فصلنامه علمی مطالعات حقوق و علوم قضایی
Journal of Law and Judicial Studies
سال دوم، شماره ۴، تابستان ۱۴۰۴، ۴۶۸-۴۵۲
http://www.Ljournal.ir

# تحلیل حقوقی جرایم سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین: ارائه چارچوب D.R.A.C.O برای مقابله با تهدیدات

عارف بخشی [۱]

تاریخ دریافت: ۱۴۰۴/۰۲/۰۱ تاریخ چاپ: ۱۴۰۴/۰۶/۱۱

**چکیده**

در سال‌های اخیر، پلتفرم‌های سرمایه‌گذاری آنلاین در ایران با رشد قابل‌توجهی مواجه بوده‌اند، اما هم‌زمان چالش‌های جدی در زمینه حفاظت از داده‌های مالی کاربران نیز بروز یافته است. این تحقیق با هدف تحلیل حقوقی سوءاستفاده از داده‌های مالی کاربران و بررسی خلأهای قانونی موجود در این حوزه انجام شده است. روش تحقیق، ترکیبی از تحلیل تطبیقی قوانین بین‌المللی نظیر GDPR اروپا و CCPA آمریکا مطالعات موردی و مصاحبه با ۳۰ متخصص حقوقی و فنی بوده است.نتایج نشان می‌دهد که قوانین فعلی ایران در زمینه حفاظت از داده‌های مالی کاربران، از نظر تعریف مفاهیم، ضمانت‌های اجرایی و پوشش فناوری‌های نوین مانند هوش مصنوعی و بلاک‌چین ناکارآمد هستند. ضعف نهادهای نظارتی نیز این مشکل را تشدید کرده است. در پاسخ به این چالش‌ها، چارچوب نوآورانه‌ای با عنوان D.R.A.C.O (تعریف–رصد–ارزیابی–جبران–به‌روزرسانی) پیشنهاد شده است که شامل پنج محور کلیدی است: تعریف دقیق داده‌های مالی، رصد مداوم تراکنش‌ها، ارزیابی ریسک‌های قانونی و فنی، جبران خسارت از طریق صندوق بیمه سایبری، و به‌روزرسانی قوانین و آموزش‌های مرتبط.همچنین، ایجاد نهاد مستقل حفاظت از داده‌های مالی با عنوان IFDPA، اصلاح قوانین جرایم سایبری، و راه‌اندازی صندوق بیمه سایبری به‌عنوان اقدامات تکمیلی پیشنهاد شده‌اند. این اقدامات با هدف ارتقاء امنیت داده‌های مالی، تقویت اعتماد عمومی و فراهم‌سازی زیرساخت‌های قانونی و نهادی برای توسعه پایدار صنعت فین‌تک ایران طراحی شده‌اند. پژوهش حاضر با ارائه چارچوب D.R.A.C.O و راهکارهای اجرایی، گامی مهم در جهت بهبود سیاست‌گذاری و تنظیم‌گری در فضای دیجیتال مالی ایران به‌شمار می‌رود.

**واژگان کلیدی**

حفاظت از داده‌های مالی، پلتفرم‌های سرمایه‌گذاری آنلاین،چارچوبD.R.A.C.O ، نهاد نظارتی مستقل(IFDPA) ، جرایم سایبری و مقررات حریم خصوصی

[۱] دانشجوی کارشناسی ارشد جزا و جرم شناسی، گروه حقوق، دانشکده حقوق، دانشگاه آزاد اسلامی، رفسنجان، ایران.

**مقدمه**

با افزایش استفاده از فناوری‌های نوین مانند هوش مصنوعی و بلاک‌چین در این پلتفرم‌ها، تهدیدات سایبری نیز پیچیده‌تر شده‌اند. سوءاستفاده‌هایی نظیر فروش غیرمجاز داده‌ها به شرکت‌های تبلیغاتی، کلاهبرداری‌های الگوریتمی، یا دستکاری الگوهای سرمایه‌گذاری، به‌وضوح نشان می‌دهند که چارچوب‌های قانونی موجود در ایران، توان کافی برای مقابله با این نوع تهدیدات را ندارند. عدم وجود تعریف جامع از "داده مالی"، نبود سازوکارهای الزام‌آور برای گزارش‌دهی نقض‌های امنیتی، و فقدان نهاد نظارتی مستقل، تنها بخشی از مشکلات ساختاری هستند که بر ضرورت بازنگری جدی در سیاست‌گذاری‌های حاکم بر این حوزه تأکید دارند(کرمی، ۱۴۰۴) .پژوهش حاضر، به‌عنوان نخستین مطالعه جامع در سطح ملی، به بررسی عمیق این چالش‌ها پرداخته و تلاش کرده است تا ضمن شناسایی شکاف‌های قانونی و اجرایی موجود، راهکارهایی نوآورانه برای ارتقاء سطح حفاظت از داده‌های مالی کاربران ارائه دهد. یکی از مهم‌ترین دستاوردهای این پژوهش، طراحی و ارائه چارچوبی جامع با عنوان D.R.A.C.Oاست. این چارچوب، که به‌طور خاص برای مقابله با سوءاستفاده‌های داده‌ای در بستر پلتفرم‌های سرمایه‌گذاری آنلاین طراحی شده، شامل پنج مرحله کلیدی است :تعریف دقیق داده‌های مالی، رصد و نظارت مداوم، ارزیابی ریسک‌های قانونی و فنی، جبران خسارات مالی از طریق صندوق بیمه سایبری، و به‌روزرسانی مداوم قوانین و آموزش‌ها.چارچوب D.R.A.C.O رویکردی تلفیقی و میان‌رشته‌ای دارد که هم‌زمان ابعاد حقوقی و فنی حفاظت از داده‌ها را در نظر می‌گیرد. این مدل، علاوه‌بر ارائه سازوکارهای پاسخگویی سریع از جمله الزام به گزارش‌دهی ۷۲ ساعته موارد نقض امنیتی، بر جبران مالی قربانیان از طریق ابزارهایی مانند صندوق بیمه سایبری تأکید دارد؛ موضوعی که تاکنون کمتر در سیاست‌گذاری‌های داخلی به آن پرداخته شده است. همچنین با هدف ارتقاء کارآمدی نظارت و پاسخگویی، پژوهش حاضر پیشنهاد تأسیس نهاد مستقلی با عنوان IFDPA (Independent Financial Data Protection Authority)را مطرح می‌کند. این نهاد، با الگوبرداری از تجربه‌های موفق جهانی نظیر GDPRاتحادیه اروپا و CCPAایالات متحده، می‌تواند مرجع اصلی نظارت، تدوین دستورالعمل‌ها، و اجرای مقررات مربوط به حفاظت از داده‌های مالی در ایران باشد(اردبیلی، ۱۳۸۶).از دیگر جنبه‌های نوآورانه این تحقیق، تأکید بر به‌کارگیری فناوری‌های نوین در خدمت شناسایی و پیشگیری از تهدیدات سایبری است. هوش مصنوعی می‌تواند در تحلیل رفتارهای تراکنشی مشکوک، شناسایی الگوهای کلاهبرداری و پیش‌بینی حملات سایبری نقشی کلیدی ایفا کند.( اباذری، ۱۴۰۳) همچنین، استفاده از بلاک‌چین در رمزنگاری تراکنش‌ها و جلوگیری از دستکاری داده‌ها، می‌تواند ضریب اطمینان کاربران را به طرز چشمگیری افزایش دهد. در این راستا، پژوهش حاضر پیشنهادهایی عملی برای یکپارچه‌سازی این فناوری‌ها با چارچوب‌های قانونی ارائه کرده است.ضرورت این پژوهش از آنجا ناشی می‌شود که خلأهای قانونی و ضعف در نظارت مؤثر، نه‌تنها امنیت کاربران را به خطر انداخته، بلکه اعتماد عمومی به پلتفرم‌های داخلی را نیز متزلزل کرده است. در صورت تداوم این روند و نبود اصلاحات ساختاری، احتمالاً شاهد مهاجرت سرمایه‌گذاران به پلتفرم‌های خارجی، کاهش مشارکت عمومی در بازارهای دیجیتال داخلی و در نهایت آسیب‌پذیری جدی اقتصاد دیجیتال کشور خواهیم بود. از این‌رو، تحقیق پیش‌رو با نگاهی آینده‌نگر، به دنبال آن است تا مبنایی برای بازنگری در سیاست‌گذاری‌ها و تدوین مقررات نوین در حوزه داده‌های مالی باشد.در مجموع، این پژوهش با طراحی مدلD.R.A.C.O ، تحلیل تطبیقی مقررات بین‌المللی، و ارائه پیشنهاداتی برای اصلاح نظام نظارتی و قانون‌گذاری، گامی مؤثر در جهت ارتقاء امنیت داده‌های مالی در فضای فین‌تک ایران برداشته

است. امید است نتایج این تحقیق بتواند در تدوین سیاست‌های ملی، ارتقاء سطح آگاهی فعالان این حوزه، و توسعه چارچوب‌های حفاظت از داده در آینده نزدیک مورد استفاده قرار گیرد.

## مبانی نظری و چارچوب‌های قانونی در سطح بین‌المللی

GDPR (General Data Protection Regulation)

GDPR که در سال ۲۰۱۶ توسط اتحادیه اروپا به تصویب رسید، یکی از جامع‌ترین و سخت‌گیرانه‌ترین مقررات جهانی در زمینه حفاظت از داده‌های شخصی است. این مقررات شامل قوانین ویژه‌ای برای داده‌های مالی است که به‌طور خاص از حقوق کاربران برای کنترل و دسترسی به داده‌های شخصی‌شان حفاظت می‌کند.( سوتیل، پیلو، تیلور، ۱۳۸۸). یکی از نکات برجسته این قانون، لزوم گزارش‌دهی هرگونه نقض داده‌ها ظرف ۷۲ ساعت است که می‌تواند به‌طور مستقیم بر حفاظت از داده‌های مالی تأثیر بگذارد.( Daoud, 2023 ) GDPR همچنین حق درخواست حذف داده‌ها (حق فراموشی) و حق انتقال داده‌ها را برای کاربران تضمین می‌کند که از دیدگاه حقوقی، از نظر عملیاتی می‌تواند به حفاظت بهتر از داده‌های مالی کمک کند.( افراسیابی، ۱۴۰۳)

CCPA (California Consumer Privacy Act)

CCPA که در ایالات متحده و به‌ویژه در کالیفرنیا به تصویب رسید، از قوانین مهم دیگر در زمینه حفاظت از داده‌های شخصی است. این قانون به کاربران کالیفرنیا این امکان را می‌دهد که اطلاعات شخصی خود را به‌طور کامل کنترل کنند و حتی از فروش داده‌هایشان به شرکت‌های ثالث جلوگیری کنند.(Muammar, Shehada, Mansoor, 2023 ) CCPA علاوه بر این که به کاربران این امکان را می‌دهد که داده‌های خود را مشاهده کنند، حق دریافت غرامت به ازای هر نقض داده‌ها را نیز فراهم کرده است.( جعفری، ۱۳۹۳)

PIPL (Personal Information Protection Law) چین

چین در سال ۲۰۲۱ قانون حفاظت از داده‌های شخصی (PIPL) را تصویب کرد که به‌طور مشابه با GDPR اروپا و CCPA ایالات متحده به حفاظت از داده‌های شخصی و مالی کاربران پرداخته است. این قانون شامل جریمه‌های سنگین برای نقض داده‌ها و الزامات ویژه برای کسب‌وکارها و پلتفرم‌های آنلاین است. به‌ویژه در بخش داده‌های مالی، این قانون از شرکت‌ها می‌خواهد که اطلاعات مالی کاربران را تنها در صورت رضایت صریح جمع‌آوری کنند.( سیداصفهانی، ۱۳۹۲).

## قانون جرایم رایانه‌ای ایران (۱۳۸۸)

در ایران، قانون جرایم رایانه‌ای که در سال ۱۳۸۸ به تصویب رسید، به‌طور کلی به سوءاستفاده‌های رایانه‌ای و نقض حریم خصوصی در فضای مجازی پرداخته است. این قانون که عمدتاً به جرایم سایبری مانند هک کردن، نفوذ به سیستم‌های رایانه‌ای، و دزدی اطلاعات شخصی می‌پردازد، هنوز نتواسته است به‌طور خاص و دقیق به مسائل داده‌های مالی پرداخته و آن‌ها را به‌طور مستقل جرم‌انگاری کند. در این قانون، داده‌های شخصی به‌طور کلی مورد توجه قرار گرفته است، اما تعریف دقیق و شفافی از داده‌های مالی در آن وجود ندارد که این یکی از چالش‌های اصلی در حقوق ایران برای مقابله با سوءاستفاده از داده‌های مالی به شمار می‌آید(فرجی ها، ۱۳۸۸)..در حال حاضر، لایحه‌ای تحت عنوان لایحه حریم خصوصی در ایران در دست بررسی است که به‌طور خاص به مسائل مربوط به حفاظت از داده‌های شخصی و مالی می‌پردازد. این لایحه، در صورت تصویب، ممکن است باعث ایجاد شفافیت بیشتری در زمینه حفاظت از داده‌های مالی

کاربران و سوءاستفاده‌های ناشی از آن‌ها شود. این لایحه همچنین برخی از حقوق کاربران را برای کنترل داده‌های خود مشخص می‌کند، اما هنوز بخش‌های زیادی از آن نیاز به بازنگری دارد.( انصاری، ۱۴۰۰)

## چالش‌های اجرایی و حقوقی در ایران

### عدم تعریف دقیق «داده مالی»

یکی از مشکلات اصلی در قوانین ایران، عدم تعریف دقیق «داده مالی» در قوانین است. در حالی که GDPR و CCPA به‌طور خاص داده‌های مالی را در قالب قوانین خود گنجانده و برای آن‌ها حفاظت‌های ویژه‌ای در نظر گرفته‌اند، قوانین ایران هنوز تعریفی دقیق از این نوع داده‌ها ندارند. این ابهام باعث می‌شود که در هنگام نقض داده‌ها، فرآیندهای حقوقی و اجرایی پیچیده‌تر شود.به‌رغم وجود نهادهای نظارتی مختلف در ایران، نظیر پلیس فتا، سازمان بورس، و مرکز ملی فضای مجازی، نظارت و هماهنگی میان این نهادها ضعیف است. نبود یک نهاد نظارتی مستقل و قوی برای نظارت بر پلتفرم‌های سرمایه‌گذاری آنلاین و داده‌های مالی کاربران یکی از چالش‌های اصلی در این زمینه است. این پژوهش به این موضوع پرداخته و پیشنهاد می‌دهد که یک نهاد نظارتی مستقل (IFDPA) برای نظارت بر پلتفرم‌های فین‌تک ایجاد شود. آموزش‌های حقوقی و فنی در خصوص حفاظت از داده‌های مالی هنوز در ایران به‌طور جدی و گسترده در دسترس نیست. قضات، وکلا، و حتی مدیران پلتفرم‌های آنلاین باید به‌طور مداوم در زمینه قوانین و تکنولوژی‌های جدید آموزش ببینند. نبود چنین آموزش‌هایی، فرآیند اجرایی در رسیدگی به نقض‌های داده‌ای را پیچیده‌تر می‌کند و منجر به عدم کارآیی در مقابله با تهدیدات سایبری می‌شود. (تقوی فرد، تقوا، فقیهی، جمشیدی، ۱۴۰۳)

### پیشینه پژوهش

تحلیل حقوقی جرایم مرتبط با سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین از جمله مباحثی است که با رشد روزافزون فناوری‌های دیجیتال و گسترش فعالیت‌های فین‌تک، به‌ویژه در دهه اخیر، به یکی از دغدغه‌های جدی نظام‌های حقوقی و سیاست‌گذاران در سطح جهانی تبدیل شده است. در ادبیات بین‌المللی، موضوع حفاظت از داده‌های مالی در بستر دیجیتال، به‌ویژه در زمینه سرمایه‌گذاری آنلاین، تحت مفاهیمی چون «حریم خصوصی دیجیتال»، «امنیت داده‌های حساس مالی» و «پاسخگویی قانونی به نقض‌های امنیتی» مورد توجه قرار گرفته و نهادهای نظارتی و قانون‌گذار تلاش کرده‌اند تا با تصویب مقررات جامع، چارچوب‌های حفاظتی مؤثری را تدوین کنند.در سطح بین‌المللی، مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا موسوم به GDPR (General Data Protection Regulation)از سال ۲۰۱۸ به‌عنوان یکی از کامل‌ترین قوانین مربوط به حریم خصوصی دیجیتال شناخته می‌شود. این مقررات نه‌تنها داده‌های مالی را در زمره داده‌های حساس طبقه‌بندی می‌کند، بلکه پلتفرم‌های خدمات مالی آنلاین را ملزم به دریافت رضایت آگاهانه، تضمین امنیت داده‌ها، امکان انتقال امن اطلاعات و گزارش‌دهی فوری در صورت بروز نقض‌های امنیتی (معمولاً در بازه ۷۲ ساعته) کرده است. همچنین، قانون CCPA (California Consumer Privacy Act)در ایالات متحده، به‌عنوان یک چارچوب ایالتی، بر حقوق مصرف‌کننده نسبت به داده‌های شخصی‌اش تأکید دارد و به کاربران اجازه می‌دهد تا کنترل بیشتری بر داده‌های مالی و تراکنشی خود داشته باشند.پژوهش‌های متعددی در این زمینه صورت گرفته‌اند که از جمله آن‌ها می‌توان به مطالعه‌ی Solove (2019) اشاره کرد که در آن، ریسک‌های حقوقی ناشی از جمع‌آوری و ذخیره‌سازی داده‌های مالی کاربران توسط پلتفرم‌ها بررسی شده و ضرورت وجود سازوکارهای پاسخگویی و جبران خسارت مورد تأکید قرار گرفته است. همچنین،

Zarsky (2020)در پژوهشی دیگر به اهمیت شفاف‌سازی مسئولیت پلتفرم‌ها در برابر کاربران و طراحی ساختارهای قانونی چندلایه برای مقابله با تهدیدات نوین، از جمله سوءاستفاده‌های مبتنی بر الگوریتم، پرداخته است.از منظر فنی نیز پژوهشگران به بررسی نقش فناوری‌های نوین مانند بلاک‌چین و هوش مصنوعی در حفاظت از داده‌های مالی پرداخته‌اند. به‌عنوان نمونه، Chen & Zhao (2021)در مطالعه‌ای پیرامون کاربرد بلاک‌چین در تضمین امنیت داده‌های مالی، بر توانایی این فناوری در کاهش تقلب و بهبود قابلیت ردیابی داده‌های حساس تأکید کرده‌اند.در ایران، موضوع حفاظت از داده‌های مالی در بستر دیجیتال به‌ویژه در حوزه سرمایه‌گذاری آنلاین، تا همین اواخر کمتر مورد توجه قرار گرفته بود. بیشتر قوانین موجود مانند قانون جرایم رایانه‌ای ۱۳۸۸ قانون تجارت الکترونیکی ۱۳۸۲، و قانون حمایت از حقوق مصرف‌کننده به‌طور عمومی به موضوع جرایم سایبری و حریم خصوصی پرداخته‌اند اما فاقد توجه خاص به داده‌های مالی حساس در حوزه سرمایه‌گذاری هستند.مطالعات محدودی در سال‌های اخیر در این حوزه صورت گرفته‌اند. به‌عنوان مثال، حسینی‌نژاد ۱۳۹۹در مقاله‌ای به بررسی خلأهای قانونی در برخورد با جرایم سوءاستفاده از داده‌های بانکی کاربران پرداخت و پیشنهاد ایجاد یک نهاد نظارتی مستقل برای حفاظت از داده‌های مالی را مطرح کرد .محمدی و رجبی ۱۴۰۰ نیز در تحقیقی تطبیقی به مقایسه چارچوب قانونی ایران و اتحادیه اروپا در حوزه حریم خصوصی مالی پرداختند و نشان دادند که قوانین ایران فاقد تعاریف جامع، ضمانت‌های اجرایی مشخص و نهاد ناظر یکپارچه برای پاسخ‌گویی به نقض داده‌های مالی هستند.با این حال، آنچه در بیشتر این پژوهش‌ها مشهود است، نبود رویکردی ساختاریافته و یکپارچه برای مقابله با سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین است. تاکنون چارچوبی جامع که بتواند در سطح عملیاتی به این مسئله بپردازد و قابلیت اجرا در سیستم حقوقی ایران را داشته باشد، پیشنهاد نشده است.پژوهش حاضر با هدف پر کردن این خلأ، برای نخستین‌بار در ایران، چارچوبی جامع و کاربردی با عنوان D.R.A.C.Oارائه کرده که برگرفته از رویکردی میان‌رشته‌ای (حقوقی – فناورانه) است. این چارچوب، ضمن تبیین مراحل پنج‌گانه شامل تعریف، رصد، ارزیابی، جبران و به‌روزرسانی مستمر، تلاش می‌کند تا ابعاد مختلف مسئله را از زاویه‌ای ترکیبی بررسی و برای آن راهکارهای اجرایی ارائه دهد.در واقع، در حالی که بیشتر پژوهش‌های پیشین، یا تمرکز خود را بر تحلیل مقررات حقوقی قرار داده‌اند و یا جنبه‌های فنی مسئله را مورد بررسی قرار داده‌اند، این تحقیق تلاش کرده است تا بین این دو بعد پیوندی منسجم ایجاد کند. افزون بر آن، پیشنهاد تشکیل نهاد IFDPAبه‌عنوان مرجع مستقل نظارت بر داده‌های مالی، الگوبرداری از تجربه‌های موفق بین‌المللی بوده که در ادبیات داخلی سابقه‌ای نداشته است.همچنین، ورود به مسئله کاربرد فناوری‌هایی نظیر هوش مصنوعی برای کشف الگوهای مشکوک در تراکنش‌ها، و پیشنهاد سازوکارهایی نظیر صندوق بیمه سایبری برای جبران خسارات کاربران، از جمله ابعاد تازه‌ای هستند که این پژوهش را از مطالعات پیشین متمایز می‌سازند. درواقع، مدل D.R.A.C.O نه‌تنها چارچوبی نظری، بلکه یک نقشه‌راه عملی برای مقابله با تهدیدات سوءاستفاده از داده‌های مالی در ایران ارائه می‌کند.در مجموع، بررسی پیشینه داخلی و بین‌المللی نشان می‌دهد که گرچه در سطح جهانی تلاش‌هایی برای قانون‌مند ساختن فضای دیجیتال و محافظت از داده‌های مالی صورت گرفته، اما نظام حقوقی ایران همچنان با چالش‌هایی بنیادین در این زمینه مواجه است. نبود تعریف روشن از داده مالی، ضعف ضمانت اجرا، عدم وجود نهاد نظارتی مستقل، و عدم تطبیق با فناوری‌های نوین، از جمله مهم‌ترین مشکلات موجود به‌شمار می‌آید.پژوهش حاضر، با ارائه چارچوب D.R.A.C.O و تحلیل تطبیقی تجارب جهانی، تلاشی نوین در جهت ارائه راهکاری عملی، بومی و مؤثر برای مقابله با جرایم سوءاستفاده از داده‌های

مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین در ایران به‌شمار می‌رود. این چارچوب می‌تواند مبنایی برای اصلاح قوانین، به‌روزرسانی نهادهای نظارتی و ارتقاء سطح امنیت سایبری کشور در حوزه مالی دیجیتال باشد.

## روش تحقیق

این پژوهش با اتخاذ رویکردی ترکیبی از روش‌های کیفی و کمّی بهره گرفته است تا تصویری چندلایه و جامع از مسئله سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین در ایران ارائه دهد. روش‌شناسی تحقیق در دو سطح «تحلیل نظری-حقوقی» و «ارزیابی تجربی و آماری» طراحی شده و مراحل آن بر اساس منطق تطبیقی و تحلیلی تنظیم گردیده است.در بخش کیفی، پژوهش ابتدا با تحلیل اسناد حقوقی آغاز شده و تمامی مقررات و قوانین مرتبط با داده‌های مالی، از جمله قانون جرایم رایانه‌ای (۱۳۸۸)، قانون تجارت الکترونیکی، و پیش‌نویس لایحه حریم خصوصی بررسی شده‌اند. تمرکز این تحلیل بر مفاهیمی چون تعریف داده مالی، ساختار نهادهای ناظر، ضمانت اجرا، و نقش مقامات قضایی و وکلا در رسیدگی به نقض داده‌ها بوده است. در ادامه، مطالعه موردی روی ۲۰ پرونده قضایی در حوزه جرایم سایبری (۱۴۰۰ تا ۱۴۰۲) انجام شده که مشتمل بر موارد نفوذ، فروش غیرقانونی داده و کلاهبرداری الگوریتمی بوده است.در بخش کمّی، داده‌ها از طریق پرسشنامه‌های آنلاین و مصاحبه‌های نیمه‌ساختاریافته با ۳۰ متخصص شامل ۱۵ قاضی، ۱۰ وکیل، و ۵ مدیر پلتفرم گردآوری شدند. برای تحلیل آماری داده‌ها از آزمون $\chi^2$ کای دو جهت سنجش رابطه بین نقض داده و کاهش اعتماد کاربران، و رگرسیون لجستیک برای پیش‌بینی اثر نقض‌ها بر میزان سرمایه‌گذاری استفاده شده است.همچنین، پژوهش با بهره‌گیری از تحلیل تطبیقی حقوقی، مقررات ایران را با اسناد بین‌المللی نظیر GDPRاتحادیه اروپا و CCPAایالات متحده مقایسه نموده است تا خلأهای ساختاری و حقوقی شناسایی و در چارچوب مدل پیشنهادی D.R.A.C.O رفع شود. این روش‌شناسی، امکان ارائه راهکارهایی مستند، کاربردی و مبتنی بر شواهد را فراهم کرده است

## مقایسه قوانین ایران با قوانین بین‌المللی

در این بخش، مقایسه دقیقی میان قوانین موجود در ایران و GDPR اتحادیه اروپا و CCPA ایالات متحده انجام شده است. این مقایسه به‌ویژه بر روی تعریف داده مالی، مجازات‌ها، حقوق کاربران و نهادهای نظارتی متمرکز است تا خلأهای موجود در قوانین ایران شناسایی شده و راهکارهای عملی برای هم‌راستا کردن قوانین ایران با استانداردهای بین‌المللی پیشنهاد گردد.

## تجزیه و تحلیل داده‌ها

برای تجزیه و تحلیل داده‌ها از نرم‌افزار SPSS استفاده شده است. داده‌های جمع‌آوری‌شده از مصاحبه‌ها، پرسشنامه‌ها و مطالعه پرونده‌ها در این نرم‌افزار وارد شده و سپس با استفاده از آزمون‌های آماری مختلف، روابط میان متغیرها تحلیل شده است. آزمون $\chi^2$: برای بررسی همبستگی میان نقض داده‌های مالی و کاهش اعتماد کاربران به پلتفرم‌ها و همچنین کاهش سرمایه‌گذاری در پلتفرم‌های آنلاین مورد استفاده قرار گرفته است. رگرسیون لجستیک: برای تحلیل رابطه میان تغییرات قوانین و میزان کاهش سوءاستفاده از داده‌ها در پلتفرم‌های سرمایه‌گذاری آنلاین استفاده شده است. این تحلیل به‌ویژه برای شناسایی تأثیر اصلاحات قانونی بر جلوگیری از نقض داده‌ها مؤثر است.این پژوهش با برخی محدودیت‌ها مواجه بوده است. یکی از مهم‌ترین محدودیت‌ها، دسترسی محدود به پرونده‌های محرمانه قضائی بوده است. علاوه بر این، داده‌های جمع‌آوری‌شده از طریق پرسشنامه‌ها و مصاحبه‌ها ممکن است تا حدودی تحت تأثیر نظرات شخصی افراد

قرار گرفته باشد. همچنین، محدودیت زمانی تحقیق باعث شده که تنها پرونده‌های قضائی مرتبط با جرایم سایبری از سال‌های اخیر بررسی شوند.

## چارچوب نظری D.R.A.C.O

چارچوب D.R.A.C.O از پنج مرحله اصلی تشکیل شده است که به‌طور مستقیم و مؤثر در راستای ارتقای حفاظت از داده‌های مالی کاربران و کاهش جرایم سایبری در پلتفرم‌های سرمایه‌گذاری آنلاین عمل می‌کند. در اینجا به بررسی دقیق‌تر و جزئیات بیشتر هر مرحله می‌پردازیم:

۱) D – Definition .تعریف دقیق داده مالی

تعریف دقیق «داده مالی» به‌عنوان اولین و مهم‌ترین مرحله در چارچوبD.R.A.C.O ، یکی از ارکان اصلی است که در آن تمام اطلاعاتی که به‌طور مستقیم یا غیرمستقیم با وضعیت مالی کاربر مرتبط است، شفاف و جامع تعریف می‌شود. این تعریف به منظور جلوگیری از سوءاستفاده از داده‌ها ضروری است و باید به‌طور کامل از داده‌های شخصی تفکیک شود.

جزئیات این مرحله:

- داده‌های مالی شامل تمامی اطلاعاتی است که به‌طور مستقیم به وضعیت مالی کاربر وابسته است. این داده‌ها عبارت‌اند از:
- اطلاعات حساب بانکی (مانند شماره حساب، شماره شبا، موجودی حساب)
- سوابق تراکنش‌ها (تاریخ، مبلغ، گیرنده/فرستنده)
- الگوهای سرمایه‌گذاری (سهم خریداری‌شده، زمان‌بندی معاملات، میزان ریسک پذیرفته‌شده)
- اطلاعات کارت‌به‌کارت و ابزارهای پرداخت الکترونیک

داده‌های ناشناس‌شده :در صورتی که داده‌ها به‌گونه‌ای تغییر داده شده باشند که امکان شناسایی هویت کاربران وجود نداشته باشد، این داده‌ها خارج از شمول «داده مالی» قرار می‌گیرند. این امر به‌ویژه در مواقعی که داده‌ها به‌صورت کلی و غیرشخصی جمع‌آوری می‌شوند، اهمیت دارد.

تعریف دقیق داده‌های مالی از نظر قانونی باعث می‌شود که در صورت بروز هرگونه سوءاستفاده، قابلیت پیگیری و شناسایی نقض‌ها افزایش یابد. این تعریف باید از تمامی داده‌های شخصی و غیرمالی تفکیک شود تا اطمینان حاصل شود که داده‌های غیرمرتبط با امور مالی تحت قوانین محافظت از داده‌ها قرار نمی‌گیرند.

۲) R – Real-time Monitoring .رصد و نظارت مستمر

برای جلوگیری از سوءاستفاده از داده‌های مالی کاربران، لازم است که پلتفرم‌ها از سیستم‌های هوش مصنوعی و الگوریتم‌های یادگیری ماشین استفاده کنند که قادر به شناسایی و رصد هرگونه فعالیت مشکوک به‌صورت لحظه‌ای باشند.

جزئیات این مرحله:

- نظارت لحظه‌ای بر تراکنش‌ها: استفاده از الگوریتم‌هایی که می‌توانند تراکنش‌های مشکوک یا رفتارهای غیرمعمول را شبیه‌سازی و شناسایی کنند. این الگوریتم‌ها باید به‌طور خودکار به محض شناسایی هرگونه فعالیت غیرعادی، هشدارهای فوری ارسال کنند.

- الگوهای مشکوک: سیستم‌های هوش مصنوعی می‌توانند الگوهای غیرطبیعی یا مشکوک در تراکنش‌ها را شناسایی کنند. به‌عنوان مثال، اگر یک کاربر شروع به انجام تراکنش‌های بزرگ با سرعت بالا کند، یا اگر الگوی معاملاتی او به‌طور ناگهانی تغییر کند، این موارد باید مورد بررسی قرار گیرند.
- بهبود الگوریتم‌ها: سیستم‌های رصد باید به‌طور مداوم آپدیت شوند تا با تهدیدات جدید هم‌راستا شوند. به‌ویژه با گسترش فناوری‌های نوینی مانند بلاک‌چین و هوش مصنوعی، باید از این ابزارها برای پیشگیری از نقض داده‌های مالی استفاده کرد.

رصد لحظه‌ای به پلتفرم‌ها این امکان را می‌دهد که به‌محض شناسایی هرگونه فعالیت مشکوک، اقدامات فوری انجام دهند و از بروز هرگونه سوءاستفاده جلوگیری کنند. این سیستم‌ها می‌توانند به‌طور مستقیم در کاهش زمان واکنش به تهدیدات سایبری و جلوگیری از خسارت‌های بیشتر کمک کنند.

۳) A – Assessment .ارزیابی ریسک حقوقی و فنی

برای اطمینان از رعایت استانداردهای امنیتی و حفظ داده‌های مالی، باید یک ارزیابی منظم و مستمر از وضعیت فنی و حقوقی پلتفرم‌ها انجام شود. این ارزیابی‌ها باید به‌طور دوره‌ای برای شناسایی آسیب‌پذیری‌ها و ریسک‌های موجود در سیستم‌های داده‌محور صورت گیرد.

جزئیات این مرحله:

ممیزی‌های امنیتی دوره‌ای: انجام ممیزی‌های فنی به‌منظور شناسایی آسیب‌پذیری‌های بالقوه در پلتفرم‌ها، به‌ویژه در سیستم‌های ذخیره‌سازی داده‌ها، سیستم‌های پردازش تراکنش و الگوریتم‌های امنیتی. این ارزیابی‌ها باید بر اساس استانداردهای بین‌المللی مانند ISO/IEC 27001 صورت گیرد.

ممیزی‌های حقوقی: بررسی تطابق پلتفرم‌ها با مقررات حفاظت از داده‌ها) مثل GDPR یا قوانین ملی (برای اطمینان از رعایت تمامی الزامات قانونی و حقوق کاربران. این بررسی‌ها می‌تواند شامل ارزیابی نحوه ذخیره، پردازش، انتقال و اشتراک‌گذاری داده‌های مالی کاربران باشد.

ارزیابی مستمر به پلتفرم‌ها این امکان را می‌دهد که پیش از بروز هرگونه نقض امنیتی، آسیب‌پذیری‌ها و ریسک‌ها شناسایی و اصلاح شوند. این ارزیابی‌ها می‌توانند نقشی کلیدی در جلوگیری از تهدیدات آینده ایفا کنند.

۴) C – Compensation .جبران خسارت و مسئولیت‌پذیری

در صورت نقض داده‌های مالی کاربران، باید یک سیستم برای جبران خسارت‌های واردشده به‌طور مؤثر ایجاد شود. این جبران خسارت می‌تواند از طریق ایجاد صندوق‌های بیمه سایبری یا مکانیسم‌های دیگر به‌منظور پوشش هزینه‌های کاربران آسیب‌دیده صورت گیرد.

جزئیات این مرحله:

صندوق بیمه سایبری مشترک: ایجاد صندوقی که مسئولیت جبران خسارت کاربران آسیب‌دیده را بر عهده گیرد. این صندوق می‌تواند منابع مالی لازم برای پوشش خسارت‌های کاربران از نقض‌های داده‌ای فراهم آورد. این صندوق باید به‌صورت مشترک توسط پلتفرم‌ها و دولت تأسیس شود.

دعوای جمعی :به‌منظور جبران خسارت‌های گسترده و افزایش دسترسی به عدالت، باید امکان اقامه دعوای جمعی برای کاربران فراهم شود. این اقدام به‌ویژه برای پلتفرم‌های بزرگ و با تعداد کاربران زیاد ضروری است.

این مرحله به‌ویژه در مواقعی که نقض داده‌های مالی گسترده است، می‌تواند به‌عنوان ابزاری برای جبران سریع و مؤثر خسارت‌های کاربران عمل کند و از این طریق به حفظ اعتماد عمومی به پلتفرم‌ها کمک کند.

۵) O – Ongoing Update .به‌روزرسانی مستمر قوانین و آموزش

باید قوانین و استانداردها به‌طور دوره‌ای به‌روزرسانی شوند تا با تحولات فناوری و تهدیدات جدید همگام شوند. علاوه بر این، آموزش‌های مداوم برای قضات، وکلا و مدیران پلتفرم‌ها در زمینه قوانین جدید و نحوه برخورد با تهدیدات سایبری ضروری است.

جزئیات این مرحله:

بازنگری مستمر قوانین: قوانین باید به‌طور دوره‌ای به‌روزرسانی شوند تا با تغییرات فناوری و تهدیدات جدید همخوانی داشته باشند. این بازنگری‌ها باید توسط نهادهای نظارتی و قانونی انجام شود.

دوره‌های آموزشی برای قضات، وکلا و مدیران پلتفرم‌ها: برگزاری دوره‌های آموزشی برای افزایش آگاهی حقوقی و فنی افراد مرتبط با داده‌های مالی. این آموزش‌ها باید بر اساس آخرین تغییرات قوانین و فناوری‌های نوین طراحی شوند.

این مرحله به‌منظور ارتقای سطح آگاهی و مسئولیت‌پذیری افراد در سیستم‌های قانونی و فنی طراحی شده است. به‌ویژه با گسترش تکنولوژی‌های نوین مانند هوش مصنوعی، لازم است که افراد مرتبط با داده‌ها به‌طور مستمر آموزش‌های جدیدی دریافت کنند.چارچوب D.R.A.C.O یک مدل جامع و نوآورانه برای مقابله با سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین است که به‌طور کامل به تمامی ابعاد حقوقی و فنی این تهدیدات پرداخته است. پیاده‌سازی این چارچوب می‌تواند به‌طور قابل‌توجهی میزان تهدیدات سایبری را کاهش داده و از داده‌های مالی کاربران به‌طور مؤثری محافظت کند. این چارچوب نیازمند همکاری و مشارکت بین نهادهای دولتی و پلتفرم‌ها است و به‌ویژه نیازمند اصلاح قوانین و ایجاد نهادهای نظارتی مستقل مانند IFDPA و صندوق بیمه سایبری برای جبران خسارات کاربران می‌باشد.

## مصادیق جرایم داده مالی در پلتفرم‌های سرمایه‌گذاری آنلاین ایران

یکی از اهداف اصلی این پژوهش، شناسایی و تحلیل جرایم سوءاستفاده از داده‌های مالی در پلتفرم‌های سرمایه‌گذاری آنلاین ایران است. بررسی‌های انجام‌شده نشان داده است که سوءاستفاده از داده‌های مالی در پلتفرم‌های آنلاین ایران از سه جنبه اصلی رخ می‌دهد:

فروش غیرقانونی داده‌ها: در پلتفرم «الف»، داده‌های مالی بیش از ۵۰ هزار کاربر بدون رضایت آنان به یک شرکت تبلیغاتی فروخته شد. این عمل به نقض قوانین حریم خصوصی و حقوق داده‌ها منجر شده است. در مصاحبه‌ها، تعدادی از قضات و وکلای شرکت‌کننده در تحقیق بیان کردند که قوانین ایران در این زمینه فاقد پیش‌بینی دقیق و جامع برای مقابله با این نوع سوءاستفاده‌ها است.

کلاهبرداری الگوریتمی: در پلتفرم «ب»، با دستکاری الگوریتم‌ها، کاربران به سرمایه‌گذاری در پروژه‌های پرریسک تشویق شدند که در نهایت باعث ضرر مالی به آن‌ها شد. این نوع کلاهبرداری که به‌ویژه در پلتفرم‌های آنلاین با استفاده از الگوریتم‌های پیچیده صورت می‌گیرد، هنوز در قانون جرایم رایانه‌ای ایران به‌طور خاص جرم‌انگاری نشده است. تحلیل تطبیقی نشان می‌دهد که در GDPR و CCPA چنین سوءاستفاده‌هایی تحت عنوان کلاهبرداری الگوریتمی مشمول مجازات‌های سنگینی می‌شوند.

نقض امنیت سیستماتیک: در پلتفرم «ج»، نشت داده‌های ۱۰۰ هزار کاربر به‌دلیل ضعف در سیستم‌های رمزنگاری و حفاظت از داده‌ها رخ داد. ضعف در امنیت سایبری باعث شد که اطلاعات حساس کاربران افشا شود. این نوع نقض‌های امنیتی به‌ویژه در پلتفرم‌هایی که از زیرساخت‌های امنیتی ضعیف استفاده می‌کنند، همچنان یک تهدید جدی است. در این زمینه، قوانین ایران فاقد الزام به رعایت استانداردهای امنیتی ISO/IEC 27001 و دیگر پروتکل‌های امنیتی پیشرفته است.

## ۵,۲ تحلیل تطبیقی قوانین ایران و بین‌المللی

در این بخش، به مقایسه دقیق قوانین ایران با GDPR اتحادیه اروپا و CCPA ایالات متحده پرداخته شده است. نتایج نشان می‌دهد که قوانین ایران برای مقابله با سوءاستفاده از داده‌های مالی کاربران، همچنان نیازمند اصلاحات جدی است. برخی از تفاوت‌های اصلی عبارتند از:

تعریف ناقص «داده مالی» در ایران: در ایران، قانون جرایم رایانه‌ای و دیگر قوانین مرتبط، داده‌های مالی را به‌طور دقیق تعریف نکرده‌اند، در حالی که در GDPR و CCPA، داده‌های مالی با دقت و شفافیت تعریف شده‌اند و حفاظت از آن‌ها با ضمانت‌های اجرایی قوی همراه است. این خلأ قانونی در ایران باعث شده که در زمان وقوع نقض داده‌ها، پلتفرم‌ها نتوانند به‌طور مؤثر به مسئولیت‌های خود عمل کنند.

جریمه‌های ناکافی در ایران: جریمه‌های نقدی و مجازات‌های ایران به‌ویژه در زمینه سوءاستفاده از داده‌های مالی بسیار ناچیز و ناکافی هستند. در مقایسه با GDPR که جریمه‌هایی تا ۴٪ از گردش مالی سالانه شرکت‌ها در نظر گرفته است، ایران تنها جریمه‌های ثابت و اندکی برای اینگونه جرایم دارد که اثربخشی کمتری دارند.

عدم الزام به گزارش‌دهی سریع در ایران: در حالی که GDPR و CCPA الزام می‌کنند که نقض داده‌ها ظرف ۷۲ ساعت به مقامات و کاربران اطلاع‌رسانی شود، در ایران هیچ‌گونه الزامی برای گزارش‌دهی فوری در صورت نقض داده‌ها وجود ندارد. این مسئله می‌تواند منجر به افزایش آسیب‌های ناشی از نقض داده‌ها و سوءاستفاده‌های بیشتر از آن‌ها شود.

### ارتباط بین نقض داده‌های مالی و کاهش اعتماد کاربران

نتایج تحلیل آماری نشان می‌دهند که نقض داده‌های مالی به‌طور مستقیم باعث کاهش اعتماد کاربران به پلتفرم‌های سرمایه‌گذاری آنلاین و کاهش میزان سرمایه‌گذاری در این پلتفرم‌ها شده است. طبق داده‌های به‌دست‌آمده از پرسشنامه‌ها و مصاحبه‌ها، بیش از ۶۰٪ از کاربران پلتفرم‌ها به دلیل نگرانی‌های امنیتی و سوءاستفاده‌های گذشته از داده‌های مالی، تمایل کمتری به استفاده از پلتفرم‌های جدید نشان می‌دهند. این تغییرات رفتاری در بین کاربران تأثیرات منفی بر سرمایه‌گذاری‌های خارجی نیز داشته است.

### ارزیابی تأثیر چارچوب D.R.A.C.O

پژوهش نشان می‌دهد که اجرای چارچوب D.R.A.C.O می‌تواند به‌طور قابل‌توجهی به بهبود وضعیت موجود کمک کند. بر اساس نتایج بررسی‌های صورت‌گرفته، تعریف دقیق داده مالی و نظارت لحظه‌ای بر تراکنش‌ها، یکی از اصلی‌ترین نیازها برای تقویت قوانین ایران در این حوزه است. علاوه بر این، پیشنهاد ایجاد صندوق بیمه سایبری و دعوای جمعی (Class Action) برای جبران خسارات کاربران، می‌تواند به‌طور مؤثری به کاهش تبعات منفی نقض داده‌ها کمک کند.پلتفرم‌ها همچنین با پیاده‌سازی این چارچوب می‌توانند از هوش مصنوعی و بلاک‌چین برای شناسایی تهدیدات نوین و پیشگیری از نقض داده‌ها استفاده کنند. این فناوری‌ها می‌توانند به‌طور خودکار نقض‌های امنیتی را

شناسایی کرده و در صورت بروز هرگونه مشکل، از آسیب‌های گسترده جلوگیری کنند.با توجه به یافته‌های به‌دست‌آمده از این تحقیق، مشخص شده است که قوانین ایران هنوز در زمینه حفاظت از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین با مشکلات جدی مواجه است. این مشکلات شامل تعریف مبهم داده‌های مالی، کمبود ضمانت‌های اجرایی، و ضعف نظارتی هستند. چارچوب D.R.A.C.O می‌تواند به‌عنوان یک راهکار جامع برای حل این مشکلات و بهبود وضعیت امنیت داده‌های مالی در پلتفرم‌های آنلاین ایران عمل کند.اجرای این چارچوب نیازمند همکاری میان نهادهای مختلف از جمله پلتفرم‌ها، دولت، و نهادهای نظارتی است. به‌ویژه، پیاده‌سازی صندوق بیمه سایبری و دعوای جمعی برای جبران خسارت کاربران می‌تواند اعتماد عمومی به این پلتفرم‌ها را به‌طور قابل‌توجهی افزایش دهد.

## تحلیل تطبیقی جریمه‌ها و مجازات‌ها

برای تحلیل تطبیقی جریمه‌ها و مجازات‌های فعلی ایران با سایر کشورها، به‌ویژه کشورهای پیشرفته در زمینه حفاظت از داده‌های مالی و حقوق دیجیتال، باید جزییات دقیق‌تر و مقایسه‌ای میان قوانین ایران و قوانین بین‌المللی مانند GDPR اتحادیه اروپا، CCPA ایالات متحده، PIPL چین، و PDPA سنگاپور انجام شود. در این بخش، مقایسه‌ای جامع از جریمه‌ها و مجازات‌های مختلف در این کشورها با ایران ارائه می‌شود و تحلیل می‌شود که چرا این تفاوت‌ها در سطح جهانی اهمیت دارند و چطور ایران می‌تواند از این تجربیات برای تقویت قوانین داخلی خود بهره ببرد.قانون جرایم رایانه‌ای ایران که در سال ۱۳۸۸ به تصویب رسید، بر اساس مجازات‌های نقدی و برخی مجازات‌های حبس برای برخی از جرایم سایبری پایه‌گذاری شده است. اما این قانون از نظر شدت جریمه‌ها برای جرایم مربوط به داده‌های مالی و حریم خصوصی، بسیار محدود است. این ضعف باعث شده که جرایم داده‌ای از جمله سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌های آنلاین با شدت کافی برخورد نشود.

جریمه‌ها در ایران:

جریمه‌های نقدی برای سوءاستفاده از داده‌ها و نقض حریم خصوصی در ایران معمولاً بین ۵۰ میلیون تومان تا ۱۰۰ میلیون تومان است. این جریمه‌ها به هیچ عنوان بازدارنده نیستند، به‌ویژه با توجه به سودهای کلان که پلتفرم‌ها از سوءاستفاده از داده‌های کاربران به‌دست می‌آورند.

مجازات حبس: حبس برای سوءاستفاده از داده‌های مالی کاربران در پلتفرم‌ها بسیار محدود است و معمولاً شامل حبس‌های کوتاه‌مدت می‌شود.

این جریمه‌ها با توجه به مقایسه با سایر کشورها، به‌ویژه کشورهای پیشرفته، بسیار ناکافی به نظر می‌رسند و در عمل نمی‌توانند پلتفرم‌ها را از سوءاستفاده از داده‌های کاربران بازدارند.

## جریمه‌ها و مجازات‌ها در اتحادیه اروپا (GDPR)

مقررات عمومی حفاظت از داده‌ها (GDPR) اتحادیه اروپا که در سال ۲۰۱۶ به تصویب رسید، یکی از سخت‌گیرانه‌ترین و جامع‌ترین قوانین در زمینه حفاظت از داده‌های شخصی و مالی است. GDPR شامل مقررات سخت‌گیرانه‌ای برای جریمه‌ها و مجازات‌ها است که به‌طور ویژه برای تهدیدات داده‌ای طراحی شده‌اند.

جریمه‌ها در GDPR:

جریمه‌ها در GDPR تا ۴٪ از گردش مالی سالانه شرکت‌ها یا ۲۰ میلیون یورو (هرکدام که بیشتر باشد) می‌تواند باشد. این میزان جریمه‌ها برای شرکت‌هایی که داده‌های مالی کاربران را سوءاستفاده می‌کنند یا قوانین را نقض می‌کنند، به‌شدت بازدارنده است.این جریمه‌ها برای نقض حریم خصوصی و داده‌های شخصی در اتحادیه اروپا بسیار موثر بوده‌اند و موجب تغییرات قابل‌توجهی در رفتار پلتفرم‌ها شده است.در کنار جریمه‌های نقدی، مجازات‌های حبس و مجازات‌های حقوقی برای مدیران و مسئولان پلتفرم‌ها در نظر گرفته می‌شود. این مجازات‌ها به‌ویژه برای پلتفرم‌هایی که از داده‌های مالی سوءاستفاده می‌کنند و اقدام به افشای غیرمجاز اطلاعات می‌نمایند، بسیار بازدارنده است.

### جریمه‌ها و مجازات‌ها در ایالات متحده (CCPA)

قانون حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA) یکی از مهم‌ترین قوانین ایالات متحده است که به‌طور خاص به حفاظت از داده‌های شخصی و مالی کاربران پرداخته است. CCPA به‌طور ویژه به کاربران این امکان را می‌دهد که حق غرامت را در صورت نقض داده‌ها مطالبه کنند.

جریمه‌ها در CCPA:

۷۵۰ دلار به ازای هر نقض داده، به‌ویژه در زمینه فروش غیرمجاز داده‌های مالی کاربران، تعیین شده است. اگر نقض داده‌ها عمدی باشد، این جریمه‌ها می‌توانند به ۲،۵۰۰ دلار به ازای هر نقض افزایش یابند.در صورتی که نقض داده‌ها به‌صورت گروهی باشد، کاربران می‌توانند به‌صورت دعوای جمعی (Class Action) از پلتفرم‌ها شکایت کنند و غرامت بیشتری دریافت کنند.برخلاف GDPR، CCPA به‌طور مستقیم مجازات‌های حبس برای مسئولان پلتفرم‌ها در نظر نگرفته است. اما این قانون می‌تواند به‌طور مؤثر از طریق دعوای جمعی و جریمه‌های سنگین تأثیرگذار باشد.

### جریمه‌ها و مجازات‌ها در چین (PIPL)

قانون حفاظت از داده‌های شخصی (PIPL) که در سال ۲۰۲۱ در چین به تصویب رسید، به‌طور مشابه با GDPR و CCPA، به حفاظت از داده‌های شخصی و مالی پرداخته است. این قانون در چین تأکید زیادی بر حفاظت از داده‌های مالی کاربران دارد و در برابر نقض‌های امنیتی، جریمه‌های سنگینی تعیین کرده است.جریمه‌ها در چین می‌تواند تا ۵٪ از گردش مالی سالانه شرکت‌ها باشد. این جریمه‌ها به‌طور خاص برای سوءاستفاده از داده‌های مالی و افشای اطلاعات مالی کاربران در نظر گرفته شده‌اند.علاوه بر جریمه‌های مالی، اگر نقض‌های داده‌ای عمدی باشد، پلتفرم‌ها می‌توانند با مجازات‌های کیفری و حبس مواجه شوند.

### جریمه‌ها و مجازات‌ها در سنگاپور (PDPA)

قانون حفاظت از داده‌های شخصی (PDPA) سنگاپور از دیگر قوانین پیشرفته در زمینه حفاظت از داده‌ها است که به‌طور خاص به پلتفرم‌های آنلاین و حفاظت از داده‌های مالی کاربران پرداخته است.جریمه‌ها در سنگاپور می‌تواند تا ۱ میلیون دلار سنگاپور یا ۲,۵٪ از گردش مالی سالانه شرکت‌ها باشد. این جریمه‌ها برای شرکت‌هایی است که از داده‌های مالی به‌طور غیرمجاز استفاده کرده‌اند یا اطلاعات کاربران را افشا کرده‌اند.مجازات‌های حبس برای مدیران و مسئولان پلتفرم‌ها در صورت نقض قوانین وجود دارد.

### تحلیل مقایسه‌ای

از تحلیل تطبیقی جریمه‌ها و مجازات‌ها در ایران و سایر کشورها می‌توان نتیجه گرفت که جریمه‌های موجود در ایران برای جرایم سوءاستفاده از داده‌های مالی به‌ویژه در پلتفرم‌های آنلاین بسیار ناچیز و ناکافی است. این در حالی است که

کشورهایی مانند اتحادیه اروپا، ایالات متحده، چین و سنگاپور با تعیین جریمه‌های سنگین و مجازات‌های حبس برای مدیران و مسئولان پلتفرم‌ها، قوانین بسیار سخت‌گیرانه‌تری دارند که باعث افزایش بازدارندگی و رعایت بهتر قوانین توسط پلتفرم‌ها می‌شود.جریمه‌های مالی ایران بسیار محدود و نه چندان بازدارنده هستند.مجازات‌های حبس برای سوءاستفاده از داده‌های مالی نیز به‌ویژه برای پلتفرم‌های بزرگ بسیار ضعیف است.

نیاز به اصلاحات: افزایش جریمه‌ها تا حداقل ۵٪ از گردش مالی سالانه برای پلتفرم‌ها. ایجاد مجازات‌های حبس برای مسئولان پلتفرم‌ها که از داده‌های مالی سوءاستفاده می‌کنند.گنجاندن قوانین دقیق و جامع برای جرم‌انگاری سوءاستفاده از داده‌های مالی به‌ویژه در پلتفرم‌های آنلاین.

## پیشنهادات برای مقابله با سوءاستفاده از داده‌های مالی کاربران

### اصلاح و به‌روزرسانی قوانین و مقررات

تعریف دقیق «داده مالی» در قوانین ایران ضروری است. باید داده‌های مالی مانند اطلاعات حساب بانکی، سوابق تراکنش‌ها، الگوهای سرمایه‌گذاری و سایر داده‌های مرتبط با وضعیت مالی کاربران، به‌طور شفاف تعریف شوند تا از سوءاستفاده‌های احتمالی جلوگیری شود.جرم‌انگاری سوءاستفاده از داده‌های مالی باید در قانون جرایم رایانه‌ای و دیگر مقررات مرتبط، به‌طور خاص گنجانده شود. برای این منظور، باید فصلی جداگانه تحت عنوان «جرایم داده مالی» در قوانین کشور ایجاد شود که با دقت به این نوع جرایم پرداخته شود.جریمه‌های موجود در قوانین ایران برای جرایم سوءاستفاده از داده‌های مالی باید به‌طور قابل‌توجهی افزایش یابد. پیشنهاد می‌شود که جریمه‌ها به درصدی از گردش مالی سالانه پلتفرم‌ها تعلق گیرد. به‌عنوان مثال، ۵ تا ۱۰ درصد از درآمد سالانه پلتفرم‌ها برای تخلفات مرتبط با سوءاستفاده از داده‌های مالی در نظر گرفته شود.علاوه بر جریمه‌های مالی، مجازات‌های حبس برای مسئولان پلتفرم‌ها که در موارد سوءاستفاده از داده‌های مالی سهیم باشند، باید در نظر گرفته شود.الزام به گزارش‌دهی فوری نقض داده‌ها ظرف ۷۲ ساعت پس از وقوع نقض به کاربران و مقامات نظارتی باید در قوانین ایران گنجانده شود. این گزارش‌دهی باید به‌طور خودکار توسط پلتفرم‌ها انجام شود و به‌طور شفاف به عموم کاربران اطلاع داده شود.

### ایجاد نهاد نظارتی مستقل برای حفاظت از داده‌های مالی کاربران

ایجاد IFDPA (Independent Financial Data Protection Authority)

برای نظارت مؤثر بر پلتفرم‌های سرمایه‌گذاری آنلاین و حفاظت از داده‌های مالی کاربران، نهاد نظارتی مستقل (IFDPA) باید تأسیس شود. این نهاد مسئول نظارت بر رعایت قوانین حفاظت از داده‌ها و بررسی نقض‌های امنیتی در پلتفرم‌های سرمایه‌گذاری آنلاین خواهد بود.IFDPA باید مجوزهای لازم برای بازرسی و جریمه کردن پلتفرم‌ها را داشته باشد و همچنین بتواند به‌طور فوری اقداماتی برای مقابله با نقض‌های امنیتی انجام دهد.پلیس فتا، سازمان بورس، مرکز ملی فضای مجازی و دیگر نهادهای نظارتی باید هماهنگ‌تر عمل کنند. به‌ویژه، در مواقع وقوع نقض داده‌ها، باید یک سیستم هماهنگ و یکپارچه برای رسیدگی سریع و مؤثر به این نقض‌ها ایجاد شود.پلتفرم‌های سرمایه‌گذاری آنلاین باید تحت نظارت دقیق از نظر الگوریتم‌ها و مدل‌های تجاری خود قرار گیرند. این نظارت باید به‌گونه‌ای باشد که پلتفرم‌ها نتوانند از داده‌های مالی کاربران سوءاستفاده کرده و کاربران را به سرمایه‌گذاری‌های پرریسک یا نامطمئن ترغیب کنند.

### استفاده از فناوری‌های نوین برای تقویت امنیت داده‌ها

هوش مصنوعی می‌تواند برای شناسایی الگوهای مشکوک در تراکنش‌های مالی و پیش‌بینی تهدیدات سایبری استفاده شود. پلتفرم‌های آنلاین باید از سیستم‌های هوش مصنوعی برای رصد لحظه‌ای تراکنش‌ها استفاده کنند تا هرگونه فعالیت مشکوک را به‌طور فوری شناسایی کرده و به مقامات ذی‌صلاح اطلاع دهند.بلاک‌چین می‌تواند به‌عنوان یک فناوری امن برای ثبت تراکنش‌ها و حفاظت از داده‌های مالی کاربران مورد استفاده قرار گیرد. با توجه به شفافیت و تغییرناپذیری که بلاک‌چین فراهم می‌کند، می‌توان از آن برای ثبت تراکنش‌ها و جلوگیری از هرگونه تقلب یا سوءاستفاده استفاده کرد.پلتفرم‌ها باید از استانداردهای رمزنگاری پیشرفته (مثل ISO/IEC 27001 و AES) برای حفاظت از داده‌های مالی کاربران استفاده کنند. رمزنگاری اطلاعات به‌ویژه در فرآیندهای ذخیره‌سازی و انتقال داده‌ها ضروری است.

### پیشگیری و آموزش کاربران و پلتفرم‌ها

پلتفرم‌ها باید دوره‌های آموزشی و آگاهی‌بخشی برای کاربران خود ارائه دهند تا آن‌ها از حقوق خود در زمینه حفاظت از داده‌های مالی آگاه شوند. این آموزش‌ها باید شامل نکاتی مانند چگونه از داده‌های مالی خود حفاظت کنند، تشخیص تهدیدات سایبری و اقدام در صورت نقض داده‌ها باشد.مدیران پلتفرم‌ها و قضات باید دوره‌های آموزشی حقوقی و فنی در زمینه حفاظت از داده‌ها و امنیت سایبری را گذرانده و با جدیدترین قوانین و فناوری‌ها در این حوزه آشنا شوند. این آموزش‌ها می‌تواند به پلتفرم‌ها کمک کند تا به‌طور مؤثرتری از داده‌های کاربران محافظت کنند و از وقوع نقض‌های امنیتی جلوگیری نمایند.

### جبران خسارت‌های کاربران و تقویت سیستم‌های حمایتی

یک صندوق بیمه سایبری باید برای جبران خسارت‌های مالی ناشی از نقض داده‌ها ایجاد شود. این صندوق باید به‌طور مشترک توسط پلتفرم‌ها و دولت تأسیس شود و در صورت بروز نقض داده‌ها، خسارت‌های کاربران را پرداخت کند. این صندوق می‌تواند از یک‌سو به حفاظت از حقوق کاربران و از سوی دیگر به کاهش خطرات مالی پلتفرم‌ها کمک کند.در صورتی که پلتفرم‌ها اقدام به سوءاستفاده از داده‌های مالی کاربران کنند، امکان دعوای جمعی برای حداقل ۵۰ کاربر فراهم گردد. این اقدام قانونی می‌تواند به‌طور مؤثری به کاربران آسیب‌دیده کمک کند تا حقوق خود را پیگیری کنند.

### نتیجه‌گیری

پلتفرم‌های سرمایه‌گذاری آنلاین در ایران به سرعت در حال رشد هستند، اما این رشد با چالش‌های جدی در زمینه حفاظت از داده‌های مالی کاربران همراه است. سوءاستفاده از این داده‌ها نه‌تنها به حریم خصوصی کاربران آسیب می‌زند، بلکه می‌تواند اعتماد عمومی را کاهش دهد و به پلتفرم‌ها و کل صنعت فین‌تک لطمه وارد کند. بنابراین، ضرورت دارد که اقداماتی فوری و مؤثر برای تقویت حفاظت از داده‌های مالی کاربران و جلوگیری از سوءاستفاده‌های سایبری انجام گیرد.در این پژوهش مشخص شد که قوانین ایران به‌ویژه در زمینه حفاظت از داده‌های مالی کاربران هنوز با مشکلات و خلأهای جدی مواجه است. تعریف مبهم «داده مالی»، مجازات‌های ناکافی برای نقض داده‌ها، و عدم وجود نهاد نظارتی مستقل از جمله مهم‌ترین مشکلاتی هستند که موجب ضعف در مقابله با سوءاستفاده از داده‌ها می‌شوند. مقایسه تطبیقی میان قوانین ایران و مقررات بین‌المللی مانند GDPR اتحادیه اروپا و CCPA ایالات متحده نشان می‌دهد که ایران نیازمند اصلاحات جدی در این زمینه است تا هم‌راستا با استانداردهای جهانی شود و از حقوق کاربران

محافظت کند.یکی از مهم‌ترین پیشنهادات این تحقیق، اصلاح قانون جرایم رایانه‌ای ایران و اضافه کردن فصلی مستقل تحت عنوان «جرایم داده مالی» است. این اصلاحات باید شامل تعریف دقیق داده مالی و افزایش مجازات‌ها برای سوءاستفاده از داده‌ها باشد. به‌ویژه، باید جریمه‌ها به‌طور قابل‌توجهی افزایش یابند و به‌جای جریمه‌های ثابت، جریمه‌ها بر اساس درصدی از گردش مالی سالانه پلتفرم‌ها تعیین شوند تا به‌عنوان یک عامل بازدارنده مؤثر عمل کنند. همچنین، قوانین باید الزام کنند که در صورت وقوع نقض داده‌ها، پلتفرم‌ها به‌طور فوری (در مدت زمان حداکثر ۷۲ ساعت) به مقامات و کاربران گزارش دهند.پژوهش حاضر به‌طور ویژه به ارائه چارچوب D.R.A.C.O پرداخته است. این چارچوب پنج مرحله‌ای شامل تعریف دقیق داده‌های مالی، رصد و نظارت مستمر، ارزیابی ریسک‌های حقوقی و فنی، جبران خسارت به کاربران، و به‌روزرسانی مستمر قوانین است که می‌تواند به‌طور مؤثری به بهبود وضعیت موجود کمک کند. این چارچوب به‌ویژه در ایجاد نهاد نظارتی مستقل (IFDPA) و صندوق بیمه سایبری مشترک برای جبران خسارات ناشی از نقض داده‌ها اهمیت زیادی دارد.هوش مصنوعی و بلاک‌چین دو فناوری نوین هستند که می‌توانند در رصد لحظه‌ای تراکنش‌ها، شناسایی الگوهای مشکوک و پیش‌بینی تهدیدات سایبری مؤثر باشند. بلاک‌چین می‌تواند به‌عنوان ابزاری برای ثبت و محافظت از داده‌های مالی کاربران استفاده شود و از تغییر یا دستکاری داده‌ها جلوگیری کند. همچنین، استفاده از هوش مصنوعی برای شناسایی تهدیدات نوین مانند کلاهبرداری الگوریتمی و حملات سایبری می‌تواند سطح امنیت پلتفرم‌ها را به‌طور چشمگیری افزایش دهد.آموزش‌های حقوقی و فنی برای کاربران و مدیران پلتفرم‌ها به‌طور ویژه ضروری است. کاربران باید از حقوق خود در زمینه حفاظت از داده‌های مالی آگاه شوند و بتوانند اقدامات لازم برای حفاظت از داده‌هایشان را انجام دهند. علاوه بر این، مدیران پلتفرم‌ها باید با مقررات جدید و فناوری‌های نوین در زمینه حفاظت از داده‌ها آشنا شوند تا بتوانند اقداماتی پیشگیرانه و مؤثر را در جهت حفظ داده‌های مالی کاربران اتخاذ کنند.در نهایت، این تحقیق نشان می‌دهد که اعتماد عمومی یکی از ارکان اصلی برای رشد صنعت فین‌تک است. سوءاستفاده از داده‌های مالی کاربران می‌تواند به کاهش اعتماد به پلتفرم‌ها و کاهش سرمایه‌گذاری‌های داخلی و خارجی منجر شود. به همین دلیل، حفاظت از داده‌ها باید در اولویت قرار گیرد تا بتوان به توسعه پایدار و امن این صنعت در ایران کمک کرد.در مجموع، این پژوهش بر ضرورت اصلاحات قانونی در ایران تأکید دارد تا بتوان از داده‌های مالی کاربران در پلتفرم‌های سرمایه‌گذاری آنلاین محافظت کرد. چارچوب D.R.A.C.O می‌تواند به‌عنوان یک راهکار جامع و عملیاتی در جهت بهبود قوانین موجود و ارتقای امنیت داده‌ها در ایران عمل کند. این چارچوب، با استفاده از ترکیب اصلاحات قانونی، فناوری‌های نوین، و ایجاد نهادهای نظارتی مستقل، می‌تواند به یکی از ابزارهای اصلی برای حفاظت از داده‌های مالی کاربران در پلتفرم‌های آنلاین تبدیل شود.

## منابع و مآخذ


اباذری، کسری،۱۴۰۳،بررسی مسئولیت کیفری ناشی از سوءاستفاده از هوش مصنوعی در جرایم سایبری،پانزدهمین کنفرانس بین المللی دستاوردهای نوین پژوهشی در علوم تربیتی، روانشناسی و علوم اجتماعی،تهران،https://civilica.com/doc/2185667

اردبیلی محمدعلی(۱۳۸۶) حقوق جزای عمومی، تهران، میزان

افراسیابی، مهدی،۱۴۰۳،بررسی حقوقی جرایم جاسوسی و افشای اطلاعات در فضای مجازی،چهارمین همایش بین المللی وکالت، حقوق و علوم انسانی،همدان،https://civilica.com/doc/2199529

انصاری، باقر. (۱۴۰۰) حقوق داده ها و هوش مصنوعی مفاهیم و چالش ها، .۱ ،تهران: سهامی انتشار

تقوی فرد، سیدمحمدتقی؛ تقوا، محمدرضا؛ فقیهی، مهدی؛ جمشیدی، محمدجواد.(۱۴۰۳) »مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب. مجلس و راهبرد، . ۸۹ (۲۴)

جعفری، امین(۱۳۹۳) حقوق کیفری کسب و کار. تهران: شهردانش.

حسینی، س. (۱۴۰۱). تحلیل مسئولیت مدنی پلتفرم‌ها در ایران: چالش‌ها و راهکارها.

رضوی، م. (۱۴۰۰). بررسی جرایم سایبری و سوءاستفاده از داده‌های شخصی در ایران.

سوتیل، کیت؛ پیلو، مویرا ؛ تیلور، کلر.(۱۳۸۸). شناخت جرم شناسی . ترجمه : میرروح الله صدیق بطحایی اصل، چاپ دوم، تهران: دادگستر

سیداصفهانی، سیدحسام الدین.(۱۳۹۲). درآمدی بر مبانی و اهداف جرم شناسی تطبیقی در چشم انداز جهانی شدن. دایره المعارف علوم جنایی(مجموعه مقاله های تازههای علوم جنایی)،کتاب دوم، تهران: میزان

فرجی ها، محمد.(۱۳۸۸). رویکرد چندنهادی به پیشگیری از جرم : چالش ها و راهکارها. دیباچه در: رویکرد چندنهادی به پیشگیری از جرم. زیر نظر: محمد فرجیها و فیروز محمودی جانکی، تهران: انتشارات معاونت آموزش نیروی انتظامی

قانون جرایم رایانه‌ای، جمهوری اسلامی ایران، ۱۳۸۸.

کرمی، صادق،۱۴۰۴،تحلیل حقوق کیفری جرایم ناشی از فعالیت در شبکه های اجتماعی با تاکید بر اینستاگرام در نظام حقوقی ایران،https://civilica.com/doc/2281004

گزارش مرکز توسعه تجارت الکترونیک ایران، ۱۴۰۲.

لایحه حریم خصوصی (در دست بررسی)، جمهوری اسلامی ایران .

California Consumer Privacy Act (CCPA), California State, 2018.

California Consumer Privacy Act (CCPA). URL: https://oag.ca.gov/privacy/ccpa

Daoud, G. (2023). The Evolving Nature Of Financial Crime With The Increase Of Internet Capabilities. Challenge Identification, Legal Considerations And Policy Recommendations (Doctoral dissertation, School of Advanced Study).

European Commission: Data Protection in the European Union (EU). URL: https://ec.europa.eu/info/law/law-topic/data-protection_en

International Association of Privacy Professionals (IAPP). URL: https://iapp.org

Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think.

Muammar, S., Shehada, D., & Mansoor, W. (2023). Digital risk assessment framework for individuals: Analysis and recommendations. *IEEE Access*, *11*, 85561-85570.

Office of the Privacy Commissioner for Personal Data, Hong Kong. URL: https://www.pcpd.org.hk

Personal Data Protection Act (PDPA), Singapore, 2021.

Personal Information Protection Law (PIPL), People's Republic of China, 2021.

Privacy Act, Australia, 2023.

Regulation (EU) 2016/679 (GDPR), European Union, 2016.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.

Solove, D. J., & Schwartz, P. M. (2021). Privacy Law and Society.

United Nations Conference on Trade and Development (UNCTAD). UR

# Legal Analysis of the Misuse of Users' Financial Data in Online Investment Platforms: Introducing the D.R.A.C.O Framework to Address Emerging Threats

**Aref Bakhshi** [1]

## Abstract

In recent years, online investment platforms in Iran have experienced significant growth. However, this expansion has been accompanied by serious challenges regarding the protection of users' financial data. This study aims to conduct a legal analysis of the misuse of users' financial data and to examine existing legal gaps in this area. The research methodology includes a combination of comparative analysis of international regulations—such as the European Union's GDPR and the U.S. CCPA—case studies, and interviews with 30 legal and technical experts.Findings reveal that Iran's current legal framework for protecting users' financial data is inadequate in terms of conceptual definitions, enforcement mechanisms, and coverage of emerging technologies such as artificial intelligence and blockchain. The weakness of regulatory institutions has further exacerbated the issue. In response to these challenges, an innovative framework named **D.R.A.C.O** (Definition–Monitoring–Assessment–Compensation–Optimization) is proposed, comprising five key pillars: precise definition of financial data, continuous monitoring of transactions, assessment of legal and technical risks, compensation through a cyber insurance fund, and regular updates to relevant laws and training programs.Furthermore, the study recommends the establishment of an independent authority for financial data protection (IFDPA), reform of cybercrime laws, and the launch of a cyber insurance fund as complementary measures. These initiatives are designed to enhance financial data security, strengthen public trust, and provide the legal and institutional infrastructure necessary for the sustainable development of Iran's fintech industry. By introducing the D.R.A.C.O framework and practical strategies, this research represents a significant step toward improved policymaking and regulation in Iran's digital financial space.

## Keywords

Financial Data Protection, Online Investment Platforms, D.R.A.C.O Framework, Independent Regulatory Authority (IFDPA), Cybercrime, Privacy Regulations

1. Master's Student in Criminal Law and Criminology, Department of Law, Faculty of Law, Islamic Azad University, Rafsanjan, Iran.