلاعات ناقص یا غلط صورت نگیرد. در حوزه بانکداری برخط، اهمیت این اصل حیاتی است، زیرا بسیاری از تصمیمات خودکار (مانند تأیید هویت برای ورود، ارزیابی اعتبار، یا ارسال رمز پویا) به طور لحظه‌ای و صرفاً بر اساس دقت داده‌های موجود در سیستم‌های بانکی انجام می‌پذیرد. اصل دقت صرفاً یک مسئولیت اداری نیست، بلکه یک تعهد حقوقی برای بانک ایجاد می‌کند. این تعهد شامل سه جنبه اصلی است:

۱. دقت مستمر: بانک باید تدابیر فنی و سازمانی معقولی را در نظر بگیرد تا اطمینان حاصل شود که داده‌های شخصی «نادرست» در اسرع وقت «پاک» یا «اصلاح» شوند. این امر مستلزم ایجاد مکانیزم‌های بازبینی دوره‌ای و همچنین بسترهای تعاملی برای مشتری است تا بتواند به آسانی و بدون صرف هزینه، اطلاعات خود را اصلاح کند. ۲. حق اصلاح: این اصل، که در ماده ۱۶ مقررات عمومی حفاظت از داده اتحادیه اروپا به صورت یک حق صریح برای مشتری تعریف شده است، به مشتری امکان می‌دهد تا از بانک درخواست کند که هرگونه داده نادرست یا ناقص او را بدون تأخیر غیرموجه اصلاح نماید. بانکداری برخط باید این حق را از طریق رابط‌های کاربری ساده (مانند بخش پروفایل کاربری در اپلیکیشن) فراهم کند. ۳. جلوگیری از تصمیم‌گیری خودکار نادرست: اگر داده‌ها نادرست باشند، ممکن است نتایج تصمیمات خودکار (مانند رد درخواست کارت اعتباری یا مسدود شدن حساب به دلیل اطلاعات تماس قدیمی) کاملاً غلط و تبعیض‌آمیز باشد. اصل دقت، بانک را مسئول می‌داند که پیش از اتخاذ هر تصمیم قانونی یا اثرگذار بر فرد (مانند تصمیمات اعتبارسنجی)، صحت داده‌های مورد استفاده را به طور ویژه تأیید کند.

عدم رعایت این اصول، عواقب حقوقی جدی به دنبال دارد. برای مثال، اگر به دلیل عدم به‌روزرسانی آدرس توسط بانک، یک اخطار به مهم به دست مشتری نرسد و مشتری متضرر شود، بانک به دلیل نقض اصل دقت پاسخگو خواهد بود. بنابراین، بانک‌ها نه تنها باید داده‌ها را به‌روز نگه دارند، بلکه باید سوابق و مستنداتی از «اقدامات اصلاحی» که در قبال داده‌های نادرست انجام داده‌اند، نگهداری نمایند. این امر به شفافیت و پاسخگویی بانک در برابر نهادهای نظارتی کمک می‌کند.

⁵ Accuracy

۳,۴. محدودیت ذخیره‌سازی^۶

این اصل که در ماده ۵ (بند ۱-ه) مقررات عمومی حفاظت از داده اتحادیه اروپا گنجانده شده است، مستقیماً با اصل «محدودیت هدف» در ارتباط است. اگر داده‌ها دیگر برای اهدافی که به موجب آن جمع‌آوری شده‌اند (مثلاً ارائه خدمات فعال بانکی) ضروری نباشند، نگهداری آن‌ها صرفاً بار امنیتی و حقوقی برای بانک ایجاد کرده و حقوق بنیادین مشتری را نقض می‌کند.

اصل محدودیت ذخیره‌سازی، بانک‌ها را ملزم می‌سازد که «دوره نگهداری (Retention Period)» مشخصی را برای هر دسته از داده‌های شخصی خود تعریف و شفاف‌سازی کنند. این دوره باید با طول زمانی که برای تحقق هدف اصلی پردازش نیاز است، متناسب باشد.

برای رعایت این اصل، بانک باید یک «سیاست جامع نگهداری داده» تدوین کرده و آن را به اطلاع مشتری برساند. سیستم‌های مدیریت داده بانکداری برخط نیز باید به گونه‌ای طراحی شوند که پس از انقضای دوره نگهداری مشخص شده، حذف یا آرشیو داده‌ها به صورت خودکار و بدون دخالت انسانی صورت پذیرد. این رویکرد پیشگیرانه، ریسک نقض حریم خصوصی و جرمه‌های نظارتی ناشی از نگهداری بی‌رویه داده‌ها را به شدت کاهش می‌دهد.

۳,۵. یکپارچگی و محرمانگی^۷

این اصل، که در ماده ۵ (بند ۱-و) مقررات عمومی حفاظت از داده اتحادیه اروپا به آن اشاره شده است، وجهه عملی تمامی اصول حقوقی پیشین را تشکیل می‌دهد. تمام تلاش‌های حقوقی برای تعریف حدود قانونی پردازش، در نهایت به توانایی بانک در اجرای تدابیر فنی و سازمانی قوی برای حفظ امنیت داده‌ها وابسته است. این اصل به صراحت بانک را ملزم به رعایت محرمانگی (جلوگیری از دسترسی و افشای غیرمجاز)، و یکپارچگی (جلوگیری از تغییر یا تخریب داده‌ها به صورت تصادفی یا عمدی) می‌کند.

در فضای بانکداری برخط، که حملات سایبری به یک تهدید مستمر تبدیل شده‌اند، بانک موظف است اقدامات امنیتی خود را بر اساس "سطح ریسک"^۸ مربوط به داده‌های مشتری تنظیم کند. تدابیر امنیتی نه تنها باید داده‌ها را در زمان انتقال (مانند استفاده از پروتکل‌های رمزنگاری لایه انتقال) حفظ کنند، بلکه باید در زمان "سکون" (نگهداری روی سرورها یا پایگاه داده) نیز با رمزنگاری قوی محافظت شوند.

به بیان دیگر، اصل یکپارچگی و محرمانگی صرفاً به معنای نصب فایروال^۹ نیست، بلکه ایجاد یک چارچوب مدیریت امنیت اطلاعات جامع است که به طور مستمر بازبینی شده و به‌روزرسانی می‌شود تا در برابر تهدیدات نوظهور (مانند حملات باج‌افزار یا بدافزار) مقاوم باشد. نقض این اصل، علاوه بر جرمه‌های سنگین نظارتی، عواقب مدنی و کیفری برای بانک و مدیران آن در پی خواهد داشت.

^۶ Storage Limitation

^۷ Integrity and Confidentiality

^۸ Risk level

^۹ firewall

۳،۶. پاسخگویی^{۱۰}

رعایت اصول جامع حفاظت داده‌ها شامل محرمانگی، صحت، دسترسی‌پذیری و پاسخگویی در نظام بانکی به طور مستقیم موجب افزایش اعتماد مشتریان و کاهش ریسک‌های حقوقی و امنیتی می‌شود. بانک‌هایی که این اصول را به طور کامل اجرا کرده‌اند، توانسته‌اند هم از افشای داده‌ها جلوگیری کنند و هم از بروز دعاوی حقوقی سنگین پیشگیری نمایند. (اصغری و همکاران، ۱۴۰۴، ص ۱۰۵). بنابراین، این اصول، پایه حقوقی و فنی حاکم بر محافظت از داده‌های شخصی در بانک‌های سراسر جهان هستند و رعایت کامل آنها، جزو الزامات قانونی و استانداردهای بین‌المللی در مواجهه با تهدیدات سایبری و نیازهای نظارتی است.

بانک‌ها باید قادر به اثبات اجرای قواعد حفاظتی داده‌ها باشند و در مقابل مراجع نظارتی و مشتریان پاسخگو باشند. مثلاً مستندسازی اقدامات امنیتی و ارائه گزارش‌های سالانه عملکرد در حفاظت داده‌ها از مصادیق مهم این اصل است. اصل پاسخگویی، که به عنوان سنگ بنای نظام‌های مدرن حفاظت از داده شناخته می‌شود، نه تنها بانک‌ها را ملزم به رعایت تمام اصول شش‌گانه (قانونمندی، شفافیت، محدودیت هدف، دقت، محدودیت ذخیره‌سازی، و یکپارچگی/محرمانگی) می‌کند، بلکه تعهد می‌آفریند که بتوانند رعایت این اصول را در عمل به اثبات برسانند. ماده ۵ (بند ۲) مقررات عمومی حفاظت از داده اتحادیه اروپا به صراحت بیان می‌دارد که «کنترل‌کننده [بانک] مسئول بوده و باید بتواند رعایت بند ۱ [اصول شش‌گانه] را نشان دهد.» در حوزه بانکداری برخط، که پردازش‌ها پیچیده، خودکار و با ریسک بالا هستند، پاسخگویی نیازمند زیرساخت‌های سازمانی و فنی خاص است. در نهایت، اصل پاسخگویی، زیربنای اعتماد مشتریان است. این اصل، بانک را از یک نهاد منفعل به یک نهاد مسئولیت‌پذیر و فعال در قبال حفظ حریم خصوصی داده‌ها تبدیل می‌کند. بدون توانایی در اثبات رعایت این اصول، هرگونه ادعای بانک در خصوص حفاظت از داده‌ها، فاقد ارزش حقوقی و عملی خواهد بود.

۴. چالش‌ها

نظام حقوقی ایران در خصوص حفاظت از داده‌های شخصی، به ویژه در بانکداری برخط، با خلأهای تقنینی، مفهومی و ساختاری عمیقی مواجه است که مانع از تحقق کامل حمایت‌های قانونی و اجرایی مؤثر می‌شود. نتایج پژوهش‌های داخلی در حوزه بانکداری برخط نشان می‌دهد که عدم وجود یک نهاد نظارتی مستقل و ضعف در زیرساخت‌های فنی و اداری برای تضمین حاکمیت داده‌ها، از موانع کلیدی در اجرای کارآمد حمایت حقوقی از داده‌های شخصی در ایران است که اجرای اصول شفافیت و پاسخگویی را با چالش مواجه می‌سازد. (خورشیدوند، ۱۳۹۹، صص ۱۳۷-۱۴۴، ۱۷۷-۱۷۹) این ضعف‌ها در قالب عدم تطابق قوانین موضوعه با فناوری‌های نوین، ضعف ضمانت اجرا، کمبود نهادهای نظارتی مؤثر و نبود چارچوب‌های فنی و اجرایی مناسب نمایان می‌شوند. تحلیل این چالش‌ها، با رویکرد تطبیقی به مقررات عمومی حفاظت از داده اتحادیه اروپا، نشان می‌دهد که شکاف عمیقی میان تعهدات حقوق بین‌الملل و نظام داخلی ایران وجود دارد.

۴،۱. خلأهای تقنینی و فقدان چارچوب مفهومی جامع

قوانین موجود در حوزه حفاظت از داده‌های شخصی در ایران، علی‌رغم برخی پیشرفت‌ها، از انسجام و جامعیت کافی برخوردار نیستند و بیشتر جنبه‌های حمایت از داده‌ها به صورت پراکنده و ناقص مورد توجه قرار گرفته‌اند. فقدان یک

¹⁰ Accountability

قانون جامع و مستقل، که صرفاً به حفاظت از داده‌ها پردازد، موجب شده است تا نظام بانکداری برخط ایران در مواجهه با تحولات سریع دیجیتال، از یک مرجع قانونی روشن و یکپارچه محروم باشد و اصول کلیدی حمایت از داده‌ها (شامل قانونمندی، شفافیت و محدودیت هدف) به درستی اجرا نشوند.

یکی از بنیادی‌ترین خلأها در ساختار حقوقی ایران، عدم تفکیک و تعریف دقیق دو نقش کلیدی در پردازش داده است: کنترل‌کننده داده (مانند خود بانک) و پردازشگر داده (شرکت‌های فین‌تک، یا پیمانکاران فناوری که داده‌ها را از طرف بانک پردازش می‌کنند). در مقررات داخلی، مسئولیت‌ها اغلب به طور کلی بر دوش بانک به عنوان صاحب اصلی داده قرار می‌گیرد، بدون آنکه وظایف خاص و الزامات قراردادی پردازشگر به وضوح مشخص شود.

در مقابل، مقررات عمومی حفاظت از داده اتحادیه اروپا به صراحت، تعهدات کنترل‌کننده (شامل نظارت، مستندسازی و تضمین امنیتی) و پردازشگر (شامل عمل بر اساس دستورات کنترل‌کننده و حفظ امنیت) را تفکیک می‌کند. این ابهام در قوانین ایران، به ویژه با افزایش برون‌سپاری خدمات بانکی به شرکت‌های ثالث (مانند کیف پول‌های الکترونیکی و سامانه‌های اعتبارسنجی)، زمینه‌ساز بروز چالش‌های جدی در زمان وقوع نقض امنیتی می‌شود، چرا که تعیین مسئولیت نهایی برای جبران خسارت به مشتری، با موانع حقوقی و قراردادی پیچیده‌ای مواجه است.

همچنین تصریح بر حقوق ذینفعان داده‌ها به عنوان هسته اصلی حمایت از فرد، در قوانین مرتبط با بانکداری اینترنتی ایران وجود ندارند. حقوقی مانند حق دسترسی به داده‌ها، حق اصلاح، و حق اعتراض به پردازش، که اصولاً در حقوق شهروندی دیجیتال باید تضمین شوند، عملاً فاقد مکانیزم اجرایی مؤثر هستند.

از جمله مهم‌ترین خلأها، نبود حق انتقال‌پذیری داده‌ها است. این حق که در مقررات اتحادیه اروپا برای تضمین رقابت در بازار و افزایش کنترل مشتری بر داده‌ها ضروری است، در نظام ایران غایب بوده و مشتریان را عملاً به بانک اولیه‌شان وابسته نگه می‌دارد. نبود این حق، مانع از توسعه کامل خدمات فین‌تک‌های نوآور می‌شود، چرا که امکان جابه‌جایی آسان و امن سوابق مالی مشتریان میان رقبا وجود ندارد.

همچنین، فقدان الزامات حقوقی صریح برای اجرای اصل شفافیت در فرآیند اخذ رضایت، موجب می‌شود که رضایت مشتری اغلب مبهم، کلی و غیرآگاهانه باشد. بانک‌ها رضایت‌نامه‌های طولانی و پیچیده‌ای را به مشتریان تحمیل می‌کنند که عملاً امکان درک کامل دامنه استفاده از داده‌ها را از مشتری سلب می‌کند که این امر با روح اصل قانونمندی و شفافیت در تضاد است.

۴.۲. چالش‌های ضمانت اجرا و کمبود نهاد نظارتی مستقل

ضعف ضمانت اجرا و فقدان نهاد نظارتی تخصصی، دومین چالش ساختاری در نظام حقوقی ایران است که ماهیت بازدارندگی و جبران خسارت را دچار اختلال جدی کرده است. در اتحادیه اروپا، سکوها مسئولیت‌های قانونی گسترده تری نسبت به ایران دارند، به طوری که قوانین اتحادیه اروپا، این سکوها را به رعایت استانداردهای خاصی در قبال کیفیت، اصالت و ایمنی محصولات ملزم می‌کند و از آنان می‌خواهد که از بروز آسیب به مصرف کنندگان جلوگیری کنند. همچنین، این سکوها ملزم به همکاری با نهادهای نظارتی و ارائه اطلاعات کافی به مصرف کنندگان هستند. در ایران، قوانین مرتبط با سکوها اینترنتی و مسئولیت‌های آنها، نسبت به اتحادیه اروپا کمتر توسعه یافته است. اگرچه برخی از اصول نظارتی و حقوقی مشابه با اتحادیه اروپا وجود دارد، اما جایگاه قانونی و نظارتی این سکوها هنوز نیازمند بازبینی و به روزرسانی است. (استا، محمد حسین، شهبازی نیا، مرتضی، پارساپور، محمدباقر، ۱۴۰۴، صص ۳۱-۳۲)

فقدان نهاد نظارتی مستقل و تخصصی با اختیارات اجرایی لازم (مانند جریمه، الزام به تغییر فرایندها و رسیدگی سریع به شکایات)، موجب گردیده رسیدگی به دعاوی و شکایات مربوط به نقض امنیت داده‌ها به کندی و با ضعف مواجه شود. در حال حاضر، مسئولیت نظارت بر داده‌ها میان نهادهایی چون بانک مرکزی (نظارت بر عملکرد مالی و امنیتی بانک)، مرکز توسعه تجارت الکترونیک، و قوه قضائیه تقسیم شده که این تضاد صلاحیت‌ها و پراکندگی اختیارات، مانع از نظارت مستمر، قاطع و هماهنگ می‌شود.

مقررات عمومی حفاظت از داده اتحادیه اروپا برای مقابله با این مشکل، نهادهای نظارتی مستقل را پیش‌بینی کرده که دارای استقلال مالی، فنی و اجرایی کامل برای اعمال جریمه و بازرسی‌های فنی هستند. فقدان چنین نهادی در ایران، موجب می‌شود که بانک‌ها در مواجهه با چالش‌های فنی پیچیده، مرجع واحد و تخصصی برای دریافت مشورت حقوقی و فنی نداشته باشند و این خود بر ضعف در اجرای مقررات می‌افزاید. علاوه بر این، ضعف در توانایی بانک مرکزی و سایر نهادهای ناظر در نظارت مستمر، ناشی از محدودیت منابع و عدم به‌روزرسانی سیستم‌های اطلاعاتی است که اجرای مقررات را ضعیف می‌کند (اصغری و همکاران، ۱۴۰۴، ص ۱۰۵).

۴.۳. چالش‌های فنی و رویارویی با هوش مصنوعی و کلان‌داده و انتقال داده

نظام حقوقی ایران در مواجهه با فناوری‌های تحول‌آفرین مانند هوش مصنوعی و تحلیل کلان‌داده‌ها، که ستون فقرات بانکداری برخط نوین را تشکیل می‌دهند، با خلأهای جدی روبه‌رو است که مستقیماً اصول محدودیت هدف و دقت داده‌ها را به چالش می‌کشد. این نیاز به بازبینی، همسو با الزامات لایحه صیانت از داده‌های شخصی است که تأکید دارد حقوق اشخاص باید در تمامی فرآیندهای پردازش داده‌ها، شامل طراحی فنی و سازمانی، به رسمیت شناخته و تضمین شود (لایحه صیانت از داده‌های شخصی، ماده ۵).

وانگهی با گسترش استفاده بانک‌ها از فناوری‌های هوش مصنوعی برای ساخت پروفایل‌های رفتاری و اعتباری دقیق، چالش‌های نوینی در حوزه حریم خصوصی پدید آمده است. نظام حقوقی ایران فاقد مقررات صریحی برای نظارت بر تصمیم‌گیری‌های کاملاً خودکار است. در این فرآیندها، تصمیماتی حیاتی مانند رد درخواست وام یا تعیین سقف اعتباری، بدون دخالت انسان و صرفاً بر اساس تحلیل الگوریتم‌ها اتخاذ می‌شود.

مقررات عمومی حفاظت از داده اتحادیه اروپا به صراحت، حق عدم تابعیت از تصمیم‌گیری‌های صرفاً خودکار را به مشتری می‌دهد، به جز در موارد استثنایی و با تضمین‌های کافی. همچنین، بر اساس حق اعتراض، مشتری می‌تواند خواستار توضیح در مورد منطق تصمیم‌گیری الگوریتم شود. با این حال، تحلیلگران معتقدند که چارچوب GDPR به تنهایی برای مقابله با کلان‌داده‌ها و تصمیم‌گیری‌های الگوریتمی پنهان کافی نیست و این مقررات در عصر کلان‌داده‌ها، به‌ویژه در بخش مالی، ناسازگار هستند (Zarsky, 2017, p. 1010). علاوه بر این، باید مطمئن شد که تبعیض‌های اجتماعی و زمینه‌ای در داده‌های اولیه وارد مدل‌های هوش مصنوعی بانکی نشوند (Wachter). و همکاران تأکید دارند که پدیده «بی‌عدالتی الگوریتمی» می‌تواند منجر به رد شدن ناعادلانه درخواست وام مشتریان شود که این امر نیازمند یک بازبینی انسانی است (Wachter et al., 2017, p. 30). اما نظام ایران در این خصوص ساکت است و این خلأ قانونی، دست بانک‌ها را برای استفاده‌های نامحدود از داده‌ها در فرآیندهای ماشینی باز می‌گذارد.

علاوه بر این استفاده از کلان‌داده‌ها در بانکداری، به طور ذاتی با اصل حداقل‌سازی داده‌ها که در مقررات اتحادیه اروپا تصریح شده است، در تضاد است. این اصل بیان می‌کند که داده‌ها باید صرفاً در حد ضروری و متناسب با هدف

پردازش جمع آوری شوند. اما تحلیل کلان داده اغلب نیازمند جمع آوری هر چه بیشتر داده‌های شخصی (از جمله موقعیت مکانی، الگوی مصرف و اطلاعات شبکه‌های اجتماعی) است تا مدل‌های هوش مصنوعی دقیق‌تر عمل کنند. در غیاب یک نظارت حقوقی قوی در ایران، بانک‌ها برای افزایش سودآوری و بهبود دقت الگوریتم‌ها، تمایل دارند داده‌ها را فراتر از حد نیاز جمع آوری و برای اهداف ثانویه استفاده کنند، که این نقض آشکار اصل محدودیت هدف نیز محسوب می‌شود.

همچنین با افزایش برون‌سپاری خدمات بانکداری برخط به شرکت‌های فین‌تک یا شرکت‌های ثالث برای ارائه خدمات پردازش، چالش‌های مربوط به اصل یکپارچگی و محرمانگی و پاسخگویی افزایش یافته است. این برون‌سپاری، در غیاب قراردادهای شفاف، مسئولیت بانک را در قبال نقض امنیت توسط شرکت‌های پردازشگر، به طور جدی تضعیف می‌کند. در حقوق تطبیقی، تمرکز بر مسئولیت مشترک و تضامنی میان کنترل‌کننده و پردازشگر در زمان نقض است، اما نظام حقوقی ایران فاقد مکانیسم روشنی برای پاسخگویی به این نوع روابط قراردادی پیچیده است. از این رو، مسئولیت مدنی ارائه‌دهندگان خدمات الکترونیکی (از جمله فین‌تک‌ها) یکی از جدی‌ترین چالش‌های نظام حمایت از داده‌های شخصی ایران محسوب می‌شود و ضرورت دارد چارچوب قانونی روشنی برای تنظیم رابطه فین‌تک‌ها با مشتریان بانک تدوین شود (رزم‌آرا، ۱۳۹۹، ص ۱۲۰).

بیش از آن انتقال داده‌های شخصی مشتریان به خارج از مرزهای کشور برای پردازش یا میزبانی ابری یک واقعیت است. نظام حقوقی ایران فاقد قوانین مشخص برای تعیین کفایت سطح حفاظت در کشور گیرنده است. در مقررات عمومی حفاظت از داده اتحادیه اروپا، انتقال داده به خارج از اتحادیه اروپا تنها در صورت احراز "سطح کفایت حمایت" مجاز است یا نیازمند اجرای مکانیسم‌های قراردادی استاندارد است. این خلأ در ایران ریسک‌هایی را به دنبال دارد، زیرا داده‌های شخصی ممکن است به کشورهایی منتقل شوند که از استانداردهای حفاظتی ضعیف‌تری برخوردار باشند و این به معنای نقض تعهد بانک در قبال محرمانگی داده‌ها است و می‌تواند منجر به دسترسی غیرقانونی دولت‌های خارجی به داده‌های حساس شهروندان شود.

۴,۴. ضعف در پیاده‌سازی الزامات فنی و امنیتی

فقدان زیرساخت فنی مناسب و ضعف در توسعه فناوری‌های حفاظتی در بانک‌های ایران، باعث می‌شود اجرای قواعد حتی در صورت وجود قانونی نیز به طور کامل ممکن نباشد. ضعف در استانداردهای فرایندهای بانکی و عدم تدوین دقیق و هماهنگ آیین‌نامه‌های اجرایی (مانند دستورالعمل‌های رمزنگاری و احراز هویت قوی) گاهی منجر به تضاد و سردرگمی در نیل به اهداف قانونی می‌گردد. بانک‌ها در عمل، الزامی برای اجرای تکنیک‌های امنیتی پیشرفته مانند ناشناس‌سازی یا نام مستعار سازی ندارند، در حالی که این تکنیک‌ها ستون فقرات حفاظت از داده در حقوق بین‌الملل هستند و اجرای آن‌ها در مراحل اولیه طراحی سرویس‌ها ضروری است.

۴,۵. ناکارآمدی ساختار جبران خسارت و عدم تناسب با ریسک بانکی

برخلاف مقررات سخت‌گیرانه مقررات عمومی حفاظت از داده اتحادیه اروپا که جریمه‌های مالی متناسب با تخلف و حجم فعالیت اقتصادی بانک را در نظر می‌گیرد، در ایران ضمانت اجراهای کیفری و مدنی موجود، سقف و میزان مشخصی ندارند یا متناسب با حجم سودآوری و ریسک فعالیت‌های مالی بزرگ بانک‌ها نیستند. به دلیل عدم وجود یک

قانون جامع، مجازات‌ها صرفاً بر اساس جرایم عمومی (مانند کلاهبرداری یا تخریب داده) تعیین می‌شوند که ماهیت خاص نقض حریم خصوصی داده‌ها را در نظر نمی‌گیرند.

بنابراین، بانک‌ها صرفاً با خطرات محدود مواجه بوده و الزامات اجرای دقیق قوانین را به عنوان اولویت نمی‌بینند. ضمانت اجراهای ضعیف، خاصیت بازدارندگی اقتصادی خود را از دست داده‌اند و هزینه نقض قانون برای مؤسسات مالی بسیار کمتر از هزینه اجرای کامل و به‌روزرسانی زیرساخت‌های حفاظت از داده است. این امر به طور مستقیم با اصل پاسخگویی در حقوق داده‌ها در تضاد است، چرا که بانک هیچ انگیزه‌ای برای اثبات رعایت کامل اصول ندارد. در نتیجه، بانک‌ها صرفاً با خطرات محدود مواجه بوده و الزامات اجرای دقیق قوانین را به عنوان اولویت نمی‌بینند. ضمانت اجراهای ضعیف، خاصیت بازدارندگی اقتصادی خود را از دست داده‌اند و هزینه نقض قانون برای مؤسسات مالی بسیار کمتر از هزینه اجرای کامل و به‌روزرسانی زیرساخت‌های حفاظت از داده است. جریمه‌های مالی GDPR می‌تواند بر اساس ماهیت تخلف و حجم جهانی عملیات بانکی، تا ۲۰ میلیون یورو یا ۴ درصد از گردش مالی سالانه جهانی بانک تعیین شود (GDPR ماده ۸۳) که نشان‌دهنده ماهیت بازدارنده آن در حقوق بین‌الملل است. در کنار این، چالش مدرن در نظام بانکی، یافتن تعادلی میان محرمانگی سنتی و ضرورت شفافیت در فرآیندهای داده‌محور است تا از تصمیم‌گیری‌های پنهان جلوگیری شود. (Chambers, 2004, pp.389_ 410)

نظام حقوقی ایران قراردادهای استاندارد و جامعی برای تنظیم روابط میان بانک (کنترل‌کننده) و شرکت‌های پردازشگر (مانند خدمات ابری یا سامانه‌های اعتبارسنجی) ندارد. در نتیجه، در صورت وقوع نقض داده در سیستم شرکت‌های ثالث، تعیین مسئولیت نهایی برای جبران خسارت به مشتری، با ابهامات حقوقی مواجه می‌شود. در مقررات عمومی حفاظت از داده اتحادیه اروپا، بانک‌ها موظف به انعقاد قراردادهای پردازش داده‌ها هستند که در آن، تمامی تعهدات امنیتی، نظارتی و مسئولیتی طرفین به وضوح مشخص می‌شود. این فقدان قراردادهای استاندارد در ایران، ریسک حقوقی بانک‌ها را افزایش می‌دهد و حاشیه امنی برای پردازشگران ایجاد می‌کند تا در قبال کوتاهی‌های امنیتی پاسخگو نباشند.

۵. مقایسه تطبیقی نظام حقوقی ایران با الزامات اتحادیه اروپا

در مقابل چالش‌های ساختاری ایران، مقررات عمومی حفاظت از داده اتحادیه اروپا، چهارچوبی جامع برای حفاظت از داده‌های شخصی ارائه می‌دهد که نه تنها شامل تعریف دقیق مفاهیم کلیدی است بلکه ضمانت اجراهای بازدارنده و الزامات اجرایی روشن دارد.

ویژگی کلیدی در مقررات اتحادیه اروپا	خلأ متناظر و پیامد آن در نظام ایران
اصول پیش‌فرض و طراحی مبتنی بر حریم خصوصی	عدم وجود الزام قانونی برای رعایت این اصل در طراحی خدمات بانکی جدید. پیامد: تولید سیستم‌هایی که از ابتدا امنیت داده را در اولویت قرار نداده‌اند.
نهاد نظارتی مستقل	تشتت صلاحیت میان بانک مرکزی، مرکز توسعه تجارت الکترونیک و قوه قضاییه و نبود استقلال اجرایی. پیامد: ضعف در نظارت مستمر و عدم اعمال جریمه‌های قاطع.

ویژگی کلیدی در مقررات اتحادیه اروپا	خلا متناظر و پیامد آن در نظام ایران
جریمه‌های بازدارنده (تا ۴٪ گردش مالی)	ضمانت اجراهای کیفی و مدنی ناکارآمد و سقف جریمه‌های نامتناسب با سودآوری بانک‌ها. پیامد: کم‌اهمیت شدن اجرای دقیق قوانین برای بانک‌ها.
حق انتقال‌پذیری داده‌ها	فقدان این حق که مانع از رقابت و انتقال آسان داده‌ها میان فین‌تک‌ها و بانک‌ها می‌شود. پیامد: ایجاد انحصار اطلاعاتی برای بانک‌ها و کاهش قدرت چانه‌زنی مشتری.
الزام ارزیابی اثرات حریم خصوصی	فقدان الزام قانونی برای ارزیابی ریسک‌های حریم خصوصی پیش از اجرای پروژه‌های بزرگ بانکی (مانند هوش مصنوعی). پیامد: افزایش ریسک‌های امنیتی غیرمنتظره در محصولات جدید.
حق توضیح در تصمیم‌گیری خودکار	سکوت قانون در مواجهه با پروفایل‌سازی‌های پیچیده و خودکار توسط بانک‌ها. پیامد: امکان بروز تبعیض الگوریتمی و تضییع حقوق مشتری بدون حق اعتراض مؤثر.

۶. راهکارها و الزامات اصلاحی

با توجه به این تفاوت‌ها و چالش‌های عمیق، اصلاح نظام حقوقی ایران در حوزه حفاظت داده‌ها باید در سه محور اصلی صورت گیرد:

۶.۱. اصلاحات تقنینی و تدوین قانون جامع داده‌های شخصی

نخست، تدوین و تصویب قانونی جامع و کاربردی که ضمن تطابق با فناوری‌های نوین، حقوق ذینفعان و تعهدات نهادهای پردازشگر را به دقت تعریف کند. این قانون باید صراحتاً مفاهیم کلیدی مانند کنترل‌کننده، پردازشگر و داده‌های حساس را تعریف کرده و حقوقی نظیر حق لغو رضایت، حق انتقال‌پذیری و حق اعتراض به پروفایل‌سازی خودکار را برای مشتریان به رسمیت بشناسد. تمرکز باید بر پیاده‌سازی الزامات قانونی برای تضمین شفافیت لایه‌ای در فرآیند اخذ رضایت باشد، به طوری که مشتری بتواند به آسانی مقاصد پردازش داده‌های خود را درک کند. همچنین، تعیین تکلیف دقیق برای سیاست‌های نگهداری داده‌ها (مطابق با اصل محدودیت ذخیره‌سازی) و لزوم حذف داده‌ها پس از انقضای هدف پردازش، باید به صراحت در این قانون گنجانده شود.

۶.۲. تأسیس نهاد نظارتی مستقل و توانمندسازی اجرایی

دوم، ایجاد نهاد مستقل نظارتی تخصصی که قادر باشد نظارت مداوم و اعمال ضمانت اجراهای لازم را انجام دهد. این نهاد باید از استقلال مالی و اجرایی کافی برخوردار باشد و اختیار اعمال جریمه‌های مالی متناسب و بازدارنده (مشابه مدل اتحادیه اروپا) را داشته باشد تا اصل پاسخگویی بانک‌ها به طور واقعی محقق شود. همچنین باید به این نهاد، صلاحیت

نظارت بر قراردادهای برون‌سپاری داده‌ها و ارزیابی سطح کفایت حمایت در انتقال داده‌های بین‌المللی اعطا شود. تفکیک وظایف این نهاد از بانک مرکزی در حوزه حفاظت از داده‌های شخصی، مانع از تضاد منافع خواهد شد.

۶,۳. مقتضی‌سازی تضمین‌های فنی و سازمانی

سوم، مقتضی‌سازی تضمین‌های فنی و اجرایی نظیر الزامات رمزنگاری سرتاسری و ذخیره‌سازی رمزنگاری‌شده، احراز هویت چندمرحله‌ای و مدیریت ریسک امنیتی. بانک‌ها باید ملزم به رعایت رویکرد طراحی مبتنی بر حریم خصوصی و پیش‌فرض حریم خصوصی شوند. این یعنی از همان مرحله طراحی سیستم‌های جدید، اصول حفاظت از داده‌ها لحاظ شده و از طریق تکنیک‌هایی مانند ارزیابی اثرات حفظ حریم خصوصی، ریسک‌های احتمالی پیش‌بینی و مدیریت گردند. این ارزیابی باید برای هر محصول یا سرویس جدید بانکی که شامل پردازش داده‌های حساس است، اجباری باشد و نتایج آن به نهاد نظارتی ارائه گردد.

۶,۴. توسعه فرهنگ حقوقی و تخصصی

علاوه بر اصلاحات ساختاری، فرهنگ‌سازی حقوقی و تخصصی در میان کارکنان بانکی و آگاهی‌بخشی به عموم مشتریان از حقوق خود و اهمیت حفاظت از داده‌ها نیز از دیگر ضروریات است. توسعه دانش تخصصی در حوزه حقوق فناوری اطلاعات در نهادهای قضایی و نظارتی، برای رسیدگی مؤثر به دعاوی پیچیده نقض داده‌ها، امری حیاتی است. آموزش مستمر و تخصصی به کارکنان بانک‌ها در مورد الزامات حفظ محرمانگی و یکپارچگی داده‌ها باید به عنوان یک تعهد سازمانی تعریف شود. توجه به استانداردهای بین‌المللی و تجربه کشورهای پیشرو، می‌تواند راهگشای رفع بسیاری از مشکلات حقوقی و اجرایی در ایران باشد.

در نهایت، می‌توان گفت نظام حقوقی ایران در زمینه حمایت از داده‌های شخصی در بانکداری برخط با چالش‌های اساسی مواجه است که پیامد آن، کاهش اعتماد کاربران، افزایش ریسک‌های امنیتی و اهداف ناقص سیاست‌های پولی و بانکی است. تطابق قوانین با استانداردهای بین‌المللی و تقویت ضمانت‌های اجرایی و فناوری، علاوه بر اصلاحات فنی، لازمه تضمین امنیت و حاکمیت مؤثر داده‌ها در نظام بانکی دیجیتال کشور است.

۷. نتیجه‌گیری و پیشنهادات

پژوهش حاضر با تحلیل تطبیقی چالش‌های حقوقی و اجرایی حفاظت از داده‌های شخصی در نظام بانکداری برخط ایران در قیاس با الزامات مقررات عمومی حفاظت از داده اتحادیه اروپا، به این نتیجه کلیدی دست یافت که نظام حقوقی ایران با شکاف‌های ساختاری بنیادین در سه حوزه تقنینی، نظارتی و فنی مواجه است. این خلأها، حمایت مؤثر از حقوق ذینفعان داده‌ها و اصول بنیادین حفظ حریم خصوصی را در معرض تهدید جدی قرار داده است.

جمع‌بندی یافته‌ها

۱. خلأ تقنینی در تفکیک مسئولیت‌ها: فقدان قانون جامع و مستقل، منجر به ابهام در تعریف مفاهیم بنیادین حقوق داده از جمله مسئولیت تفکیک‌شده کنترل‌کننده و پردازشگر و نبود ضمانت اجرایی برای حقوق کلیدی مشتریان، به‌ویژه حق انتقال‌پذیری داده‌ها شده است
۲. ناکارآمدی نظارت و ضمانت اجرا: ضعف در ساختار نظارتی (تشتت صلاحیت میان نهادها) و فقدان یک نهاد نظارتی مستقل تخصصی همراه با ضمانت اجراهای مالی بازدارنده و متناسب، موجب شده است که اصل پاسخگویی بانک‌ها تضعیف شده و هزینه نقض قانون برای مؤسسات مالی بسیار کمتر از هزینه اجرای آن باشد

۳. چالش‌های نوظهور فناوری: نظام حقوقی ایران در مواجهه با پردازش کلان‌داده‌ها و هوش مصنوعی دچار سردرگمی است و فاقد مقررات صریح برای مقابله با تبعیض الگوریتمی و تضمین حق اعتراض و حق توضیح در فرآیندهای تصمیم‌گیری کاملاً خودکار در بانکداری است
۴. این یافته‌ها نشان می‌دهد که سیاست‌های حقوقی موجود در ایران، به دلیل عدم انطباق با سرعت تحولات دیجیتال و استانداردهای بین‌المللی، زمینه‌ساز کاهش اعتماد عمومی به خدمات بانکداری دیجیتال و افزایش ریسک‌های امنیتی و حقوقی در فضای سایبری کشور شده است.

پیشنهادهای ساختاری و اجرایی

- با عنایت به تحلیل‌های تطبیقی صورت گرفته و به منظور رفع چالش‌های فوق‌الذکر، اتخاذ تدابیر اصلاحی زیر در نظام حقوقی و اجرایی ایران ضروری است:
- اصلاحات تقنینی (تصویب قانون جامع و هماهنگ):
 - تصویب قانونی جامع و هماهنگ مبتنی بر اصول بین‌المللی حقوق داده، با تأکید بر شفاف‌سازی کامل حقوق دینفعان (از جمله حق انتقال‌پذیری و حق اعتراض)
 - تغییر رویکرد در رضایت‌گیری، با الزام به اخذ رضایت آگاهانه، صریح و مشخص و تعریف شفاف ضوابط پردازش قانونی داده‌ها برای بانک‌ها
 - تقویت ساختار نظارتی (استقلال و تخصص):
 - ایجاد نهاد ناظر مستقل و تخصصی با قدرت اجرایی و نظارتی کافی (مشابه نهادهای نظارتی اروپا) که صلاحیت انحصاری رسیدگی به شکایات و اعمال جریمه‌های متناسب و بازدارنده را دارا باشد
 - الزام به گزارش‌دهی نقض داده به نهاد نظارتی و مشتریان متأثر در یک بازه زمانی محدود (مانند ۷۲ ساعت)، به منظور افزایش شفافیت و پاسخگویی
 - الزامات فنی و فناورانه (حریم خصوصی در طراحی):
 - الزام بانک‌ها به رعایت حداقل استانداردهای امنیت داده (مانند رمزنگاری قوی، کنترل دسترسی و ذخیره‌سازی نام مستعار)
 - نهادینه کردن اصل طراحی مبتنی بر حریم خصوصی و ارزیابی اثرات حریم خصوصی برای تمامی محصولات و خدمات بانکی جدید که شامل پردازش داده‌های حساس هستند
 - تدوین ضوابط مشخص برای استفاده از هوش مصنوعی و پردازش خودکار، با تضمین حق توضیح و حق اعتراض برای مشتریان
 - تضمین حقوقی و آموزش:
 - تقویت ضمانت‌های اجرایی کیفری و مدنی با تعیین سقف جریمه‌های متناسب با ریسک و سودآوری بانک‌ها
 - آموزش تخصصی قضات و مدیران بانکی در زمینه حقوق داده، الزامات فنی امنیتی و رویه‌های حقوقی بین‌المللی
- بهبود تدابیر حقوقی و فنی یادشده می‌تواند با جبران خلأهای حقوقی در مواجهه با فناوری‌های نوین، اعتماد شهروندان را به بانکداری دیجیتال تقویت کرده و زمینه رشد پایدار و رقابتی خدمات مالی در کشور را فراهم سازد.

۸. پیشنهاد مطالعات آتی

با توجه به ماهیت پویا و تحول‌آفرین فناوری‌های نوین در بانکداری، انجام پژوهش‌های آتی در حوزه‌های زیر می‌تواند زمینه‌ساز تعمیق هرچه بیشتر مطالعات حقوقی در ایران باشد:

- * مطالعه تطبیقی در خصوص نحوه اجرای حق توضیح در تصمیمات خودکار هوش مصنوعی در نظام‌های حقوقی پیشرو (مانند اتحادیه اروپا و کانادا) و ارائه الگوی بومی‌سازی
- * پژوهش در ساختار نهادهای نظارتی مستقل داده‌ها، با تمرکز بر مدل‌های تأمین مالی و استقلال اجرایی در کشورهای دارای تجربه موفق، برای ارائه مدل مطلوب در ایران
- * بررسی تأثیر حقوقی فناوری بلاکچین و دفتر کل توزیع شده بر حریم خصوصی و امنیت داده‌های بانکی و تبیین الزامات قانونی مربوطه در نظام حقوقی ایران
- * تحلیل محدودیت‌ها و فرصت‌های استفاده از تکنیک‌های ناشناس‌سازی پیشرفته در محیط کلان‌داده‌های بانکی با هدف حفظ محرمانگی و تسهیل تحلیل داده‌ها

منابع فارسی

- ۱_ احمدوند، بهناز (۱۴۰۲) بررسی مقایسه‌ای قواعد حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا در نظام‌های حقوقی منتخب. پژوهشگاه نظام‌های حقوقی ایران.
- ۲_ استا، محمدرضا، شهبازی نیا، مرتضی، پارسا پور، محمدباقر (۱۴۰۴) معیارهای شناسایی نقش سکوها‌های معاملاتی اینترنتی؛ مطالعه تطبیقی حقوق ایران و اتحادیه اروپا، فصلنامه پژوهش‌های حقوق تطبیقی.
- ۳_ اصغری، مهدی، رضایی، سارا، احمدی، علی (۱۴۰۴) طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور. فصلنامه پژوهش‌های مدیریت فناوری اطلاعات دانشگاه تهران.
- ۴_ رزم‌آرا، احمدرضا (۱۳۹۹) مسئولیت مدنی ارائه‌دهندگان خدمات الکترونیکی. تهران: انتشارات سمت.
- ۵_ زرکلام، ستار (۱۳۸۶) حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا). فصلنامه پژوهش حقوق عمومی (دانشگاه علامه طباطبائی)، دوره ۸، شماره ۲۵.
- ۶_ زرکلام، ستار (۱۳۹۰) حقوق تجارت الکترونیک: همراه با تحلیل قانون تجارت الکترونیکی ایران. ترجمه پروفسور زویه لینان دو بلفون. تهران: موسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
- ۷_ قانون تجارت الکترونیک جمهوری اسلامی ایران. مصوب ۱۳۸۲/۱۰/۱۷.
- ۸_ قوانین جرایم رایانه‌ای و قانون مسئولیت مدنی ایران. ۱۳۸۸.
- ۹_ خورشیدوند، ایمان (۱۳۹۹) حمایت حقوقی از داده‌های شخصی در بانکداری برخط. پایان‌نامه کارشناسی ارشد حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس.
- ۱۰_ لایحه صیانت از داده‌های شخصی. لایحه پیشنهادی صیانت و حمایت از داده‌های شخصی و حریم خصوصی.
- ۱۱_ مرتضوی، سیدمرتضی؛ خدائی فام، حجت. (۱۴۰۳) بررسی آثار به کارگیری هوش مصنوعی بر حریم خصوصی اشخاص و مسئولیت مدنی ناشی از آن. نورمگز.
- ۱۲_ وزارت ارتباطات و فناوری اطلاعات ایران (۱۴۰۴) پیش‌نویس لایحه حمایت از داده و حریم خصوصی در فضای مجازی

منابع انگلیسی

۱. "Al-Zaben, N., Lee, Y., Onik, H. M., Kim, S. C., & Yang, J.", 2018, General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management. IEEE Access.
۲. "Chambers, S.", 2004, "Behind Closed Doors", Publicity, Secrecy, And The Quality Of Deliberation. Journal Of Political Philosophy, Vol. 12, Issue 4, 488-502."
۳. GDPR, 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
۴. "Kilonzo, K. D.", 2007, "An Analysis of the Legal Challenges Posed by Electronic Banking. Keyna Law Review, Vol. 1."
۵. "Wachter, S., Mittelstadt, B., & Russell, C.", 2017, "Why Fairness Cannot Be Left to Algorithms: The Role of Social Context in Algorithmic Decision-Making." Harvard Law Review, 130(10), 1-45."
۶. Zarsky, Z. T., 2017, "Incompatible: The GDPR in the Age of Big Data. Fordham Law Review, Vol. 47:995, 1007-1030".

Limitations of the Iranian legal system in protecting personal data in online banking; A comparative study with the accountability requirements in the European Union General Data Protection Regulation

Abstract

Online banking, as a key innovation in financial systems, processes vast amounts of sensitive personal data of customers. Protecting these data legally is a complex challenge from both technological and legal perspectives. This article comparatively examines the legal frameworks of Iran and the European Union (General Data Protection Regulation - GDPR), analyzes the governing principles of data processing, challenges, and legislative gaps in the Iranian banking system. Moreover, the enforcement mechanisms for personal data breaches are reviewed emphasizing the approaches of both legal systems. The findings reveal that the lack of comprehensive legal structure and the necessity to strengthen effective enforcement are the main obstacles for efficient data protection, and recommendations are provided to improve policies and legislation.

Keywords

Online banking, personal data, legal protection, General Data Protection Regulation (GDPR), civil liability
