Necessity of Providing Comprehensive Legal Frameworks in the Iranian Legal System to Protecting the Security of Land and deeds Registration Systems against Cyber Threats

Peyman Namamian[1]

Abstract

Given the rapid advancement of digital technologies and the expansion of threats arising from cybercrimes, there is an urgent need for providing comprehensive and up-to-date legal frameworks within the Iranian legal system, particularly to protect the land registration systems against such threats. These registration systems, as critical infrastructures and the official reference for property information, are always at risk from complex threats such as unauthorized access, document forgery, and targeted cyberattacks, which could jeopardize individuals' property rights and the credibility of notarial deeds. Regulations such as the Computer Crimes Law and despite the existence of the National Data and Information Management Law, are not equipped to counter modern and complex threats, nor do they align with international standards. Therefore, the formulation of comprehensive and up-to-date legal frameworks capable of safeguarding sensitive information and protecting digital property rights is an undeniable necessity. These frameworks should address emerging cyber threats, technological developments, and the need for alignment with international standards, with the establishment of independent and appropriate judicial and executive bodies to oversee and implement these laws.

Keywords: Cyber Threats, Land and deeds Registration Systems, Data Protection, Cybersecurity, Digital Property Rights.

1. Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran.
Corresponding author: p_namamian1512@yahoo.com

شناسهٔ دیجیتال (DOI): 10.22106/rlr.2025.2068475.1118
مقالهٔ پژوهشی، دورهٔ سوم، شمارهٔ دوم، پاییز و زمستان ۱۴۰۴، صفحات ۲۲۱ تا ۲۴۱
تاریخ دریافت: ۱۴۰۴/۰۵/۱۹ - تاریخ پذیرش: ۱۴۰۴/۰۷/۱۶

ضرورت‌سنجی تدوین چارچوب‌های حقوقی جامع در نظام حقوقی ایران برای حفاظت از امنیتِ سامانه‌های ثبت اسناد و املاک کشور در قبال تهدیدهای سایبری علیه آن‌ها

پیمان نمامیان*

چکیده

باتوجه به پیشرفت سریع فناوری‌های دیجیتالی و گسترش تهدیدهای ناشی از جرایم سایبری، ضرورت تدوین چارچوب‌های حقوقی جامع و روزآمد در نظام حقوقی ایران به‌ویژه برای حفاظت از سامانه‌های ثبت اسناد و املاک در قبال چنین تهدیدهایی احساس می‌شود. سامانه‌های ثبت اسناد و املاک به‌عنوان زیرساخت‌های حیاتی و مرجع رسمی اطلاعات مالکیت و اسناد، همواره در معرض تهدیدات پیچیده‌ای نظیر دسترسی غیرمجاز، جعل اسناد و حملات سایبری هدفمند قرار دارند که می‌تواند حقوق مالکیت افراد و اعتبار اسناد رسمی را به خطر اندازد. مقرراتی همچون قانون جرایم رایانه‌ای و البته به‌رغم وجود «قانون مدیریت داده‌ها و اطلاعات ملی»، توان مقابله با تهدیدهای نوین و پیچیده را ندارند و هم‌راستایی لازم با استانداردهای بین‌المللی را نیز ندارند. بنابراین، تدوین چارچوب‌های حقوقی جامع و روزآمد که قادر به محافظت از اطلاعات حساس و حفاظت از حقوق مالکیت دیجیتال باشند، ضرورتی انکارناپذیر است. این چارچوب‌ها باید تهدیدهای نوین سایبری، تحولات فناوری و نیاز به هم‌راستایی با استانداردهای بین‌المللی را

* دانشیار، گروه حقوق کیفری و جرم شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران. (نویسنده مسئول)

p_namamian1512@yahoo.com

مدنظر قرار داده و نهادهای قضائی و اجرائی مستقل و متناسب برای نظـارت و اجـرای ایـن قـوانین ایجاد شود.

واژگان کلیدی: تهدیدات سایبری، سامانه‌های ثبت اسناد و املاک، حفاظت از داده‌ها، امنیت سایبری، حقوق مالکیت دیجیتال.

مقدمه

درحال‌حاضر، سامانه‌های ثبت اسناد و املاک[1] به‌عنوان زیرساخت‌های حیاتی و اساسی در نظام حقوقی و اقتصادی کشورها ازجمله ایران شناخته می‌شوند و امنیت و اعتبار آن‌ها از اهمیت قابل ملاحظه‌ای برخوردار است. این سامانه‌ها که مسئولیت ثبت اسناد رسمی و مدیریت مالکیت‌ها را برعهده دارند، به دلیل حساسیت و نقش اساسی آن‌ها در حفظ حقوق مالکیت و تنظیم روابط اقتصادی، همواره در معرض تهدیدهای جدی، به‌ویژه تهدیدهای سایبری قرار دارند(ریاحی، ۱۳۹۹: ۱۷۹-۱۸۱). در ضمن، این سامانه‌ها نقش حیاتی در حفظ حقوق مالکیت و تنظیم معاملات در جامعه ایفا می‌کنند. آن‌ها به‌عنوان مرجع رسمی و قانونی برای ثبت مالکیت‌ها، اسناد رسمی و قراردادهای ملکی عمل کرده و از این طریق، اطمینان از صحت و اعتبار این اطلاعات را فراهم می‌آورند. درنتیجه، سامانه‌های ثبت اسناد و املاک پایه‌گذار نظم حقوقی و اقتصادی در جامعه هستند و با نقش خود در پیشگیری از اختلافات مالکیتی، موجب شفافیت و وضوح در روابط اقتصادی و اجتماعی می‌شوند. به‌علاوه، این سامانه‌ها در فرایند تنظیم معاملات، به افراد این امکان را می‌دهند که با اعتماد به اطلاعات ثبت‌شده، وارد معاملات ملکی شوند و از حمایت‌های حقوقی برخوردار گردند(فدائی و محسنی‌ثانی، ۱۴۰۲: ۳۴۷-۳۴۵). بدین‌ترتیب،

۱. این سامانه مشتمل بر «درگاه الکترونیک سازمان ثبت اسناد و املاک کشور»، «درگاه یکپارچه خدمات الکترونیکی»، «سامانه مدیریت کشوري املاک»، «سامانه کاتب (کارتابل الکترونیکی تبادل اطلاعات ثبتی)»، «سامانه شمیم (شبکه موقعیت‌یابی یکپارچه مالکیت‌ها)»، «سامانه میثم (مدیریت یکپارچه اطلاعات مکانی)»، «سامانه ثبت درخواست صدور سند مالکیت(تعیین تکلیف)»، «سامانه مدیریت اطلاعات و مستندسازی املاک دولتی»، «سامانه ثبت الکترونیک اسناد (ثبت آنی)»، «سامانه ثبت املاک و کاداستر»، «سامانه استعلامات الکترونیک»، «سامانه جامع ثبت شرکت‌ها»، «سامانه صدور شناسه یکتا برای اسناد رسمی»، «سامانه شناسه ملي اشخاص حقوقي»، «سامانه جامع مالکیت صنعتي»، «سامانه ثبت ازدواج و طلاق»، «سامانه مدیریت یکپارچه اجراي اسناد رسمي»، «سامانه ثبت الکترونیکي پذیرش درخواست صدور سند مالکیت»، «سامانه پاسخ‌گویی به شکایات و پیگیری‌ها»، «سامانه پیگیري و نظارت بر خدمات الکترونیک ثبتي»، «بانک جامع اطلاعات سردفتران و دفتریاران»، «سامانه اطلاع‌رسانی وضعیت املاک (میز خدمت الکترونیک)»، و غیره است.

این سامانه‌ها با ایجاد بستر قانونی و ایمن، به پیشبرد توسعه اقتصادی و اجتماعی جامعه کمک می‌کنند. ازاین‌رو، جرایم سایبری نظیر دسترسی غیرمجاز، جعل داده‌ها و سرقت هویت می‌توانند موجب تزلزل اعتبار و صحت این اسناد و درنتیجه تهدید جدی برای حقوق مالکیت افراد شوند(مرسی و متولی‌زاده‌نائینی، ۱۴۰۲: ۳۶-۳۴).

«قانون جرایم رایانه‌ای، مصوب ۱۳۸۸» به‌طورکلی به مقابله با جرایم سایبری و تهدیدهای مرتبط با داده‌ها و اطلاعات پرداخته است و تهدیدهایی مانند دسترسی غیرمجاز، جعل داده‌ها و سرقت هویت را پوشش می‌دهد(طبیبی و خدادادی، ۱۳۹۴: ۹۰-۹۱). بااین‌حال، این قانون در قبال تهدیدهای نوظهور و پیچیده‌تر، تهدیدهای مبتنی بر هوش مصنوعی، ناکافی است. علاوه‌براین، به‌رغم تحولات فزاینده علم و فناوری‌های نوین و تهدیدهای قابل تأمل و تهاجمی جرایم سایبری در این عرصه، قانون جرایم رایانه‌ای هم‌راستا با استانداردهای بین‌المللی در زمینه امنیت سایبری نیست. بنابراین، برای مقابله مؤثر با تهدیدهای سایبری علیه سامانه‌های ثبت اسناد و املاک، تدوین چارچوب‌های حقوقی جامع و روزآمد که به‌طور خاص به تهدیدهای سایبری مرتبط با این سامانه‌ها پرداخته و از داده‌های حساس و اسناد رسمی حمایت کنند، الزام‌آور است. این چارچوب‌ها باید با قوانین بین‌المللی در زمینه امنیت سایبری و حفاظت از حریم خصوصی هم‌راستا باشند(نگهدار، پورقهرمانی و بیگی، ۱۴۰۲: ۹۸-۹۹).

مقررات مصوب نظیر قانون جرایم رایانه‌ای برای مقابله با تهدیدهای سایبری علیه سامانه‌های ثبت اسناد و املاک با چالش‌هایی مواجه هستند. سرعت تکامل این تهدیدها و ظهور فناوری‌های نوین، به‌ویژه حملات مختل‌کننده دسترسی به خدمات برخط یا وبگاه‌ها[1] و تهدیدهای مبتنی بر هوش مصنوعی، ازجمله مسائلی هستند که مقررات ناظر به چارچوب تقنینی قانون جرایم رایانه‌ای، قادر به پوشش کامل آن‌ها نیستند. به‌علاوه، با استانداردهای بین‌المللی در زمینه امنیت سایبری و حفاظت از داده‌ها فاصله دارند و نمی‌توانند به‌طور مؤثر از اطلاعات حساس محافظت کنند. البته قانون مزبور فاقد سازوکارهای نظارتی و اجرایی مناسب برای مقابله با تهدیدات خاص این سامانه‌ها هستند.

با پیشرفت فناوری‌های دیجیتال و افزایش فزاینده تهدیدهای سایبری، ضرورت تدوین چارچوب‌های حقوقی جامع و روزآمد در نظام حقوقی ایران، به‌ویژه در حوزه امنیت سایبری و حفاظت از سامانه‌های ثبت اسناد و املاک، بیش از پیش احساس می‌شود(نفر و پاوند، ۱۴۰۲:

1. Distributed Denial of Service

۱۴-۱۶). به‌علاوه، سامانه‌های ثبت اسناد و املاک به‌عنوان مرجع رسمی ثبت اطلاعات مالکیت و اسناد قانونی، با تهدیدات متعدد نظیر دسترسی غیرمجاز، جعل اسناد و حملات سایبری پیچیده مواجه هستند که می‌تواند تهدیدهای جدی برای حقوق مالکیت افراد و اعتبار اسناد رسمی ایجاد کند. بنابراین، باتوجه به تحولات سریع فناوری و گسترش تهدیدهای سایبری، بازنگری و روزآمدی مقررات موجود، تدوین و اجرای چارچوب‌های حقوقی کارآمد در قبال تهدیدها و نیز حفاظت از داده‌ها در سامانه‌های ثبت اسناد و املاک، ضرورتی انکارناپذیر است. به‌همین‌دلیل، تدوین چارچوب‌های حقوقی جامع و به‌روز که هم‌راستا با استانداردهای بین‌المللی باشد و توان مقابله با تهدیدهای سایبری نوظهور را داشته باشد، ضروری است؛ اگرچه می‌توان با وضع «قانون مدیریت داده‌ها و اطلاعات ملی، مصوب ۱۴۰۱»[1] از سوی قانونگذار بخشی از شکاف‌ها را ازحیث امنیت سایبری مرتفع ساخت.

درعینِ‌حال، تحولات سریع در زمینه فناوری‌های دیجیتالی و سایبری، ازجمله توسعه بلاک‌چین، رمزنگاری پیشرفته، سامانه‌های شناسایی چندعاملی و سایر فناوری‌های نوین، ضرورت بازنگری و روزآمدسازی مقررات موجود را بیش از پیش آشکار می‌سازد(نظری‌خانقاء، جعفرزاده و نیک‌خواه‌سرنقی، ۱۴۰۰: ۱۶۳-۱۶۴). این مقررات باید توانایی انطباق با تهدیدات جدید را داشته باشند و از داده‌ها و اطلاعات حساس سامانه‌های ثبت اسناد و املاک در قبال حملات پیچیده محافظت کنند. برای تحقق این امر، تدوین قوانین خاص برای حفاظت از داده‌های شخصی، حقوق مالکیت دیجیتال و تقویت امنیت سامانه‌های دیجیتال ضروری به‌نظر می‌رسد. در ضمن، از دیگر چالش‌های اساسی در اجرای مقررات جدید، تأسیس نهادهای قضائی و اجرائی مستقل است که امکان نظارت مؤثر بر اجرای مقررات را داشته و مبادرت به پیگیری تخلفات سایبری نمایند. علاوه‌براین، برگزاری دوره‌های آموزشی مستمر برای مسئولان قضائی، دولتی و کارشناسان امنیت سایبری جهت آگاهی از تهدیدهای نوین و روش‌های مقابله با آن‌ها، از دیگر ضرورت‌های قانونی در این زمینه است.

---

۱. این قانون با هدف حفاظت، مدیریت و بهره‌برداری بهینه از داده‌ها و ارتقای امنیت اطلاعات طراحی شده است. به‌علاوه، ضمن تأکید بر حفاظت از اطلاعات حساس سامانه‌های ثبت اسناد و املاک، بهره‌گیری از فناوری‌های امنیتی نظیر رمزنگاری و احراز هویت چندعاملی را امری ضروری اطلاق می‌کند. در ضمن، در چارچوب این قانون، دسترسی به داده‌ها باید محدود به افراد مجاز باشد و سنجش و آموزش امنیتی مداوم صورت پذیرد. البته همکاری نهادهای مختلف برای تأمین امنیت سامانه‌ها امری الزام‌آور است.

به‌هرروی، هدف این پژوهش، بررسی ضرورت‌ها و الزامات تدوین چارچوب‌های حقوقی جامع در قبال تهدیدهای سایبری علیه سامانه‌های ثبت اسناد و املاک کشور است. این چارچوب‌ها باید از داده‌های حساس و حقوق مالکیت دیجیتال در قبال چنین تهدیدهایی محافظت کنند. همچنین، هم‌راستایی با استانداردهای بین‌المللی، روزآمدی مقررات، و ایجاد زیرساخت‌های قانونی برای حفاظت از اطلاعات و پیشگیری از جعل و دسترسی غیرمجاز، از دیگر اهداف است. البته، آموزش مسئولان و تأسیس نهادهای قضائی مستقل برای نظارت و رسیدگی به تخلفات سایبری امری الزام‌آور به‌نظر می‌رسد. ازاین‌رو، این پژوهش با بهره‌گیری از روش توصیفی تحلیلی، درصدد پاسخ به این پرسش‌هاست: «چرا سامانه‌های ثبت اسناد و املاک کشور در معرض تهدیدهای سایبری قرار دارند؟» و «چه تحولات حقوقی و فناوری باید در چارچوب مقررات ایران برای مقابله مؤثر با تهدیدهای سایبری لحاظ شود؟»

۱. تهدیدهای نوین سایبری و نقض امنیت سامانه‌های ثبت اسناد و املاک

تهدیدهای سایبری علیه سامانه‌های ثبت اسناد و املاک کشور به‌دلیل ارتباط با اطلاعات حساس مانند مالکیت‌ها و اسناد رسمی از اهمیت قابل ملاحظه‌ای برخوردار است.[۱] دسترسی غیرمجاز به اطلاعات، مانند هک و نفوذ به پایگاه‌های داده، تهدیدی اساسی علیه سامانه‌های ثبت اسناد و املاک است که می‌تواند منجر به نقض حقوق مالکیت، سرقت هویت و اختلال در فرایندهای حقوقی شود(رضوی‌فرد و موسوی، ۱۳۹۵: ۳۳-۳۶). بنابراین، جعل داده‌ها و تغییر اطلاعات در سامانه‌های ثبت اسناد و املاک تهدیدی جدی برای اعتبار و صحت اسناد رسمی و حقوق مالکیت افراد است. این تهدیدها می‌توانند منجر به ایجاد سندهای جعلی و تغییرات غیرمجاز در اطلاعات ثبت‌شده شوند که به نقض حقوق مالکیت و فساد قانونی می‌انجامد. در نظام حقوقی ایران، قانون جرایم رایانه‌ای به‌طورکلی جعل داده‌ها را تحت پوشش قرار داده است، اما در قبال تهدیدهای پیچیده‌ای نظیر حملات نوین سایبری و نفوذ به سامانه‌ها با چالش‌هایی مواجه است(تبریزی، الهی‌منش، عالی‌پور، طهماسبی و فضلی، ۱۴۰۱: ۱۱۶). بنابراین، نیاز به تدوین

۱. به‌عنوان نمونه، درگاه الکترونیکی اطلاع‌رسانی سازمان ثبت اسناد و املاک کشور از سوی «گروه هک مافیا» در پنجم خرداد ۱۳۹۵مورد حمله سایبری قرار گرفت؛

- https://www.irna.ir/news/82091306/

چارچوب‌های حقوقی جامع و به‌روز برای پیشگیری از جعل داده‌ها و حفظ حقـوق مالکیـت افـراد احساس می‌شود.

سرقت هویت و سوءاستفاده از اطلاعات شخصی در سامانه‌های ثبت اسناد و املاک تهدیـدی جدی برای حریم خصوصی و امنیت اجتماعی است. این تهدیدها می‌توانند با دسترسـی غیرمجـاز به اطلاعات حساس افراد، مانند داده‌های هویتی، اسناد رسمی و مالکیت‌ها، منجر به نقض حقـوق مالکیت و سوءاستفاده‌های مالی و اجتماعی شوند. در نظام حقوقی ایـران، مقـررات موجـود ماننـد مفاد مقرر در ماده ۱۲ قانون جرایم رایانه‌ای تا حدودی به مقابله با سرقت هویت پرداخته‌اند(خالقی و صالح‌آبادی، ۱۳۹۴: ۱۱۰)، اما این مقررات در قبال تهدیدات پیچیـده‌تر ماننـد اسـتفاده از فنـون پیشرفته در سرقت داده‌ها و هویت افراد، ناکافی هستند(بیابـانی، مهـراب و عبـدالهی، ۱۳۹۹: ۱۱-۱۲).[1] علاوه‌براین، حفاظت از داده‌های شخصی در چارچوب استانداردهای بین‌المللی در مقررات ایران به‌طورکامل لحاظ نشده است. این در حالی است، ضـرورت تـدوین چارچوب‌هـای حقـوقی جامع و روزآمد در حفاظت از اطلاعات شخصی و پیشـگیری از سوءاسـتفاده‌های احتمـالی قابـل ملاحظه است؛ این در حالی است که قانونگذار راجع‌به پاسخ کیفری در قبال سـرقت هویـت وفـق ماده ۹ «قانون مـدیریت داده‌هـا و اطلاعـات ملـی، مصـوب ۱۴۰۱» مقـرر مـی‌دارد «متخلـف یـا اخلال‌کننده در پردازش و تبادل یـا مسـتنکف از اجـرای ایـن قـانون مشـمول مجـازات انفصـال از خدمت به مدت شش‌ماه تا پنج‌سال یا حبس تعزیری به مدت نود و یک روز تا شش‌ماه مـی‌شـود». بنابراین قانونگذار در این ارتباط سعی بر آن داشته تا نسبت به حمایت کیفری از بزه‌دیدگان را در این چارچوب مدنظر قرار دهد(میرشکاری، پیش‌نماز و رکنی، ۱۴۰۳: ۲۸۱-۲۸۳).

ازبین‌بردن اعتبار و صحت اسناد یکی از آثار بحرانی تهدیـدهای سـایبری اسـت کـه مـی‌توانـد موجب نقض حقوق مالکیت، ایجاد اختلافات قانونی و حتی بحران‌های اقتصادی شود. در صورت دستکاری یا جعل اطلاعات موجود در سامانه‌های ثبت اسـناد، صـحت اسـناد رسـمی کـه مبنـای قانونی برای مالکیت‌ها و قراردادهای ملکی است، تحت تأثیر قرار می‌گیرد(صبح‌خیز، پورقهرمانی،

۱. افزون‌براین، قانونگذار وفق ماده ۳۷ «قانون گذرنامه، مصوب ۱۳۵۳»، «قانون تخلفات، جرایم و مجازات‌های مربوط به اسناد سجلی و شناسنامه، مصوب ۱۳۷۰»، ماده ۵۴۱ «قانون مجازات اسـلامی، مصـوب ۱۳۷۵»، مواد ۶۷ و ۷۵ «قانون تجارت الکترونیکی، مصوب ۱۳۸۲»، بند ج ماده ۲۴ و ۱۳۱ «قـانون مجـازات جـرایم نیروهای مسلح، مصوب ۱۳۸۲»، سرقت هویت را جرم‌انگاری کرده است.

و صفاری، ۱۳۹۹: ۷۷-۷۹). قانون جرایم رایانه‌ای به‌طورکلی با دستکاری داده‌ها مقابله می‌کند، اما در قبال تهدیدهای پیچیده‌تر مانند حملات سایبری که به‌طور مستقیم به اسناد رسمی آسیب می‌زنند، واکنش کافی ندارد.

گسترش تهدیدات سایبری در عصر دیجیتال و توسعه فناوری‌های نوین، تهدیدات سایبری را به معضلی متغیر و روبه گسترش تبدیل کرده است. این تهدیدات، به‌ویژه در زمینه سامانه‌های ثبت اسناد و املاک، شامل حملات پیچیده‌ای همچون نفوذ به سامانه‌ها، تغییر داده‌ها، و مختل‌کننده دسترسی به خدمات برخط یا وبگاه‌ها هستند. این تهدیدات نوین با سرعت بالا و به‌طور مستمر تکامل می‌یابند و سیستم‌های قانونی موجود قادر به مقابله با آن‌ها نیستند. مقررات فعلی ایران، نظیر قانون جرایم رایانه‌ای، به‌دلیل عدم هم‌راستایی با فناوری‌های نوین و تهدیدات جدید، نیازمند به‌روزرسانی و تکمیل هستند. در این راستا، تدوین چارچوب‌های حقوقی جامع و روزآمد برای مقابله با تهدیدات سایبری و حفاظت از داده‌های حساس و اسناد رسمی، امری ضروری است.

۲. امکان‌سنجی تدوین چارچوب‌های حقوقی جامع

تدوین چارچوب‌های حقوقی جامع در نظام حقوقی ایران به‌منظور مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک، به دلیل پیچیدگی و تکامل سریع تهدیدات سایبری، از اهمیت ویژه‌ای برخوردار است. سامانه‌های ثبت اسناد و املاک به‌عنوان زیرساخت‌های حیاتی در معرض تهدیداتی مانند دسترسی غیرمجاز، جعل داده‌ها و حملات پیچیده قرار دارند که می‌توانند حقوق مالکیت افراد و اعتبار اسناد رسمی را به خطر اندازند. بنابراین، این چارچوب‌ها باید تحولات فناوری را در نظر گرفته و پاسخ مناسبی به تهدیدات نوین داده و از حقوق مالکیت و داده‌های شخصی حفاظت کنند.

تضمین امنیت داده‌ها و حفظ حقوق مالکیت در دنیای دیجیتال از مسائل حیاتی در مقابله با تهدیدات سایبری است که به تدوین چارچوب‌های حقوقی جامع و به‌روز در نظام حقوقی ایران نیاز دارد(حکاک و همکاران، ۱۴۰۴: ۶-۸). سامانه‌های ثبت اسناد و املاک باید در قبال تهدیداتی مانند دسترسی غیرمجاز، دستکاری داده‌ها و جعل اسناد محافظت شوند. بنابراین، تدوین قوانین جامع و به‌روز متناسب با تحولات فناوری و تهدیدات جدید برای حفاظت از حقوق مالکیت افراد و اطلاعات حساس ضروری است.

ایجاد اعتماد عمومی و امنیت در معاملات و اسناد رسمی در قبال تهدیدات سایبری، به‌ویژه در سامانه‌های ثبت اسناد و املاک، از ارکان مهم هر چارچوب حقوقی جامع است. این سامانه‌ها به‌عنوان مرجع رسمی برای ثبت اطلاعات مالکیت و اسناد، باید از امنیت کافی برخوردار باشند تا اعتماد عمومی به آن‌ها حفظ گردد. تهدیدات سایبری نظیر دسترسی غیرمجاز، جعل داده‌ها، حملات مختل‌کننده دسترسی به خدمات برخط یا وبگاه‌ها می‌تواند به اعتبار این اسناد و حقوق مالکیت افراد آسیب وارد کند(میرزامحمدی، موسوی‌صالح و مرتب، ۱۴۰۳: ۱۷-۱۸). بنابراین، تدوین چارچوب‌های حقوقی که به‌طور مؤثر از امنیت داده‌ها و صحت اسناد رسمی محافظت کند، ضروری است. این چارچوب‌ها باید تضمین کنند که اسناد ثبت‌شده و اطلاعات مالکیتی قابل اعتماد و قابلِ‌استناد باشند.

عدم تطابق قوانین فعلی با تحولات سریع فناوری و تهدیدات سایبری جدید، یکی از چالش‌های اساسی در مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک در ایران است. قوانین حاک در نظام حقوق ایران مانند قانون جرایم رایانه‌ای به‌طور عمده به تهدیدات ساده‌تری پرداخته‌اند و قادر به پوشش تهدیدات پیچیده و نوظهور مانند حملات مختل‌کننده دسترسی به خدمات برخط یا وبگاه‌ها، استفاده از هوش مصنوعی یا نفوذهای مبتنی بر فناوری‌های پیشرفته نیستند(رجبی، ۱۴۰۳: ۲۷-۲۹). این عدم تطابق موجب ضعف در محافظت از داده‌های حساس و اسناد رسمی در قبال تهدیدات سایبری می‌شود. بنابراین، برای مقابله با تهدیدات جدید و پیچیده، نیاز به بازنگری و به‌روزرسانی قوانین موجود و تدوین چارچوب‌های حقوقی جامع و به‌روز که بتوانند به‌طور مؤثر از سامانه‌های ثبت اسناد و املاک محافظت کنند، ضروری است.

محدودیت‌های قوانین موجود در مقابله با تهدیدات سایبری پیچیده و پیشرفته، یکی از چالش‌های اساسی در نظام حقوقی ایران است. قوانین فعلی، که به‌طور عمده برای تهدیدات ابتدایی طراحی شده‌اند، قادر به پوشش تهدیدات جدید و پیچیده‌تری مانند حملات هدفمند به سامانه‌های ثبت اسناد و املاک، حملات مختل‌کننده دسترسی به خدمات برخط یا وبگاه‌ها و استفاده از هوش مصنوعی برای نفوذ به سامانه‌ها نیستند. این محدودیت‌ها منجر به آسیب‌پذیری‌های جدی در قبال تهدیدات سایبری و نقض حقوق مالکیت و اسناد رسمی می‌شود. برای مقابله با تهدیدات پیچیده، تدوین چارچوب‌های حقوقی جدید و جامع که هم‌راستا با تحولات فناوری و تهدیدات نوظهور باشد، ضروری است.

لزوم هم‌راستایی قوانین با استانداردهای بین‌المللی و فناوری‌های نوین به‌عنوان ضرورت اساسی برای به‌روزرسانی قوانین در نظام حقوقی ایران مطرح است(علیزاده، ۱۴۰۱: ۲۳). قوانین موجود، به دلیل ناتوانی در پوشش تهدیدات نوین، نمی‌توانند به‌طورکامل از اطلاعات حساس و اسناد رسمی حفاظت کنند. تطابق با استانداردهای بین‌المللی مانند مقررات عمومی حفاظت از داده‌ها[۱] و اصول امنیت سایبری جهانی به‌ویژه در زمینه حفاظت از داده‌ها[۲] ضروری است. این هم‌راستایی علاوه بر ایجاد اعتماد عمومی، به مقابله با تهدیدات نوظهور و حفظ امنیت اطلاعات در سامانه‌های ثبت اسناد و املاک کمک خواهد کرد. ازاین‌رو، این قوانین باید بر مفاهیمی چون حفاظت از حریم خصوصی، امنیت داده‌ها و حقوق مالکیت دیجیتال متمرکز شوند و با استانداردهای بین‌المللی امنیت سایبری هم‌راستا باشند.

۳. ضرورت حفاظت از اطلاعات هویتی و اسناد مالکیت در قبال تهدیدات سایبری

باتوجه به تهدیدات سایبری روزافزون و پیچیدگی‌های آن‌ها، تدوین قوانین ویژه برای حفاظت از اطلاعات هویتی و اسناد مالکیت در سامانه‌های ثبت اسناد و املاک به‌عنوان بخشی از حفاظت از داده‌های شخصی و خصوصی در نظام حقوقی ایران ضروری است.[۳] اطلاعات هویتی و اسناد مالکیت از داده‌های بسیار حساس به شمار می‌آیند که هرگونه دسترسی غیرمجاز، دستکاری یا

---

۱. مقررات عمومی حفاظت از داده‌ها (General Data Protection Regulation (GDPR), https://gdpr-info.eu/) که از سوی اتحادیه اروپا مصوب شده است، معیارهای سخت‌گیرانه‌ای را برای حفاظت از داده‌های شخصی در سراسر اروپا تعیین کرده است؛

- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016 O.J. (Apr. 27, 2016).

- https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/.

۲. اصول امنیت سایبری در سطح جهانی، به‌ویژه در حوزه حفاظت از داده‌ها، چارچوب‌های استانداردی را جهت مقابله با تهدیدات سایبری، پیشگیری از دسترسی‌های غیرمجاز و صیانت از حریم خصوصی اشخاص و نهادها فراهم می‌سازند. این اصول، هم در قالب استانداردهای بین‌المللی و هم به‌عنوان رویه‌های مطلوب در سطح جهانی مورد شناسایی و پذیرش قرار گرفته‌اند.

۳. در این راستا، سازمان ثبت‌احوال کشور با بهره‌برداری از «سامانه صدور گواهی الکترونیک ولادت» در کشور طی بهمن سال ۱۴۰۳، اقدام به کاهش امکان جعل اطلاعات هویتی نموده است که این امر منجر به افزایش ضریب اطمینان در داده‌های پایگاه اطلاعاتی سازمان ثبت‌احوال کشور خواهد شد.

- https://www.moi.ir/news/246138/

جعل آن‌ها می‌تواند به نقض حقوق مالکیت افراد و تهدید امنیت اجتماعی و اقتصادی منجر شود. بنابراین، تدوین قوانین خاص و روزآمد که به‌طور خاص از اطلاعات هویتی و اسناد مالکیت در قبال تهدیدات سایبری محافظت کند، می‌تواند به کاهش خطرات ناشی از دسترسی غیرمجاز، جعل اسناد و سایر تهدیدات سایبری کمک کند(مقدسی‌لیچاهی و همت، ۱۳۹۷: ۱۱۲-۱۱۴). بنابراین، ایجاد یک چارچوب حقوقی جامع که به‌طور خاص به حفاظت از اطلاعات هویتی و اسناد مالکیت توجه داشته باشد، از اهمیت ویژه‌ای برخوردار است و به‌منظور حفظ امنیت حقوق مالکیت و حریم خصوصی افراد در دنیای دیجیتال ضروری به‌نظر می‌رسد.

ایجاد سازوکارهای شفاف و مؤثر برای دسترسی به اطلاعات، نقش اساسی در حفاظت از داده‌های شخصی و خصوصی ایفا می‌کند. سامانه‌های ثبت اسناد و املاک حاوی اطلاعات حساس هویتی و مالکیتی افراد هستند و در صورت نبود ضوابط روشن برای دسترسی و استفاده از این داده‌ها، زمینه سوءاستفاده، نقض حریم خصوصی و تهدید امنیت حقوقی فراهم می‌شود(احمدوند و جهانشاهی، ۱۴۰۲: ۱۲۱-۱۱۹). درحال‌حاضر، خلأهایی در قوانین موجود، ازجمله در «قانون جرایم رایانه‌ای»، در زمینه تعریف دقیق نحوه دسترسی، نظارت بر استفاده از اطلاعات، و پیگیری سوءاستفاده از داده‌ها وجود دارد. این ضعف‌ها منجر به آسیب‌پذیری سامانه‌های ثبت در قبال نفوذهای غیرمجاز و انتشار یا جعل اطلاعات می‌شود(یعقوبی، جعفری و سلمان‌زاده، ۱۴۰۳: ۵۰۶-۵۰۹). البته، تدوین چارچوب‌های حقوقی به‌روز که در آن سازوکارهای دقیق، شفاف و نظارت‌پذیر برای دسترسی به داده‌ها تعریف شده باشد، ضروری است(محسنی و همکاران، ۱۳۹۸: ۳۲۹-۳۳۱). این چارچوب‌ها باید ضمن حفظ شفافیت اداری، از افشای غیرمجاز اطلاعات پیشگیری کرده و حقوق شهروندان را در قبال سوءاستفاده‌های سایبری تضمین نمایند(رئیسی‌دزکی و قاسم‌زاده‌لیاسی، ۱۳۹۹: ۱۳۵-۱۳۶). به‌علاوه، انطباق این سازوکارها با استانداردهای بین‌المللی در حوزه حفاظت از داده‌های شخصی، به تقویت اعتماد عمومی و مشروعیت نظام ثبت اسناد و املاک در فضای دیجیتال کمک خواهد کرد.

تدوین استانداردهای امنیتی برای سامانه‌ها و پایگاه‌های داده از اهمیت ویژه‌ای برخوردار است. سامانه‌های ثبت اسناد و املاک به‌عنوان زیرساخت‌های حیاتی و حاوی اطلاعات حساس مالکیتی و هویتی افراد، در معرض تهدیدات سایبری پیچیده‌ای قرار دارند که می‌توانند به اعتبار اسناد و حقوق مالکیت افراد آسیب برساند. بااین‌حال، به‌رغم اینکه سازمان ملی استاندارد ایران نسبت به

تدوین سند «امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی- سامانه مدیریت امنیت اطلاعات- الزامات»[1] طی سال ۱٤۰۲ اهتمام ویژه‌ای داشته است، اما وجود استانداردهای منسجم و دقیق برای امنیت سایبری در سامانه‌های ثبت اسناد و املاک در قوانین ایران به‌طور مشخص تعریف نشده است و این کمبود موجب آسیب‌پذیری در قبال حملات سایبری، نفوذ غیرمجاز و سرقت داده‌ها می‌شود. البته در راستای مقابله با تهدیدهای سایبری علیه زیرساخت‌های حیاتی، «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری» به‌عنوان یک برنامه جامع به‌منظور حفاظت از زیرساخت‌های حساس کشور[2] در قبال چنین تهدیدهایی، توسط مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات ریاست‌جمهوری ایران تدوین و در سال ۱۳۹۸ به کلیه سازمان‌ها و دستگاه‌های اجرایی دارای زیرساخت‌های حیاتی کشور ابلاغ شده است.[3] البته می‌توان به اسنادی دیگر نظیر «سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات(افتا)، ابلاغی ۱۳۸۹»، «سند راهبردی پدافند سایبری کشور، مصوب ۱۳۹٤»، «سند تبیین الزامات شبکه ملی اطلاعات، مصوب ۱۳۹۵»، «آیین‌نامه اجرایی قانون تعیین حریم حفاظتی- امنیتی اماکن و تأسیسات کشور، مصوب ۱۳۹۷»، «سند راهبردی جمهوری اسلامی ایران در فضای مجازی، مصوب ۱٤۰۱»، «نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور، مصوب ۱٤۰۲» و «طرح راهبردی حفاظت از زیرساخت‌های کشور، مصوب ۱٤۰۲» اشاره داشت که امکان مقابله با آماج‌های ناشی از جرایم سایبری علیه امنیتِ زیرساخت‌های حیاتی کشور را فراهم می‌نماید(ر.ک: نظری‌نژاد و پورشاسب، ۱۳۹۹: ۲۹٦؛ تقی‌پور و همکاران، ۱۳۹۸: ۱۷-۲۱). براین‌اساس، این استانداردها باید الزامات امنیتی خاص برای پیشگیری از تهدیداتی هم‌چون نفوذهای غیرمجاز، و دستکاری داده‌ها را دربَر گیرد و نظارت دقیق بر پیاده‌سازی این تدابیر را تضمین نماید. افزون‌براین، باید با الزامات بین‌المللی امنیت سایبری

1. https://sec.ito.gov.ir/uploads/images/gallery/inso-iso-iec%2027001-1402.pdf

۲. لازم به تأکید است که وفق بند (ب-۱) از ماده نخست «نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور، مصوب ۱۴۰۲» و بند هفتم از ماده نخست «طرح راهبردی حفاظت از زیرساخت‌های کشور، مصوب ۱۴۰۲» توصیف زیرساخت‌ها و نحوه حفاظت از آن‌های مورد پردازش قرار گرفته است.

3. https://amnafzar-rayka.ir/.pdf

هم‌راستا باشند تا از هرگونه آسیب و نقض اطلاعات حساس پیشگیری شود و ضمن حفظ امنیت داده‌ها، اعتماد عمومی به سامانه‌های ثبت اسناد و املاک تقویت گردد.

سامانه‌های ثبت اسناد و املاک به‌عنوان زیرساخت‌های حیاتی در ثبت و حفظ اطلاعات مالکیتی و هویتی افراد، در معرض تهدیدات سایبری پیچیده‌ای قرار دارند. برای مقابله مؤثر با این تهدیدات، علاوه بر تدوین استانداردهای امنیتی، نیاز است که نهادهایی برای نظارت و بازرسی بر اجرای دقیق این استانداردها ایجاد شود.[1] این نهادها می‌توانند مسئول نظارت بر پیاده‌سازی تدابیر امنیتی، انجام ارزیابی‌های دوره‌ای امنیتی، و بررسی تأثیر اقدامات حفاظتی در قبال تهدیدات سایبری باشند. همچنین، این نهادها باید قادر به شناسایی آسیب‌پذیری‌ها، گزارش‌گیری از وضعیت امنیتی سامانه‌ها و اتخاذ تدابیر اصلاحی باشند.[2] با تأسیس چنین نهادهایی، سامانه‌های ثبت اسناد و املاک می‌توانند از یک سامانه نظارتی مؤثر بهره‌برداری کنند که با ارزیابی‌های مستمر، بهبود وضعیت امنیتی و پیشگیری از تهدیدات سایبری را تضمین کند. تضمین این فرایند نظارتی و بازرسی در چارچوب یک چارچوب حقوقی جامع، باعث خواهد شد تا علاوه بر ارتقای امنیت سایبری، اعتماد عمومی به سامانه‌های ثبت اسناد و املاک نیز تقویت شود و از حقوق مالکیت و داده‌های حساس افراد محافظت بهینه گردد(فرزاد و فریدزاده، ۱۴۰۳: ۳۴۹-۳۵۱).

تدوین و تصویب قوانین برای محافظت از مالکیت‌های دیجیتال از الزامات حیاتی است. باتوجه به گسترش روزافزون فناوری‌های دیجیتال و مهاجرت اطلاعات مالکیتی به بسترهای برخط، ضروری است که حقوق مالکیت دیجیتال به‌ویژه در سامانه‌های ثبت اسناد و املاک به‌طور قانونی و مستند حمایت شوند(محسنیان و قاسم‌زاده‌عراقی، ۱۴۰۳: ۱۴-۱۵). مالکیت‌های دیجیتال، شامل اطلاعات شخصی و اسناد رسمی ثبت‌شده، به‌راحتی می‌توانند هدف حملات سایبری، دستکاری یا جعل قرار گیرند. در این زمینه، تصویب قوانین و مقررات خاص برای محافظت از این نوع مالکیت‌ها ضروری است(فروغی و حسین‌زاد سرشکی، ۱۳۹۸: ۴۰-۴۲). این قوانین باید به‌طور خاص از اطلاعات حساس افراد در سامانه‌های ثبت اسناد و املاک محافظت کرده و از جعل یا تغییر غیرمجاز اسناد پیشگیری کنند. همچنین، قوانین جدید باید به‌گونه‌ای تنظیم شوند که

1. https://gerdab.ir/fa/news/35189/

2. https://mydejban.com/

نه‌تنها از تهدیدات سایبری موجود پیشگیری کنند، بلکه قابلیت پاسخ‌گویی به تهدیدات نوظهور و پیچیده را نیز داشته باشند. در این راستا، چارچوب‌های حقوقی باید با استانداردهای بین‌المللی در زمینه امنیت سایبری و حقوق مالکیت دیجیتال هم‌راستا باشند تا از اعتبار و امنیت سامانه‌های ثبت اسناد و مالکیت در دنیای دیجیتال اطمینان حاصل شود(اکرمی، ۱۴۰۳: ۸-۹). در ضمن، تدوین این قوانین موجب ارتقای سطح امنیت، اعتماد عمومی و حفاظت از حقوق مالکیت دیجیتال افراد در قبال تهدیدات سایبری خواهد شد.

باتوجه به پیچیدگی‌های تهدیدات سایبری و حملات به سامانه‌های ثبت اسناد و املاک، نظارت مستمر بر عملکرد این سامانه‌ها و مقابله با تخلفات باید از یک ساختار قانونی مستقل و معتبر برخوردار باشد. نهادهای نظارتی باید به‌طور دقیق و کارآمد بر رعایت استانداردهای امنیتی و حقوقی در سامانه‌های ثبت اسناد و املاک نظارت کنند. این نهادها می‌توانند به‌عنوان مرجعی مستقل برای رسیدگی به شکایات، تخلفات و نقض حقوق مالکیت دیجیتال عمل کنند و در صورت وقوع هرگونه تهدید سایبری، اقدامات لازم برای پیشگیری از گسترش آن را انجام دهند. علاوه‌براین، این نهادها باید توانایی تحلیل تهدیدات سایبری نوین و پیچیده را داشته باشند و در صورت لزوم، به‌طور سریع و مؤثر به مراجع قضائی ارجاع دهند. در ضمن، با تأسیس چنین نهادهایی و ایجاد سازوکارهای نظارتی شفاف، می‌توان از حقوق مالکیت دیجیتال در قبال تهدیدات سایبری محافظت کرد و اعتماد عمومی به سامانه‌های ثبت اسناد و املاک تقویت شود. این اقدامات همچنین باعث می‌شود تا فرایندهای قانونی و اجرایی در راستای رعایت حقوق مالکیت دیجیتال و امنیت داده‌ها به‌طورکامل و مؤثر دنبال شوند.

۴. الزامات تدوین چارچوب حقوقی جامع از طریق همکاری‌های بین‌المللی

همان‌گونه که پیشتر این یافته پژوهشی حاصل گردید، برای تدوین چارچوب حقوقی جامع در مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک، تدوین قوانین ویژه برای حفاظت از داده‌های شخصی و حقوق مالکیت دیجیتال که هم‌راستا با استانداردهای بین‌المللی باشد، ضروری است. نهادهای نظارتی باید مستقل و کارآمد باشند و مسئولان قضائی و دولتی باید آموزش‌های مستمر در زمینه تهدیدات سایبری و امنیت داده‌ها دریافت کنند. همچنین، تقویت زیرساخت‌های امنیتی و هماهنگی میان دستگاه‌های دولتی، قضائی و متخصصان فناوری

اطلاعات برای مقابله مؤثر با تهدیدات سایبری الزامی است. این اقدامات به تقویت امنیت سامانه‌ها و افزایش اعتماد عمومی کمک خواهد کرد.

آموزش و آگاهی‌بخشی به مسئولان دولتی و قضائی در زمینه تهدیدات سایبری و امنیت داده‌ها، یکی از ارکان بنیادین برای اجرای مؤثر قوانین و چارچوب‌های حقوقی است.[1] ضعف آگاهی در این حوزه می‌تواند منجر به تصمیم‌گیری‌های نادرست، اعمال ناقص قوانین و عدم توانایی در پیشگیری یا مقابله با حملات سایبری شود. بنابراین، آموزش مستمر مسئولان، قضات و مدیران سامانه‌های ثبت اسناد در زمینه اصول امنیت سایبری، حفاظت از داده‌ها و حقوق مالکیت دیجیتال، ضروری است. این آموزش‌ها باید در چارچوب یک سیاست ملی جامع و با همکاری نهادهای فنی و حقوقی طراحی و اجرا شوند. البته برگزاری دوره‌های آموزشی برای آشنایی مردم با حقوق دیجیتال و امنیت سایبری به‌عنوان ابزاری مهم برای آگاهی‌بخشی به مسئولان و شهروندان در راستای تدوین چارچوب‌های حقوقی جامع در مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک ضروری است(رضایی و بابازاده‌مقدم، ۱۳۹۳: ۵۴-۵۶). این آموزش‌ها می‌تواند مسئولان قضائی و دولتی را برای پاسخ‌گویی مؤثر به تهدیدات سایبری آماده کند و شهروندان را در حفاظت از حقوق دیجیتال و اطلاعات شخصی خود آگاه سازد.

تقویت زیرساخت‌های فنی برای مقابله با حملات سایبری و حفاظت از اطلاعات در چارچوب تدوین یک چارچوب حقوقی جامع در نظام حقوقی ایران، امری ضروری است. این اقدام نیازمند توسعه زیرساخت‌های فناوری و امنیتی است تا از سامانه‌های ثبت اسناد و املاک در قبال تهدیدات سایبری محافظت شود. از دیدگاه حقوقی، این تقویت زیرساخت‌ها باید همسو با استانداردهای امنیتی بین‌المللی انجام شود و قوانین خاصی برای نظارت و ارزیابی این زیرساخت‌ها تدوین شود تا در صورت وقوع تهدیدات، سامانه‌ها قادر به واکنش سریع و مؤثر باشند(سپهری، ۱۴۰۰: ۹۳-۹۶). در ضمن، همکاری با بخش خصوصی و سازمان‌های بین‌المللی برای تقویت امنیت سایبری در چارچوب تدوین یک چارچوب حقوقی جامع در نظام حقوقی ایران، به‌ویژه در مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک، از اهمیت ویژه‌ای برخوردار است. این همکاری‌ها می‌تواند به تبادل تجربیات، استفاده از فناوری‌های پیشرفته

1. https://rahbangroup.ir/blog/post/

و بهره‌برداری از استانداردهای بین‌المللی کمک کند و موجب تقویت زیرساخت‌های فناوری، ارتقای امنیت داده‌ها و حفاظت از حقوق مالکیت دیجیتال افراد شود.

نظارت مستمر و نظام‌مند بر اجرای قوانین جدید در راستای مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک از جنبه حقوقی ضروری است.[1] این نظارت باید توسط نهادهای مستقل و کارآمد صورت گیرد که از اختیارات کافی برای ارزیابی و برخورد با نقض‌های قانونی برخوردار باشند. چنین نظارتی می‌تواند به حفظ امنیت سامانه‌های ثبت اسناد و املاک، حفاظت از حقوق مالکیت دیجیتال و افزایش اعتماد عمومی به ساختارهای حقوقی کشور کمک کند. ازاین‌رو، ایجاد نهادهای قضائی و اجرائی برای رسیدگی به تخلفات در زمینه تهدیدات سایبری، از جنبه حقوقی ضروری است. این نهادها باید با اختیارات قانونی مشخص و به‌طور مستقل مسئول نظارت و پیگیری تخلفات سایبری باشند. به‌علاوه، نقش حیاتی در اجرای مؤثر قوانین، شناسایی و مقابله با تهدیدات سایبری و اعمال مجازات‌های قانونی در صورت وقوع تخلف دارند. همچنین، باید فرایندهای شفاف و استانداردشده‌ای برای رسیدگی به شکایات و تخلفات فراهم کنند تا حقوق افراد و امنیت اطلاعات در سامانه‌های ثبت اسناد و املاک حفظ شود.

نتیجه‌گیری

تهدیدات سایبری به چالش عمده‌ای برای سامانه‌های ثبت اسناد و املاک تبدیل شده است. برای مقابله با این تهدیدات، تدوین چارچوب حقوقی جامع در ایران ضروری است. این چارچوب شامل تدوین قوانین برای حفاظت از داده‌های شخصی، تقویت زیرساخت‌های امنیتی، و آموزش مستمر مسئولان و مردم در زمینه امنیت سایبری است. همچنین، هماهنگی با استانداردهای بین‌المللی، تأسیس نهادهای قضائی مستقل و تقویت همکاری میان دستگاه‌های دولتی، قضائی و بخش خصوصی از اهمیت ویژه‌ای برخوردار است. به‌روزرسانی مداوم قوانین امنیت سایبری و استفاده از فناوری‌های نوین مانند بلاک‌چین و رمزنگاری برای تقویت امنیت سامانه‌ها ضروری است. این اقدامات به تقویت امنیت و اعتماد عمومی به سامانه‌های دیجیتال کمک خواهد کرد و برای توسعه پایدار و ایمن نظام حقوقی ایران ضروری است.

1. https://www.mizanonline.ir/fa/news/4840380/

برای مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک در ایران، تصویب قوانین جدید ضروری است. این قوانین باید حفاظت از داده‌های شخصی و مالکیت دیجیتال را تضمین کرده و با استانداردهای بین‌المللی مانند مقررات عمومی حفاظت از داده‌ها هم‌راستا باشند. همچنین، مقرراتی برای پیشگیری از دسترسی غیرمجاز و مقابله با حملات سایبری هدفمند باید وضع شود. استفاده از فناوری‌های نوین مانند بلاک‌چین و رمزنگاری قوی، برگزاری دوره‌های آموزشی مستمر برای مسئولان و تأسیس نهادهای قضائی مستقل از دیگر الزامات است. علاوه‌براین، تصویب قوانینی برای همکاری با نهادهای بین‌المللی و به‌روزرسانی مستمر قوانین امنیت سایبری امری ضروری است. این اصلاحات به تقویت امنیت سامانه‌ها و کاهش تهدیدات سایبری کمک خواهد کرد.

برای مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک در ایران، پیشنهاد تشکیل کارگروه‌های حقوقی، فنی و امنیتی ضروری است. همچنین، کارگروه فنی و امنیتی باید فناوری‌های نوین مانند بلاک‌چین، رمزنگاری و سامانه‌های شناسایی چندعاملی[1] را برای تقویت امنیت سامانه‌ها مشخص کند. کارگروه امنیتی نیز مسئول مقابله با حملات سایبری هدفمند و آموزش مسئولان خواهد بود. این کارگروه‌ها باید با نهادهای دولتی، قضائی و بخش خصوصی همکاری کنند تا چارچوب‌های حقوقی و فنی به‌طور مؤثری به‌روزرسانی شوند.

بااین‌همه، برای مقابله با تهدیدات سایبری علیه سامانه‌های ثبت اسناد و املاک در ایران، همکاری با کشورهای پیشرفته در زمینه امنیت سایبری و تبادل تجربیات ضروری است. این همکاری‌ها به تدوین چارچوب‌های حقوقی جامع، بهبود زیرساخت‌های امنیتی و هم‌راستایی با استانداردهای بین‌المللی کمک می‌کند. همچنین، تبادل اطلاعات در زمینه‌های حفاظت از داده‌ها و مقابله با حملات سایبری، برگزاری دوره‌های آموزشی و ایجاد شبکه‌های همکاری میان نهادهای مختلف را تسهیل می‌کند. درنتیجه، این همکاری‌ها می‌توانند به تقویت امنیت سایبری و حفاظت از اطلاعات حساس در سامانه‌های ثبت اسناد و املاک ایران منجر شوند.

1. Multi-Factor Authentication

منابع

۱. احمدوند، بهناز و جهانشاهی، آرتین (۱۴۰۲). بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیه اروپا و ایران. پژوهش‌های حقوق تطبیقی، ۲۷(۱)، ۱۰۵-۱۳۲.

۲. اکرمی، خدیجه (۱۴۰۳). رسانه‌های دیجیتالی و حقوق مالکیت معنوی. علوم خبری، ۱۳(۳)، ۱-۲۰.

۳. بیابانی، غلامحسین؛ مهراب، شادی و عبدالهی، علیرضا (۱۳۹۹). شناسایی شیوه‌های نوین مبارزه با جعل اسناد هویتی. کارآگاه، ۱۳(۵۱)، ۷-۲۵.

۴. تبریزی، صادق؛ الهی‌منش، محمدرضا؛ عالی‌پور، حسن؛ طهماسبی، جواد و فضلی، مهدی (۱۴۰۱). اصل قانون‌مندی توقیف داده و سامانه در فرایند کیفری؛ جلوه‌ها و تضمین‌ها. تعالی حقوق، ۸(۲)، ۱۰۹-۱۴۰.

۵. تقی‌پور، رضا و همکاران (۱۳۹۸). الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران. امنیت ملی، ۹(۳۴)، ۴۸-۷.

۶. سپهری، محمد (۱۴۰۰). مصون‌سازی زیرساخت‌های سایبری کشور در برابر تهدیدهای آمریکا. مطالعات جنگ، ۸(۳)، ۱۰۹-۸۷.

۷. حکاک، اسمهان؛ کوهی‌اصفهانی، احمد؛ یوسفی، عطیه و نصراصفهانی، علیرضا (۱۴۰۴). روندهای مؤثر بر آینده حکمرانی ملی داده‌ها. ماهنامه گزارش‌های کارشناسی مرکز پژوهش‌های مجلس شورای اسلامی، ۳۳(۱)، ۱-۴۱.

۸. خالقی، ابوالفتح و صالح‌آبادی، زهرا (۱۳۹۴). مطالعه سرقت هویت در حقوق فدرال آمریکا با نگاهی اجمالی به حقوق ایران. حقوق تطبیقی، ۱۱(۲)، ۱۱۴-۸۷.

۹. فرزاد، الهام و فریدزاده، محمد (۱۴۰۲). حفاظت از حریم خصوصی مخاطبان در دنیای دیجیتال؛ نقش حیاتی سواد رسانه‌ای. مطالعات فقه و حقوق رسانه، ۶(۲)، ۳۵-۵۳.

۱۰. فروغی، سیدعلیرضا و حسین‌زاده‌سرشکی، اسماء (۱۳۹۸). بررسی فقهی و حقوقی مالیت و مالکیت داده‌های دیجیتال در فضای سایبری. فقه و حقوق خصوصی، ۲(۳)، ۳۳۷-۳۶۸.

۱۱. فدائی، الناز و محسنی‌ثانی، مصطفی (۱۴۰۲). تحلیل حقوقی تحولات نظام اداری سازمان ثبت اسناد و املاک کشور؛ در پرتو سند تحول قوه قضائیه. پژوهش‌های نوین حقوق اداری، ۵(۱۷)، ۳۳۶-۳۶۵.

۱۲. محسنیان، سیدعلی؛ و قاسم‌زاده‌عراقی، مرتضی (۱۴۰۴). فساد در زنجیره تأمین داده‌های فضای مجازی. ماهنامه گزارش‌های کارشناسی مرکز پژوهش‌های مجلس شورای اسلامی، ۳۲(۱)، ۱-۲۶.

۱۳. صبح‌خیز، رضا؛ پورقهرمانی، بابک و صفاری، علی (۱۳۹۹). الگوی راهبردی مقابله با جرایم سایبری در ایران. مطالعات راهبردی ناجا، ۵(۱۸)، ۱۱۲-۷۷.

۱۴. رجبی، ابوالقاسم (۱۴۰۳). مروری بر مفاهیم و نهادهای مرتبط با فضای مجازی (رایاسپهر) و ارائه چشم‌انداز تقنینی و نظارتی مجلس دوازدهم. ماهنامه گزارش‌های کارشناسی مرکز پژوهش‌های مجلس شورای اسلامی، ۳۲(۱۱)، ۱-۳۴.

۱۵. رضایی، مهدی و بابازاده‌مقدم، حامد (۱۳۹۳). اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا. پژوهش حقوق عمومی، ۱۵(۴۲)، ۴۳-۸۲.

۱۶. رضوی‌فرد، بهزاد و موسوی، سیدنعمت‌اله (۱۳۹۵). مسئولیت کیفری در فضای سایبر در حقوق ایران. پژوهش حقوق کیفری، ۵(۱۶)، ۲۹-۴۵.

۱۷. ریاحی، نوربخش (۱۳۹۹). سازمان ثبت اسناد و املاک و رابطه آن با استقلال قوه قضاییه. تحقیق و توسعه در حقوق تطبیقی، ۳(۹)، ۱۷۸-۲۱۰.

۱۸. رئیسی‌دزکی، لیلا و قاسم‌زاده‌لیاسی، فلور. (۱۳۹۹). چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر. مجله حقوقی دادگستری، ۸۴(۱۱۰)، ۱۲۳-۱۴۶.

۱۹. علیزاده، پریسا (۱۴۰۱). تحلیل اسناد بالادستی در راستای تدوین سند نوآوری در حوزه علوم تحقیقات و فناوری. طرح پژوهشی، مرکز تحقیقات سیاست علمی کشور، پائیز.

۲۰. طبیبی، مرتضی و خدادادی، انیس (۱۳۹۴). سرقت هویت. مطالعات تطبیقی حقوق معاصر، ۶(۱۰)، ۷۵-۹۵.

۲۱. مرسی، هادی و متولی‌زاده‌نائینی، نفیسه (۱۴۰۲). راهبرد مقابله با حملات سایبری علیه سامانه‌های رایانه‌ای ارائه‌دهنده خدمات ضروری در قانون مجازات اسلامی مصوب ۱۳۹۲. مجلس و راهبرد، ۳۰(۱۱۳)، ۲۹-۵۵.

۲۲. محسنی، وجیهه؛ هاشمی، سیدمحمد؛ جاوید، محمدجواد و عباسی، بیژن (۱۳۹۸). تحلیل حقوقی نسبت‌سنجی حق دسترسی عموم به اطلاعات با تحقق حقوق شهروندی با تأکید بر نظام حقوقی ایران. پژوهش حقوق عمومی، ۲۱(۶۲)، ۳۲-۳۵۴.

۲۳. میرشکاری، عباس؛ پیشنماز، سیدامین و رکنی، امیرعباس (۱۴۰۳). تراست داده سازوکاری برای مدیریت منافع ذی‌نفعان داده؛ رهنمودهایی برای نظام داده در حقوق ایران. مطالعات تطبیقی حقوق معاصر، ۱۵(۳۴)، ۲۷۹-۳۲۰.

۲۴. میرزامحمدی، ایلیا؛ موسوی‌صالح، محمد و مرتب، یحیی. (۱۴۰۳). نظارت بر پروژه استقرار هویت هوشمند اشخاص حقوقی در راستای اجرای ۲۳ پروژه اولویت‌دار دولت الکترونیک. ماهنامه گزارش‌های کارشناسی مرکز پژوهش‌های مجلس شورای اسلامی، ۳۳(۱)، ۱-۴۱.

۲۵. مقدسی‌لیچاهی، امیرحسین و همت، حمید (۱۳۹۷). ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه. آینده‌پژوهی دفاعی، ۳(۱۰)، ۱۰۳-۱۲۰.

۲۶. نفر، زینب و پاوند، محمدحسین (۱۴۰۲). تدابیر پیشگیری از جرایم درگاه‌های پرداخت اینترنتی. فقه و حقوق نوین، ۵(۱۳)، ۱-۲۲.

۲۷. نظری‌خانقاء، سیدغنی؛ جعفرزاده، سیامک و نیک‌خواه‌سرنقی، رضا (۱۴۰۰). نقش سیاست جنایی مشارکتی در پیشگیری از جرایم سایبری در ایران. پژوهش‌های سیاسی جهان اسلام، ۱۱(۴)، ۱۵۱-۱۷۴.

۲۸. نظری‌نژاد، احمدعلی؛ عبدالعلی‌پورشاسب، عبدالعلی (۱۳۹۹). الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران. مطالعات دفاعی استراتژیک، ۱۸(۸۲)، ۳۱۳-۳۳۶.

۲۹. نگهدار، ایرج؛ پورقهرمانی، بابک و بیگی، جمال (۱۴۰۲). سیاست‌گذاری جنایی در نقض امنیت سایبری و رهیافت‌های پیشگیری اجتماعی. سیاست‌گذاری عمومی، ۹(۲)، ۹۷-۱۱۴.

۳۰. یعقوبی، محدثه؛ جعفری، علی و سلمان‌زاده، جعفر (۱۴۰۲). بررسی نقاط قوت و ضعف قانون انتشار و دسترسی آزاد به اطلاعات از دیدگاه حقوق‌دانان. مجلس و راهبرد، ۳۱(۱۱۷)، ۴۹۷-۵۲۸