



مقدمه حقوق



دوره ۹ - شماره ۲۸ - تابستان ۱۴۰۵

آثار حقوقی ناشی از گشایش اعتبار اسنادی نسبت به خریدار و ذینفع
همایون مافی، محسن رئیس، احمدرضا امیری لاریجانی
امکان سنجی عدالت کیفری بین‌المللی برای رسیدگی به اکوساید در چهارچوب تغییرات اقلیمی
سبحان طیبی، ماجده معقولی
تحلیل ماهیت و سازوکار اجرای تصمیمات دیوان بین‌المللی دادگستری با تأکید بر رویه دیوان در مواجهه با خلأ حقوقی
سمیه رحمانیان، پوریا ابراهیم زاده
منع سوءاستفاده از اضطرار در نظام حقوقی ایران
زینب قادری، عبدالمجید یوسفی، ستار فخرایی
مطالعه تطبیقی شرط انفساخ در حقوق ایران و نهاد انحلال قرارداد در کنوانسیون بیع بین‌المللی کالا
حکیمه محمودسلطانی، مهدی شیخ محمودی
ارکان و مبانی جرم‌انگاری تبانی برای ارتکاب جرم در حقوق کیفری ایران و فرانسه
صابر سیاری زهان
چالش‌های اسناد الکترونیکی در حقوق ایران
محمدرضا عبدی، ساسان وزین پور
نقش دوگانه هوش مصنوعی در مقابله با اطلاعات نادرست و جعل عمیق: چالش‌ها و راهکارها
عاطفه لرججوری، سیداحمد پیروندیزی
ماهیت حقوقی شرط بنایی در فقه امامیه و حقوق ایران؛ تبیین مبانی اعتبار و قلمرو آن در قراردادهای مشارکت مدنی
سیدعلیرضا حسینی، محمدرضا رستمی، طاهره جعفری
بررسی فقهی و حقوقی جایگاه و نقش وصیت اشخاص بلاوارث در تعیین تکلیف دارایی بعد از فوت
سیده نازنین موسوی
مبانی، شرایط و آثار قراردادهای تأمین کیفری متهم در نظام کیفری ایران
کامران رحیمی سکه روانی
بررسی فقهی بطلان معاملات در قانون الزام به ثبت رسمی معاملات اموال غیرمنقول
مهدی رجائیان، جعفر قجه بیگلر
بره دیدگی اطفال و نوجوانان در فضای سایبری و متاورس: مروری بر شناخت علل تا راهکارهای پیشگیری و مقابله با آن
جواد چراغی
تحلیل نقش‌های حمایتی کنوانسیون بیع بین‌المللی کالا در زمینه تسهیل و صیانت از تجارت بین‌المللی
اسماعیل چوگانی
کارکرد سیاست جنایی دادستانی در پیشگیری و تعقیب جرائم ناقض حقوق عامه
وحید کیومرثی
مطالعه تطبیقی قاعده استقلال شرط دآوری در حقوق ایران، فرانسه، انگلستان و قانون نمونه آنسیترال؛ نظریه‌ها و رویه‌ها
سعید جوهر
وضعیت معاملات مجنون ادواری در حقوق ایران و انگلستان
امیرمحمد توکلی، ستایش حاج رجبعلی طهرانی، فاطمه اله وردی، امیررضا نقروی
تأثیر قوانین سختگیرانه بر رفتارهای مرتبط با خرید و فروش مواد مخدر
حمیدرضا قناعتیان
نقش صلح آمیز انرژی هسته‌ای در حقوق ایران و نظام بین‌الملل با رویکرد جدید
مجاهد امیری، فاطمه اصغرزاده شیرازی
تأثیر فناوری‌های نوین، هوشمندسازی و تحول دیجیتال در اجرای قانون الزام به ثبت رسمی معاملات اموال غیرمنقول
نگار فولادی، وجیهه محسنی
تحلیل جرم شناختی قاچاق کالا در استان هرمزگان
احمد پدیدار، محمد کمالی
قرارداد هوشمند در نظام حقوقی ایران
مهدی صالحی زاده
چالش‌های حقوقی دولت الکترونیک و مسئولیت مدنی دولت
سعید سردشتی بیرجندی
اصل بی طرفی تحصیل دلیل در فرآیند دادرسی کیفری ایران
محمدحسن ملک محمدی
تحلیل کیفی مبانی و قلمرو مسئولیت کیفری در ارتکاب جرائم ناشی از سندرم پای بی قرار: تعامل اختلال عصبی-حرکتی با
ارکان تقصیر و قابلیت انتساب
زهره عنالوی اصفهانی
نسبت قاعده و استثناء در حقوق مدنی ایران: با تأکید بر اصل لزوم قراردادهای و موارد خروج از آن
امیررضا علی تبار
نهادسازی اساسی: ثبت‌نام در ارتش و حبس دسته‌جمعی در ایالات متحده آمریکا
برایان سایکز، امی کیتی بابلی، یاسر شاکری



Legal Challenges of E-Government and Government Civil Liability

چالش‌های حقوقی دولت الکترونیک و مسئولیت مدنی دولت

Saeed Sardashti Birjandi

Master of Science in Criminal Law and Criminology, Faculty of Humanities, Islamic Azad University, Rafsanjan Branch, Rafsanjan, Iran

سعید سردشتی بیرجندی

کارشناس ارشد حقوق کیفری و جرم‌شناسی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد رفسنجان، رفسنجان، ایران

sardashti.saeid@iran.ir

Abstract

The expansion of e-government as a strategy for enhancing public service efficiency has transformed the nature of legal interactions between the state and citizens. Relying on automated and data-driven systems, new challenges have emerged in the realm of state civil liability that traditional laws cannot adequately address. This research aims to analyze the legal challenges arising from the implementation of e-government and clarify the foundations of the state's civil liability regarding damages suffered by citizens due to system errors. The main research question is: In the event of failures in digital government processes, what legal basis exists for compensating damages and determining liability? The present study employs a descriptive-analytical method, utilizing library and documentary sources. The findings indicate that shifting from the theory of fault to the theory of risk and strict liability is essential for compensating damages caused by software bugs, server outages, or algorithmic decision-making. Furthermore, ambiguity regarding the boundaries of liability between private contractors and the state remains a primary obstacle to citizens' access to justice. The final conclusion suggests that to achieve digital justice, there is a need to revise civil liability laws, ensure algorithmic transparency, and establish independent supervisory mechanisms, thereby increasing citizens' confidence in legal security within the digital space.

Keywords: E-government, State Civil Liability, System Error, Damage Compensation, Digital Rights.

چکیده

گسترش دولت الکترونیک به عنوان راهکاری برای کارآمدسازی خدمات عمومی، ماهیت تعاملات حقوقی میان دولت و شهروندان را دگرگون کرده و چالش‌های جدیدی در حوزه مسئولیت مدنی دولت پدیدار شده که قوانین سنتی پاسخگوی آن‌ها نمی‌باشند. گسترش دولت الکترونیک صرفاً «دیجیتالی کردن خدمات» نیست؛ بلکه معیار تصمیم‌گیری و ارائه خدمت عمومی را از الگوی انسانی-اداری به الگوی سیستمی، خودکار و داده‌محور تغییر می‌دهد. همین تغییر، ماهیت تعاملات حقوقی دولت و شهروند را از چند جهت دگرگون کرده و در نتیجه، صورت‌بندی کلاسیک مسئولیت مدنی دولت که معمولاً بر خطای انسانی، فعل یا ترک فعل مأمور و رابطه مستقیم میان تصمیم اداری و زیان بنا شده با چالش‌های تازه‌ای روبرو می‌شود. هدف این پژوهش، واکاوی چالش‌های حقوقی ناشی از پیاده‌سازی دولت الکترونیک و تبیین مبنای مسئولیت مدنی دولت در قبال خسارات وارده به شهروندان ناشی از خطاهای سیستمی است. حال پرسش این است که در صورت بروز نقص در فرایندهای دیجیتال دولتی، چه مبنای حقوقی برای جبران خسارت و تعیین مسئولیت وجود دارد؟ یافته‌های پژوهش حاضر که با روش توصیفی-تحلیلی انجام شده نشان می‌دهند که گذار از نظریه تقصیر به سمت نظریه ریسک و مسئولیت بدون تقصیر، برای جبران خسارات ناشی از باگ‌های نرم‌افزاری، قطعی سرورها یا تصمیم‌گیری‌های الگوریتمی ضروری است. همچنین، ابهام در مرزهای مسئولیت پیمانکاران خصوصی و دولت، یکی از موانع اصلی دسترسی شهروندان به عدالت است. نتیجه نهایی حاکی از آن است که برای تحقق عدالت دیجیتال، نیازمند بازنگری در قوانین مسئولیت مدنی، شفاف‌سازی الگوریتم‌های تصمیم‌گیر و ایجاد سازوکارهای نظارتی مستقل می‌باشیم تا اطمینان شهروندان از امنیت حقوقی در فضای دیجیتال افزایش یابد.

واژگان کلیدی: دولت الکترونیک، مسئولیت مدنی دولت، خطای سیستمی، جبران خسارت، حقوق دیجیتال.

ارجاع:

سردشتی بیرجندی، سعید؛ (۱۴۰۵)، چالش‌های حقوقی دولت الکترونیک و مسئولیت مدنی دولت، تمدن حقوقی، شماره ۲۸.

Copyrights:

Copyright for this article is retained by the author (s) , with publication rights granted to Legal Civilization. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>) , which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



CC BY-NC-SA



مقدمه

در دهه‌های اخیر، فناوری اطلاعات و ارتباطات نه تنها ابزارهایی برای تسهیل ارتباطات، بلکه پیشران اصلی تغییرات ساختاری در حکمرانی بوده‌اند. ظهور «دولت الکترونیک» به‌عنوان پارادایمی نوین در ارائه خدمات عمومی، ماهیت تعامل میان دولت و شهروندان را دگرگون ساخته است. در این مدل جدید، مرزهای فیزیکی حذف شده و فرایندهای اداری، تصمیم‌گیری‌ها و حتی اجرای قوانین، به سیستم‌های خودکار، پایگاه‌های داده و الگوریتم‌های نرم‌افزاری سپرده می‌شوند (قیاسی و همکاران، ۱۴۰۱، ۵۴۰). این گذار سریع از بوروکراسی سنتی به دیجیتال، اگرچه از نظر کارایی و شفافیت وعده‌های بزرگی داده است، اما چالش‌های حقوقی پیچیده‌ای را نیز به همراه داشته است. یکی از مهم‌ترین این چالش‌ها، مسئله «مسئولیت مدنی دولت» در قبال خساراتی است که شهروندان ممکن است در بستر این سیستم‌های دیجیتال متحمل شوند.

مسئله اصلی این جا است که قوانین مسئولیت مدنی سنتی که عمدتاً بر پایه «تقصیر» انسانی و رابطه علیت مستقیم میان رفتار فیزیکی و خسارت استوارند، در مواجهه با خطاهای سیستمی، باگ‌های نرم‌افزاری، قطعی سرورها یا تصمیم‌گیری‌های الگوریتمی دچار خلأ می‌شوند. وقتی یک شهروند به دلیل خطای محاسباتی در سامانه مالیاتی جریمه می‌شود یا به دلیل نقص در سامانه ثبت احوال از

دریافت خدمات محروم می‌گردد، اثبات تقصیر یک «کارمند» یا «مدیر» دشوار و گاهی غیرممکن است. در این جا، عامل خسارت یک سیستم غیرزنده و پیچیده است. علاوه بر این، با برون‌سپاری بسیاری از خدمات دولتی به پیمانکاران خصوصی، مرزهای مسئولیت میان دولت و بخش خصوصی کمرنگ شده و شهروندان در مسیر جبران خسارت با موانع رویه‌ای و حقوقی روبرو می‌شوند. ابهام در حاکمیت قانون بر فضای مجازی و عدم شفافیت الگوریتم‌های تصمیم‌گیر^۱، این چالش را تشدید کرده است (لطیف زاده، ۱۴۰۳، ۷۱).

بنابراین، سؤال این جا است که در نظام حقوقی فعلی، چه مبنایی برای جبران خسارت شهروندان ناشی از ناکارآمدی یا خطای سیستم‌های دولت الکترونیک وجود دارد و چگونه می‌توان تعادل میان بهره‌وری دولت و حقوق شهروندی را حفظ کرد؟ هدف اصلی این پژوهش، واکاوی چالش‌های حقوقی ناشی از پیاده‌سازی دولت الکترونیک و تبیین مبانی نظری و عملی مسئولیت مدنی دولت در قبال خطاهای سیستمی است. روش پژوهش حاضر، توصیفی-تحلیلی است و با بهره‌گیری از منابع کتابخانه‌ای، اسناد بالادستی و مقالات علمی داخلی و خارجی انجام شده است. داده‌ها با روش استقرایی و تحلیل محتوای اسناد حقوقی مورد بررسی قرار گرفته‌اند.

۱- پیشینه پژوهش

بررسی پیشینه پژوهش نشان می‌دهد که پژوهش‌های متعددی در حوزه دولت الکترونیک انجام شده است. برای مثال، پژوهش «چالش‌های حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک»، بیشتر بر جنبه‌های حفاظتی و داده‌محور شهروندان تمرکز داشته است. همچنین، پژوهشی با عنوان «درآمدی بر مسئولیت مدنی در فضای سایبر» به‌طور کلی به مسئولیت در فضای مجازی پرداخته، اما تمرکز ویژه‌ای بر ساختار خاص «دولت» و تفاوت آن با بخش خصوصی نداشته است.

وجه تمایز پژوهش حاضر با این مطالعات، تمرکز اختصاصی بر «رابطه علیت در سیستم‌های خودکار دولتی» و «نقش پیمانکاران خصوصی در زنجیره مسئولیت» است. درحالی که پژوهش‌های قبلی بیشتر به کلیات پرداخته‌اند، این پژوهش به‌طور خاص به خلأهای قانونی در جبران خسارت‌های مالی و معنوی شهروندان ناشی از خطاهای فنی دولت می‌پردازد.

جنبه نوآوری این پژوهش در ارائه مدلی ترکیبی از «مسئولیت تضامنی دولت و پیمانکار» و پیشنهاد مکانیسم‌های نظارتی مستقل برای شفاف‌سازی الگوریتم‌ها است. یافته‌های پژوهش نشان می‌دهند که تکیه صرف بر نظریه تقصیر در دولت الکترونیک منجر به بی‌عدالتی برای شهروندان می‌شود؛ بنابراین، پیشنهاد می‌شود که قانون‌گذار با پذیرش «نظریه ریسک»، دولت را مسئول هرگونه خسارت ناشی از عملکرد سیستم‌های تحت مدیریت خود بداند، صرف‌نظر از تقصیر مستقیم کارکنان. همچنین، شفاف‌سازی الگوریتم‌ها و ایجاد صندوق‌های جبران خسارت تخصصی، از راهکارهای کلیدی برای کاهش این چالش‌ها است. در نتیجه، دولت الکترونیک بدون تضمین حقوقی قوی برای جبران خسارات، نمی‌تواند پایدار بماند. شفافیت، مسئولیت‌پذیری و به‌روزرسانی مستمر قوانین، سه رکن اصلی برای ایجاد اعتماد عمومی در فضای دیجیتال هستند.

۲- مفهوم دولت الکترونیک

دولت الکترونیک^۲ در ادبیات حقوقی و مدیریتی معاصر، فراتر از یک تعریف ساده «استفاده از فناوری اطلاعات برای ارائه خدمات دولتی» است. این مفهوم، تجلی‌گاه گذار از «دولت بوروکراتیک» به «دولت شبکه‌ای» و «دولت داده‌محور» محسوب می‌شود. برای درک عمیق این مفهوم در بستر حقوقی، باید آن را به‌عنوان یک بازآرایی ساختاری در روابط قدرت، مسئولیت و شفافیت بررسی کرد.

دولت الکترونیک به معنای ادغام زیرساخت‌های فناوری اطلاعات و ارتباطات^۳ در فرایندهای داخلی و خارجی دولت است تا کارایی، اثربخشی و پاسخگویی نهاد حاکمیتی افزایش یابد. اما این تعریف عمل‌گرایانه، ابعاد حقوقی پیچیده‌تری را پنهان می‌کند. دولت الکترونیک در واقع، «دیجیتالی شدن حاکمیت» است. در این فرایند، قوانین و مقررات که پیش‌تر به صورت متنی و انسانی تفسیر می‌شدند، به کدها و الگوریتم‌های نرم‌افزاری تبدیل می‌شوند. این پدیده که گاهی تحت عنوان «قانون‌گذاری از طریق کد»^۴ شناخته می‌شود، ماهیت اجرای قانون را دگرگون می‌سازد. در دولت سنتی، مأمور اجرایی دارای اختیارات تفسیری و قضاوت انسانی بود؛ اما در دولت الکترونیک، این اختیارات به سیستم‌های خودکار سپرده می‌شود که بر اساس منطق صفر و یک عمل می‌کنند (معمارزاده طهران و همکاران، ۱۴۰۳، ۱۰۲)؛ بنابراین، مفهوم دولت الکترونیک تنها به معنای الکترونیکی شدن فرم‌ها نیست، بلکه به معنای بازتعریف رابطه میان حاکم و مرزوبند از طریق واسطه‌گری تکنولوژیک است.

این مفهوم را می‌توان در چهار بعد اصلی تحلیل کرد که هر کدام بار حقوقی خاص خود را دارند: اول- بعد زیرساختی و حقوقی: پایه و اساس دولت الکترونیک، وجود زیرساخت‌های قانونی برای اعتباربخشی به داده‌های الکترونیکی است. بدون وجود قوانینی که «امضای دیجیتال»، «سند الکترونیکی» و «تراکنش‌های الکترونیکی» را از نظر حقوقی معتبر و لازم‌الاجرا بدانند، دولت الکترونیک وجود خارجی نخواهد داشت؛ بنابراین، مفهوم دولت الکترونیک گره خورده با مفهوم «حاکمیت سایبری» و «امنیت اطلاعات» است. در این بعد، دولت الکترونیک به معنای ایجاد فضایی امن و قابل اعتماد برای تبادل اطلاعات میان دولت، شهروندان و بخش خصوصی است.

دوم- بعد خدماتی و تعاملی: در این بعد، دولت الکترونیک به معنای تغییر کانال‌های ارائه خدمات

3- ICT

4- Law through Code

از حضوری به غیرحضوری است. این تغییر، اگرچه از نظر اداری صرفاً یک تسهیل‌گری به نظر می‌رسد، اما از دیدگاه حقوقی، مفهوم «دسترسی به عدالت» و «حق دریافت خدمات عمومی» را بازتعریف می‌کند. وقتی خدمات از طریق سامانه‌های آنلاین ارائه می‌شود، موانع فیزیکی و جغرافیایی حذف می‌شوند، اما موانع جدیدی مانند «شکاف دیجیتال» و «سواد فناوری» ایجاد می‌گردند؛ بنابراین، مفهوم دولت الکترونیک در این جا با اصل «برابری در برابر قانون» و «عدم تبعیض» در تعامل است. دولت موظف است اطمینان حاصل کند که گذار به فضای دیجیتال، منجر به محرومیت گروه‌هایی از جامعه از حقوق شهروندی‌شان نشود.

سوم- بعد مشارکتی و دموکراتیک: دولت الکترونیک پیشرفته، تنها به ارائه خدمات محدود نمی‌شود، بلکه بستری برای مشارکت شهروندان در تصمیم‌گیری‌های کلان فراهم می‌کند. این بعد، مفهوم «شفافیت» و «پاسخگویی» را تقویت می‌کند. در این مدل، دولت الکترونیک به معنای باز بودن داده‌های^۵ دولتی برای نظارت عمومی است (Nakamura&Saito, 2025, 3). این شفافیت، ابزار قدرتمندی برای کنترل فساد اداری و افزایش اعتماد عمومی است. از منظر حقوقی، این بعد مستقیماً با «حق دسترسی به اطلاعات» و «حق نظارت مردم بر اداره کشور» پیوند می‌خورد.

چهارم- بعد حکمرانی و تصمیم‌گیری: عمیق‌ترین لایه مفهوم دولت الکترونیک، استفاده از کلان‌داده‌ها و هوش مصنوعی برای تصمیم‌گیری‌های استراتژیک است. در این مرحله، دولت الکترونیک به معنای «حکمرانی داده‌محور» است. تصمیمات سیاسی و اجرایی دیگر صرفاً بر اساس تجربه و شهود مدیران گرفته نمی‌شوند، بلکه بر اساس تحلیل‌های آماری و پیش‌بینی‌های الگوریتمی صورت می‌گیرند. این امر چالش‌های جدی حقوقی را در حوزه «مسئولیت تصمیم‌گیری» و «حق بر تفسیر انسانی» ایجاد می‌کند. وقتی یک الگوریتم تصمیمی می‌گیرد که به حقوق شهروندی لطمه می‌زند، چه کسی مسئول است؟ این پرسش، هسته اصلی بحث حقوقی در مفهوم مدرن دولت الکترونیک است.

به دیدگاه نگارنده، مفهوم دولت الکترونیک یک مفهوم ایستا نیست، بلکه یک فرایند پویا و چندلایه است که از سطح فنی آغاز شده و به لایه‌های عمیق حقوقی، اخلاقی و اجتماعی نفوذ می‌کند. درک صحیح این مفهوم، پیش‌نیاز ضروری برای تدوین قوانین کارآمد در حوزه مسئولیت مدنی و حقوق شهروندان در عصر دیجیتال است. بدون درک این ابعاد چندگانه، هرگونه تلاش برای تنظیم‌گری حقوقی در این حوزه، ناقص و ناکارآمد خواهد بود.

۳- تغییر ماهیت رابطه دولت و شهروند

گذار از دولت سنتی به دولت الکترونیک، تنها یک تغییر تکنولوژیک در کانال‌های ارتباطی نیست، بلکه دگرگونی بنیادین در ساختار قدرت و ماهیت رابطه حاکمیت با شهروندان است. در پارادایم کلاسیک، این رابطه بر پایه «سلسله‌مراتب اداری» و «تعامل چهره‌به‌چهره» استوار بود که در آن، مامورین دولتی به‌عنوان نمایندگان اراده حاکم، دارای اختیارات تفسیری و قضاوت انسانی بودند. این مدل، رابطه‌ای خطی، سلسله‌مراتبی و مبتنی بر سلب اعتماد اولیه از سوی شهروند نسبت به سیستم بود. اما با ظهور دولت الکترونیک، این رابطه به سمت «تعاملات غیرمتمرکز»، «خودکار» و «داده‌محور» تغییر جهت داده است.

در این پارادایم نوین، واسطه‌گری انسان‌ها در فرایندهای روتین اداری حذف یا به حداقل می‌رسد و جای خود را به «الگوریتم‌ها» و «سیستم‌های خودکار» می‌دهد. این امر منجر به پدیده‌ای به نام «دیجیتالی شدن حاکمیت» می‌شود که در آن، قوانین نه در ذهن مامور اجرا می‌شوند، بلکه در کدهای نرم‌افزاری تجسم می‌یابند. نتیجه این تحولات، تغییر ماهیت رابطه از «رابطه انسانی-حقوقی» به «رابطه سیستمی-فنی» است. شهروند دیگر با یک نهاد انتزاعی یا یک مامور خاص روبرو نیست، بلکه با یک سامانه الکترونیکی تعامل دارد که بر اساس منطق صفر و یک عمل می‌کند. این تغییر، مفهوم «تقصیر اداری» را تحت الشعاع قرار می‌دهد، زیرا خطا دیگر ناشی از بی‌احتیاطی یا سوءنیت یک فرد نیست،

بلکه محصول نقص در طراحی سیستم، باگ‌های نرم‌افزاری یا عدم تطابق داده‌هاست.

علاوه بر این، این تغییر ماهیت، تعادل قدرت را نیز دگرگون می‌سازد. در دولت سنتی، دولت به دلیل انحصار در اطلاعات و فرایندها، در موقعیت برتری قرار داشت. اما در دولت الکترونیک، با شفاف‌سازی فرایندها و دسترسی شهروندان به اطلاعات از طریق پورتال‌های خدماتی، این عدم تقارن اطلاعاتی کاهش می‌یابد. با این حال، چالش جدیدی به نام «عدم تقارن اطلاعاتی الگوریتمی» پدیدار می‌شود (Baguma&Lubega, 2013, 196). شهروندان از نحوه عملکرد، معیارهای تصمیم‌گیری و منطق پشت الگوریتم‌های دولتی بی‌خبرند؛ درحالی‌که دولت به داده‌های کامل و لحظه‌ای از رفتار شهروندان دسترسی دارد. این وضعیت، رابطه را از یک تعامل دوجانبه به یک نظارت یک‌سویه و کنترل‌گرانه تغییر می‌دهد.

به دیدگاه نگارنده، سرعت و مقیاس‌پذیری در این رابطه جدید، ماهیت «زمان» در حقوق اداری را تغییر داده است. در گذشته، فرایندهای اداری زمان‌بر و تدریجی بودند که فرصت تجدیدنظر و اعتراض را فراهم می‌کردند. اما در دولت الکترونیک، تصمیم‌گیری‌ها در کسری از ثانیه و به صورت خودکار انجام می‌شوند. این شتاب، فرصت‌های قانونی برای دفاع از حقوق را محدود کرده و شهروند را در موقعیتی آسیب‌پذیرتر قرار می‌دهد؛ بنابراین، رابطه دولت و شهروند در عصر دیجیتال، رابطه‌ای پیچیده است که در آن کارایی و سرعت، گاهی به قیمت کاهش تضمین‌های رویه‌ای و حقوقی تمام می‌شود. این دگرگونی، نیازمند بازتعریف مفاهیم کلاسیکی مانند «عدالت اداری»، «حق شنیده شدن» و «مسئولیت‌پذیری» در بستر فناوری است تا از تحمیل بار نامتوازن بر دوش شهروندان جلوگیری شود.

۴- چالش‌های حقوقی در بستر دولت الکترونیک

گذار از ساختارهای بوروکراتیک سنتی به اکوسیستم دیجیتال، اگرچه کارایی و شفافیت را افزایش

داده است، اما هم‌زمان خلأهای ساختاری و مبهمی را در نظام حقوقی پدید آورده است. ماهیت غیرملموس، سرعت بالای پردازش و ماهیت فرامرزی داده‌ها در فضای مجازی، قواعد کلاسیک حقوقی را با چالش‌های جدی مواجه ساخته‌اند.

در این بخش، به بررسی سه محور اصلی که ستون‌های حقوقی دولت الکترونیک را تهدید می‌کنند، پرداخته می‌شود: نخست، چالش‌های ناشی از اعتباربخشی به امضاءهای دیجیتال و اسناد الکترونیکی که پایه اعتبار حقوقی تعاملات هستند؛ دوم، تعارضات پیچیده میان بهره‌برداری از داده‌های کلان برای ارائه خدمات و لزوم حفظ حریم خصوصی و امنیت اطلاعات شهروندان؛ سوم، ابهامات حاکم بر حاکمیت قانون در فضای سایبر، از جمله مسائل مربوط به صلاحیت قضایی، اعمال قوانین ملی در بستر غیرمتمرکز و چالش‌های اثبات ادله در دادگاه‌ها. این سه چالش، نه تنها زیربنای اعتماد عمومی را سست می‌کنند، بلکه نیازمند بازنگری بنیادین در فقه و حقوق مثبت کشور هستند.

۴-۱- چالش اعتبار و امضای دیجیتال

امضاء دیجیتال، به‌عنوان معادل حقوقی امضاء خطی در فضای مجازی، سنگ بنای اعتباربخشی به اسناد و تراکنش‌های الکترونیکی در بستر دولت الکترونیک است. با این حال، تبدیل یک مفهوم فنی به یک ابزار حقوقی معتبر، با چالش‌های عمیق و چندلایه‌ای روبرو است که فراتر از مسائل فنی رمزنگاری، ابعاد حقوقی و اثباتی پیچیده‌ای را دربرمی‌گیرد. مسئله اصلی در این جا، «تطابق معیارهای فنی با استانداردهای اثبات در دادگاه‌های حقوقی» است.

در نظام‌های حقوقی کلاسیک، اعتبار سند منوط به احراز هویت امضاءکننده و اثبات اصالت امضاء از طریق کارشناسی خط و امضاء است. اما در امضای دیجیتال، این اصالت توسط الگوریتم‌های ریاضی و گواهی‌های دیجیتال صادر شده توسط مراجع تأییدیه^۷ تضمین می‌شوند. چالش نخست، «اعتبار حقوقی گواهی‌های دیجیتال» است. آیا گواهی صادر شده توسط یک مرجع خصوصی یا

نیمه دولتی، همان وزن حقوقی گواهی‌های رسمی دولتی را دارد؟ در بسیاری از موارد، عدم شفافیت در فرایند صدور و تمدید گواهی‌ها و همچنین عدم هماهنگی بین‌المللی در استانداردهای تأییدیه، منجر به ایجاد ابهام در اعتبار اسناد تولید شده می‌شود. اگر یک مرجع تأییدیه دچار نقص امنیتی شود یا به صورت نادرست گواهی صادر کند، مسئولیت جبران خسارت ناشی از اسناد باطل‌الامضاء با چه کسی است؟ این خلأ مسئولیت‌پذیری، ریسک حقوقی را برای شهروندان و دولت افزایش می‌دهد.

چالش دوم، مربوط به «یکپارچگی داده‌ها»^۸ است. امضاء دیجیتال تضمین می‌کند که سند پس از امضاء دستکاری نشده است، اما تضمینی برای اصالت محتوای سند در لحظه تولید ارائه نمی‌دهد. در دولت الکترونیک، داده‌ها اغلب به صورت خودکار و بدون دخالت مستقیم انسان تولید می‌شوند (Apriyanto & Sara, 2024, 13). در چنین شرایطی، اثبات این که داده‌ها دقیقاً بازتاب‌دهنده واقعیت خارجی هستند، دشوار می‌شود. برای مثال، اگر یک سامانه مالیاتی به دلیل باگ نرم‌افزاری، درآمدی را کمتر از واقعیت ثبت کند و امضاء دیجیتال روی آن سند زده شود، اعتبار حقوقی این سند در برابر ادعای مالیات‌دهنده چگونه خواهد بود؟ آیا امضاء دیجیتال می‌تواند جایگزین کامل برای «قوه قضاییه» در کشف حقیقت شود؟ پاسخ منفی است، زیرا فناوری نمی‌تواند جایگزین قضاوت انسانی در تفسیر نیت و قصد طرفین قرارداد یا عمل اداری شود.

چالش سوم، «مدیریت کلیدهای خصوصی» و مسئولیت ناشی از سوءاستفاده از آن‌ها است. در امضاء خطی، امضاء فیزیکی و منحصر به فرد است و تقلید از آن دشوار. اما در امضاء دیجیتال، کلید خصوصی که مبنای امضاء است، ممکن است به دلیل ضعف امنیتی، بدافزارها یا خطای انسانی در اختیار اشخاص ثالث قرار گیرد. در این حالت، آیا عملیات انجام شده با کلید سرقت شده، به نام دارنده کلید محسوب می‌شود؟ نظام حقوقی فعلی در بسیاری از کشورها، اصل «مسئولیت دارنده کلید» را پذیرفته است (Pedrosa et al., 2021, 4)، مگر این که خلاف آن ثابت شود. این اصل، بار

اثبات را بر دوش شهروندان سنگین کرده و در صورت عدم توانایی در اثبات سرقت کلید، شهروند مسئول تمام تعهدات ناشی از امضاء دیجیتال خواهد بود. این رویکرد، با اصل «تقصیر» در حقوق مدنی در تعارض است و نیازمند بازنگری در قوانین مسئولیت مدنی است.

به دیدگاه نگارنده، قوانین موجود اغلب بر جنبه‌های فنی تمرکز دارند و از تعاریف دقیق حقوقی مانند «قصد ایجاد تعهد» یا «آگاهی از محتوای سند» در بستر دیجیتال غافل اند؛ بنابراین، برای رفع این چالش‌ها، نیازمند تدوین قوانینی هستیم که نه تنها اعتبار فنی امضاء دیجیتال را بپذیرند، بلکه مکانیسم‌های شفاف برای حل اختلافات ناشی از خطاهای سیستمی، سرقت هویت دیجیتال و تفسیر اسناد الکترونیکی را نیز پیش‌بینی کنند. بدون این اقدامات، امضاء دیجیتال تنها یک ابزار فنی با ثبات حقوقی ضعیف باقی خواهد ماند و اعتماد عمومی به دولت الکترونیک را خدشه‌دار خواهد کرد.

۴-۲- حریم خصوصی و حفاظت از داده‌ها

در بستر دولت الکترونیک، داده‌ها نه تنها به عنوان بایگانی‌های غیرفعال، بلکه به عنوان دارایی‌های استراتژیک و سوخت محرک الگوریتم‌های تصمیم‌گیری هوشمند تلقی می‌شوند. این تحول پارادایمی، چالش‌های بنیادینی را در حوزه «حریم خصوصی» و «حفاظت از داده‌ها» پدید آورده است. مسئله اصلی، گذار از مفهوم سنتی «حق بر تنهایی» به مفهوم مدرن «حق بر کنترل بر داده‌های شخصی» است که در تقابل مستقیم با نیاز دولت به «شفافیت» و «بهینه‌سازی خدمات» قرار می‌گیرد.

یکی از چالش‌های محوری، پدیده «تجمع داده‌ها» و «استنتاج اطلاعاتی» است. در دولت‌های سنتی، اطلاعات شهروندان در دپارتمان‌های ایزوله نگهداری می‌شدند. اما در دولت الکترونیک، یکپارچه‌سازی پایگاه‌های داده امکان ایجاد پروفایل‌های جامع از رفتار، ترجیحات و موقعیت اجتماعی افراد را فراهم می‌کند. این تجمع، اگرچه کارایی خدمات را افزایش می‌دهد، اما ریسک «بازشناسایی مجدد» داده‌های ناشناس‌سازی شده را به شدت افزایش می‌دهد. پژوهش‌های اخیر نشان می‌دهد که با ترکیب چندین مجموعه داده عمومی و نیمه‌عمومی، هویت افراد حتی در صورت حذف نام و نام

خانوادگی قابل احراز است (تقوی فرد و همکاران، ۱۳۹۵، ۱۰۴). این امر، مکانیسم‌های سنتی ناشناس‌سازی را ناکارآمد ساخته و نیازمند گذار به استانداردهای سخت‌گیرانه‌تر مانند «حریم خصوصی تفاضلی»^۹ و «محاسبات چندجانبه امن»^{۱۰} است (Li, 2018, 3).

چالش دیگر، عدم تعادل قدرت میان «کنترل‌کننده داده»^{۱۱} و «ذینفع داده»^{۱۲} است. در ساختارهای غیرمتمرکز و مبتنی بر بلاک‌چین یا ابررایانش، شفافیت فنی لزوماً به معنای شفافیت حقوقی نیست. شهروندان اغلب از چگونگی پردازش، ذخیره‌سازی و اشتراک‌گذاری داده‌های خود بی‌خبرند. این «ناهمگونی اطلاعاتی»^{۱۳} منجر به نقض اصل «رضایت آگاهانه»^{۱۴} می‌شود. در بسیاری از سامانه‌های دولتی، رضایت کاربران به‌صورت ضمنی و از طریق کلیک بر روی دکمه‌های طولانی و پیچیده اخذ می‌شود که فاقد ماهیت حقوقی معتبر است (Tampubolon et al., 2021, 4957)؛ بنابراین، نیازمند چهارچوب‌های حقوقی جدیدی هستیم که «شفافیت الگوریتمی» را الزامی کند و به شهروندان حق «فراموش شدن» و «قابلیت حمل داده» را بدهد.

علاوه بر این، چالش «حفاظت در برابر نظارت توده‌ای»^{۱۵} و «استفاده‌های ثانویه»^{۱۶} داده‌ها مطرح است (Savage, 2018, 1763). داده‌های جمع‌آوری شده برای ارائه خدمات خاص^{۱۷}، ممکن است بدون مجوز قضایی یا قانونی صریح، برای اهداف نظارتی، بازاریابی یا تحلیل‌های اجتماعی مورد استفاده قرار گیرند. این پدیده که در ادبیات حقوقی به آن «تغییر ماهیت داده»^{۱۸} گفته می‌شود

9- Differential Privacy

10- Secure Multi-Party Computation

۱۱- دولت

۱۲- شهروند

13- Information Asymmetry

14- Informed Consent

15- Mass Surveillance

16- Secondary Use

۱۷- مانند بیمه یا مالیات

18- Function Creep

(Luksch, 2012, 142)، حریم خصوصی را به صورت سیستماتیک نقض می‌کند. منابع به روز حقوقی تأکید دارند که هرگونه پردازش داده باید منطبق با اصل «تناسب» و «ضرورت» باشد و محدود به اهداف مشخص، صریح و مشروع گردد.

به دیدگاه نگارنده، چالش «امنیت سایبری» و «مسئولیت نشت داده»^{۱۹} نیز حائز اهمیت است. با تمرکز داده‌ها در مراکز داده دولتی، این مراکز به اهداف جذابی برای حملات سایبری تبدیل می‌شوند. شکست در پیاده‌سازی استانداردهای امنیتی مانند رمزنگاری سرتاسری^{۲۰} و مدیریت هویت دسترسی محور^{۲۱}، منجر به خسارات جبران‌ناپذیر به حریم خصوصی شهروندان می‌شود؛ بنابراین، حفاظت از داده‌ها در دولت الکترونیک، تنها یک مسئله فنی نیست، بلکه یک الزام حقوقی و اخلاقی است که نیازمند تدوین قوانین جامع حفاظت از داده‌های شخصی^{۲۲} با بومی‌سازی متناسب با نظام حقوقی داخلی است. بدون این چهارچوب، اعتماد عمومی که پایه مشروعیت دولت الکترونیک است، به شدت مخدوش خواهد شد.

۳-۴- حاکمیت قانون در فضای مجازی

حاکمیت قانون در بستر دولت الکترونیک، با بن‌بست‌های عمیق ژئوپلیتیک و حقوقی روبرو است که ریشه در ماهیت غیرمتمرکز، بی‌مرز و سیال فضای سایبر دارد. نظام‌های حقوقی ملی که بر پایه اصل «حاکمیت سرزمینی» و جغرافیای فیزیکی استوارند، در مواجهه با اکوسیستم دیجیتال که مرزهای جغرافیایی را نادیده می‌گیرد، دچار نوعی «ناکارآمدی صلاحیت» شده‌اند. این چالش، سه محور اصلی را در بر می‌گیرد: ابهام در «صلاحیت قضایی»، تعارض در «اعمال قانون» و دشواری در «اجرای احکام». نخستین چالش، مسئله «تعیین صلاحیت قضایی» است. در حقوق بین‌الملل خصوصی و داخلی،

19- Data Breach Liability

20- End-to-End Encryption

21- Access-centric identity management

22- GDPR

معیارهای سنتی برای تعیین دادگاه صالح، معمولاً محل اقامت خواننده، محل وقوع عمل مجرمانه یا محل نتیجه جرم است. اما در فضای مجازی، این معیارها به دلیل ماهیت توزیع شده داده‌ها و سرورها، مبهم و چندپهلوی می‌شوند. یک تراکنش الکترونیکی ممکن است از سروری در کشور الف، توسط کاربری در کشور ب و با واسطه‌گری یک پلتفرم در کشور ج انجام شود. در چنین شرایطی، کدام نظام حقوقی صلاحیت رسیدگی دارد؟ رویکردهای فعلی حقوقی، نظیر «اصل تأثیر قابل پیش‌بینی»^{۲۳} یا «نظریه هدف‌گذاری»^{۲۴}، اگرچه تلاش می‌کنند معیارهای جدیدی ارائه دهند (Bagshaw, 2024, 151)، اما همچنان در تفسیرهای قضایی با ابهامات جدی روبرو هستند. این ابهام، منجر به «شکار دادگاه‌ها» می‌شود، یعنی طرفین دعوا به دنبال دادگاهی می‌روند که قوانین یا رویه‌های قضایی آن به نفع آن‌ها است، نه لزوماً دادگاهی که بیشترین ارتباط منطقی با موضوع دعوا دارد.

چالش دوم، «تعارض قوانین» در اعمال مقررات ملی در فضای فرامرزی است. هر کشور قوانین خاص خود را در حوزه‌های حریم خصوصی، مالکیت فکری، جرائم سایبری و نظارت محتوا دارد. وقتی داده‌ها به صورت آنی و بدون مرز جابجا می‌شوند، اعمال هم‌زمان قوانین متضاد کشورهای مختلف، منجر به «بار تعارضات حقوقی» برای شهروندان و شرکت‌ها می‌شود. برای مثال، قوانین «حق فراموش شدن» در اتحادیه اروپا^{۲۵} با قوانین آزادی بیان یا الزامات حفظ داده در سایر کشورها در تعارض است (لطیف زاده و همکاران، ۱۴۰۱، ۳۳۲). این تعارض، نه تنها اجرای قانون را مختل می‌کند، بلکه منجر به ایجاد «جزایر حقوقی» می‌شود که در آن‌ها شرکت‌های فناوری مجبور به تبعیت از سخت‌گیرانه‌ترین قوانین^{۲۶} می‌شوند تا از جریمه‌های سنگین در امان بمانند. این پدیده، نوعی «جهانی شدن غیررسمی قوانین» را پدید آورده که

23- Foreseeability Test

24- Targeting Theory

۲۵- مقررات عمومی حمایت از داده‌ها

۲۶- معمولاً قوانین اروپایی

مشروعیت دموکراتیک قوانین ملی را زیر سؤال می‌برد، زیرا قوانینی که توسط پارلمان‌های ملی تصویب نشده‌اند، عملاً بر فضای دیجیتال حاکم می‌شوند.

چالش سوم، «اجرای احکام» در فضای مجازی است. حتی اگر صلاحیت قضایی و قانون حاکم مشخص شود، اجرای حکم دادگاه در برابر اشخاص یا نهادهای مستقر در حوزه قضایی دیگر، با موانع دیپلماتیک و فنی روبرو است. مکانیسم‌های سنتی کمک‌های قضایی متقابل^{۲۷} که فرایندی کند و بوروکراتیک دارند (Boutros, 2019, 557)، با سرعت بالای تحولات دیجیتال سازگار نیستند. علاوه بر این، ماهیت غیرمتمرکز فناوری‌هایی مانند بلاک‌چین و رمزارزها، امکان ردیابی و توقیف دارایی‌ها را برای مراجع قضایی ملی دشوار می‌سازد. این شکاف میان «قدرت نظارتی دولت‌ها» و «قابلیت فرار دیجیتال»^{۲۸}، حاکمیت قانون را تضعیف کرده و احساس بی‌عدالتی و فرار از قانون را تقویت می‌کند.

به دیدگاه نگارنده، چالش «حاکمیت داده‌ها» به‌عنوان بازتابی از حاکمیت ملی در فضای سایبر مطرح است. دولت‌ها تلاش می‌کنند با الزام به ذخیره‌سازی داده‌ها در داخل مرزهای جغرافیایی، کنترل خود را بر جریان اطلاعات بازپس بگیرند. اگرچه این اقدام می‌تواند به امنیت ملی و حفظ حریم خصوصی کمک کند، اما ازسوی دیگر، منجر به «بالکانیزاسیون»^{۲۹} اینترنت^{۳۰} می‌شود که با اصل جهانی بودن فضای مجازی در تضاد است و هزینه‌های اقتصادی و فناوری را افزایش می‌دهد؛ بنابراین،

27- Mutual Legal Assistance Treaties-MLATs

28- Digital Evasion

۲۹- بالکانیزاسیون (Balkanization): اصطلاحی سیاسی-جغرافیایی که به فرایند تکه‌تکه شدن یک منطقه یا ساختار بزرگ به واحدهای کوچک‌تر، ناسازگار و اغلب خصمانه اشاره دارد. این واژه از شبه‌جزیره بالکان در اروپا گرفته شده که پس از فروپاشی امپراتوری‌های متعدد، به کشورها و گروه‌های قومی کوچک و متخاصمی تقسیم شد. در بستر اینترنت و فضای سایبر، «بالکانیزاسیون اینترنت» به معنای شکسته شدن شبکه جهانی اطلاعات به شبکه‌های ملی یا منطقه‌ای مجزا و غیرمتصل است که هر کدام قوانین، استانداردها و دسترسی‌های متفاوتی دارند. این پدیده که تحت تأثیر سیاست‌های «حاکمیت داده» و فیلترینگ‌های ملی رخ می‌دهد، با اصل جهانی و یکپارچه بودن اینترنت در تضاد است و منجر به ایجاد «اینترنت‌های ملی» می‌شود که تبادل آزاد اطلاعات را محدود کرده و هزینه‌های اقتصادی و فناوری را افزایش می‌دهد (Ashiku, 2024, 56).

۳۰- تکه‌تکه شدن اینترنت

بازتعریف حاکمیت قانون در فضای مجازی، نیازمند گذار از رویکردهای ارضی صرف به سمت همکاری‌های بین‌المللی، استانداردسازی فرامرزی و ایجاد مکانیسم‌های حل اختلاف دیجیتال کارآمد است. بدون این تحول، حاکمیت قانون در دولت الکترونیک، صرفاً یک ایده‌آل نظری باقی خواهد ماند و در عمل، خلأهای قانونی گسترده‌ای ایجاد می‌کند که سوءاستفاده‌گران از آن بهره‌برداری خواهند کرد.

۵- مسئولیت مدنی دولت در قبال خطاهای سیستمی

در بستر دولت الکترونیک، خطاهای سیستمی دیگر صرفاً مشکلات فنی محسوب نمی‌شوند، بلکه می‌توانند منجر به خسارات مالی، نقض حقوق شهروندی و بی‌اعتمادی عمومی گردند؛ بنابراین، تبیین چهارچوب‌های نظری مسئولیت مدنی، تحلیل دقیق ماهیت خطاهای فنی^{۳۱} و شفاف‌سازی مرزهای مسئولیت میان دولت و پیمانکاران خصوصی، از ارکان اساسی برای ایجاد تعادل میان نوآوری دیجیتال و حمایت از حقوق افراد است. این مبحث به بررسی چگونگی اعمال مسئولیت در شرایطی می‌پردازد که تصمیم‌گیری‌های انسانی با الگوریتم‌های خودکار و زیرساخت‌های پیچیده در هم می‌آمیزند.

۵-۱- نظریه‌های مسئولیت مدنی در بستر دولت الکترونیک

در نظام‌های حقوقی معاصر، مسئولیت مدنی دولت در قبال خسارات ناشی از خطاهای سیستمی، تحت تأثیر تحولات فناوری و تغییر ماهیت خدمات عمومی، دستخوش دگردیسی‌های بنیادینی شده است. رویکردهای سنتی مبتنی بر «نظریه تقصیر» که نیازمند اثبات قصور یا غفلت کارمند دولت یا نقص در نظارت اداری بود، در مواجهه با پیچیدگی‌های فنی و خودکارسازی فرایندها، کارایی خود را از دست داده‌اند. در این راستا، نظریه‌های نوین مسئولیت، به ویژه «نظریه خطر» و «نظریه ضمانت»^{۳۲}، جایگاه ویژه‌ای یافته‌اند.

۳۱- نرم‌افزاری و سخت‌افزاری

نظریه خطر، بر این اصل استوار است که هرگاه دولت از فناوری‌های پیشرفته برای ارائه خدمات عمومی استفاده می‌کند، خود را در معرض «ریسک‌های فنی» قرار داده است. از آن جا که دولت از این فناوری‌ها منافع کارایی و سرعت می‌برد، باید عوارض و خطرات بالقوه آن را نیز بپذیرد. در این چهارچوب، اثبات تقصیر دولت الزامی نیست؛ بلکه کافی است رابطه سببی میان عملکرد سیستم و خسارت وارده اثبات شود (امیری و دشتی، ۱۴۰۳، ۳۵۷). این رویکرد، بار اثبات را از دوش شهروندان^{۳۳} برداشته و بر دوش دولت^{۳۴} قرار می‌دهد. منابع حقوقی جدید تأکید دارند که در جایی که الگوریتم‌های هوش مصنوعی یا سامانه‌های خودکار در تصمیم‌گیری‌های اداری نقش ایفاء می‌کنند، دولت به عنوان «تضمین‌کننده امنیت عمومی»، مسئول جبران خسارات ناشی از نقص‌های ذاتی این سیستم‌ها است، حتی اگر نقص ناشی از باگ‌های غیرقابل پیش‌بینی باشد.

همچنین، «نظریه برابری در برابر بار عمومی»^{۳۵} نیز حائز اهمیت است. این نظریه استدلال می‌کند که اگر خطای سیستمی منجر به خسارتی برای یک یا چند شهروند خاص شود، این خسارت نباید تنها توسط آن افراد تحمل گردد، بلکه باید به عنوان یک «بار عمومی» در نظر گرفته شده و از طریق بودجه عمومی جبران شود (Konarski, 2021, 92). این رویکرد، از منظر عدالت توزیعی، توجیه‌پذیر است، زیرا هزینه‌های ناشی از ناکارآمدی یا خطای سیستم‌های دولتی، در واقع هزینه‌ای است که جامعه برای دسترسی به خدمات مدرن پرداخت می‌کند؛ بنابراین، دولت موظف است با ایجاد صندوق‌های جبران خسارت یا بیمه‌های مسئولیت حرفه‌ای، این ریسک را مدیریت کند.

علاوه بر این، چالش «مسئولیت ناشی از تصمیم‌گیری الگوریتمی» مطرح است. در سیستم‌های هوشمند، ممکن است خطا ناشی از نقص در کدنویسی نباشد، بلکه ناشی از «سوءگیری‌های داده‌ای»

۳۳- که دسترسی به دانش فنی و شفافیت الگوریتمی ندارند

۳۴- به عنوان بهره‌بردار سیستم

یا «عدم شفافیت الگوریتم» باشد. در چنین مواردی، اعمال نظریه تقصیر دشوار است، زیرا مشخص نیست چه کسی^{۳۶} مقصر است. در این شرایط، نظریه «مسئولیت مطلق»^{۳۷} یا «مسئولیت بدون تقصیر»^{۳۸} به عنوان راهکاری برای حمایت از حقوق شهروندان پیشنهاد می‌شود. طبق این نظریه، دولت صرفاً به دلیل ارائه‌دهنده خدمات با ریسک بالا^{۳۹} مسئول جبران خسارت است، صرف‌نظر از این که آیا تقصیری مرتکب شده است یا خیر؟

به دیدگاه نگارنده، تلفیق این نظریه‌ها نیازمند تدوین چهارچوب‌های حقوقی مشخص است که مرزهای مسئولیت دولت را در قبال خطاهای فنی شفاف‌سازی کنند. این چهارچوب‌ها باید شامل الزام به «شفافیت الگوریتمی»، «ممیزی دوره‌ای سیستم‌ها» و «ایجاد مکانیسم‌های سریع جبران خسارت» باشند. بدون این چهارچوب‌ها، نظریه‌های مسئولیت مدنی، صرفاً مفاهیم انتزاعی باقی می‌مانند و در عمل، شهروندان آسیب‌دیده از دسترسی به عدالت محروم خواهند شد؛ بنابراین، تحول در نظریه‌های مسئولیت مدنی، نه تنها یک نیاز حقوقی، بلکه یک ضرورت اخلاقی و اجتماعی در عصر دولت دیجیتال است.

۵-۲- خطاهای نرم‌افزاری و سخت‌افزاری

در اکوسیستم پیچیده دولت الکترونیک، خطاهای سیستمی به عنوان عامل اصلی نقض حقوق شهروندی و ایجاد خسارات مالی و معنوی، از اهمیت راهبردی برخوردارند. تفکیک دقیق میان «خطاهای نرم‌افزاری» و «خطاهای سخت‌افزاری» برای تعیین دقیق مسئولیت مدنی و اعمال نظریه‌های حقوقی مرتبط، ضرورتی انکارناپذیر است. هریک از این دسته‌ها، ماهیت، علل پیدایش و الگوی جبران خسارت خاص خود را دارند که نیازمند واکاوی فنی-حقوقی است.

۳۶- برنامه‌نویس، مدیر سیستم یا دولت

37- Strict Liability

38- No-Fault Liability

۳۹- سیستم‌های پیچیده و خودکار

الف - خطاهای نرم‌افزاری: پیچیدگی الگوریتمی و نقص در طراحی: خطاهای نرم‌افزاری، ناشی از نقص در کدنویسی، طراحی الگوریتم، مدیریت پایگاه داده یا تعامل نادرست ماژول‌های مختلف سیستم هستند. این خطاها به دلیل ماهیت انتزاعی و پیچیدگی لایه‌های نرم‌افزاری، شناسایی و ردیابی آن‌ها دشوارتر از خطاهای سخت‌افزاری است. منابع فنی و حقوقی جدید، خطاهای نرم‌افزاری را به سه دسته اصلی تقسیم می‌کنند:

اول - نقص در طراحی و منطق کسب‌وکار: این خطاها زمانی رخ می‌دهند که الگوریتم‌ها بر اساس نیازمندی‌های نادرست یا ناقص طراحی شده‌اند. برای مثال، اگر سامانه‌ای برای محاسبه یارانه بر اساس داده‌های ورودی نادرست، مبلغی کمتر از حق شهروند پرداخت کند، این یک نقص در منطق کسب‌وکار است. در حقوق، این مورد معمولاً تحت عنوان «تقصیر در نظارت بر طراحی» یا «نقص در ایمنی محصول» بررسی می‌شود. چالش اصلی در این جا، اثبات رابطه سببی میان «نقص طراحی» و «خسارت» است، زیرا پیچیدگی کدها^{۴۰} و عدم شفافیت الگوریتم‌های هوش مصنوعی، اثبات این رابطه را برای کارشناسان غیرمتخصص و حتی قضات دشوار می‌سازد.

دوم - باگ‌های اجرایی و مدیریت خطا: این خطاها در حین اجرای برنامه و تحت شرایط خاص^{۴۱} ظاهر می‌شوند. عدم مدیریت صحیح خطاها می‌تواند منجر به از دست رفتن داده‌ها، نشت اطلاعات یا توقف خدمات شود (Neville-Neil, 2017, 31). از منظر مسئولیت مدنی، دولت موظف است سیستم‌هایی با «تاب‌آوری بالا» و «مدیریت خطای ایمن» پیاده‌سازی کند. شکست در این امر، نشانه‌ای از قصور در نگهداری و به‌روزرسانی سیستم است.

سوم - سوءگیری‌های الگوریتمی و نقص در داده‌ها: در سیستم‌های مبتنی بر هوش مصنوعی، خطا می‌تواند ناشی از داده‌های آموزشی نادرست یا سوءگیری‌های پنهان در مدل‌های یادگیری ماشین

40- Code Complexity

۴۱ - مانند ترافیک بالای شبکه یا ورود داده‌های غیرمجاز

باشد. این نوع خطا، اگرچه لزوماً یک «باگ» فنی نیست، اما منجر به تصمیمات ناعادلانه و تبعیض آمیز می شود (Martin, 2021, 72). منابع حقوقی جدید تأکید دارند که دولت در قبال «عدالت الگوریتمی» مسئول است و باید مکانیسم های ممیزی و نظارتی برای کشف و اصلاح این سوء گیری ها داشته باشد. عدم انجام این امر، می تواند مبنای مسئولیت مدنی ناشی از «نقض حقوق برابر» باشد.

ب- خطاهای سخت افزاری: نوسانات فیزیکی و شکست زیرساخت: خطاهای سخت افزاری، ناشی از نقص در قطعات فیزیکی سرورها، تجهیزات شبکه، دی اس پی ها^{۴۲} یا زیرساخت های فیزیکی دیتاسترها هستند. این خطاها معمولاً قابل پیش بینی تر از خطاهای نرم افزاری هستند و ریشه در فرسودگی تجهیزات، نوسانات برق، خطاهای انسانی در نصب یا نگهداری، یا حملات سایبری فیزیکی دارند.

اول- شکست قطعات و فرسودگی: قطعات سخت افزاری عمر مفید محدودی دارند. عدم جایگزینی به موقع قطعات فرسوده^{۴۳} می تواند منجر به از دست رفتن داده های حیاتی یا توقف خدمات شود. در حقوق، این مورد تحت عنوان «تقصیر در نگهداری و تعمیرات» بررسی می شود. دولت موظف است برنامه های نگهداری پیشگیرانه را اجرا کند.

دوم- نوسانات انرژی و محیطی: نوسانات برق، دمای نامناسب یا رطوبت در دیتاسترها می تواند منجر به خاموشی ناگهانی یا آسیب فیزیکی به سرورها شود. اگرچه این عوامل ممکن است «قوه قهریه» تلقی شوند، اما اگر دولت از سیستم های پشتیبان^{۴۴} و سیستم های سرمایه گذاری مناسب استفاده نکرده باشد، مسئولیت جبران خسارت بر عهده اوست. منابع فنی تأکید دارند که استانداردهای بین المللی^{۴۵}، الزامات سخت گیرانه ای برای پایداری محیطی دیتاسترها تعیین می کنند که رعایت آنها

42- DSPs

۴۳- مانند هاردهای سخت یا ماژول های حافظه

44- UPS

۴۵- مانند ISO 27001

برای سلب مسئولیت ضروری است.

سوم- حملات سایبری فیزیکی و خرابی عمدی: در مواردی، خطای سخت‌افزاری می‌تواند ناشی از خرابی عمدی یا حملات فیزیکی به زیرساخت‌ها باشد. در این شرایط، مسئولیت دولت ممکن است مشروط به اثبات «تقصیر در امنیت فیزیکی» باشد. اگر دولت از تدابیر امنیتی لازم^{۴۶} استفاده نکرده باشد، مسئول جبران خسارات ناشی از این حملات خواهد بود (ضیایی و خلیل زاده، ۱۳۹۲، ۱۰۱).

به دیدگاه نگارنده، تفاوت بنیادین میان این دو نوع خطا، در «قابلیت پیش‌بینی» و «ماهیت رفع نقص» است. خطاهای سخت‌افزاری معمولاً با تعویض قطعه قابل رفع هستند، درحالی‌که خطاهای نرم‌افزاری نیازمند بازنگری در کد، الگوریتم یا داده‌ها هستند. از منظر حقوقی، خطاهای نرم‌افزاری به دلیل پیچیدگی و پنهان‌کاری ذاتی، بار اثبات سنگین‌تری بر دوش دولت می‌گذارند؛ بنابراین، در صورت بروز خسارت، فرض بر این است که دولت در انتخاب، طراحی یا نگهداری سیستم نرم‌افزاری قصور ورزیده است، مگر این که خلاف آن ثابت شود. این رویکرد، با هدف حمایت از شهروندان آسیب‌دیده و تشویق دولت به سرمایه‌گذاری در کیفیت و امنیت سیستم‌های دیجیتال، توجیه‌پذیر است.

۵-۳- نقش پیمانکاران خصوصی

با گسترش پدیده «برون‌سپاری فناوری اطلاعات»^{۴۷} و مشارکت بخش خصوصی در توسعه و نگهداری زیرساخت‌های دولت الکترونیک، مرزهای سنتی مسئولیت مدنی دولت کمرنگ شده است. امروزه، دولت‌ها نه تنها به عنوان «کارفرما»، بلکه به عنوان «ناظر بر خدمات عمومی» عمل می‌کنند. این دوگانگی نقش، منجر به ایجاد یک «خلأ مسئولیت» می‌شود که در آن، شهروندان آسیب‌دیده از خطاهای سیستمی، با موانع حقوقی جدی در مسیر جبران خسارت روبرو هستند. تحلیل دقیق نقش پیمانکاران خصوصی نیازمند واکاوی سه محور اصلی است: ماهیت قراردادهای پیمانکاری، اصل «تفکیک

۴۶- مانند کنترل دسترسی فیزیکی، دوربین‌های مداربسته و سیستم‌های اطفاء حریق

وظایف» و مسئولیت تضامنی یا تقسیمی.

اول- ماهیت قراردادهای پیمانکاری و محدودیت‌های حقوقی: در اکثر پروژه‌های دولت الکترونیک، پیمانکاران خصوصی تحت قراردادهای پیچیده‌ای با دولت فعالیت می‌کنند که معمولاً شامل بندهای «سلب مسئولیت» و «معافیت از خسارت» است (سلامی‌نژاد، ۱۴۰۳، ۵۱۹). این بندها، پیمانکاران را از مسئولیت در قبال خطاهای غیرعمدی یا باگ‌های نرم‌افزاری معاف می‌کنند، مگر در مواردی که «تقصیر سنگین» یا «خیانت در امانت» اثبات شود. از منظر حقوقی، این رویکرد اگرچه برای جذب سرمایه بخش خصوصی ضروری است، اما منجر به عدم تعادل در توزیع ریسک می‌شود. منابع جدید حقوقی تأکید دارند که وقتی پیمانکاران به «انحصارگرهای فناوری» تبدیل می‌شوند، نمی‌توانند از مزیت اطلاعاتی خود برای فرار از مسئولیت مدنی استفاده کنند؛ بنابراین، قراردادهای دولتی باید شامل الزامات سخت‌گیرانه‌تری برای «ضمانت کیفیت» و «پشتیبانی پس از اجرا» باشند تا از سوءاستفاده پیمانکاران از بندهای سلب مسئولیت جلوگیری شود.

دوم- اصل تفکیک وظایف و مسئولیت نظارتی دولت: یکی از چالش‌های اصلی، تعیین مرز میان «مسئولیت اجرایی پیمانکار» و «مسئولیت نظارتی دولت» است. بر اساس اصول حکمرانی داده، دولت موظف است بر عملکرد پیمانکار نظارت کند و اطمینان حاصل نماید که سیستم‌های پیاده‌سازی شده، منطبق با استانداردهای امنیتی و حقوقی هستند (کریمی تازه کند و همکاران، ۱۳۹۶، ۶۴). اگر خطای سیستمی ناشی از «نقص در کدنویسی» یا «باگ نرم‌افزاری» باشد، مسئولیت اولیه بر عهده پیمانکار است. اما اگر خطا ناشی از «عدم نظارت کافی دولت»، «تصویب نیازمندی‌های نادرست» یا «عدم به‌روزرسانی سیستم‌های امنیتی» باشد، دولت مسئول است. منابع فنی-حقوقی جدید، مفهوم «مسئولیت مشترک» را مطرح می‌کنند. در این مدل، پیمانکار مسئول «ایمنی محصول» و دولت مسئول «ایمنی محیط اجرا» و «نظارت بر انطباق» است. شکست در هریک از این وظایف، منجر به مسئولیت مدنی طرف متخلف می‌شود.

سوم- مسئولیت تضامنی در برابر تقسیم مسئولیت: در صورت بروز خسارت جدی ناشی از خطای سیستمی، پرسش اصلی این است که آیا دولت و پیمانکار «مسئولیت تضامنی» دارند یا «تقسیم مسئولیت»؟ رویکرد سنتی حقوقی، مسئولیت تضامنی را ترجیح می‌دهد، زیرا به شهروندان آسیب‌دیده اجازه می‌دهد خسارت خود را از هریک از طرفین مطالبه کنند. این رویکرد، از منظر حمایت از حقوق مصرف‌کننده^{۴۸}، توجیه‌پذیر است. با این حال، پیمانکاران خصوصی معمولاً بر مسئولیت تقسیمی اصرار ورزیده و مدعی می‌شوند که تنها به اندازه سهم تقصیر خود مسئول هستند (صفایی و همکاران، ۱۳۹۷، ۱۵۹). در پروژه‌های حیاتی دولتی، باید «بیمه مسئولیت حرفه‌ای اجباری» برای پیمانکاران الزامی شود تا در صورت بروز خطا، خسارت شهروندان از طریق صندوق بیمه جبران گردد، بدون این که نیاز به درگیری‌های طولانی حقوقی بین دولت و پیمانکار باشد. این مکانیسم، نه تنها سرعت جبران خسارت را افزایش می‌دهد، بلکه ریسک مالی پیمانکاران را نیز مدیریت می‌کند.

چهارم- چالش شفافیت الگوریتمی و دسترسی به داده‌ها: یک مانع بزرگ در پیگیری مسئولیت پیمانکاران، «عدم شفافیت الگوریتمی» و «مالکیت معنوی کدها» است. پیمانکاران اغلب کدهای منبع را به عنوان «اسرار تجاری» محافظت می‌کنند و از ارائه آن به مراجع قضایی یا کارشناسان مستقل خودداری می‌نمایند. این امر، اثبات تقصیر یا نقص فنی را برای شهروندان غیرممکن می‌سازد. منابع حقوقی جدید تأکید دارند که در قراردادهای دولتی، باید شرط «حق دسترسی به کد منبع در صورت بروز خطای بحرانی» گنجانده شود. این شرط، به دولت و مراجع نظارتی اجازه می‌دهد در صورت شکایت شهروندان، کدها را برای ممیزی و تحلیل خطا بررسی کنند (Kvitsinia, 2020, 55). بدون این شفافیت، مسئولیت مدنی پیمانکاران، صرفاً یک ادعای نظری باقی می‌ماند و در عمل، فرار از قانون تسهیل می‌شود.

به دیدگاه نگارنده، نقش پیمانکاران خصوصی در دولت الکترونیک، نیازمند بازتعریف

چهارچوب‌های مسئولیت مدنی است. گذار از رویکردهای سنتی مبتنی بر تقصیر فردی به سمت «مسئولیت ساختاری» و «بیمه‌سازی ریسک»، راهکاری کارآمد برای مدیریت خطاهای سیستمی است. دولت باید با تدوین قراردادهای هوشمند، الزام به شفافیت الگوریتمی و ایجاد مکانیسم‌های جبران خسارت سریع، تعادل میان منافع بخش خصوصی و حقوق شهروندان را حفظ کند. در غیر این صورت، خلأهای مسئولیت، منجر به بی‌اعتمادی عمومی و تضعیف مشروعیت دولت الکترونیک خواهد شد.

نتیجه

گذار از مدیریت سنتی به دولت الکترونیک، تنها یک تغییر تکنولوژیک نیست، بلکه دگرگونی بنیادین در ماهیت رابطه حقوقی میان دولت و شهروندان است که مسئولیت مدنی را از یک مفهوم انفعالی به یک الزام فعال و ساختاری تبدیل کرده است. حال در پاسخ به چالش اصلی که چگونه می‌توان در پیچیدگی‌های فنی و ابهامات ناشی از عملکرد الگوریتم‌ها، عدالت و جبران خسارت را تضمین کرد؟ می‌توان گفت پاسخ نهایی در گرو پذیرش این واقعیت است که خطای سیستمی، محصولی از تعامل سه‌جانبه میان نقص‌های ذاتی نرم‌افزار و سخت‌افزار، ضعف‌های نظارتی دولت و ابهامات قراردادی با پیمانکاران خصوصی است.

بنابراین، رویکردهای سنتی مبتنی بر اثبات تقصیر فردی، در برابر ماهیت غیرقابل پیش‌بینی و پیچیده خطاهای دیجیتال، ناکارآمد و ناعادلانه هستند. برای پر کردن این خلأ حقوقی و ایجاد تعادل، باید از نظریه‌های نوینی همچون «نظریه خطر» و «مسئولیت بدون تقصیر» به‌عنوان پایه‌های حقوقی جدید استفاده کرد، زیرا دولت به‌عنوان بهره‌بردار نهایی و ناظر بر خدمات عمومی، باید عوارض ناشی از ریسک‌های فنی را بپذیرد. در این راستا، تفکیک دقیق میان خطاهای نرم‌افزاری^{۴۹} و خطاهای

۴۹- که ریشه در منطق و داده دارند

سخت‌افزاری^{۵۰}، برای تعیین دقیق مقصر و نوع مسئولیت ضروری است. همچنین، نقش پیمانکاران خصوصی نیازمند بازتعریف است؛ چرا که انحصار فنی و پنهان‌کاری الگوریتمی، شهروندان را از حق دسترسی به عدالت محروم می‌کند؛ بنابراین، شفافیت و نظارت دولت بر پیمانکاران، نه یک انتخاب، بلکه یک الزام حقوقی برای سلب مسئولیت از دولت و تحمیل مسئولیت به مجری واقعی خطا است.

پیشنهاد

برای تحقق این چهارچوب نظری و عملیاتی، دو پیشنهاد راهبردی و اجرایی ارائه می‌گردد که می‌تواند تحولی جدی در نظام مسئولیت مدنی دولت الکترونیک ایجاد کند. نخست، الزام قانونی و فوری به استفاده از «قراردادهای امانی کد منبع» در تمامی قراردادهای کلان فناوری اطلاعات دولت است. این سازوکار تضمین می‌کند که کدهای منبع پروژه‌ها نزد یک نهاد ثالث مستقل و مورد اعتماد امانت گذاشته شود و در صورت بروز خطای بحرانی، شکایت شهروندان، یا ورشکستگی پیمانکار، دولت و مراجع قضایی دسترسی فوری و مستقل به این کدها برای ممیزی، عیب‌یابی و اثبات رابطه سببی داشته باشند. این اقدام، مانع از استفاده پیمانکاران از بهانه «اسرار تجاری» برای فرار از شفافیت و مسئولیت‌پذیری شده و با باز کردن «جعبه سیاه» الگوریتم‌ها، امکان تشخیص دقیق تقصیر را فراهم می‌آورد.

دوم، تأسیس «صندوق ملی جبران خسارت‌های دیجیتال» با تأمین مالی از محل درصدی از بودجه پروژه‌های فناوری و بیمه‌های مسئولیت حرفه‌ای اجباری پیمانکاران است. این صندوق با حذف موانع دادرسی طولانی و اثبات دشوار تقصیر در پرونده‌های پیچیده فنی، امکان جبران سریع، عادلانه و بدون نیاز به اثبات تقصیر مستقیم، خسارات شهروندان ناشی از باگ‌ها، سوءگیری‌های الگوریتمی یا قطعی‌های سیستمی را فراهم می‌کند. این مکانیسم نه تنها سرعت جبران خسارت را افزایش می‌دهد، بلکه با توزیع ریسک مالی بر عهده صنعت فناوری، انگیزه‌ای قوی برای ارتقای کیفیت خدمات و

۵۰- که ریشه در فرسودگی و محیط دارند

کاهش خطاهای سیستمی ایجاد می‌کند. تنها با اجرای این دو سازوکار، می‌توان تعادل میان نوآوری فناوری و حاکمیت قانون را برقرار کرد و دولت الکترونیک را به پلتفرمی امن، شفاف و پاسخگو برای همه شهروندان تبدیل نمود.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

- امیری، مصطفی و دشتی، محمدتقی، ۱۴۰۳، امکان سنجی اعمال نظریه خطر به‌عنوان مبنای مسئولیت مدنی

دولت در حقوق ایران، **فصلنامه پژوهش‌های نوین حقوق اداری**، شماره ۱۸.

- تقوی فرد، محمدتقی؛ تقوا، محمدرضا؛ فقیهی، مهدی؛ جمشیدی، محمدجواد، ۱۳۹۵، الگوی صیانت از

حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک برای کشورهای در حال توسعه، **فصلنامه**

پژوهش‌های مدیریت عمومی، شماره ۳۱.

- جمشیدی، محمدجواد، ۱۳۹۸، چالش‌های حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک،

فصلنامه مطالعات حقوق شهروندی، شماره ۱۳.

- سلامی نژاد، نصرالله، ۱۴۰۳، مروری بر اصول حاکم بر قراردادهای پیمانکاری دولتی، **فصلنامه رویکردهای**

پژوهشی نوین در مدیریت و حسابداری، شماره ۳۱.

- صفایی، حسین؛ صالحی، سعیده؛ عباسلو، بختیار؛ بادینی، حسن، ۱۳۹۷، معیار تقسیم مسئولیت در فرض تعدد

اسباب و تحول آن در حقوق ایران، **فصلنامه دیدگاه‌های حقوق قضایی**، شماره ۸۴

- ضیایی، سیدياسر و خلیل زاده، مونا، ۱۳۹۲، مسئولیت بین‌المللی دولت ناشی از حملات سایبری، **فصلنامه**

پژوهش‌های حقوقی، شماره ۳۲.

- معمارزاده طهران، غلامرضا؛ ممینی، مهدی؛ فقیهی، مهدی، ۱۴۰۳، **دولت الکترونیک**، چاپ پنجم، تهران، انتشارات اندیشه‌های گهربار.

- قیاسی، فاطمه؛ درویش پور، حجت الله؛ توحیدفام، محمد؛ امینی، علی اکبر، ۱۴۰۱، نقش فناوری اطلاعات و دولت الکترونیک در ارتقای شاخص‌های حکمرانی صالح، **دوفصلنامه دانش سیاسی**، شماره ۳۶.

- کریمی تازه کند، شهرام؛ عرفانی، محمود؛ واحدی زاده، جواد، ۱۳۹۶، مبنا و حدود مسئولیت مدنی پیمانکار، **فصلنامه پژوهش‌های حقوقی**، شماره ۳۲.

- لطیف زاده، مهدیه؛ قبولی درافشان، سیدمحمد مهدی؛ محسنی، سعید؛ عابدی، محمد، ۱۴۰۱، تبیین اسباب مشروعیت پردازش داده شخصی از منظر حقوق اتحادیه اروپا و ایران، **فصلنامه مطالعات حقوقی**، شماره ۳.

- لطیف زاده، مهدیه، ۱۴۰۳، تحلیل حقوقی فریب الگوریتمی در عصر هوش مصنوعی: چالش‌ها و راهکارها، **فصلنامه سیاست علم و فناوری**، شماره ۴.

- ملکوتی، رسول و ساورایی، پرویز، ۱۳۹۵، درآمدی بر مسئولیت مدنی در فضای سایبر، **فصلنامه پژوهش حقوق خصوصی**، شماره ۱۴.

لاتین

- Apriyanto, Teguh & Sara, Rineke, 2024, The Role of Blockchain Technology in Improving Data Security and Integrity in the law Enforcement Process of Corruption Crimes, Proceedings of the 4th International Conference on law, Social Sciences, Economics, and Education.
- Ashiku, Liridona Veliu, 2024, balkanization and the Euro-Atlantic Processes of the (Western) Balkans, Routledge.
- Bagshaw, Roderick, 2024, Torts on Three Continents, Oxford University Press Oxford.
- Baguma, Rehema & Lubega, Jude, 2013, Factors for success and failure of E-Government projects, Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance.
- Boutros, Andrew, 2019, From Baksheesh to Bribery, Oxford University Press New York.
- Konarski, Marcin Jerzy, 2021, Public Burdens in Situations of Constitutional Emergency,

Przegląd Prawa Administracyjnego Journal.

- Kvitsinia, Natalia, 2020, Prospects for the Development of the Escrow Agreement in Russia, Legal Concept Journal.
- Li, Meng, 2018, Encyclopedia of Wireless Networks, Springer International Publishing.
- Luksch, Manu, 2012, Interventionen: Alltagslabor Function Creep, Brill Fink.
- Martin, Kirsten E. M., 2021, Algorithmic Bias and Corporate Responsibility, SSRN Electronic Journal.
- Nakamura, Makoto & Saito, Daichi, 2025, The Evolution of Defined Terms in law: A Diachronic Study Using Open Legal Data, 2025 17th International Conference on Knowledge and System Engineering (KSE).
- Neville-Neil, George V., 2017, Forced Exception Handling, Communications of the ACM Journal, vol. 60.
- Pedrosa, Micael et al., 2021, Holder-of-Key threshold access token for anonymous data resources, IEEE Symposium on Computers and Communications (ISCC).
- Savage, Stefan, 2018, Lawful Device Access without Mass Surveillance Risk, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.
- Tampubolon, Ezra et al., 2021, On Information Asymmetry in Online Reinforcement Learning, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

- Legal Effects Arising from the Opening of Letters of Credit on the Buyer and the Beneficiary
Homayoun Mafi, Mohsen Raeisi, Ahmadreza Amiri Larijani
- Examining the Potential for International Criminal Justice to Address Ecocide in the Context of Climate Change
Sobhan Tayebi, Majede Magholi
- Analyzing the Nature and Mechanism of Enforcing Decisions of the International Court of Justice with an Emphasis on the Court's Practice in Facing Legal Lacunae
Somayah Rahmanian, Pouria Ebrahimzadeh
- Prohibiting the Abuse of Emergency in the Iranian Legal System
Zeinab Ghaderi, Abdolmajid Yousefi, Sattar Fakhræi
- Comparative Study of the Automatic Termination Clause in Iranian Law and the Contract Avoidance Mechanism under the United Nations Convention on Contracts for the International Sale of Goods
Hakime Mahmood Soltani, Mahdi Sheikh Mahmoodi
- A Comparative Study of the Elements and Principles of Criminalizing Collusion to Commit a Crime in Iranian and French Criminal Law
Saber Sayyari Zohan
- Challenges of Electronic Documents in Iranian Law
Mohammadreza Abdi, Sasan Vazin Puor
- The Dual Role of Artificial Intelligence in Countering Misinformation and Deep Forgery: Challenges and Solutions
Atefeh Lorkijori, Seyed Ahmad Peyrovnaziri
- Legal Nature of the Foundational Condition in Imamiyya Jurisprudence and Iranian Law; Explaining the Bases of Its Validity and Its Scope in Civil Partnership Contracts
Seyyed Alireza Hosseini, Mohammadreza Rostami, Tahere Jafari
- A Jurisprudential Legal Study of the Status and Role of Wills of Intestate Persons in Determining the Disposition of Property After Death
Sayede Nazanin Mousavi
- Foundations, Conditions and Effects of Criminal Sentences in the Iranian Criminal System
Kamran Rahimi Sekkeh Ravani
- A Jurisprudential Study of the Invalidity of Transactions in the Law Requiring Official Registration of Immovable Property Transactions
Mahdi Rajaiean, Jafar Ghajeh Beigloo
- Child and Adolescent Victimization in the Metaverse: a Review of Understanding Causes to Prevention and Countermeasures
Javad Cheraghi
- Analysis of the Supporting Roles of the Convention on the International Sale of Goods in Facilitating and Protecting International Trade
Esmaeil Chogani
- The Function of the Prosecutors Criminal Policy in the Prevention and Prosecution of Crimes Violating Public Rights
Vahid Kioumars
- Comparative Study of the Rule of Independence of Arbitration Clause in Iranian, French, English Law and the UNCITRAL Model Law; Theories and Practices
Saeed Johar
- the Legal Status of Transactions of Periodically Insane Persons in the Law of Iran and England
Amirmohammad Tavakoli, Setayesh Haj Rajabali Tehrani, Fatemeh Allahverdi, Amirreza Noghravi
- The Impact of Strict Laws on Drug-related Behaviors
Hamidreza Ghanaatian
- The Peaceful Role of Nuclear Energy in Iranian law and the International System with a New Approach
Mojahed Amiri, Fatemeh Asgharzadeh Shirazi
- The Impact of New Technologies, Smartification, and Digital Transformation on the Implementation of the Mandatory Registration Law
Negar Fouladi, Vajihe Mohseni
- Criminological Analysis of Smuggling of Goods in Hormozgan Province
Ahmad Padidar, Mohammad Kamali
- Smart Contract in the Iranian Legal System
Mahdi Salehi Zadeh
- Legal Challenges of E-Government and Government Civil Liability
Saeed Sardashti Birjandi
- the Principle of Impartiality of the Reason for Education in the Iranian Criminal Procedure
Mohammadhasan Malek Mohammadi
- Qualitative Analysis of the Foundations and Scope of Criminal Liability in the Commission of Crimes Caused by Restless Legs Syndrome: the Interaction of Neuromotor Disorder with the Elements of Fault and Attributability
Zahra Enalouy Esfahani
- The Relationship Between Rule and Exception in Iranian Civil Law with Emphasis on the Principle of the Binding Force of Contracts and Its Exceptions
Amirreza Alitabar
- Institutional Castling: Military Enlistment and Mass Incarceration in the United States
Bryan L. Sykes, Amy Kate Bailey, Yasser Shakeri