کاربست رویکرد داده‌بنیان در پیشگیری از پولشویی

باقر شاملو[1]

سمیه پرهیزکاری*[2]

چکیده

رویکرد داده‌بنیان در سال‌های اخیر به عنوان پارادایمی نوین در پیشگیری از جرایم اقتصادی مطرح شده است. گذار از نظام‌های سنتی قاعده‌محور و ریسک‌مدار به سامانه‌های مبتنی بر کلان‌داده، داده‌های جایگزین و الگوریتم‌های یادگیری ماشین، این امکان را فراهم آورده است که فرآیند شناسایی مشتری و بازشناسی تراکنش‌های مشکوک، به عنوان دو رکن اساسی مورد تأکید اسناد بین‌المللی در راستای مبارزه با جرایم اقتصادی (از جمله اسناد گروه ویژه اقدام مالی)، به‌طور کارآمدتری انجام پذیرد. نوشتار حاضر با هدف شناسایی ظرفیت‌ها و چالش‌های کاربست این رویکرد، به روش توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای نگارش یافته است. یافته‌های پژوهش نشان می‌دهد که الگوریتم‌های یادگیری ماشین در شاخه‌های نظارت‌شده و بدون نظارت توانایی قابل توجهی در کشف الگوهای پنهان و ناهنجار تراکنش‌های مالی دارند و نرخ خطاهای مثبت و منفی کاذب را کاهش می‌دهند. در مقابل، کاربست این رویکرد با چالش‌هایی چون عدم شفافیت الگوریتمی و تعارض آن با حق دفاع و آسیب‌پذیری ادله الگوریتمی در برابر حملات تخاصمی مواجه است. نتیجه آنکه اگرچه رویکرد داده‌بنیان مسیری روشن و کارآمد در پیشگیری از جرایم اقتصادی و به‌ویژه پولشویی فراروی نهادهای مالی و عدالت کیفری گشوده است، اما تحقق کامل این ظرفیت‌ها بدون توجه همزمان به طراحی چارچوب‌های قانونی و تنظیم‌گری هوشمند، امکان‌پذیر نخواهد بود.

واژگان کلیدی: رویکرد داده‌بنیان، پیشگیری، شناسایی مشتری، تراکنش‌های مشکوک، یادگیری ماشین، شفافیت الگوریتمی.

---

[1] . استاد گروه حقوق کیفری و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی، تهران، ایران.

[2] . دانشجوی دکتری حقوق کیفری و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی، تهران، ایران. (نویسنده مسئول). ایمیل: parhizkary1998@gmail.com.

مقدمه

درسال‌های اخیر، مبارزه‌با جرایم جهانی، به‌ویژه جرایم اقتصادی، در چارچوب هدف‌شانزدهم توسعه پایدار سازمان‌ملل متحد، مصوب ۲۰۱۵ مبنی‌بر تقویت نهادهای مؤثر درجهت شفافیت، عدالت و صلح اهمیت قابل‌توجهی یافته است.(حجازی و صلح‌چی، ۱۳۹۹، ص ۹) در این میان، پولشویی به‌عنوان یکی‌از مهم‌ترین جرایم اقتصادی، سهم عمده‌ای‌از دغدغه‌های نظام‌های عدالت‌کیفری را به خود اختصاص داده است. هرچه نظام عدالت کیفری در کشف و پیشگیری‌از پولشویی مؤثرتر عمل کند، مسیر برای جرایم‌منشاء دشوارتر شده و به‌تبع آن، از حجم این جرایم کاسته خواهد شد. با این‌حال این هدف زمانی به‌طور مطلوب محقق می‌شود که نظام عدالت‌کیفری، اولویت خود را به پیشگیری اختصاص دهد. به‌همین دلیل، امروزه پیشگیری به‌عنوان رکن اساسی در ادبیات علوم‌جنایی مطرح است و اهمیتی فراتر از مقابله‌کیفری دارد.

این مسئله به‌ویژه از آن رو حائز اهمیت است که درسال‌های اخیر، پولشویی دگرگونی اساسی یافته و از شیوه‌های‌سنتی به طرح‌های پیچیده‌ای تکامل پیدا کرده است که از فناوری پیشرفته بهره می‌برند.(کدخدایی و نوروزپور،۱۳۹۹،ص ۷) ظهور عصردیجیتال، این فضا را به‌طور قابل‌توجهی تغییر داده است. با افزایش استفاده‌از رمزارزهایی مانند بیت‌کوین، پولشویان مسیر تازه‌ای یافته‌اند که گمنامی و سهولت انجام تراکنش‌های‌فرامرزی را بدون سطح نظارتی مشابه با سیستم‌های‌بانکی سنتی فراهم می‌کند.

باتوجه به تحول چشم‌انداز پولشویی و گذار از روش‌های سنتی به استفاده پیچیده از فناوری، روش‌های تشخیص این فعالیت‌های غیرقانونی نیز ناگزیر باید پیشرفتی قابل‌توجه پیدا کنند. در این مرحله، داده نیز ارزشی بنیادین یافته و تمامی فرآیندها برپایه آن سامان می‌یابد. درگذشته، تشخیص جرم عمدتاً بر شناسایی بی‌قاعدگی‌ها‌درجریان‌های‌نقدی و تراکنش‌های بانکی سنتی متمرکز بود. اما درسال‌های اخیر چابکی ابزارهای‌فناورانه درتشخیص ناهنجاری‌ها پیش‌از وقوع جرم، آن‌ها را به‌ابزاری غیرقابل‌جایگزین درعصر مدرن تبدیل کرده است.

در این‌راستا آموزه‌های جرم‌شناختی و کیفرشناختی، درسایه تحولات‌مستمر پدیده‌مجرمانه و دگرگونی فضای بزهکاری، مکاتب بسیاری را به‌خود دیده‌اند. برخی‌از این مکاتب برای سال‌ها به‌عنوان رویکردهای مسلط درنظام عدالت کیفری مطرح بوده‌اند. ازجمله رویکردهای تأثیرگذار در مواجه با بزهکاران‌خطرناک و دارای سابقه‌کیفری، عدالت‌سنجشی یا عدالت آماری[1] است که ریشه‌در اندیشه‌های مدیریت ریسک و کنترل جرم دارد.(بک، ۱۳۸۸، ص ۵۳) مبنای اصلی این رویکرد، نه اصلاح فرد بزهکار، بلکه کاهش نرخ‌کلی جرم ازطریق پیش‌بینی و مدیریت آماری خطر است. به‌بیان دیگر، هرچه احتمال وقوع یا

[1] . Actuarial Justice

تکرار جرم برای یک فرد یا گروه بالاتر ارزیابی شود، سطح نظارت‌اجتماعی و مداخلات کیفری اعمال‌شده سخت‌تر و گسترده‌تر خواهد بود. (نجفی ابرندآبادی، ۱۳۸۸، صص ۷۲۲-۷۲۳)

این رویکرد درگذشته عمدتاً ماهیتی واکنشی داشت؛ بدین‌معنا که شاخص‌های خطرناکی نظیر سابقه‌ارتکاب مجددجرم یا تمایل‌به نقض هنجارها، پس از وقوع جرم و درفرآیند پاسخ‌دهی کیفری برآورد می‌شدند.(نجفی ابرندآبادی و ایارگر، ۱۳۹۹،ص ۹) اما امروزه، این مفهوم معنایی پیش‌دستانه و فعالانه یافته است. امروزه نظام عدالت کیفری درصدد است تا با شناسایی پیش‌دستانه شاخص‌های بزهکاری و نشانه‌های‌مشکوک، وقوع جرم را پیش‌بینی و سپس ازآن پیشگیری کند؛ (اسماعیلی،۱۳۹۶، ص ۳۰۵) امری‌که به‌دلیل ماهیت پیشگیرانه و شناسایی ریسک، به احتمالات و آمار وابستگی پیدا کرده است.

بر این اساس، آخرین روزآمدسازی راهنمای گروه ویژه اقدام مالی با عنوان «ارزیابی ملی ریسک پولشویی»[1] (اوت ۲۰۲۵)، در چارچوب توصیه شماره (۱) پیشین خود، بر ضرورت شناسایی، ارزیابی و اتخاذ اقدامات متناسب با ریسک تأکید می‌کند. در این سند، ارزیابی ریسک، فرآیندی مستمر و پویا تلقی شده که باید متناسب با تغییرات محیطی، اطلاعات جدید و ریسک‌های در حال ظهور، به‌طور مستمر مورد بازنگری قرار گیرد. از این‌رو، بر اتخاذ رویکردی ساختاریافته و منسجم برای دستیابی به درکی به‌روز از ریسک تأکید شده و ارزیابی ملی ریسک به‌عنوان یکی از مهم‌ترین ابزارهای تحقق این هدف معرفی شده است. (FATF, 2025, p.4)

در این‌راستا یکی‌از این ابزاهای فناورانه، یادگیری ماشین است که درعرصه اقتصاد از رهگذر قابلیت‌هایی نظیر، بینش‌های داده‌بنیان[2]، خودکارسازی فرآیندهای تحلیلی و قابلیت مقیاس‌پذیری در رویارویی با حجم عظیم‌داده (اعم از ساختاریافته و بدون‌ساختار) امکانِ پیش‌بینی معاملات‌مالی و همچنین پیشگیری‌از تقلب، پولشویی و سایر جرایم‌مالی را پدید آورده است. (Mallika, Ramasubramanian, 2025. P. 386)

این پیشرفت، اشخاص مشمول[3] در مبارزه با پولشویی را قادر می‌سازد تا روندهای مالی نظیر سرمایه‌گذاری و نقل و انتقالات مالی را بادقت بیشتری در نظر گیرند، ریسک را کاهش دهند، بی‌نظمی‌ها را شناسایی کرده و درکوتاه‌ترین زمان ممکن به تراکنش‌های مشکوک واکنش نشان دهند.(خیرانی و دیگران، ۱۴۰۱،ص ۳۹) به‌عنوان مثال، سیستم‌های کشف تقلب که برپایه یادگیری‌ماشین طراحی شده‌اند، با بهره‌گیری‌از الگوریتم‌های پیشرفته طبقه‌بندی و شبکه‌های‌عصبی، الگوهای‌پنهان در

---

[1] . Money Laundering National Risk Assessment Guidance

[2] . Data-driven insights

[3] . منظوراز شخص‌مشمول هر شخص اعم‌از حقیقی یا حقوقی است که ملزم‌به اجرای تدابیر پیشگیرانه معرفی شده توسط گروه ویژه اقدام مالی در برابر پولشویی است. این اشخاص شامل بانک‌ها، موسسسات‌اعتباری، صرافی‌ها، حسابداران و... می‌شود.

تراکنش‌های مشکوک را آشکار می‌سازند.[1] این قابلیت، افزون‌بر کاهش چشمگیر زیان‌های مالی، اعتمادعمومی به سیستم‌های بانکداری و پرداخت‌آنلاین را نیز تقویت می‌کند(Abdulalem. et al. 2022, p.1) لذا شناسایی ظرفیت‌ها و چالش‌های مدل‌های هوشمندِ موثر در پیش‌گیری از جرم، به‌منظور کاربست آن در نظام عدالت‌کیفری ضروری می‌نماید.

بر این اساس، پرسش اصلی نوشتار حاضر آن است که رویکرد داده‌بنیان، با بهره‌گیری از ابزارهای مبتنی بر یادگیری ماشین، تا چه اندازه ظرفیت ارتقای فرآیند شناسایی و ارزیابی ریسک پولشویی را داراست و در عین حال، کاربست این فناوری با چه چالش‌ها و ملاحظات حقوقی مواجه است. اهمیت این پرسش از آن جهت است که با وجود گسترش کاربرد ابزارهای مبتنی بر یادگیری ماشین در حوزه مبارزه با پولشویی، ابعاد حقوقی و الزامات حاکم بر کاربست آن‌ها هنوز به‌صورت منسجم مورد تحلیل قرار نگرفته و همچنان نیازمند بررسی است.

بدین‌سان و در راستای پاسخ به این پرسش، مقاله حاضر در سه بخش سامان یافته است. در بخش نخست، مبانی و چارچوب حقوقی رویکرد داده‌بنیان در پرتو تحول نظام پیشگیری از پولشویی مورد تحلیل قرار می‌گیرد. بخش دوم، به بررسی مهم‌ترین ابزارها و کارکردهای فنی این رویکرد در فرآیند شناسایی و ارزیابی ریسک اختصاص دارد و در بخش سوم، چالش‌ها و ملاحظات حقوقی ناشی از به‌کارگیری این فناوری تحلیل می‌شود. همچنین، تلاش خواهد شد رویکرد نظام حقوقی ایران در قبال این تحولات و میزان همگامی آن با رویکردهای نوین مبارزه با پولشویی نیز مورد بررسی قرار گیرد.

پیشینه پژوهش: پولشویی از موضوعاتی است که در ادبیات حقوق کیفری و جرم‌شناسی، از ابعاد مختلف مورد توجه قرار گرفته است. بخش قابل‌توجهی از پژوهش‌های موجود، به تبیین ابعاد کیفری و جرم‌شناختی پولشویی، تحلیل سیاست‌های جنایی در قبال آن و نیز بررسی تطبیقی مقررات داخلی با کنوانسیون‌ها و اسناد بین‌المللی اختصاص یافته است. با این حال، در سال‌های اخیر، توجه به نقش «ریسک» و «اطلاعات» در طراحی سازوکارهای پیشگیرانه نیز در برخی مطالعات مورد توجه قرار گرفته است.

در این میان، شاملو و خلیلی پاجی (۱۳۹۹) در مقاله «رویکرد ریسک‌مدار سیاست جنایی در برابر پولشویی»، با تمرکز بر ماهیت فراملی پولشویی، رویکرد ریسک‌مدار را در سیاست جنایی مقابله با این جرم مورد بررسی قرار داده‌اند. نویسندگان، ضمن توجه به نقش اسناد و سازوکارهای بین‌المللی در مبارزه با پولشویی، بر اهمیت اطلاعات مالی در مدیریت ریسک تأکید کرده و نقش واحدهای اطلاعات مالی و گروه اگمونت را در ارزیابی ریسک و اتخاذ تدابیر متناسب پیشگیرانه مورد توجه قرار

---

[1] . به‌عنوان نمونه نهادهای‌نظارتی ایالات‌متحده، ازجمله ازطریق قانون ضدپولشویی ۲۰۲۰ و راهبردملی مقابله‌با جرایم مالی، بانک‌ها را به‌پذیرش فناوری‌های پیشرفته از جمله یادگیری‌ماشین و کاهش موانع‌نظارتی تشویق کرده‌اند.

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer.

داده‌اند. این پژوهش از حیث تبیین مبانی رویکرد ریسک‌مدار و جایگاه اطلاعات مالی در سیاست جنایی مبارزه با پولشویی، برای پژوهش حاضر اهمیت دارد؛ با این حال، تمرکز آن بر ظرفیت‌های فناورانه و تحلیل داده در تحقق این رویکرد نیست.

در منبع دیگری نیز ثالث مؤید و همکاران در کتاب «نکات کاربردی جرم پولشویی»، با رویکردی حقوقی، تطبیقی و کاربردی، مقررات مربوط به جرم پولشویی را به‌صورت ماده‌به‌ماده بررسی کرده‌اند. این اثر از منظر تبیین چارچوب قانونی حاکم بر مبارزه با پولشویی در ایران، از منابع قابل توجه در تدوین پژوهش حاضر به شمار می‌رود؛ هرچند موضوع بهره‌گیری از داده و فناوری‌های نوین برای شناسایی و ارزیابی ریسک پولشویی در کانون بحث آن قرار ندارد.

در ادبیات بین‌المللی، پیوند میان فناوری‌های نوین و مبارزه با پولشویی، با انتشار گزارش «فرصت‌ها و چالش‌های فناوری‌های نوین برای مبارزه با پولشویی و تأمین مالی تروریسم» از سوی گروه ویژه اقدام مالی (FATF, 2021) با توجه بیشتری مواجه شده است. این گزارش، ضمن اشاره به چالش‌هایی که فناوری‌های نوین از حیث پیچیدگی و سرعت تراکنش‌های مالی ایجاد می‌کنند، ظرفیت همین فناوری‌ها را برای تقویت سازوکارهای مبارزه با پولشویی نیز مورد توجه قرار می‌دهد. اهمیت این گزارش برای پژوهش حاضر از آن جهت است که امکان پیوند میان فناوری‌های نوین و اجرای مؤثرتر رویکرد مبتنی بر ریسک را مطرح می‌سازد.

همچنین، برخی پژوهش‌های تخصصی‌تر نیز به قابلیت تحلیل داده در مبارزه با پولشویی پرداخته‌اند. برای نمونه، Hu و همکاران (۲۰۲۲) در پژوهشی با عنوان «تحلیل کلان‌داده برای مبارزه با پول‌شویی: مطالعه موردی کاربرد گرین‌پلوم متن‌باز» ظرفیت تحلیل کلان‌داده در پردازش و تحلیل اطلاعات مرتبط با پولشویی بررسی کرده‌اند. این دسته از مطالعات، از حیث تبیین ظرفیت‌های فنی داده و فناوری‌های نوین برای تحلیل الگوهای مالی و شناسایی فعالیت‌های مشکوک، زمینه مناسبی برای بررسی رویکرد داده‌بنیان فراهم می‌کنند.

همچنین (Vududala. 2024, p. 2) در مقاله با عنوان «ارتقای انطباق با مبارزه با پول‌شویی با استفاده از نیس اکتی‌مایز: رویکردی داده‌محور » با تمرکز بر یک سامانه خاص، ظرفیت رویکرد داده‌بنیان را در ارتقای فرایندهای انطباق و مبارزه با پولشویی بررسی کرده است. این پژوهش نشان می‌دهد که بهره‌گیری از تحلیل داده و سامانه‌های هوشمند می‌تواند با بهبود پایش تراکنش‌ها و شناسایی الگوهای مشکوک، کارآمدی سازوکارهای مبارزه با پولشویی را ارتقا دهد. با این حال، تمرکز اصلی پژوهش مزبور بر کاربست یک سامانه مشخص و ابعاد اجرایی انطباق است و مسئله را از منظر حقوقی و پیشگیرانه به‌صورت جامع بررسی نمی‌کند.

مرور این مطالعات نشان می‌دهد که اگرچه هر یک از پژوهش‌های پیشین بخشی از مسئله، از مبانی رویکرد ریسک‌مدار و الزامات حقوقی مبارزه با پولشویی تا ظرفیت‌های فناوری و تحلیل کلان‌داده، را مورد توجه قرار داده‌اند، میان این حوزه‌ها همچنان فاصله‌ای قابل مشاهده وجود دارد. به بیان دیگر، در پژوهش‌های مورد بررسی، کمتر تلاش شده است تا رویکرد

داده‌بنیان به‌عنوان حلقه اتصال میان شناسایی و ارزیابی ریسک از یک سو و پیشگیری از پولشویی از سوی دیگر، در یک چارچوب واحد مورد تحلیل قرار گیرد و هم‌زمان الزامات حقوقی و ابزارهای فنی تحقق آن نیز بررسی شود. ازاین‌رو، وجه تمایز پژوهش حاضر، صرفاً معرفی فناوری‌های نوین در مبارزه با پولشویی نیست؛ بلکه تلاش می‌شود با تمرکز بر کاربست رویکرد داده‌بنیان، ابتدا جایگاه آن در تحول سازوکارهای پیشگیرانه و شناسایی و ارزیابی ریسک تبیین شود، سپس ابزارهای فنی، به‌ویژه گونه‌های یادگیری ماشین، مورد بررسی قرار گیرد و در نهایت، چالش‌های حقوقی و اجرایی ناشی از این تحول تحلیل شود. افزون بر این، با توجه به ضرورت سنجش امکان تحقق این رویکرد در نظام حقوقی ایران، مقررات داخلی و زیرساخت‌های موجود نیز مورد توجه قرار گرفته است تا تصویری منسجم‌تر از ظرفیت‌ها و محدودیت‌های کاربست رویکرد داده‌بنیان در پیشگیری از پولشویی ارائه شود.

۱. مبانی نظری و الزامات کاربست رویکرد داده بنیان در پیشگیری از پولشویی

اولین نسل‌از سامانه‌های‌مبارزه‌باپولشویی برمبنای رویکردقاعده‌محور[1] استوار بود. در این رویکرد، فرایند نظارت‌بر تراکنش‌های‌مالی، رفتار مشتریان و سایر کنش‌های‌مالی بر اساس قوانین و آستانه‌های ازپیش تعیین‌شده هدایت می‌شد؛ به‌گونه‌ای‌که هرگونه تراکنش یا رفتاری که فراتر از این آستانه‌ها قرار می‌گرفت، به‌طور خودکار به‌عنوان مورد مشکوک به پولشویی یا جرایم مالی نشانه‌گذاری می‌گردید. (Ai. 2012, p. 200)

به‌عبارتی، این رویکرد فاقد هرگونه توانایی برای تمایز قائل شدن میان زمینه‌ها و بافت‌های متفاوت رفتاری یا تراکنشی است. برای نمونه، اگر قاعده‌ای مقرر دارد که «هر تراکنش نقدی بالای ۱۰۰۰۰ دلار باید گزارش شود»، سیستم بدون درنظرگرفتن نحوهٔ فعالیت قانونی مشتری، سابقهٔ‌شغلی او، الگوی‌مالی متعارف و یا هرگونه توجیه‌اقتصادی روشن، صرفاً براساس عبوراز آستانهٔ‌عددی، هشدار تولید می‌کند.[2]

---

[1] . Rule Based Approach.

[2] . این انعطاف‌ناپذیری افزون‌بر آنکه موجب قضاوت‌یکسان در موقعیت‌های‌ناهمسان می‌شود، این آسیب را نیز به‌همراه دارد که پولشویان با شناسایی دقیق همان‌قوانین، از خلاء‌قانونی سوءاستفاده کنند. (مانند اسمورفینگ؛ به‌معنای شکستن مبلغ‌تراکنش به واحدهای‌کوچک‌تر زیرآستانه گزارش‌دهی). همچنین چالش دیگر، نرخ بالای هشدارهای‌مثبت کاذب[2] در این رویکرد است. از آنجاکه قوانین در این رویکرد عمدتاً برپایهٔ آستانه‌های عددی تعریف می‌شوند، شمار قابل‌توجهی‌از تراکنش‌های کاملاً قانونی که صرفاً با یکی‌از آن آستانه‌ها یا الگوها مطابقت ظاهری پیدا می‌کنند، به‌عنوان مشکوک علامت‌گذاری می‌شوند. در این وضعیت، حجم انبوه هشدارهای بی‌نتیجه، ظرفیت پردازشی محدود تیم‌های تطبیق را مختل می‌کند؛ امری‌که منجربه هدررفت منابع محدود پردازشی و ناکارآمدی در شناسایی تهدیدهای‌اصلی می‌شود.(Omoseebi, et.al. 2025, p.17)

با توجه به چالش‌های موجود و عدم کارآمدی لازم، رویکرد قاعده‌محور کنار گذاشته شد و به‌جای آن درسال ۲۰۰۳، رویکرد ریسک‌مدار[1] متعاقب اصلاحات توصیه‌های گروه ویژه اقدام‌مالی[2] در توصیه شماره یک، معرفی شد و به‌مرور زمان ارتقاء یافت. (Koker, 2009, p.335) اتخاذ رویکرد ریسک‌مدار دربرابر پولشویی از مزیت‌هایی برخوردار است. مهم‌ترین مزیت این رویکرد، استفاده کاراتر از منابع و عملکرد مؤثرتر است. بر این اساس، از یک سو، حوزه‌های پولی و مالی و مشتریان پرریسک مورد نظارت بیشتر قرار می‌گیرند و از سوی دیگر هزینهٔ کمتری صرف مشتریان کم ریسک می‌شود. مزیت دیگر این رویکرد، انعطاف‌پذیری و پویایی آن است. ازآنجاکه ریسک حوزه‌های پولی‌و مالی ایستا نیست و باسرعت، روزآمد می‌شود، اتخاذ این رویکرد و سامانه‌پایش آن، باسرعتی بیشتر قادربه شناسایی ریسک‌های نوین خواهد بود. (شاملو؛ خلیلی پاجی، ۱۳۹۹، ص ۱۳۴) با این حال این تحول، صرفاً به دگرگونی شیوه‌های مبارزه با پولشویی محدود نمانده، بلکه در سطحی کلان‌تر، بر مبانی مداخله نظام عدالت کیفری نیز اثرگذار بوده است. در پرتو رویکرد مبتنی بر ارزیابی ریسک، حقوق کیفری به‌تدریج از الگوی صرفاً واکنشی فاصله گرفته و به سوی رویکردی احتمال‌محور حرکت کرده است. در این چارچوب، هدف اصلی دیگر صرفاً واکنش به جرم تحقق‌یافته نیست، بلکه شناسایی موقعیت‌های پرخطر و مداخله پیش از تحقق کامل رفتار مجرمانه نیز اهمیت می‌یابد.

با این‌حال با پیچیده‌تر شدن روش‌های ارتکاب‌جرم و به‌ویژه پولشویی، اتکای صرف به‌روش‌های‌سنتی ناکارآمد خواهد بود. رویکرد ریسک‌مدار اگرچه تحولات مثبتی ایجاد کرد و به کارآمدی فرآیند شناسایی مرتکبان انجامید، اما به‌دلیل ماهیت پنهان جرم پولشویی، که همواره در اشکالی‌نوظهور بروز می‌یابد و بخشی‌از داده‌های مرتبط‌با آن هیچ‌گاه کشف نمی‌شود، با کاستی‌هایی مواجه است. در واقع اعتبار و کارآمدی این رویکرد، وابستگی مستقیمی به کیفیت داده‌های مورد استفاده و دقت ابزارهای تحلیل آن‌ها دارد.(Massimiliano, 2025, p.2) در نتیجه، هر اندازه امکان گردآوری، پردازش و تحلیل داده‌های مرتبط با ریسک پولشویی افزایش یابد، زمینه برای اتخاذ تصمیم‌های پیشگیرانه دقیق‌تر نیز فراهم خواهد شد.

از سوی‌دیگر، اساسِ رویکرد ریسک‌مدار برپایه رهنگاشت‌های گروه‌ویژه شکل می‌گیرد که در آن، به‌عنوان نمونه ملاحظات‌سیاسی به‌ویژه در فرآیند تدوین فهرست‌سیاه، اثرگذار است.(Riccardi.2022, p.1) بدین‌سان ممکن است کشوری نه به‌دلیل ریسک واقعی پولشویی، بلکه به دلایل‌سیاسی در این فهرست قرار گیرد. بنابراین، باوجود ارزیابی کلی مثبت رویکرد ریسک‌مدار، تا زمانی که این رویکرد با رویکرد داده‌محور،[3] که توانایی درک الگوهای‌مجرمانه برای پیشگیری‌از جرم ازطریق تحلیل طیف‌گسترده‌ای از داده را داراست، تلفیق نشود، نمی‌توان بر کارآمدی آن به‌طور کامل تکیه کرد.

درواقع ظهور تحلیل داده‌های‌بزرگ[4] سرآغاز دوران تازه‌ای در نظام‌مبارزه با پولشویی با رویکرد مبتنی‌بر داده است. (Hu,et.al. 2022, p.637) این رویکرد از قدرت الگوریتم‌های‌پیچیده برای غربالگری مجموعه‌داده‌های بزرگ بهره می‌گیرد تا الگوها،

---

[1] . Risk Based Approach
[2] . FATF
[3] . Data Based Approach
[4] . Big Data Analytics

همبستگی‌ها و ناهنجاری‌هایی را که می‌توانند نشانه‌هایی از فعالیت مشکوک باشند، جستجو کند. (موسوی فر، نجفی، ۱۴۰۴، ص ۱۸۰) برخلاف رویکردهای پیشین که صرفاً به قوانین ایستا متکی بودند، این رویکرد با ابزارهای خود قادر است تا روابط پنهان و غیرخطی میان تراکنش‌ها را آشکار سازد. در این راستا ادغام یادگیری‌ماشین و هوش‌مصنوعی جدیدترین مرز درتوسعه سامانه‌های ضدپولشویی را نمایان ساخت و قابلیت‌های بی‌سابقه‌ای در تحلیل داده ارائه نمود. این سیستم‌های هوشمند با یادگیری‌از داده‌های تاریخی، الگوهای‌نوظهور پولشویی را شناسایی کرده و رویکردی فعالانه در برابر جرم اتخاذ می‌کنند. بدین‌ترتیب نظام عدالت کیفری بیش‌از گذشته بر ریل پیش‌بینی حرکت خواهد کرد. در واقع این‌گونه‌از عدالت با اتکاء بر تجزیه‌و تحلیل حجم عظیم داده بر پایه محاسبه احتمالات (ابراهیمی،۱۴۰۱، ص ۳۶) تا حد امکان به‌کشف جرایم خواهد انجامید. لذا پیشگیری با تعریفی عام تر قابل طرح است: انجام اقداماتی مبتنی‌بر پیش بینی، شناسایی و ارزیابی‌علمی خطر یا امکان‌وقوع جرم برای جلوگیری‌از وقوع یا کاهش یا به تعویق‌انداختن یا حتی تعدیل آثار، تغییر آماج، زمان، مکان یا شیوه ارتکاب‌جرم. (ابوذری؛ ۱۴۰۳، ص ۴۲)

بر این اساس، دو رکن بنیادین نظام پیشگیری از پولشویی، یعنی شناسایی مشتری (مطابق با توصیه‌نامه شماره‌ی ۱۰) و «شناسایی و گزارش تراکنش‌های مشکوک» (مطابق با توصیه‌نامه شماره‌ی ۲۰) گروه ویژه اقدام مالی[1]، در چارچوب رویکرد داده‌محور مورد واکاوی قرار خواهد گرفت.

۱،۱. شناسایی مشتری داده‌بنیان

از نخستین‌و اساسی‌ترین ارکان توصیه‌شده توسط گروه‌ویژه، شناسایی‌مشتری است. به‌عبارتی احراز هویت‌دقیق مشتری و ایجاد یک شناسه‌ریسک متناسب‌با فعالیت مشتری، در پیشگیری‌از پولشویی نقش موثری دارد. بند ۳۳ ماده ۱ آیین‌نامه اجرایی مقابله و پیشگیری از جرایم پولشویی و تأمین مالی تروریسم مصوب ۱۳۹۸/۰۷/۲۱ هیات وزیران نیز شناسایی مشتری را به‌عنوان یکی از مهم‌ترین ارکان پیشگیری از جرم به شمار آورده و آن را متناسب با سطح ریسک ارباب رجوع که مستمراً می‌بایست مورد ارزیابی قرار گیرد به سه سطح ساده، معمول و مضاعف تقسیم نموده است. این تقسیم‌بندی و لزوم پایش مستمر ریسک مشتری نشان می‌دهد که اطلاعات و داده در شناسایی ریسک مشتری اهمیتی بنیادین دارد.

این الزام، امروزه و دربطن رویکرد داده‌بنیان، با کیفیتی به‌مراتب دقیق‌تر از گذشته، انجام می‌پذیرد. در این راستا بهره‌گیری از انواع داده اعم از کلان‌داده[2] و داده‌جایگزین[3] اهمیت انکارناپذیری در پروفایل‌سازی ریسک مشتریان و دسته‌بندی ایشان خواهد

---

[1] . FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, Franc.

[2] . Big Data

به‌مجموعه‌ای‌از داده‌های ساختاریافته، نیمه‌ساختار یافته یا بدون‌ساختار اطلاق می‌شود که برای ذخیره‌سازی، پردازش‌وتحلیل به فناوری‌ها و رویکردهای خاصی نیاز دارد و درمقایسه با داده‌های‌سنتی، از چهار ویژگی حجم، سرعت، تنوع‌و دقت برخوردار است.

[3] . Alternative Data

داشت. در واقع امروزه صنعت‌مالی به‌طور ذاتی، حجم عظیمی‌از داده‌ها را تولید می‌کند که شامل داده‌های‌مصرف‌کننده، گزارش‌های محصولات‌مالی و جزئیات تراکنش‌ها می‌شود. در سطح اجرایی، لایه جذب‌داده[1] داده‌های تراکنش مالی را از منابع‌متعددی از جمله سیستم‌های بانکی، درگاه‌های‌پرداخت، شبکه‌های بلاک‌چین و تأمین‌کنندگان داده‌های‌مالی شخص ثالث جمع‌آوری و یکپارچه می‌سازد. این لایه به‌طور همزمان شامل داده‌های ساختاریافته (مانند اطلاعات‌تراکنش) و داده‌های بدون‌ساختار (مانند ایمیل‌هاو تعاملات مشتری) می‌شود. .(Husnaningtyas, et.al. 2023, p.100)

این داده‌ها درصورت ترکیب‌با منابع اطلاعاتی‌مکمل نظیر داده‌های‌شبکه‌های اجتماعی (مانند فیسبوک) و آدرس‌های وب؛ که از آن به‌عنوان داده‌جایگزین نیز یاد می‌شود می‌توانند با فراهم‌آوردن امکان‌درک عمیق‌تر از ترجیحات‌خرید و نیز شناسایی نوع‌رفتارهای‌مالی هر مشتری، این قابلیت را به‌اشخاص مشمول بدهند که رفتارهای نامنظم‌و مشکوک را براساس پروفایلِ شخصی‌سازی شده هر مشتری شناسایی کنند. سیستم‌های مبتنی‌بر کلان‌داده با بهره‌گیری‌از هوش‌مصنوعی، به‌صورت بلادرنگ علائم‌تقلب را بررسی کرده، کاربران یا تراکنش‌های‌غیرمجاز را پیش‌بینی و هشدارهای‌احتیاطی صادر می‌کنند.

شناسایی‌دقیق مشتری برپایه داده‌های‌کلان و جایگزین از آن‌رو حائز اهمیت است که از منظر علت‌شناس جنایی نیز، بسیاری‌از جرایم اقتصای، به دلیل خلاء اطلاعاتی ناشی از شناسایی‌دقیق مشتری رخ می‌دهند. این امر به‌ویژه درخصوص موسسات‌مالی چندلایه و فرامرزی که شناسایی‌دقیق ذی‌نفع اصلی دشوار است، پیچیده‌تر می‌شود.

به‌عنوان نمونه اصل‌شفافیت درشناسایی ذی‌نفع[2] نقش‌اساسی در پیشگیری، کشف‌و تعقیب جرایم‌مرتبط با پولشویی‌و تامین مالی تروریسم دارد. ذی‌نفع نهایی به شخص‌حقیقی اطلاق می‌شود که مالکیت‌اصلی وجوه یا سهام یک‌شرکت را در اختیار دارد. بااین‌حال، درموارد متعددی هویت این شخص در اختیار نهادهای‌قانونی برای پایش‌اطلاعات قرار نمی‌گیرد و او فاقد هرگونه اختیار ظاهری در اداره شرکت است. چنین وضعیتی موجب می‌شود که هویت‌مالک‌واقعی، به‌رغم اعمال‌کنترل‌مؤثر بر دارایی‌ها، در ساختار رسمی‌شرکت مخفی بماند. در این شرایط، داده‌های‌کلان و جایگزین می‌توانند به‌عنوان ابزاری‌کارآمد، شکاف‌اطلاعاتی یادشده را پر کنند.

یکی‌از اصلی‌ترین داده‌های قابل‌دسترسی در این زمینه، داده‌های مالکیت مؤثر است. در این راستا گروه‌ویژه اولین استانداردهای‌بین‌المللی درخصوص شفافیت‌مالکیت ذی‌نفع را درسال ۲۰۰۳ منتشر نمود که مطابق‌با آن کلیه اشخاص‌مشمول ملزم‌به شناسایی‌و تایید اطلاعات درباره مالکیت‌نهایی اشخاص‌حقوقی شدند.(FATF, 2003, pp.11-12). در این‌میان کلان‌داده

به‌مجموعه داده‌های غیرسنتی و غیرمالی اطلاق می‌شود که از منابعی مانند شبکه‌های‌اجتماعی، آدرس‌های وب، صورتحساب‌های تلفن همراه یا داده‌های مکان‌محور گردآوری می‌شوند و یکی‌از کاربردهای آن تکمیل پروفایل ریسک مشتری است.

[1] . Data Ingestion Layer

[2] . Beneficial ownership transparency

و داده‌جایگزین بادسترسی به داده‌های تلفن‌همراه، داده‌های موقعیت‌جغرافیایی، شاخص‌های‌تحرک[1]مبتنی بر حسگرهای تلفن‌هوشمند؛ داده‌های شعاع‌چرخش[2] و آنتن‌هایی که تلفن‌همراه بیشترین اتصال را با آنها داشت؛ تا حد زیادی می‌توانند نسبت‌به هویت کاربر مشکوک و شاخه‌های ارتباطی او اطلاع پیدا کرده و تدابیرکنشی را دربرابر او اتخاذ کنند.[3]

۱/۲. بازشناسی تراکنش‌های مشکوک از رهگذر داده‌های رفتاری

یکی دیگر از ارکان اساسی در پایش نظام اقتصادی و پیشگیری از وقوع جرم، که توصیه‌های گروه ویژه اقدام مالی نیز بر آن تاکید نموده‌اند، ردیابی تراکنش‌های مشکوک و گزارش به‌موقع آنها[4] به نهادهای ناظر همچون مرکز اطلاعات مالی[5] است. در واقع، گزارش به‌هنگام عملیات مشکوک در بازه‌ای معقول، نقشی تعیین‌کننده در رهگیری به‌موقع عواید مجرمانه، کشف جرایم، تعقیب و مجازات مجرمان حرفه‌ای ایفا می‌کند. ماده ۱۳۵ آیین‌نامه اجرایی مقابله و پیشگیری از جرایم پولشویی و تأمین مالی تروریسم نیز در همین راستا، اشخاص مشمول را مکلف کرده است که هرگاه پس از بررسی اولیه، ظن به وقوع پولشویی، تأمین مالی تروریسم یا سایر جرایم منشأ حاصل شود، بدون اطلاع ارباب‌رجوع و مطابق سازوکار اعلامی مرکز اطلاعات مالی، مراتب راگزارش کنند. بدین‌ترتیب، تشکیل ظن معقول به وقوع جرم، یکی از مهم‌ترین مبانی آغاز فرآیند گزارش‌دهی در نظام حقوقی ایران به شمار می‌رود. با این حال، پرسش اساسی آن است که این ظن بر چه مبنایی شکل می‌گیرد و چه معیارهایی می‌تواند آن را از یک حدس یا گمان صرف متمایز سازد؟

در ادبیات مبارزه با پولشویی و همچنین در ضوابط حاکم بر نظام حقوقی ایران، شکل‌گیری ظن معمولاً بر پایه مجموعه‌ای از شاخص‌های خطر صورت می‌گیرد.[6] برای نمونه، معاملاتی که از حیث مبلغ یا ساختار، غیرمتعارف باشند، فاقد هدف اقتصادی یا مشروعیت ظاهری به نظر برسند، یا با الگوی شناخته‌شده فعالیت، وضعیت مالی و نیمرخ مشتری سازگار نباشند، می‌توانند از

---

[1] . mobility

[2] . radius of gyration

[3] . یکی‌از بزرگترین پرونده‌های‌کلاهبرداری‌مالی درجنوب‌شرق‌آسیا، مربوط‌به ترونگ می‌لان، رئیس‌گروه وان‌تین‌فات است. او با استفاده‌از بیش‌از ۷۰ سهامدار صوری، بدون‌آنکه نامش در هیچ سندرسمی مالکیتی قید شود، توانست کنترل‌پنهانی بربانک سایگون کامرشال بانک (SCB) که بزرگترین بانک ویتنام ازنظر دارایی است، به‌دست گیرد. طی یک‌دهه، بیش‌از ۱۲ میلیارد پوند وام کلاهبرداری‌شده ازطریق ساختارهای‌پیچیده مالکیت هدایت شد و از شرکت‌های پوسته، مدیران‌اسمی و هلدینگ‌های فراساحلی برای پنهان‌کردن کنترل‌واقعی استفاده گردید. درواقع اتکای‌صرف به آستانه‌های‌درصدی مالکیت (مانند ۲۵ درصد) کافی نیست، زیرا این‌آستانه‌ها ازطریق خردسازی سهام، سهامداران اسمی و شرکت‌های‌پوسته قابل دور زدن هستند. شناسایی‌مؤثر مالک‌نهایی مستلزم بررسی مالکیت یکپارچه، روابط غیرمستقیم و ساختارهای‌حاکمیتی است. همچنین کنترل‌واقعی ممکن است بدون هیچ‌گونه مالکیت‌قانونی و ازطریق روابط تاریخی یا غیررسمی با مدیران یا سهامداران اعمال شود. درچنین بافتاری، داده‌های‌جایگزین نظیر داده‌های ثبت‌شرکتی فرامرزی و الگوهای شبکه‌ای روابط مدیریتی، می‌توانند لایه‌های‌پنهان مالکیت مؤثر را که درساختارهای صوری نامرئی باقی مانده‌اند آشکار سازند.

AsiaVerify. (2025). Discover how hidden UBO links can derail deals and how to spot them with registry-backed data. https://asiaverify.com/resources/insights/the-hidden-ubo-web-uncover-business-ownership-risk/

[4] . Suspicious Transaction Report (STR)

[5] . Financial Intelligence Units (FIUs)

٦ . تبصره ماده ۷ قانون مبارزه با پولشویی اصلاحی ۱۳۹۷.

جمله نشانه‌های ایجاد ظن به وقوع پولشویی تلقی شوند. با وجود این، اتکای صرف به چنین شاخص‌هایی، به‌ویژه هنگامی که ارزیابی آن‌ها بر قضاوت انسانی یا قواعد از پیش تعیین‌شده استوار باشد، همواره از دقت و جامعیت کافی برخوردار نیست. پیچیده‌تر شدن الگوهای پولشویی و استفاده از شیوه‌های نوین پنهان‌سازی عواید مجرمانه، موجب شده است که بسیاری از معاملات مشکوک از فرآیند شناسایی خارج بمانند یا در مقابل، تعداد قابل توجهی هشدار کاذب تولید شود.

به همین دلیل امروزه تلاش می‌شود تا شناسایی‌داده‌های مبهم و مشکوک به صورت تحلیل هوشمند بر روی تراکنش‌های در حال اجرا با بهره گیری از یادگیری ماشین انجام شود.[1] درگذشته، به دلیل محدودیت در ابزارها و حجم داده، تنها چند مؤلفه محدود در الگوگذاری معاملات مشکوک استفاده می‌شد، حال آنکه امروزه به دلیل وجود حجم وسیعی‌از کلان‌داده و داده‌های‌جایگزین، همزمان تمامی مؤلفه‌ها درسنجه ارزیابی قرار گرفته و متعاقباً تصویر واقع‌بینانه‌تری از تراکنش‌های مشکوک به‌دست می‌آید.

آمارها نیز حاکی‌از آن است که به‌کارگیری روش‌های مبتنی‌بر هوش مصنوعی در کشف جرم، منجربه افزایش دقت تشخیص‌و کاهش هشدارهای اشتباه می‌شود، به‌گونه‌ای‌که ابزارهای هوش مصنوعی حدود ۳۰ تا ۵۰ درصد تراکنش‌های مشکوک بیشتری را نسبت‌به مدل‌های‌سنتی تشخیص می‌دهند که ازگذر آن، صدور هشدارهای اشتباه درخصوص تشخیص تراکنش به‌عنوان مشکوک/غیرمشکوک (منفی‌و مثبت کاذب) تاحدود ۶۰ درصد کاهش یافته است. (Vududala, 2024, p.3)

ازجمله مولفه‌های‌کلیدی در کارآمدی رویکرد داده‌محور و پیش‌بینی‌الگوریتم‌های مشکوک توسط یادگیری ماشین، همانا بهره‌گیری‌از منابع داده‌ای غنی و روزآمد است. در این راستا کیفیت، تنوع و کامل بودن داده‌ها به طور قابل توجهی بر دقت و پایایی سیستم تأثیر می‌گذارد. از مهم‌ترین‌اطلاعات استخراج‌شده ازمجموعه داده‌ها می‌توان به این‌موارد اشاره نمود:((Mukhamadiyev, et.al.2025: pp. 3,4.

الف) شناسه‌یکتای تراکنش[2]: برپایه اصول «قابلیت ردیابی و «حفظ مسیرحسابرسی» که همواره ازمهم‌ترین مولفه‌های پیشگیری‌از پولشویی بوده‌اند، هر تراکنش مالی باید به شناسه‌ای یکتا و تغییرناپذیر مجهز باشد تا درصورت وقوع تخلف، امکان ارجاع دقیق‌به آن رخداد برای مراجع قضایی میسر گردد.

---

[1] . بیش‌از ٪۸۰ از مدیران ضدپولشویی بانک‌های بزرگ آمریکای شمالی درحال پیاده‌سازی یادگیری ماشین هستند. این رویکرد در مؤسسات پیشرو، کشف تراکنش‌های مشکوک را ٪۴۰ و کارایی را تا ٪۳۰ افزایش داده است.

The fight against money laundering: Machine learning is a game changer | McKinsey https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/

[2] . Transaction_Id

ب) شناسه کاربر:[1] این ویژگی نه فقط برای ردیابی الگوهای‌فردی، بلکه برای کشف تغییرناگهانی رفتار کاربر حیاتی است؛ چرا که اگر تراکنشی از الگوی همیشگی یک کاربر منحرف شود، یکی‌از قوی‌ترین نشانه‌های هشدار است.

پ) شناسه کارمند:[2]ردیابی ویژگی‌های منحصربه‌فرد هر کارمند امکان شناسایی «همدستی درونی» یا «سوءاستفاده از دسترسی» را فراهم می‌کند؛ عاملی که بسیاری‌از سیستم‌های متعارف از آن غافل می‌مانند.

ت) مبلغ تراکنش:[3]اهمیت این مولفه هنگامی آشکار می‌شود که به‌نسبت با میانگین مبلغ تراکنش‌های پیشین همان کاربر یا انحراف معیار مقادیر در یک بازه‌زمانی کوتاه سنجیده شود. جهش‌ناگهانی در مبلغ، یکی‌از نشانه‌های هشدار را در الگوریتم‌های‌تشخیص ناهنجاری به‌خود اختصاص می‌دهد.

ث) زمان تراکنش:[4] تحلیل الگوهای زمانی محدودبه ساعتی از شبانه‌روز نیست؛ بلکه با استخراج ویژگی‌های مشتق‌شده مانند فاصله‌زمانی از آخرین تراکنش، تعداد تراکنش‌ها در دقیقه آخر یا تفاوت‌زمانی تراکنش با الگوی خواب و بیداری کاربر؛ می‌تواند نشانگر تلاش غیرمجاز یا سوء استفاده از اطلاعات کاربر در جهت مقاصد نامشروع باشد.

ج) روش پرداخت:[5]ارزش اصلی این ویژگی نه در ریسک ثابت هر روش پرداخت، بلکه در تغییر غیرمنتظره روش پرداخت توسط یک کاربر خاص نهفته است. درواقع، مدل یادگیری‌ماشین باید برای هرکاربر، روش‌های پرداخت او را به‌عنوان الگوی مبنا در نظر بگیرد. هر انحراف معنادار از این الگو، (مثلاً کاربری که همیشه از کارت نقدی استفاده می‌کرده، ناگهان از حواله بانکی استفاده کند)، نسبت به حالتی که کاربری همیشه از یک روش پرریسک استفاده می‌کند، هشدار قوی‌تری ایجاد می‌کند.

چ) موقعیت مکانی:[6] اهمیت این ویژگی در تشخیص ناسازگاری مکانی_زمانی نهفته است. یک موقعیت جغرافیایی به‌تنهایی نشانه هشدار نیست، مگر آنکه با ویژگی‌زمان‌تراکنش ترکیب شود. معیارتشخیصی، عدم امکان‌فیزیکی جابه‌جایی میان دو موقعیت دربازه زمانی ثبت‌شده میان دو تراکنش متوالی است. افزون‌بر این، عدم تطابق موقعیت تراکنش با آدرس‌صورت‌حساب یا محدوده‌جغرافیایی غالب فعالیت کاربر، به عنوان یک شاخص مستقل، احتمال ارتکاب جرم را افزایش می‌دهد.

---

[1] . user- Id
[2] . Merchant-Id
[3] . transaction amount
[4] . timestamps
[5] . payment method
[6] . Location

ح) نشانی پروتکل اینترنت (آی پی):[1] بررسی تعلق آی‌پی به شبکه‌های پنهان‌ساز نظیر Tor[2]،(خلیلی پاجی، ۱۴۰۱، ص ۱۰۸) پروکسی‌های عمومی و وی‌پی‌ان‌های تجاری رایگان حائز اهمیت است؛ چه آنکه حضور در چنین‌شبکه‌هایی در تراکنش‌های عادی نادر می‌نماید، اما در فعالیت‌های مشکوکی همچون پولشویی یا کلاهبرداری بسامدی قابل توجه دارد.

درصورتی که هر یک از موقعیت‌های یادشده در داده‌های موجود در سامانه‌های پرداخت رخ دهند، اقدامات قانونی به‌صورت مرحله‌ای انجام خواهد پذیرفت. این اقدامات در مرحله نخست شامل انسداد حساب‌ها و توقیف وجوه یا دارایی‌های شخص به علت ریسک بالا است و درمراحل بعدی ممکن است با آغاز اقدامات قضایی ادامه یابد.(شاملو، خلیلی پاجی، ۱۳۹۹، ص ۱۳۳) ویژگی‌های فوق، درصورت بررسی توأمان، نشانه‌های دقیقی فراهم می‌آورند که می‌توان با تکیه‌بر آن‌ها تراکنش‌های‌مشکوک را شناسایی کرد

در این‌راستا، سامانه‌های یادگیری ماشین وجود چندین‌نوع ویژگی را به‌عنوان الگوهای مشکوک و جرم‌زا شناسایی کرده‌اند. این الگوها که غالباً مبتنی‌بر سابقه پرونده‌های پیشین استخراج شده‌اند، نشانه‌هایی‌از تقلب و خروج‌از چارچوب قانونی را ارائه می‌دهند و بدین‌ترتیب، بازشناسی تراکنش‌های‌مشکوک را از فعالیت‌های‌مالی قانونی تسهیل می‌کنند.(Mukhamadiyev, et.al, 2025, p.3) ازجمله این ویژگی‌ها می‌توان به تراکنش‌های به‌طور غیرعادی بزرگ اشاره کرد؛ تراکنش‌هایی که به‌مراتب بزرگ‌تر از الگوی‌معمول هزینه‌کرد مشتری هستند. همچنین مجموعه‌ای‌از تراکنش‌های کوچک که در بازه زمانی کوتاهی انجام می‌شوند نیز می‌توانند مشکوک تلقی شوند، به‌ویژه آن دسته که ممکن است از استانداردهای پنهان برای دور زدن آستانه‌های تراکنش[3] استفاده کنند. از دیگر نشانه‌های مهم، ناهنجاری‌های‌جغرافیایی است، تراکنش‌هایی که‌از مناطقی سرچشمه می‌گیرند که مشتری پیش‌از این هرگز در آنها فعالیت‌تجاری نداشته است. همچنین تراکنش‌هایی که با کشورهای شناخته‌شده در زمینه تقلب‌یا پول‌شویی در ارتباط باشند[4]، در زمره تراکنش‌های پرخطر طبقه‌بندی می‌شوند. زمان‌بندی‌غیرعادی نیز یکی‌دیگر از شاخص‌های هشداردهنده است؛ برای‌نمونه، تراکنش‌هایی که در ساعات‌یا روزهای‌غیرمعمول برای مشتری انجام می‌شوند،

---

[1] . Ip_Address

[۲] . Tor در اصل یک شبکه توزیع رایانه‌ای است که آدرس IP واقعی کاربر را پنهان می‌کند و به‌همین علت هویت کاربران شبکه را با مسیریابی ارتباطات/ معاملات از طریق چندین رایانه در سراسر جهان از شناسایی مصون می‌سازد و آن‌ها در چندین لایه رمزگذاری شده قرار می‌دهد.

۳ . آستانه‌های‌تراکنش به مقادیراز پیش‌تعیین‌شده‌ای اطلاق می‌شوند که فراتراز آن‌ها، یک تراکنش به‌طورخودکار جهت بررسی‌بیشتر مورد جداسازی قرار می‌گیرد.

[۴] . گروه ویژه اقدام مالی در تفسیر توصیه شماره (۱۰)، برخی حوزه‌های قضایی را به‌عنوان عوامل مؤثر در ارزیابی ریسک مورد توجه قرار داده است. این موارد عبارت‌اند از: الف) کشورهایی که دارای کاستی‌های راهبردی در نظام مبارزه با پولشویی و تأمین مالی تروریسم هستند؛ ب) کشورهایی که مشمول تحریم‌ها، محدودیت‌ها یا سایر اقدامات مشابه، از جمله تحریم‌های شورای امنیت سازمان ملل متحد، قرار گرفته‌اند؛ پ) کشورهایی که به‌دلیل شیوع فساد یا فعالیت‌های مجرمانه، در معرض ریسک بالاتری قرار دارند؛ و ت) کشورها یا مناطق جغرافیایی که به‌عنوان تأمین‌کننده یا حامی فعالیت‌های تروریستی شناخته می‌شوند یا سازمان‌های تروریستیِ مشمول تحریم در قلمرو آن‌ها فعالیت دارند.

High-risk and other monitored jurisdictions https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html

به‌طور بالقوه مشکوک‌اند. درنهایت، تراکنش‌هایی با ویژگی‌های غیرعادی نظیر انتقال‌وجه بین چندین حساب بدون‌دلیل آشکار، همواره یکی‌از کلاسیک‌ترین الگوهای‌مشکوک به‌شمار می‌روند.

۲. ابزارهای فنی کاربست رویکرد داده‌بنیان

در این‌راستا، برخی‌از الگوریتم‌های پیشرفته در این حوزه توانایی‌بالایی درپیش‌بینی دقیق و پیشگیری‌مؤثر از جرایم‌اقتصادی دارند. به‌طور کلی، الگوریتم‌های‌یادگیری ماشین بر اساس ماهیت‌داده‌های ورودی و روش‌یادگیری، به دو دسته‌اصلی تقسیم می‌شوند.(Alloghani, et.al. 2020, p.4.) در این قسمت ضمن بررسی فرصت‌ها و چالش‌های این دو شاخه اصلی به تحلیل زیرشاخه‌های هریک از رویکردها نیز پرداخته خواهد شد.

در سال‌های اخیر، این رویکرد در نظام مبارزه با پولشویی ایران نیز تا حدودی مورد توجه قرار گرفته است. از جمله، مرکز اطلاعات مالی با راه‌اندازی سامانه جامع و هوشمند مبارزه با پولشویی (سمام) و سامانه برخط استعلامات (سبا)، گام‌هایی در جهت بهره‌گیری از ابزارهای داده‌بنیان برداشته است.(https://www.fiu.gov.ir/sa2ma1) سامانه «سمام» با اتصال برخط به پایگاه‌های اطلاعاتی دستگاه‌های مختلف، امکان تجمیع و پردازش یکپارچه داده‌های مالی، ارزیابی و امتیازدهی گزارش‌های معاملات مشکوک بر مبنای رویکرد مبتنی بر ریسک و ارائه تحلیل‌های هوشمند برای تصمیم‌گیری کارشناسان مرکز اطلاعات مالی را فراهم می‌آورد. همچنین، این سامانه با بهره‌گیری از فناوری‌های هوش مصنوعی و یادگیری ماشین، درصدد افزایش دقت تحلیل داده‌ها و کاهش زمان رسیدگی به گزارش‌های دریافتی است. در کنار آن، سامانه «سبا» نیز با فراهم ساختن دسترسی برخط به پایگاه‌های اطلاعاتی دستگاه‌های اجرایی و قضایی، امکان تکمیل و تقویت تحلیل گزارش‌های معاملات مشکوک را فراهم کرده است. هرچند ارزیابی میزان کارآمدی این سامانه‌ها مستلزم انتشار داده‌ها و گزارش‌های عملکردی است، راه‌اندازی آن‌ها را می‌توان نشانه‌ای از حرکت نظام مبارزه با پولشویی ایران به سوی بهره‌گیری از رویکردهای داده‌بنیان و ابزارهای هوشمند در شناسایی و ارزیابی ریسک دانست.

۲/۱. یادگیری نظارت‌شده

یادگیری‌نظارت‌شده یکی‌از متداول‌ترین رویکردها در سیستم‌های مبتنی بر یادگیری ماشین برای انطباق با مقررات ضدپولشویی به‌شمار می‌رود. در این رویکرد، الگوریتم با استفاده‌از یک مجموعه‌داده برچسب‌خورده[1] آموزش داده می‌شود؛ بدین‌معناکه به هرنمونه، برچسب مشکوک یا غیرمشکوک نسبت داده می‌شود. الگوریتم با یادگیری تابع بین ویژگی‌های‌داده و برچسب‌ها، قادر خواهد بود بر روی داده‌های‌جدید، وظیفه پیش‌بینی یا دسته‌بندی را انجام دهد.(Zhang, & Trubey. 2019, p.1050)

[1] . Labeled Dataset

این الگوریتم‌ها با به‌روزرسانی مداوم مبتنی بر داده‌های برچسب‌خورده جدید، دقت تشخیص خود را در طول زمان افزایش می‌دهند.[1]

هدف اصلی در این رویکرد، کشف تقلب‌و متوقف کردن آن درمرحله شروع به‌جرم است. با این‌حال کارآمدی این روش به‌طور قابل‌توجهی به‌وجود تمایز آشکار و قابل تشخیص میان الگوهای فعالیت‌های‌مجاز و غیرمجاز وابسته است.

در ذیل این رویکرد چندین زیرشاخه الگوریتمی صورتبندی می‌شود که عبارتند از:

۲/۱/۱. **رگرسیون لجستیک**[2]: این الگوریتم یک مدلِ طبقه‌بندی از نوع احتمالاتی است و وظیفه اصلی آن، تولید یک خروجی‌دودویی (۰ یا ۱) براساس ویژگی‌های‌ورودی می‌باشد. به‌عنوان نمونه برای طبقه‌بندی تراکنش‌های مشکوک از ۱ و برای تراکنش‌های‌عادی از ۰ استفاده می‌شود. رگرسیون لجستیک با دریافت داده‌های‌ورودی همچون مبلغ تراکنش، زمان انجام تراکنش، موقعیت جغرافیایی، سابقه حساب، نوع پایانه و تعداد تراکنش‌های قبلی در بازه‌کوتاه، احتمال قانونی یا غیرقانونی بودن هر تراکنش را محاسبه می‌کند. این مدل با اعمال تابع ریاضی روی ترکیب خطی این ویژگی‌ها، عددی بین ۰ و ۱ خروجی می‌دهد. سپس با آستانه‌ای مانند ۰.۵ تراکنش‌هایی با احتمال بالاتر از آستانه را در دسته مشکوک (۱) و مابقی را در دسته‌عادی (۰) طبقه‌بندی می‌کند.

با این‌حال اگرچه این مدل قادر به دریافت همزمان چندین ویژگی (مانند مبلغ، ساعت، موقعیت جغرافیایی، آی‌پی و...) است، اما مهم‌ترین محدودیت آن درماهیت خطی این مدل نهفته است. به عبارت دیگر، رگرسیون لجستیک فرض می‌کند که هر ویژگی به طور مستقل و بدون توجه به سایر ویژگی‌ها، سهم‌خطی خود را در خروجی نهایی اعمال می‌کند. در حالی‌که، در بسیاری از الگوهای تقلب، شرط وقوع تراکنش مشکوک به صورت غیرخطی و وابسته به چند ویژگی است؛ برای مثال، یک تراکنش تنها زمانی مشکوک محسوب می‌شود که همزمان مبلغ آن بالا، ساعت انجام آن غیرعادی و آی‌پی کاربر ناشناس باشد. درنتیجه، درمواجه با چنین الگوهای پیچیده‌ای، ممکن است خطای‌تشخیص به ویژه منفی‌کاذب[3] افزایش یابد. (Fei, et.al, 2025, p.9)

۲,۱,۲ **کا-میانگین:**[4] این مدل براساس این اصل ساده عمل می‌کند که نقاط نزدیک به هم در فضای ویژگی‌ها، معمولاً متعلق به یک دسته هستند. به عبارتی، برای آنکه مدل تشخیص دهد یک تراکنش جدید مشکوک است یا عادی،

---

[1] . Financial Crime Academy, "Safeguarding Against Money Laundering: Essential Machine Learning Algorithms for AML," July 13, 2026, https://financialcrimeacademy.org/machine-learning-algorithms-for-aml/.

[2] . Logistic Regression

[3] . False Negatives

وضعیتی که‌در آن یک‌تراکنش یا رفتار مشکوک واقعی توسط سیستم شناسایی نمی‌شود و به‌اشتباه به‌عنوان عادی تلقی می‌گردد.

[4] . K-Nearest Neighbors (KNN)

کافی است نزدیک‌ترین تراکنش‌های موجود در مجموعه‌داده را به آن بررسی کند. به‌عنوان نمونه اگر مقدار K برابر ۵ انتخاب شده باشد؛ مدل به‌دنبال ۵ تراکنشی می‌گردد که از همه نظر (از نظر ویژگی‌هایی مانند مبلغ، زمان و...) به تراکنش جدید شباهت بیشتری دارند. اگر از میان این ۵ نمونه، سه مورداز آن‌ها برچسب مشکوک و دو مورد از آنها برچسب‌عادی داشته باشند، مدل رأی‌اکثریت را می‌پذیرد و تراکنش جدید را در دسته مشکوک طبقه‌بندی می‌کند. چالش اصلی این مدل آن است که با افزایش حجم‌داده‌ها، کند عمل می‌کند. (Halder. et al, 2024, pp.4-6)

۲،۱،۳. **درخت‌های تصمیم:**[1] درخت‌تصمیم ساختاری شبیه‌به نموداردرختی برای طبقه‌بندی داده‌ها ایجاد می‌کند. این الگوریتم با پرسش درخصوص مواردی‌از ویژگی‌های یک تراکنش (مانند آیا مبلغ تراکنش بیشتر از ۱۰۰ میلیون تومان است؟ یا آدرس‌آی‌پی کاربر درمحدوده کشورهای پرخطر قرار دارد؟) در هر گام، داده‌ها را به طور مکرر به زیرمجموعه‌های کوچک‌تر تقسیم می‌کند. هرپرسش در یک گره[2] قرار می‌گیرد و پاسخ به آن، مسیر حرکت به‌سمت شاخه بعدی را مشخص می‌کند (Vorobyev and Krivitskaya. 2022, pp.2-3) این فرآیند تا رسیدن به یک برگ ادامه می‌یابد که برگ نهایی، حاوی تصمیم قطعی مدل یعنی مشکوک یا عادی بودن تراکنش است. مزیت اصلی این روش شفافیت کامل آن است، به‌گونه‌ای که مسیر طی‌شده از ریشه تا برگ را می‌توان به‌مجموعه‌ای از قوانین ساده «اگر-آنگاه» تبدیل کرد. برای نمونه، مدل تشخیص تقلب می‌تواند به‌این صورت باشد: اگر مبلغ تراکنش بالای ۱۰۰ میلیون باشد و آی‌پی کاربر خارج از کشور باشد و ساعت انجام تراکنش بین ۲ تا ۴ بامداد باشد، آنگاه تراکنش مشکوک است.

با این‌حال این‌مدل مستعد بیش‌برازش[3] است. وضعیتی‌که در آن مدل، به‌جای یادگیری‌الگوهای‌عمومی حاکم‌بر داده‌ها، جزئیات‌تصادفی، نویزهاو نقاط پرت مجموعه آموزشی را به طور کامل به خاطر می‌سپارد. درچنین حالتی، مدل توانایی تعمیم به داده‌های جدید و دیده‌نشده را از دست می‌دهد، به ویژه زمانی که عمق درخت افزایش یافته و ساختار آن پیچیده می‌شود. در واقع این مدل در مواجه با داده‌های جدید و دیده‌نشده نرخ تشخیص بسیار ضعیفی خواهد داشت.[4]

۲،۱،۴. **جنگل تصادفی**[5]**:** این مدل ترکیبی از تعداد زیادی درخت‌تصمیم را برای طبقه‌بندی معاملات مشکوک به‌کار می‌گیرد. این مدل در مقایسه با مدل‌های پایه مانند رگرسیون لجستیک یا کا-میانگین، دقت بالاتری درشناسایی تراکنش‌های‌مشکوک دارد. دلیل اصلی این امر، توانایی جنگل تصادفی درشناسایی الگوهای‌غیرخطی و

---

[1] . Decision Trees
[2] . Node
[3] . Overfitting
[4] . Fraud Detection Handbook. (2021). *Chapter 5: Model Validation and Selection - Introduction*. GitHub. Available at: https://github.com/Fraud-Detection-Handbook/fraud-detection handbook/blob/main/Chapter_5_ModelValidationAndSelection/Introduction.md
[5] . Random Forest

تعاملات پیچیده میان ویژگی‌ها و بهره‌گیری‌از تعداد بالای درخت‌های تصمیم است. در این راستا جنگل‌تصادفی با ترکیب تعداد زیادی درخت و میانگین گرفتن‌از پیش‌بینی‌های آن‌ها، ضمن حفظ‌توانایی درکشف الگوهای پیچیده، مشکل بیش‌برازش را به‌طور چشمگیری کاهش می‌دهد. (Liaw, et.al. 2002, pp.18-22)

با این‌حال، یکی‌از نقاط ضعف این رویکرد آن است که ممکن است درمواجه با داده‌هایی که دامنه وسیعی از مقادیر یا متغیرهایی با سطوح متعدد دارند، بیش‌از حد حساس عمل کرده و به‌سرعت آن‌ها را به‌عنوان تراکنش تقلبی تشخیص دهد. به‌عبارت دیگر، گاهی اوقات مدل بیش‌از اندازه محتاط بوده و تعداد زیادی تراکنش‌عادی را به‌اشتباه مشکوک اعلام می‌کند.(Ibid)

۲،۱،۵. **شبکه‌های عصبی بازگشتی**[1]: این مدل درحوزه یادگیری عمیق[2] برای مسائل مبتنی‌بر داده‌های توالی‌محور طراحی شده است. درواقع این مدل با دریافت تراکنش‌های‌تاریخی که برچسب عادی یا مشکوک دارند، رابطه بین ویژگی‌ها را یاد می‌گیرد. تفاوت اساسی این روش با سایر مدل‌های‌نظارت‌شده در رویکرد آن به وابستگی‌های‌زمانی است؛ به‌این معنا که برخلاف مدل‌هایی که هر تراکنش‌را مستقل فرض می‌کنند، شبکه‌های عصبی بازگشتی تراکنش‌های یک حساب را به‌صورت زنجیره‌ای و درتوالی‌زمانی خود بررسی می‌کنند. (Girish, et.al. 2024, pp.2-3) این ویژگی به مدل امکان می‌دهد الگوهای رفتاری مشکوک را که درگذر زمان شکل می‌گیرند (مانند افزایش ناگهانی تعداد یا مبلغ‌تراکنش‌ها در بازه‌کوتاه) شناسایی کند.[3] با این حال این مدل از نظر محاسباتی سنگین و پرهزینه هستند چرا که آموزش آنها زمان‌بر بوده و به حافظه قابل‌توجهی نیاز دارند. همچنین به‌دلیل ساختار پیچیده و لایه‌های پنهان خود به عنوان یک جعبه سیاه تفسیرناپذیر شناخته می‌شوند.

۲،۲. یادگیری بدون نظارت[4]

یادگیری بدون‌نظارت به‌عنوان یکی دیگر از رویکردهای یادگیری‌ماشین، درتقابل با رویکردنظارت‌شده قرار دارد. تمایز اصلی این دو رویکرد در بهره‌گیری یا عدم بهره‌گیری‌از داده برچسب‌خورده است. در حالی که یادگیری نظارت‌شده به‌طور کامل به مجموعه‌داده‌هایی متکی است که پیشاپیش برچسب مشکوک یا غیرمشکوک به آن‌ها نسبت داده شده، یادگیری بدون نظارت

---

[1] . Recurrent Neural Networks (RNN)

[2] . Deep Learning

[3] . به‌عنوان نمونه، یک‌حساب‌بانکی عادی بامیانگین تراکنش روزانه ۵۰۰ هزارتومان شروع می‌شود. یک فرد فعال درحوزه پولشویی طی‌دو هفته، به‌تدریج مبلغ تراکنش‌ها را از ۵۰۰ هزار به ۵ میلیون تومان افزایش می‌دهد تا رفتارحساب را به‌سطوح بالای مالی عادت دهد. در روز پانزدهم، یک تراکنش ۵۰ میلیون تومانی در ساعت ۳ بامداد انجام می‌دهد که هدف آن وارد کردن وجوه‌نامشروع به‌سیستم‌مالی است. سایر مدل‌های نظارت شده که هر تراکنش را مستقل می‌بینند، تنها تراکنش بزرگ روز پانزدهم را به‌دلیل مبلغ بالا و ساعت غیرعادی مشکوک تشخیص می‌دهند، اما قادر به شناسایی الگوی «افزایش تدریجی» در روزهای قبل نیستند. درمقابل، این مدل با حفظ‌حافظه از تراکنش‌های قبلی و به‌دلیل شناسایی الگوی صعودی در روزهای قبل (که نشانه «عادی‌سازی» رفتارحساب برای پولشویی است)، تراکنش را مشکوک اعلام می‌کند.

[4] . Unsupervised Learning

هیچ‌گونه اطلاع پیشینی از برچسب نمونه‌ها را در اختیار ندارد. این رهیافت، تمامی بار شناختی خود را بر کشف ساختارهای درونی، الگوهای نهفته و روابط پنهان در داده‌ها متمرکز می‌سازد.[1]

مزیت اصلی این رویکرد، شناسایی سناریوهایِ مجرمانه ناشناخته‌ای است که به‌دلیل نبود سابقه قبلی، هیچ برچسبی به آن‌ها تعلق نگرفته است. بر این اساس یادگیری بدون نظارت، به‌عنوان مکمل ضروری رویکرد نظارت‌شده، می‌تواند خلأ رویکرد نظارت شده را مرتفع کند. یکی از مهم‌ترین شاخه‌های اصلی این رویکرد الگوریتم خوشه‌بندی K-Means [2] است.

این مدل بدون نیاز به داده‌های برچسب‌خورده تاریخی، تراکنش‌های‌مالی را براساس معیارهای شباهت (مانند مبلغ، زمان، جغرافیا و الگوی رفتاری) گروه‌بندی می‌کند. از آنجا که تراکنش‌های عادی و تکراری به نسبت تراکنش‌های مشکوک، درصد بیشتری را به‌خود اختصاص می‌دهند، این مدل آن‌ها را درقالب یک یا چند خوشه بزرگ‌و متراکم دسته‌بندی می‌کند. درمقابل، تراکنش‌های مرتبط با پولشویی و جرایم مالی به دلیل ویژگی‌های ناهنجار خود در فاصله قابل‌توجهی از این خوشه‌های اصلی قرار گرفته و به عنوان پرت[3] یا خوشه‌های بسیار کوچک ظاهر می‌شوند.(Mubalaike, & Adali, 2018, pp. 598-600) ماهیت غیرنظارتی این مدل، آن را برای کشف پدیده‌های پنهان جرایم مالی و اقتصادی و به ویژه پولشویی، مناسب ساخته است. به عبارتی داده‌های برچسب‌خورده تاریخی از جرایم اقتصادی معمولاً نسبت زیادی را تشکیل نمی‌دهند. افزون بر این، شیوه‌های پولشویی همواره در حال تغییر است و الگوهای جدیدی پدیدار می‌شوند که ممکن است در داده‌های گذشته بازنمایی نشده باشد. در چنین بستری، روش‌های غیرنظارت‌شده، بدون نیاز به داده‌های برچسب‌خورده و صرفاً با تکیه بر ساختار ذاتی داده‌ها، می‌توانند الگوهای ناهنجار را شناسایی کنند.

نقاط پرت به‌عنوان الگوهای رفتاری ناهنجار، اولویت نخست بررسی‌های تکمیلی را به خود اختصاص می‌دهند. در چنین فرآیندی، این الگوریتم با تفکیک خودکار ساختار داده، حجم وسیع تراکنش‌های روزانه را به دو زیرمجموعه متمایز کاهش می‌دهد. در نتیجه منابع محدود نظارتی صرفاً به موارد پرخطر اختصاص می‌یابند و هزینه‌های پایش تراکنش‌های عادی کاهش می‌یابد.(Naif and Qayyum, 2025, p.3658) بنابراین این مدل با شناسایی زودهنگام رفتارهای‌ناهنجار قبل‌از تکمیل چرخه‌پولشویی، امکان مداخله‌پیش‌دستانه برای توقیف فعالیت‌های‌غیرمجاز را فراهم می‌آورد.

روش خوشه‌بندی اگرچه در دسته‌بندی‌اولیه تراکنش‌های مشکوک مفید است، اما با کاستی‌هایی نیز مواجه است. نخست آنکه این روش عملکرد همه‌جانبه‌ای درشناسایی روابط شبکه‌ای میان حساب‌های‌مختلف ندارد، حال آنکه پولشویی معمولاً ازطریق

---

[1] . Financial Crime Academy, "Safeguarding Against Money Laundering: Essential Machine Learning Algorithms for AML," July 13, 2026, https://financialcrimeacademy.org/machine-learning-algorithms-for-aml/.

[2] . K-Means Clustering Algorithm

[3] . Outlier

چندین حساب و تراکنش‌های‌مرتبط انجام می‌شود. دوم آنکه نتایج این روش همیشه پایدار و یکسان نیست و به نقاط شروع‌الگوریتم وابسته است؛ لذا نیازبه تفسیرپذیری خواهد داشت. (Pelckmans,. 2020, p.37)

۳. چالش‌های کاربست رویکرد داده بنیان

علی‌رغم مزایای مثبتی که روش‌های‌یادگیری‌ماشین درکشف، پیش‌بینی‌و پیشگیری‌از جرم دارند، این فناوری به‌دلیل نوظهور بودن و تحولات‌سریع، چالش‌هایی را درحوزه مبارزه با جرایم ایجاد نموده است. بنابراین برای بهره‌مندی‌کامل از توانمندی‌های یادگیری‌ماشین دربخش‌مالی، مسیر تحقیقات‌آینده باید برسه محور اصلی متمرکز شود: نخست، توسعه چارچوب‌هایی برای هوش‌مصنوعی قابل‌اعتماد که کارایی را بارعایت اصول‌حقوقی پیوند می‌زند؛ دوم، طراحی عامل‌های‌خودمختار مبتنی‌بر یادگیری‌ماشین که قابلیت تطبیق‌پویا با شرایط‌لحظه‌ای را داشته باشند و سوم، تقویت همکاری‌های‌میان‌بخشی باهدف تدوین و استانداردسازی حکمرانی‌هوش‌مصنوعی در اکوسیستم مالی. محورهای دوم‌وسوم به‌ترتیب به ملاحظات‌فنی و سیاست‌گذاری درحوزه هوش مصنوعی مربوط می‌شوند. با این‌حال محور نخست، بحث اصلی را درچگونگی تنظیم‌گری هوش‌مصنوعی به خود اختصاص می‌دهد؛ امری‌که نیازمند تطبیق با اصول‌بنیادین حقوق‌کیفری و اصول‌دادرسی‌عادلانه است. الگوی دادرسی عادلانه، نمونه‌آرمانی از نحوۀعملکرد سیستم‌عدالت‌کیفری است که برمبنای حاکمیت‌قانون بنا شده است و ازطریق سازمان‌قضایی قانونی، مستقل و بی‌طرف با قواعد دادرسی‌منصفانه همچون حق بردفاع، حق‌بر بهره‌مندی از اصل برائت و شفافیت در دادرسی محقق می‌شود. این اصول‌کلی و دائمی بوده که وجود آن باعث پایندگی‌و دوام و نبود آن موجب از هم‌گسیختگی حیات دادرسی و مشروعیت آن می‌گردد. (تدین و باقری نژاد، ۱۳۹۹، ص۲۱۴) در این قسمت از نوشتار به مهم‌ترین چالش‌های‌کنونی رویکرد داده‌بنیان پرداخته خواهد شد.

۳/۱. عدم شفافیت الگوریتمی؛[1] نقض حق دفاع

مدل‌های پیشرفته یادگیری‌ماشین، به‌ویژه مدل‌های مبتنی‌بر یادگیری‌عمیق، علی‌رغم دقت‌بالا درکشف الگوهای پیچیده‌و غیرخطی در داده‌های‌مالی، با چالش‌اساسی عدم شفافیت‌الگوریتمی مواجه‌اند. این عدم‌شفافیت ریشه‌در معماری این مدل‌ها دارد؛ وجود لایه‌های‌پنهان متعدد و تعداد بسیار زیاد پارامترها (از میلیون‌ها تا میلیاردها مؤلفه) باعث می‌شود تابع تصمیم‌گیری نهایی چنان پیچیده باشد که حتی برای طراحان و توسعه‌دهندگان سیستم نیز غیرقابل درک مستقیم است. به‌عبارتی، درحالی‌که مدل یک تراکنش را به‌عنوان «مشکوک» طبقه‌بندی می‌کند، مکانیسم درونیِ «چرا» و «بر اساس چه ترکیب خاصی از ویژگی‌ها» به این نتیجه رسیده است، در ابهام باقی می‌ماند. (Rudin, 2019, p. 208) این ابهام به‌ویژه در فرایند شناسایی و تعقیب ذی‌نفع اصلی در ارتکاب جرم، چالش‌برانگیزتر است، زیرا الگوریتم قادربه توضیح‌دقیق وپیوسته روابط بین تراکنش‌ها و شخص‌مشکوک نیست.

---

[1] . Algorithmic Opacity

ازسوی‌دیگر، نهادهای مبارزه باپولشویی اساساً برپایه اصل پاسخگویی و شفافیت عمل می‌کنند، اما به‌کارگیری الگوریتم‌ها این تناقض را آشکار می‌سازد که چگونه می‌توان شفافیت را تأمین کرد. اسناد فرادستی و بین‌المللی نیز بر این ضرورت تأکید دارند؛ برای نمونه، ماده ۱۴ میثاق بین‌المللی حقوق مدنی‌وسیاسی مقرر می‌دارد که متهم حق دارد در اسرع وقت و به‌تفصیل، به‌زبانی که می‌فهمد، از نوع‌وعلل اتهام مطلع شود. این امر ضرورت‌شفافیت درعلل اتهامی و چرایی آن را درچارچوب دادرسی منصفانه‌و عادلانه یادآور می‌شود. دراین‌میان، دیجیتالی‌شدن بستر ارتکاب‌جرم، علاوه‌بر تغییر درکنش مجرمانه، منجربه دگرگونی در ساختار ادله شده است؛ امروزه از این پدیده با عنوان «ادله الگوریتمی»[1] یاد می‌شود. با این‌حال، تحول در قالب و ساختار ادله به هیچ‌وجه به‌معنای تغییر یا تعلیق اصول بنیادین حقوق کیفری نیست. این اصول، به‌مثابه سنگ‌بنای حقوق‌کیفری، چارچوب ارزیابی هر نوع دلیل جدیدی را تعیین می‌کنند.(Quattrocolo, et.al,2020, pp.2-3)

از این رو، الگوریتم در نظام‌ادله اثبات دعوا، صرفاً به‌عنوان یک منبع استدلالی، پذیرفته می‌شود و مشمول همان الزامات ناظر بر دادرسی‌عادلانه است. بر این‌اساس، متهم، علی‌رغم تغییر شکل ادله، همچنان ازحق‌دفاع برخوردار است که دستیابی شایسته به این حق، شامل آگاهی‌از فرآیند استنتاج الگوریتم نیز، می‌شود. لذا کنشگران عدالت‌کیفری درصورت استنادبه ادله‌الگوریتمی موظفند اطلاعات‌معنادار درمورد منطق حاکم‌بر تصمیم الگوریتم را به‌گونه‌ای ارائه کنند که امکان فهم، ارزیابی، اعتراض و دریک کلام، حق‌بر دفاع متهم میسر گردد.

این الزام با تأکید برماده ۲۲ مقررات‌عمومی حفاظت از داده‌های اتحادیه اروپا[2]تقویت می‌شود؛ چرا که بر اساس این ماده، هرگاه نتیجه بررسی‌های‌الگوریتمی به‌طور قابل‌توجهی بر حقوق افراد تأثیر بگذارد، حق‌توضیح‌خواهی برای افراد در برابر تصمیمات خودکار الگوریتمی به‌رسمیت شناخته می‌شود.[3] در این‌مرحله، آنچه ضروری است «اطلاعات معنادار» یعنی توضیحی شفاف، مختصر و قابل‌فهم برای افراد عادی، درباره چگونگی تأثیر داده‌های‌شخصی بر تصمیم اتخاذشده است؛ زیرا بدون آگاهی‌از منطق پشت الگوریتم، شخص نمی‌تواند از چگونگی پردازش داده‌های خود مطلع شود و در نتیجه، از حق دفاع شایسته به عمل آورد.

---

[1] . Algorithmic Evidence

[2] . European Regulation on General Data Protection (GDPR)

[3] . این‌ماده مقرر می‌دارد: شخصِ موضوع داده، این حق را خواهد داشت که مشمول تصمیمی مبتنی‌بر پردازش صرفاً خودکار، از جمله نمایه‌سازی (پروفایلینگ)، که نسبت‌به او آثار حقوقی ایجاد کند یا به‌طور مشابه به‌نحو قابل‌توجهی براو تأثیر بگذارد، نباشد.

کنترل‌کننده داده باید تدابیر مناسبی برای حفظ حقوق، آزادی‌ها و منافع مشروع شخصِ موضوع داده اجرا کند، که حداقل شامل حق دریافت مداخله انسانی از سوی کنترل‌کننده، حق بیان دیدگاه خود و حق اعتراض‌به تصمیم است.

Art. 22 GDPR –https://gdpr-info.eu/art-22-gdpr/

فراتر از مقررات عمومی حفاظت از داده‌ها، قانون هوش‌مصنوعی اتحادیه اروپا (EU) 2024/1689 نیز با معرفی ماده ۸۶، حق توضیح‌خواهی[1] افراد را گسترش داده است. بر اساس این ماده، زمانی که تصمیمات با استفاده از سیستم‌های هوش مصنوعی پرخطر گرفته می‌شوند که به‌طور قابل‌توجهی بر حقوق، سلامت یا ایمنی افراد تأثیر می‌گذارند، مستقرکنندگان آن فناوری موظف‌به ارائه توضیحات واضح و معنادار درباره نقش سیستم هوش مصنوعی در رویه‌تصمیم‌گیری و عناصر اصلی تصمیم گرفته‌شده هستند.

۳،۲. نقض اصل اصالت و تمامیت دلیل در پرتو حملات تخاصمی[2]

حملات‌تخاصمی به دستکاری عمدی و هوشمندانه داده‌های ورودی اطلاق می‌شود که برای چشم انسان عادی یا سیستم‌های ساده غیرقابل تشخیص است، اما مدل یادگیری ماشین را فریب می‌دهد و آن را به خروجی‌اشتباه وامی‌دارد.(Anthi,et.al, 2021, p.1) این آسیب‌پذیری ریشه درماهیت مدل‌های یادگیری ماشین دارد و برخلاف شکاف‌های امنیتی مرسوم، از نحوه یادگیری خود مدل سوءاستفاده می‌کند.

درواقع مجرمان‌حرفه‌ای که از وجود سیستم‌های هوشمند کشف تقلب مطلع هستند، می‌توانند با استفاده‌از تکنیک‌های‌تخاصمی، تراکنش‌های غیرقانونی خود را طوری تغییر دهند که مدل آن‌ها را‌عادی تشخیص دهد. مانند آنکه شخص مقادیر عددی یک تراکنش را به اندازه‌ای ناچیز تغییر دهد، که مبلغ‌از آستانه تشخیص مشکوک به عادی تغییر کند. همچنین با استفاده از الگوریتم‌های تخاصمی، مجرمان می‌توانند تراکنش غیرقانونی را در میان الگوهای تراکنش‌های روزمره و کم‌خطر استتار کنند. این کار ازطریق شبیه‌سازی رفتار کاربران‌عادی نظیر عادات هزینه، نوع دستگاه و الگوهای موقعیت جغرافیایی انجام می‌شود؛ به‌گونه‌ای که فعالیت مجرمانه برای سیستم‌های تشخیص ناهنجاری مبتنی بر هوش مصنوعی،عادی و روزمره به نظر می‌رسد.[3]

بدین‌سان، حملات‌تخاصمی که از رهگذر دستکاری‌عمدی و غیرقابل تشخیص داده‌ها، تمامیت‌دلیل الگوریتمی را مخدوش می‌سازند، با اصول دادرسی منصفانه و مبانی حاکم بر نظام ادله‌کیفری که همواره بر صحت و اصالت ادله، تاکید دارد، ناسازگار می‌نمایند. در واقع، در ادبیات حقوق‌کیفری بحث پیرامون انتساب جرم و احراز رابطه سببیت همواره امری دشوار و وابسته به عواملی‌چندگانه بوده است. نظام‌های الگوریتمی مبتنی‌بر یادگیری ماشین، اگرچه تا اندازه‌ای توانسته‌اند از دشواری‌های سنتیِ

1 . the right to explanation of individual decision-making

2 . Adversarial Attacks

۳ . یک بررسی‌جهانی درسال ۲۰۲٤ نشان داد که نزدیک‌به یک‌چهارم مؤسسات‌فناوری مالی (Fintech) زیانی بیش‌از یک‌میلیون دلار را به‌دلیل حملات‌دیپ‌فیک متحمل شده‌اند.

Regula. (2024, October 30). Deepfake fraud costs the financial sector an average of $600,000 for each company, Regula’s survey shows. https://regulaforensics.com/news/deepfake-fraud-costs/

احراز رابطه‌سببیت بکاهند، لیکن خود این فناوری‌ها دچار آسیب‌پذیری‌های ساختاری‌اند؛ امری‌که می‌تواند اصالت ادله الگوریتمی را با چالش مواجه کند.

به عنوان یک بایسته فراتقنینی، اساسنامه رم دیوان کیفری بین‌المللی (۱۹۹۸) در بند ۷ ماده ۶۹ خود چنین مقرر داشته است که ادله‌ای که از راه نقض حقوق بشر به‌دست آمده باشند، در دو حالت قابلیت طرح در دادرسی کیفری بین‌المللی را نخواهند داشت: نخست، آنگاه که نقض مذکور، تردید عمده‌ای در اعتبار دلیل ایجاد کند؛ و دوم، زمانی‌که پذیرش دلیل با اصالت دادرسی ناسازگار بوده و به آن لطمه‌ای جدی وارد سازد.

در نظام حقوقی ایران نیز، اگرچه «اصل اصالت و تمامیت دلیل» به عنوان یک اصل مستقل و با همین عنوان تصریح نشده است، اما می‌توان مؤلفه‌های آن را که در قوانین مرتبط با ادله الکترونیکی انعکاس یافته است، مشاهده کرد. در این راستا قانون تجارت الکترونیکی با تفکیک «داده‌پیام مطمئن» از «داده‌پیام عادی» عملاً این پیش‌فرض را بنیان نهاده که یک دلیل الکترونیکی، زمانی از اعتبار و قابلیت اتکای لازم برخوردار است که امکان کشف تغییرات و احراز انتساب آن به صورت مطمئن فراهم باشد.[1] با این حال، آنچه در این مقررات دیده می‌شود، عمدتاً ناظر به داده‌های ایستا و فرایندهای‌سنتی جمع‌آوری ادله است؛ داده‌هایی که از سیستم‌های بسته و شناخته‌شده استخراج می‌شوند و حاستگاه و زنجیره انتقال آن‌ها قابل پیگیری است. اما آنچه امروزه تحت عنوان ادله‌الگوریتمی درکانون توجه قرار دارد، ماهیتی متفاوت دارد.

درواقع مقررات موجود عمدتاً بر حفاظت از داده در برابر جعل و تغییر آشکار متمرکز شده‌اند، اما در برابر تغییرات هوشمندانه‌ای که برای فریب الگوریتم طراحی می‌شوند، دچار خلأ هستند. در نتیجه، حتی اگر داده‌های ورودی اصیل و دست‌نخورده باشند، فرآیند تولیدخروجی ممکن است به‌واسطه حملات تخاصمی تمامیت‌دلیل الگوریتمی را مخدوش سازد. از این رو به نظر می‌رسد نهادهای قضایی ناگزیر از اعمال استانداردهای سختگیرانه‌تر برای احراز اصالت و تمامیت این دسته از ادله هستند؛ چه در غیر این صورت، حق بنیادین متهم بر دادرسی منصفانه نقض خواهد شد.

۳،۳. اصل برائت؛ چالش کیفیت و دسترسی به داده

رویکرد داده‌بنیان درشناسایی تراکنش‌های مشکوک به پولشویی، علیرغم توانمندی قابل توجه در کشف الگوهای پیچیده، به همان میزان که به داده وابسته است، از آسیب‌پذیری‌های ناشی از کیفیت و دسترسی به داده نیز متأثر می‌گردد. مدل‌های یادگیری ماشین، فارغ از پیچیدگی معماری خویش، قادر به ارائه کیفیتی فراتر از داده‌ای که بر آن آموزش دیده‌اند نمی‌باشند. از این رو، چنانچه داده‌های‌ورودی از کیفیت مطلوب برخوردار نباشند؛ چه به دلیل خطاهای کدگذاری، چه به دلیل کم‌نمایی برخی

---

[1]. ماده ۱۰. امضای‌الکترونیکی‌مطمئن باید دارای شرایط زیر باشد :الف) نسبت‌به امضاءکننده منحصربه‌فرد باشد .ب) هویت امضاءکننده داده‌پیام را معلوم نماید ج) به‌وسیله امضاءکننده و یا تحت اراده‌انحصاری وی صادر شده‌باشد .د) به‌نحوی به‌یک داده‌پیام متصل شود که هر تغییری در آن داده‌پیام قابل‌تشخیص و کشف باشد.

گروه‌ها .(Caglayan, et.al . 2022, p.857) و چه به دلیل سوگیری‌های ناخواسته در مرحله گردآوری داده، خروجی مدل نیز به طریق اولی معیوب و غیرقابل اتکا خواهد بود.

چالش کیفیت داده در نظام‌های مبارزه با پولشویی به ویژه می‌تواند ظهور کند. بدین معنا که اگر صرفاً بر اساس معیارهای اعلام‌شده از سوی نهادهایی چون گروه ویژه اقدام مالی، تمرکز داده‌ها بر تراکنش‌های اشخاص ساکن در مناطق جغرافیایی موسوم به «پرخطر» معطوف گردد، یا دسته‌خاصی از افراد (بر اساس ملیت، شغل یا نوع فعالیت) با فراوانی بیشتری نسبت به دیگران در فرایند ثبت و بررسی تراکنش‌ها قرار گیرند، در آن صورت احتمال وجود دارد که مجموعه‌داده‌ای ناقص و حامل سوگیریِ آماری به الگوریتم آموزش داده شود. مدلی که بر چنین داده‌هایی استوار خواهد شد، ممکن است به جای کشف الگوهای عینی و معتبر پولشویی، به همبستگی‌های تصادفیِ ناشی از همان سوگیری‌های اولیه گرایش پیدا کند و آن‌ها را به عنوان ویژگی‌های مشکوک بازآموزی نماید. . (Gupta, et. al. 2021, p.553) نتیجه آنکه مدل به طور نظام‌مند، وزن پیش‌بینی بالاتری را به تراکنش‌های منتسب به مناطق جغرافیایی خاص یا دسته‌های اجتماعی معین اختصاص می‌دهد و در نتیجه، این دسته از افراد با احتمالی بیشتر در زمره ورودی‌های مشکوک طبقه‌بندی شوند.

این پدیده با اصل برائت که در ماده ۱۴ میثاق بین‌المللی حقوق مدنی و سیاسی و نیز اصل ۳۷ قانون اساسی تصریح شده است، تعارضی آشکار دارد. اصل برائت ایجاب می‌کند که هیچ فردی مجرم انگاشته نشود، مگر آنکه جرم او برپایه ادله‌ای‌معتبر، قابل‌انتساب و بی‌طرفانه درمرجع قضایی به اثبات رسد. اما هنگامی که الگوریتم‌های یادگیری‌ماشین به‌سبب کیفیت‌داده‌ها، برچسب مشکوک را به افرادی اختصاص می‌دهند که صرفاً به‌دلیل ویژگی‌های جمعیت‌شناختی یا موقعیتی‌خاص درمجموعه‌داده با فراوانی بیشتری بازنمایی شده‌اند، عملاً بار اثبات به طور ضمنی به آنان منتقل می‌گردد؛ امری که با اصل برائت مغایرت دارد.

با این حال قانون‌گذار ایران در راستای افزایش کارآمدی نظام مبارزه با پولشویی، با الحاق تبصره‌های سه‌گانه به ماده (۲) قانون مبارزه با پولشویی، در برخی فروض، زمینه تعدیل بار اثبات را فراهم ساخته است. تبصره ۱: «هرگاه ظن نزدیک به علم به عدم صحت معاملات و تحصیل اموال وجود داشته باشد مانند آنکه نوعاً و باتوجه به شرایط امکان تحصیل آن میزان دارایی در یک زمان مشخص وجود نداشته باشد مسئولیت اثبات صحت آن‌ها بر عهده متصرف است.»

تبصره ۲ نیز مقرر می‌دارد: «دارا شدن اموال موضوع این قانون منوط به ارائه اسناد مثبته است. علاوه بر این چنانچه ارزش اموال مزبور بیش از ده میلیارد ریال برای سال پایه و معادل افزایش‌یافته آن بر اساس نرخ تورم برای سال‌های بعد باشد وجود سابقه از آن در سامانه‌های مربوطه مطابق قوانین و مقررات لازم است. عدم تقدیم اسناد مثبته که قابل راستی‌آزمایی باشد به حکم دادگاه مستوجب جزای نقدی به میزان یک‌چهارم ارزش آن اموال خواهد بود، در این صورت اصل مال موضوع قانون تا زمان

رسیدگی قضائی توقیف می‌شود. چنانچه پس از رسیدگی اثبات شود دارا شدن مشروع بوده از مال رفع توقیف و در غیراین‌صورت ضبط می‌شود.»

و تبصره ۳ نیز مقرر می‌دارد: «چنانچه ظن نزدیک به علم بر تحصیل مال از طریق نامشروع وجود داشته باشد در حکم مال نامشروع محسوب و مرتکب درصورتی‌که مشمول مجازات شدیدتری نباشد به حبس درجه شش محکوم می‌شود. در هر صورت مال مزبور ضبط خواهد شد مگر اینکه تحصیل مشروع آن اثبات شود.»

بدین‌سان همگام با پیشرفت‌های بین‌المللی در زمینه نظام مقابله با پولشویی و افزایش اختیارات نهادهای نظارتی در جهت مبارزه با ورود و گردش وجوه نامشروع در نظام اقتصادی کشورها و در پی تغییرات مثبت قانون مبارزه با پولشویی، تبصره ۱ الحاقی به ماده ۲ قانون مبارزه با پولشویی اقدام به تعدیل بار اثبات در پرونده‌های پولشویی نموده است. برای مثال اگر در یک پرونده، فردی متهم پولشویی از طریق تحصیل مال حاصل از جرم باشد، به طور معمول دادستان باید سه موضوع را ثابت کند؛ نخست، تحصیل مال توسط متهم، دوم؛ حاصل از جرم بودن مال و سوم علم و اطلاع متهم از این که مال حاصل از جرم بوده است. اما با الحاق این تبصره به ماده ۲ قانون مبارزه با پولشویی، موضوع دوم به لحاظ اثباتی تغییراتی پیدا کرده است. بر اساس این تبصره بنا به خطر (ریسک) ایجاد شده توسط خود متصرف اموال، لازم نیست «حاصل از جرم بودن مال» توسط دادستان اثبات شود، بلکه اگر شرایط تبصره مذکور فراهم باشد، این متهم است که باید ثابت کند که مال را از راه مشروع و قانونی به دست آورده است. لیکن باید در نظر داشت کماکان اثبات موضوع اول و سوم یعنی ارتکاب رفتار فیزیکی تحصیل توسط متهم و علم و اطلاع او از مجرمانه بودن مال تحصیل شده (که به طور معمول بر اساس قرائن عینی محرز می‌شود) بر عهده دادستان بوده و دستخوش تغییر قرار نگرفته است. حال پرسش این است که چه شرایطی باید وجود داشته باشد که بار اثبات «حاصل از جرم بودن مال» معکوس شود؟ تبصره ۱ الحاقی به ماده ۲ قانون مبارزه با پولشویی مبنای تغییر بار اثبات را «به وجود آمدن ظن نزدیک به علم بر عدم صحت معاملات و تحصیل اموال» عنوان کرده و برای تبیین آن به ذکر یک مثال اکتفا نموده است. این مثال به این شرح است: «نوعاً و با توجه به شرایط امکان تحصیل آن میزان دارایی در یک زمان مشخص وجود نداشته باشد.» البته باید توجه داشت که این مثال تنها جنبه تبیینی داشته و مبنا همان «به وجود آمدن ظن نزدیک به علم بر عدم صحت معاملات و تحصیل اموال است» که این ظن ممکن است از طرق دیگر به دست آید؛ برای مثال به علت ارتباط مالی شخص با مرتکبان جرایم ممکن است ظن مذکور حاصل شود؛ لیکن به نظر می‌رسد تشخیص قضایی در این زمینه بسیار با اهمیت است، اما به هر حال منشأ ظن باید معتبر و مستند باشد. (ثالث موید و همکاران،۱۴۰۳، صص. ۶۶-۶۷)

بدین‌ترتیب، قانون‌گذار، ایجاد «ظن نزدیک به علم» را مبنای تعدیل بار اثبات قرار داده است. در چنین چارچوبی، کیفیت و اعتبار داده‌هایی که منشأ شکل‌گیری این ظن هستند، اهمیتی دوچندان پیدا می‌کند. هرچه این ظن بر پایه تحلیل جامع‌تر داده‌های مالی، الگوهای رفتاری مشتری و روابط میان تراکنش‌ها استوار باشد، اتکاپذیری آن نیز افزایش خواهد یافت. از این منظر،

سامانه‌های مبتنی بر یادگیری ماشین، با پردازش حجم گسترده‌ای از داده‌های رفتاری و مالی و شناسایی الگوهایی که به‌سادگی از طریق روش‌های سنتی قابل تشخیص نیستند، می‌توانند زمینه شکل‌گیری ظنی مستندتر و نزدیک‌تر به واقع را فراهم آورند. در نتیجه، در مواردی که قانون‌گذار آثار حقوقی مهمی همچون تعدیل بار اثبات را بر وجود چنین ظنی مترتب ساخته است، بهره‌گیری از رویکردهای داده‌بنیان، در صورت رعایت الزامات قانونی و تضمین کیفیت داده‌ها، می‌تواند در جهت افزایش کارآمدی نظام مبارزه با پولشویی و صیانت از امنیت اقتصادی، نقشی مؤثر ایفا کند.

۳،۴. محدودیت‌های زیرساختی در استقرار رویکرد داده‌بنیان در ایران

تحقق رویکرد داده‌بنیان در پیشگیری از پولشویی، افزون بر وجود چارچوب‌های حقوقی، مستلزم فراهم بودن زیرساخت‌های فنی و اطلاعاتی متناسب است. هرچند قانون مبارزه با پولشویی و آیین‌نامه اجرایی آن با پذیرش رویکرد مبتنی بر ریسک، بر شناسایی، ارزیابی و مدیریت ریسک تأکید دارند، اما اجرای مؤثر این رویکرد در عصر داده، بدون دسترسی به سامانه‌های یکپارچه، داده‌های قابل اتکا و امکان تبادل برخط اطلاعات میان اشخاص مشمول و نهادهای ناظر با دشواری همراه خواهد بود. از همین رو، اگر چه در سال گذشته مرکز اطلاعات مالی ایران با راه‌اندازی سامانه جامع و هوشمند مبارزه با پولشویی (سمام) و سامانه برخط استعلامات (سبا)، گام مهمی در جهت تقویت زیرساخت‌های داده‌محور برداشته است؛ اما با وجود این، به نظر می‌رسد این زیرساخت‌ها هنوز در مرحله توسعه قرار دارند و تا دستیابی به یک نظام داده‌بنیان جامع، فاصله قابل توجهی وجود دارد. مطابق برنامه اعلام‌شده توسط مرکز اطلاعات مالی، در مرحله نخست اتصال سامانه «سمام» به شبکه بانکی پیش‌بینی شده و الحاق سایر اشخاص مشمول قانون[1]، از جمله مشاغل غیرمالی، شرکت‌های بیمه، بازار سرمایه و ...، به مراحل بعدی موکول شده است. این در حالی است که کارآمدی رویکرد داده‌بنیان، در گرو دسترسی به داده‌های جامع و برقراری ارتباط یکپارچه میان تمامی اشخاص مشمول است؛ زیرا هرگونه گسست اطلاعاتی می‌تواند اثربخشی تدابیر پیشگیرانه را کاهش دهد. از این رو، توسعه تدریجی این زیرساخت‌ها، در کنار تقویت سازوکارهای تبادل داده و اتصال کامل تمامی اشخاص مشمول، یکی از الزامات اساسی تحقق رویکرد داده‌بنیان در نظام مبارزه با پولشویی ایران به شمار می‌رود.

---

[1] . بند «ت» ماده یک قانون مبارزه با پولشویی اشخاص مشمول را با ارجاع به مواد (۵) و (٦) همین قانون، تعیین نموده است. مطابق با ماده ۵، کلیه صاحبان مشاغل غیرمالی و مؤسسات غیرانتفاعی و همچنین اشخاص حقیقی و حقوقی از جمله بانک مرکزی جمهوری اسلامی ایران، بانک‌ها، مؤسسات مالی و اعتباری، بیمه‌ها، بیمه مرکزی، صندوق‌های قرض‌الحسنه، بنیادها و مؤسسات خیریه، شهرداری‌ها، صندوق‌های بازنشستگی، نهادهای عمومی غیردولتی، تعاونی‌های اعتباری، صرافی‌ها، بازار سرمایه (بورسهای اوراق بهادار) و سایر بورسها، شرکت‌های کارگزاری، صندوق‌ها و شرکت‌های سرمایه‌گذاری و همچنین مؤسساتی که شمول قانون بر آنها مستلزم ذکر نام می‌باشد از قبیل شرکت ملی نفت ایران، سازمان گسترش و نوسازی ایران و غیر آنها، مکلفند آیین‌نامه‌های اجرائی هیأت‌وزیران در ارتباط با این قانون و قانون مبارزه با تأمین مالی تروریسم را اجراء کنند. همچنین مطابق با ماده ٦، کلیه اشخاص موضوع ماده (۵) این قانون، از جمله گمرک جمهوری اسلامی ایران، سازمان امور مالیاتی کشور، سازمان ثبت اسناد و املاک کشور، دفاتر اسناد رسمی، وکلای دادگستری، حسابرسان، حسابداران، کارشناسان رسمی دادگستری و بازرسان قانونی مکلفند اطلاعات مورد نیاز در اجرای این قانون را طبق مصوبات هیأت‌وزیران حسب درخواست شورا یا مرکز اطلاعات مالی به آنها ارائه نمایند.

نتیجه‌گیری

در نظم‌کنونی جهان، داده به‌مثابه یکی‌از ارکان بنیادین، ساختار نظام‌های‌نظارتی و حتی فرایندهای عدالت‌کیفری را دچار دگرگونی‌اساسی ساخته است. گذار از اقتصادسنتی به زیست‌بوم‌دیجیتال و فراگیرشدن تراکنش‌های‌برخط و سازوکارهای نوین پرداخت، منجر به دگرگونی اشکال‌بزهکاری شده است. در این میان، جوامع معاصر به‌ویژه در برابر جرایم اقتصادی سازمان‌یافته و فرامرزی به‌تدریج به سمت رویکردکنترل‌جرم پیش رفته‌اند. رویکردی که در آن، انتظار از نظام‌عدالت‌کیفری دیگر محدود به واکنش آتی نسبت‌به جرم ارتکاب‌یافته و اعمال مجازات پس‌از وقوع نیست، بلکه پیشگیری‌از راه پیش‌بینی به‌عنوان محوری اساسی در سیاست‌جنایی مطرح می‌گردد. در این رویکرد پیش‌بینی، نه به‌مثابه ابزاری برای تحدید آزادی‌ها، بلکه به‌عنوان ضرورتی بنیادین برای مدیریت علمی خطر و پیشگیری مؤثر از جرم، جایگاهی محوری یافته است. در چنین وضعیتی، هزینه تحمل خطا به‌مراتب بالاست و هرگونه تأخیر در شناسایی الگوهای مجرمانه می‌تواند به‌منزله تسهیل مسیر برای شبکه‌های پیچیده پولشویی و سایر جرایم‌اقتصادی تلقی گردد. در این راستا کاربست رویکرد داده‌بنیان و به‌ویژه بهره‌گیری از ابزارهای یادگیری ماشین، صرفاً به ارتقای دقت فنی در شناسایی تراکنش‌های مشکوک محدود نمی‌شود، بلکه می‌تواند الگوی پیشگیری از پولشویی را نیز دستخوش تحول سازد. درواقع، هرچه فرآیند شناسایی و ارزیابی ریسک از جامعیت، دقت و روزآمدی بیشتری برخوردار باشد، امکان اتخاذ تدابیر پیشگیرانه متناسب نیز افزایش یافته و مداخله نظام مبارزه با پولشویی از مرحله واکنش پس از وقوع جرم، به مرحله پیشگیری و مدیریت ریسک نزدیک‌تر می‌شود. با این حال، یافته‌های پژوهش نشان می‌دهد که بهره‌گیری از این فناوری، بدون فراهم شدن الزامات حقوقی و فنی، لزوماً به افزایش کارآمدی نظام مبارزه با پولشویی منجر نخواهد شد. کارآمدی این رویکرد، علاوه بر کیفیت الگوریتم‌ها، به وجود داده‌های قابل اعتماد، زیرساخت‌های اطلاعاتی یکپارچه، چارچوب‌های حقوقی متناسب و نظارت مؤثر بر فرآیندهای تصمیم‌گیری وابسته است. ازاین‌رو، توسعه ابزارهای هوشمند باید هم‌زمان با تقویت تضمین‌های حقوقی و الزامات اجرایی دنبال شود. بررسی نظام حقوقی ایران نیز نشان می‌دهد که هرچند قانون مبارزه با پولشویی و آیین‌نامه اجرایی آن، با پذیرش رویکرد مبتنی بر ریسک، زمینه حرکت به سوی بهره‌گیری از تحلیل داده را فراهم ساخته‌اند و ایجاد سامانه‌هایی نظیر «سمام» نیز بیانگر آغاز این تحول است، اما این روند همچنان در مراحل اولیه قرار دارد. محدود بودن دامنه عملیاتی برخی زیرساخت‌ها و ضرورت اتصال تمامی اشخاص مشمول به سامانه‌های هوشمند، نشان می‌دهد که تحقق کامل رویکرد داده‌بنیان، مستلزم توسعه زیرساخت‌های فنی، تکمیل نظام تبادل داده و بازنگری مستمر در مقررات متناسب با تحولات فناوری است.

فهرست منابع

۱. ابراهیمی، شهرام. (۱۴۰۱). پیشگیری از تکرار جرم از طریق هوش مصنوعی؛ مقتضیات و محدودیت‌ها، **آموزه‌های حقوق کیفری**، ۱۹ (۲۳)، ۵۴-۳۳. 10.30513/cld.2023.4345.1701

۲. ابوذری، مهرنوش. (۱۴۰۳). مقابله با بزهکاری در عصر هوش مصنوعی: پیش‌بینی به مثابه پیشگیری، **دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی**، ۱ (۲)، ۶۸-۳۴، 10.22034/jclc.2025.720961

۳. اسماعیلی، محمد. (۱۳۹۶). عدالت پیشگیرنده: مهار جرم در بستر نظام حقوقی، **مطالعات حقوق کیفری و جرم‌شناسی**، ۴ (۲)، ۳۲۶-۲۹۷، 10.22059/jqclcs.2018.239944.1232

۴. بک، اولریش، (۱۳۸۸). **جامعه در مخاطره جهانی**، ترجمه محمدرضا مهدی، تهران:انتشارات:کویر.

۵. تدین، عباس؛ باقری نژاد، زینب. (۱۳۹۹) هستی شناسی اصول بنیادین دادرسی کیفری. **فصلنامه پژوهش حقوق کیفری**، ۹ (۳۳). ۲۱۹-۱۸۷. 10.22054/JCLR.2020.49838.2060

۶. ثالث موید، احمدعلی، خلیلی پاجی، عارف، ملکوتی‌زاده، مصطفی. (۱۴۰۳) **نکات کاربردی جرم پولشویی**، مرکز اطلاعات مالی دبیرخانه شورای عالی مقابله و پیشگیری از جرایم پولشویی و تامین مالی تروریسم، چاپ اول، نشر میزان.

۷. حجازی، سید امرالدین، صلح چی، محمد علی. (۱۳۹۹) شورای امنیت سازمان ملل متحد و تاثیر آن در ایجاد امنیت و عدالت کیفری بین‌المللی، **فصلنامه پژوهش حقوق کیفری**، ۹(۳۳). ۴۶-۹. doi: 10.22054/jclr.2020.45294.1967

۸. خلیلی پاجی، عارف. (۱۴۰۳) **ارزهای مجازی؛ جهانی شدن بزهکاری و سیاست جنایی**، چاپ دوم، تهران، میزان.

۹. خیرانی، روح اله، زرنشان، شهرام، سلیمانیان، محمدهادی. (۱۴۰۱) ارزیابی وضعیت ایران در ارتباط با مقررات بین‌المللی مرتبط با پولشویی، **پژوهش‌های حقوقی**، ۲۱ (۴۹).۶۹-۳۹. 10.48300/jlr.2022.148310

۱۰. شاملو، باقر، خلیلی پاجی، عارف. (۱۳۹۹). رویکرد ریسک‌مدار سیاست جنایی دربرابر پولشویی، **پژوهشنامه حقوق کیفری**، ۱۱ (۱)، ۱۵۲-۱۲۷، 10.22124/jol.2020.12409.1649

۱۱. کدخدایی، عباسعلی، نوروزپور، حسام. (۱۳۹۹). چالش ارزهای مجازی در مبارزه با پولشویی و تأمین مالی تروریسم با تأکید بر اقدامات و توصیه‌های کارگروه ویژه اقدام مالی، **مجله حقوقی بین المللی**، ۳۷ (۶۲).۲۹-۷ 10.22066/cilamag.2019.101998.1647

۱۲. موسوی‌فر، نجفی. (۱۴۰۴) تأملی در روند هوش مصنوعی در پیشگیری از جرم، **تمدن حقوقی**، ۸ (۲۳)، ۱۹۰-۱۷۱. 10.22034/LC.2025.512833.1612.

۱۳.نجفی ابرند آبادی، علی حسین، ایارگر، حسین. (۱۳۹۹) نظارت بر مجرمان خطرناک: چالش ها و راهکارها، **فصلنامه پژوهش حقوق کیفری**، ۲ (۶). ۳۷-۹.

۱۴.نجفی ابرندآبادی، علی حسین، (۱۳۸۸)**کیفرشناسی نو-جرم شناسی نو درآمدی‌بر سیاست جنایی مدیریتی خطر مدار**، تازه‌های علوم جنایی (مجموعه مقاله‌ها)، ۷۱۷-۷۵۰، میزان.

15. Ai, Lishan. (2012). "Rule-based but risk-oriented" approach for combating money laundering in Chinese financial sectors. **Journal of Money Laundering Control**, 15(2), 198–209. https://doi.org/10.1108/13685201211218225.
16. Ali, Abdulalem, Shukor Abd Razak, Siti Hajar Othman, Taiseer Abdalla Elfadil Eisa, Arafat Al-Dhaqm, Maged Nasser, Tusneem Elhassan, Hashim Elshafie, and Abdu Saif. 2022. Financial fraud detection based on machine learning: a systematic literature review. **Appl. Sciences** 12 (19), 9637. https://doi.org/10.3390/app12199637
17. Alloghani, Mohamed & Al-Jumeily Obe, Dhiya & Mustafina, Jamila & Hussain, Abir & Aljaaf, Ahmed. (2020). **A systematic review on supervised and unsupervised machine learning algorithms for data science. Supervised and unsupervised learning for data science**, 3-21. https://doi.org/10.1007/978-3-030-22475-2_1.
18. Anthi, Eirini & Williams, Lowri & Rhode, Matilda & Burnap, Pete & Wedgbury, Adam. (2021). Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. **Journal of Information Security and Applications**, *57*, 102717. https://doi.org/10.1016/j.jisa.2020.102717
19. AsiaVerify. (2025). Discover how hidden UBO links can derail deals and how to spot them with registry-backed data. https://asiaverify.com/resources/insights/the-hidden-ubo-web-uncover-business-ownership-risk/
20. Caglayan, Mehmet., & Bahtiyar, Şerif. (2022). Money Laundering Detection with Node2Vec. **Gazi University Journal of Science**, 35(3), 854–873. https://doi.org/10.35378/gujs.854725
21. FATF (2021), Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, https://www.fatf-gafi.org/publications/ fatfrecommendations/documents/opportunities-challenges-new- technologies-aml-cft.html.
22. FATF (2025), Money Laundering National Risk Assessment Guidance, FATF, Paris, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-AssessmentGuidance.html. P. 4.
23. FATF. High-risk and other monitored jurisdictions https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html
24. Fei Yin, Qiang Li, Huihui Song, and Wen Lu. 2025. Addressing Digital Finance Challenges: The Application and Op-timization of Logistic Regression Models in Fraud Detection Sys-tems. **In Proceedings of the 2025 2nd International Conference on Innovation Management and Information System** (ICIIS '25). Association for

Computing Machinery, New York, NY, USA, 8–14. https://doi.org/10.1145/3745676.3745678
25. Financial Crime Academy, "Safeguarding Against Money Laundering: Essential Machine Learning Algorithms for AML," July 13, 2026, https://financialcrimeacademy.org/machine-learning-algorithms-for-aml/.
26. Fraud Detection Handbook. (2021). *Chapter 5: Model Validation and Selection - Introduction*. GitHub. Available at: https://github.com/Fraud-Detection-Handbook/fraud-detection handbook/blob/main/Chapter_5_ModelValidationAndSelection/Introduction.md
27. Girish K., & Bhowmik, B. (2024). "Money Laundering Detection in Banking Transactions using RNNs and Hybrid Ensemble." **15th International Conference on Computing Communication and Networking Technologies (ICCCNT)**, pp. 1-7. IEEE
28. Gupta, Dwijendra Nath Dwivedi & Jigar Shah & Ashish Jain. (2021). Data quality issues leading to sub optimal machine learning for money laundering models. **Journal of Money Laundering Control**, 25(3), 551–555. https://doi.org/10.1108/JMLC-05-2021-0049
29. Halder, Rajib & Uddin, Mohammed & Uddin, Md Ashraf & Aryal, Sunil & Khraisat, Ansam. (2024) Enhancing K-nearest neighbor algorithm: a comprehensive review and performance analysis of modifications. **Journal of Big Data** 11, 113. https://doi.org/10.1186/s40537-024-00973-y
30. Hu, Chaochen & Li, Ran & Li, Chao & Miao, Hengshuo & Yang, Zongyou & Zhang, Tengda (2022, September). Big Data Analysis for Anti-Money Laundering: A Case of Open Source Greenplum Application. In **International Conference on Web Information Systems and Applications** (pp. 638-645). Cham: Springer International Publishing.
31. Husnaningtyas, Nadia & Hanin, Ghalizha & Dewayanto, Totok & Malik, Muhammad. (2023). A systematic review of anti-money laundering systems literature: Exploring the efficacy of machine learning and deep learning integration. JEMA: **Jurnal Ilmiah Bidang Akuntansi dan Manajemen**. 20. 91-116. 10.31106/jema.v20i1.20602.
32. Koker, Louis. (2009). Identifying and managing low money laundering risk: Perspectives on FATF's risk-based guidance. **Journal of Financial Crime**. 16. 334-352. 10.1108/13590790910993717.
33. Liaw, Andy & Wiener, Matthew (2002). Classification and Regression by randomForest. R News, 2(3), 18–22.
34. Mallika, B.K., Ramasubramanian, V.H., 2025. Anti money laundering system in detecting and preventing money laundering activities: a systematic review. J. **Money Laund. Control** 28 (2), 385-407. doi: https://doi.org/10.1108/JMLC-07-2024-0108
35. Massimiliano Marletta, 2025, Probabilities, costs, and justice: rethinking precautionary measures in civil and criminal law, **Law, Probability and Risk**, Volume 24, Issue 1, mgaf007, https://doi.org/10.1093/lpr/mgaf007. P.2.
36. Mubalaike, A. M., & Adali, E. (2018, September). Deep learning approach for intelligent financial fraud detection system. In 2018 3rd **International Conference on Computer Science and Engineering** (UBMK) (pp. 598-603). IEEE.

37. Mukhamadiyev, A.; Nazarov, F.; Yarmatov, S.; Cho, J. (2025) Intelligent Algorithms for the Detection of Suspicious Transactions in Payment Data Management Systems Based on LSTM Neural Networks. **Sensors**, 25, 6683.
38. Naif Almusallam, Junaid Qayyum,(2025) A Hybrid Feature Selection and Clustering-Based Ensemble Learning Approach for Real-Time Fraud Detection in Financial Transactions, **Computers, Materials and Continua**, Volume 85, Issue 2, Pages 3653-3687, https://doi.org/10.32604/cmc.2025.067220
39. Omoseebi, Adetoyese & Ola, Godwin & Tyler, Jackson. (2025). Rule-Based Systems in AML. P.17.
40. Pelckmans, K. (2020). Monitoring High-Frequency Data Streams in FinTech: FADO Versus K-Means. **IEEE Intelligent Systems**, 35(2), 36-42
41. Quattrocolo, S., Anglano, C., Canonico, M., & Guazzone, M. (2020). Technical Solutions for Legal Challenges: Equality of Arms in Criminal Proceedings. Global Jurist, 20(1), 20190058. De Gruyter
42. Regula. (2024, October 30). Deepfake fraud costs the financial sector an average of $600,000 for each company, Regula's survey shows [Press release]. Retrieved from https://regulaforensics.com/news/deepfake-fraud-costs/
43. Riccardi, Michele. (2021). Money Laundering Blacklists. 10.4324/9781003212867.
44. Rudin, C.(2019) Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nat Mach Intell 1, 206–215. https://doi.org/10.1038/s42256-019-0048-x
45. Vorobyev , Ivan, Krivitskaya , Anna Krivitskaya, (2022). "Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models." **Computers & Security**, Volume 120, 102786
46. Vududala, Santosh Kumar, (2024)"Enhancing Anti-Money Laundering (AML) Compliance using NICE Actimize: A Data-driven Approach," **International Journal of Computer Techniques**, Volume 11 Issue 2, April 2024. ISSN 2394-2231.
47. Zhang, Y., & Trubey, P. (2019). Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. **Computational Economics**, 54(3), 1043–1063. https://doi.org/10.1007/s10614-018-9864-z

پ) وبسایت

1. www.fiu.gov.ir/sa2ma1
2. www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer.