

Submit Date: 29 September 2025

Revise Date: 01 February 2026

Accept Date: 08 February 2026

Initial Publish: 12 February 2026

Final Publish: 22 December 2026

The Encyclopedia of Comparative Jurisprudence and Law

Civil Liability of the State for Obstructing Access to Data and Digital Systems: A Perspective from English Law

Zeynab Baniyadi*¹, Hossein Baniyadi¹

1. Department of Law, S.C., Islamic Azad University, Sirjan, Iran

* Corresponding Author's Email: z.baniyadi1858@yahoo.com

ABSTRACT

With the expansion of e-government, accessibility to governmental data and digital systems has become one of the significant manifestations of citizens' rights. Nevertheless, in certain cases, due to administrative decisions, security considerations, or technical deficiencies, individuals' access to these systems is restricted or blocked, which may result in damage. This situation raises the issue of the civil liability of the state for obstructing digital accessibility in tension with the principle of state immunity. The present study adopts a descriptive-analytical and comparative approach to examine the civil liability of the state for preventing access to data and digital systems from the perspective of English law. The findings indicate that, within English law, through doctrines such as misfeasance in public office, administrative negligence, and the development of the concept of a duty of care, it has become possible to hold public authorities liable where unjustified restrictions on digital access are imposed. It is concluded that limiting state immunity and recognizing civil liability for unjustified obstruction of access to data and digital systems can contribute to enhanced accountability, transparency, and effective protection of citizens' digital rights.

Keywords: *civil liability of the state; digital accessibility; data and digital systems; state immunity; English law.*

How to cite: Baniyadi, Z., & Baniyadi, H. (2026). Civil Liability of the State for Obstructing Access to Data and Digital Systems: A Perspective from English Law. *The Encyclopedia of Comparative Jurisprudence and Law*, 4(4), 1-15.



تاریخ ارسال: ۷ مهر ۱۴۰۴
تاریخ بازنگری: ۱۲ بهمن ۱۴۰۴
تاریخ پذیرش: ۱۹ بهمن ۱۴۰۴
تاریخ چاپ اولیه: ۲۳ بهمن ۱۴۰۴
تاریخ چاپ نهایی: ۱ دی ۱۴۰۵

دانشنامه فقه و حقوق تطبیقی

مسئولیت مدنی دولت در ممانعت از دسترسی پذیری به داده و سامانه با چشم انداز به حقوق انگلیس

زینب بنی اسدی^{*}، حسین بنی اسدی^۱

۱. گروه حقوق، واحد سیرجان، دانشگاه آزاد اسلامی، سیرجان، ایران
* پست الکترونیک نویسنده مسئول: z.baniasadi1858@yahoo.com

چکیده

با گسترش دولت الکترونیک، دسترسی پذیری به داده‌ها و سامانه‌های دولتی به یکی از مصادیق مهم حقوق شهروندی تبدیل شده است. با این حال، در مواردی به دلیل تصمیمات اداری، ملاحظات امنیتی یا نقص‌های فنی، دسترسی اشخاص به این سامانه‌ها محدود یا مسدود می‌شود که می‌تواند موجب ورود خسارت گردد. این وضعیت، مسئله مسئولیت مدنی دولت در ممانعت از دسترسی پذیری دیجیتال را در تعارض با اصل مصونیت دولت مطرح می‌سازد. پژوهش حاضر با رویکردی توصیفی-تحلیلی و تطبیقی، به بررسی مسئولیت مدنی دولت در ممانعت از دسترسی به داده و سامانه‌ها با چشم‌انداز حقوق انگلیس می‌پردازد. یافته‌ها نشان می‌دهد که در حقوق انگلیس، از طریق نهادهایی چون قصور در انجام وظیفه عمومی، بی‌احتیاطی اداری و توسعه مفهوم وظیفه مراقبت، امکان مسئول شناختن نهادهای دولتی در صورت ایجاد محدودیت ناموجه در دسترسی دیجیتال فراهم شده است. نتیجه آن‌که تحدید مصونیت دولت و شناسایی مسئولیت مدنی در قبال ممانعت غیرموجه از دسترسی پذیری به داده و سامانه‌ها، می‌تواند به ارتقای پاسخگویی، شفافیت و حمایت مؤثر از حقوق دیجیتال شهروندان منجر شود.

کلیدواژگان: مسئولیت مدنی دولت، دسترسی‌پذیری دیجیتال، داده و سامانه، مصونیت دولت، حقوق انگلیس.

نحوه استناددهی: بنی اسدی، زینب، و بنی اسدی، حسین. (۱۴۰۵). مسئولیت مدنی دولت در ممانعت از دسترسی‌پذیری به داده و سامانه با چشم انداز به حقوق انگلیس. *دانشنامه فقه و حقوق تطبیقی*، ۴(۴)، ۱-۱۵.



دیگر به صورت مطلق پذیرفته نمی‌شود. به همین دلیل، بازاندیشی در دامنه این مصونیت و بررسی امکان اعمال مسئولیت مدنی دولت در حوزه دسترسی‌پذیری دیجیتال، ضرورتی اجتناب‌ناپذیر یافته است.

در این میان، مطالعه تطبیقی حقوق انگلیس از اهمیت ویژه‌ای برخوردار است. حقوق انگلیس با وجود پابندی به اصول سنتی حقوق عمومی، از طریق توسعه نهادهایی همچون قصور در انجام وظیفه عمومی (Misfeasance in Public Office)، مسئولیت ناشی از بی‌احتیاطی اداری (Negligence) و گسترش مفهوم وظیفه مراقبت (Duty of Care)، امکان مسئول شناختن نهادهای عمومی در برابر اقدامات یا ترک فعل‌های زیان‌بار را فراهم ساخته است. این رویکرد نشان می‌دهد که حتی در غیاب نقض صریح قانون، اختلال یا ممانعت ناموجه از دسترسی به داده‌ها و سامانه‌ها می‌تواند مبنای مسئولیت مدنی دولت قرار گیرد.

بر این اساس، پژوهش حاضر با هدف تبیین مبانی نظری و حقوقی دسترسی‌پذیری به داده و سامانه‌های دولتی و با اتخاذ رویکردی تطبیقی و تأکید بر حقوق انگلیس، به بررسی امکان تحقق مسئولیت مدنی دولت در ممانعت از دسترسی‌پذیری دیجیتال می‌پردازد. این پژوهش می‌کوشد ضمن حفظ ملاحظات حاکمیتی، راهکارهایی برای تقویت پاسخگویی دولت و حمایت مؤثرتر از حقوق دیجیتال شهروندان ارائه دهد و زمینه‌ای برای توسعه گفت‌وگوهای مسئولیت‌پذیری دولت در عصر داده‌محور فراهم آورد.

مفهوم شناسی و مبانی نظری پژوهش

حق دسترسی^۱ به داده و سامانه

یکی از حقوق مهم افراد دسترسی به داده و سامانه‌هایشان در هر زمان و مکان است. لذا باید گفت که این حق به هیچ وجه حتی با حکم قانون از بین نمی‌رود. چون افراد بخش وسیعی از اطلاعات خود را در سامانه‌های شخصی و یا پست الکترونیک خود ذخیره

تحول دیجیتال در دهه‌های اخیر، الگوی سنتی اداره امور عمومی را به طور بنیادین دگرگون ساخته و دولت‌ها را به سمت استفاده گسترده از داده‌ها و سامانه‌های الکترونیکی در ارائه خدمات عمومی سوق داده است. امروزه بخش قابل توجهی از تعامل شهروندان با نهادهای دولتی از طریق سامانه‌های دیجیتال انجام می‌شود و دسترسی‌پذیری به این سامانه‌ها، نقشی تعیین‌کننده در بهره‌مندی از حقوق و مزایای قانونی، تحقق شفافیت اداری و تضمین برابری شهروندان ایفا می‌کند. در این چارچوب، دسترسی به داده‌ها و سامانه‌های دولتی را می‌توان یکی از جلوه‌های نوین حقوق شهروندی و از لوازم تحقق حکمرانی مطلوب دانست.

با وجود این، واقعیت‌های عملی حاکی از آن است که در موارد متعددی، دسترسی اشخاص به داده‌ها و سامانه‌های دولتی با محدودیت، تعلیق یا انسداد مواجه می‌شود. این ممانعت‌ها ممکن است ناشی از تصمیمات اداری، سیاست‌های امنیتی، ضعف زیرساخت‌های فنی، فقدان مقررات شفاف یا ترک فعل نهادهای مسئول باشد. در بسیاری از موارد، این اقدامات نه تنها مانع استفاده مؤثر شهروندان از خدمات عمومی می‌شود، بلکه می‌تواند موجب ورود خسارات مادی، از قبیل از دست رفتن فرصت‌های شغلی یا اقتصادی، و خسارات معنوی، نظیر نقض کرامت انسانی و تضعیف اعتماد عمومی به نظام اداری گردد.

در چنین شرایطی، مسئله اساسی این است که حدود مسئولیت مدنی دولت در قبال ممانعت از دسترسی‌پذیری به داده و سامانه‌ها تا کجاست و آیا دولت می‌تواند با استناد به اصل مصونیت حاکمیتی، از جبران خسارت ناشی از این اقدامات معاف شود یا خیر. اصل مصونیت دولت، اگرچه ریشه در ملاحظات حفظ اقتدار و کارآمدی حاکمیت دارد، اما در نظام‌های حقوقی معاصر، به ویژه در حوزه‌هایی که با حقوق بنیادین شهروندان ارتباط مستقیم دارد،

¹. Access Right

می‌کنند لذا ضرورت دارد که در هر لحظه که نیاز به دارند، به آن دسترسی پیدا کرده و استفاده نمایند (Banisar, 2000).

بر اساس اصل حداقل حق دسترسی، هر برنامه و هر کاربری که به سیستم دسترسی دارد باید از حداقل دسترسی‌هایی که برای کامل کردن وظیفه‌اش ضروری است، استفاده نماید. به طور معمول، هر سیستم دارای اجزای مختلفی است که اکثر آنها نیازمند مجموعه‌ای از دسترسی‌های پایه است. اما تعداد کمی از اجزا نیازمند حق دسترسی بالاتری نسبت به دیگران است که اصطلاحاً گفته می‌شود این اجزا با حق دسترسی ارتقایافته اجرا می‌شوند. فقط برنامه‌های مربوط به این اجزا امضا یا علامت‌گذاری می‌شوند و دیگر برنامه‌هایی که نیازمند حق دسترسی ارتقایافته نیستند، نباید امضا شوند (بر اساس قانون ENVoo-J).

بند ۱ ماده ۸ از دستور العمل شماره 95/46/EC اتحادیه اروپایی مقرر می‌دارد: «کشورهای عضو پردازش داده‌های شخصی مربوط به ریشه‌های قومی و نژادی، اعتقادات سیاسی، عقاید دینی و فلسفی، عضویت در اتحادیه‌های تجاری و پردازش داده‌های مربوط به سلامتی و زندگی جنسی را ممنوع خواهد نمود» (Aslani, 2005).

داده‌های موضوع این ماده که به داده‌های شخصی حساس معروفند، تقریباً در اغلب قوانین و متون قانونی مشابه مشمول حمایت قرار گرفته اند که به شرح زیر هستند:

- داده‌های مربوط به سلامتی خصوصیات وراثتی
- داده‌های تجاری و اقتصادی
- داده‌های اعتقادی
- داده‌های جنسی
- داده‌های مربوط به محکومیت‌های کیفری
- داده‌های عمومی

چون داده‌های مذکور مورد حمایت قانونگذار هستند، افراد باید در هر زمان که می‌خواهند به آنها دسترسی داشته باشند و از آنها استفاده نمایند. پس می‌توان گفت که حق دسترسی بدان معناست که فرد باید امکان دسترسی به داده‌های خود یا حداقل اطلاعات راجع به آن از قبیل نوع و حجم و ماهیت داده‌ها، هدف پردازش و مدت ذخیره آنها را داشته باشد (Aslani, 2005).

مسئولیت مدنی و مسئولیت اخلاقی

مسئول از آن‌جا که اسم مفعول است، به معنی پرسیده‌شده، درخواست‌شده و بازخواست شده می‌باشد. لفظ مسئول ۵ بار در قرآن کریم، در آیاتی چون آیه شریفه ۲۴ از سوره مبارکه صافات آمده است، که خداوند متعال به فرشتگان درباره مجرمین می‌فرماید: «وَقَفُّهُمْ إِنَّهُمْ مَسْئُولُونَ». در روایات نیز واژه مسئول دیده می‌شود. به عنوان نمونه، پیامبر اعظم (ص) می‌فرماید: «کلکم راع و کلکم مسئول عن رعیة» که مبین مسئولیت اجتماعی است و نزدیک به مفهومی است که امروزه از مسئول به ذهن می‌آید.

لفظ مسئولیت نیز مانند الفاظ مالکیت، الوهیت و معلولیت ساخته شده و معادل responsibility انگلیسی است و به تعبیر نویسندگان عبارت است از ضرورت پاسخ‌گویی توسط شخصی که از تعهدات و وظایف خود تخلف نموده است، چه این تعهدات حقوقی باشند و چه جنبه اخلاقی و معنوی داشته باشند (Saffar, 1994).

در قانون مدنی به جای مسئول و مسئولیت از ضامن و ضمان استفاده شده است. زیرا در اسلام از مسئولیت جبران خسارت به ضمان تعبیر شده است و منظور از ضمان، ثبوت اعتباری چیزی در ذمه کسی به حکم شارع است (Gorji, 2001). بنابراین، با کمی تأمل می‌توان گفت که بحث معافیت از مسئولیت یا مصونیت که در ادبیات حقوقی امروزی متداول است و در این پژوهش به کار رفته، با مستقطات ضمان رایج در کلام فقها می‌تواند نزدیک و همسان‌سازی شود.

مسئولیت مدنی به طور عینی (نوعی) در مقایسه با یک رفتار عادی مورد ارزیابی قرار می‌گیرد. لذا یک اندیشه ساده ممکن است موجب مسئولیت اخلاقی شود؛ ولو اینکه موجب ضرر قابل لمسی به دیگری نشود. اما مسئولیت مدنی مستلزم ظهور خارجی اندیشه به صورت فعل یا ترک فعل، که همراه با ضرر و زیانی باشد، بوده و ورود ضرر شرط تحقق مسئولیت است (Khorram-Abadi, 2012).

بر خلاف مسئولیت اخلاقی که ضمانت اجرای آن شرمساری وجدان و احساس گناه است، ضمانت اجرایی مسئولیت مدنی و کیفری، جبر و الزام دستگاه‌های قانونی و قضائی کشور می‌باشد.

مسئولیت مدنی، مسئولیت کیفری و مسئولیت انتظامی

در مسئولیت مدنی و کیفری، فرد مسئول باید مرتکب فعل یا ترک فعلی شود که به دیگری ضرر می‌رساند. در مسئولیت مدنی، ضرر متوجه شخص خصوصی و در کیفری، متوجه جامعه است. لذا هدف از مسئولیت کیفری مجازات مجرم است. مجازات باید متناسب با اهمیت تقصیر ارتكابی باشد. اما هدف از مسئولیت مدنی جبران ضرر و زیان وارده به زیان‌دیده است و با میزان این زیان سنجیده می‌شود (Aghaeinia, 2008).

در مسئولیت کیفری، قصد و نیت یکی از ارکان اساسی مسئولیت است. در حقوق کیفری جرم غیر عمد جنبه استثنایی داشته و موردی وجود ندارد که قانون کسی را بدون تقصیر مجرم شناسد. ولی در مسئولیت مدنی «کسی که بر خلاف حق و در اثر بی‌مبالاتی و بی‌احتیاطی به دیگری خسارتی وارد می‌آورد، باید آن را جبران کند» (Katouzian, 2001).

مسئولیت کیفری با اجتماع سه عنصر تحقق می‌یابد. اولین پایه مسئولیت کیفری، عنصر قانونی است که عبارت از وجود متنی قانونی است که یک عمل را مجرمانه قلمداد می‌کند. دومین پایه آن، عنصر معنوی است که به واسطه قصد ارتكاب عمل زیان‌آور و مجرمانه تحقق می‌یابد. سومین، عنصر مادی است که انجام

مسئولیت مدنی مسئولیتی است که در برابر ایجاد خسارت به وجود می‌آید و به وجود آورنده خسارت را ناگزیر از جبران خسارت می‌نماید. مسئولیت مدنی به معنی مسئولیت پرداخت خسارت است (Jafari Langroudi, 1999). پس هر جا که شخص در برابر دیگری مسئول جبران خسارتی باشد، در آنجا مسئولیت مدنی وجود دارد.

بر مبنای مسئولیت مدنی بین زیان‌زننده و زیان‌دیده رابطه‌ای خاص به وجود می‌آید که همان جبران خسارت است. بنابراین، مسئولیت مدنی در معنی عام و وسیعش هم مسئولیت قراردادی و هم مسئولیت خارج از قرارداد را در بر می‌گیرد زیرا در هر دو مسئله مهم، بحث جبران خسارت مطرح است. اما تفاوت اساسی این دو با هم در وجود یا عدم وجود قرارداد بین طرفین می‌باشد. قلمرو مسئولیت مدنی از جایی آغاز می‌شود که بین طرفین قراردادی برای انجام تعهد وجود نداشته باشد. مسئولیت مدنی ناشی از نقض قرارداد نیست در حالی که مسئولیت قراردادی مسئولیتی است که در نتیجه تخلف از مفاد قرارداد خصوصی پدید می‌آید. به عبارت دیگر، مسئولیت قراردادی به این معنی است که کسی که به عهد خود وفا نکرده و باعث ضرر طرف قرارداد خود شده باشد، باید زیان وارده را جبران نماید.

منظور از مسئولیت اخلاقی این است که انسان در مقابل خداوند یا وجدان خویش جوابگوی خطای ارتكابی باشد. این مسئولیت در فعل یا ترک فعلی که به شکل مخالفت با تعالیم دینی یا قواعد اخلاقی و وجدان باشد، ظاهر می‌گردد. ولی اگر منشأ الزام به پاسخگویی، معیارهای خارجی و بر پایه رفتار متداول افراد جامعه و در برابر حقوق موضوعه باشد، آن مسئولیت را مسئولیت حقوقی گویند.

مسئولیت اخلاقی جنبه درونی و شخصی دارد و برای مسئول شناختن فاعل زیان، باید شرایط و اوضاع و احوال شخصی و اندیشه و وجدان وی را بازرسی کرد. در حالی که مسئولیت

عملیات مجرمانه است و می‌تواند جنحه، جنایت یا خلاف باشد (Baheri, 2005). با این وجود بین مسئولیت مدنی و کیفری گاهی ارتباطاتی وجود دارد. مثلاً، عمل واحد می‌تواند هر دو مسئولیت را در پی داشته باشد.

در مورد مسئولیت انتظامی به این مطلب اکتفا می‌شود که نقض مقررات صنفی به وسیله یک نفر از افراد آن صنف تخلف انتظامی محسوب می‌شود. مثلاً، قانون وکالت مصوب ۱۳۱۵/۱۱/۲۵ که قواعد اساسی لازم‌الرعايه بر وکلا را بیان می‌دارد. همچنین، آئین‌نامه انتظامی پزشکی مصوب کمیسیون‌های مشترک بهداشتی و دادگستری مجلسین به سال ۱۳۴۸، در ۶۵ ماده تخلفات انتظامی پزشکان و مجازات‌های آن را بیان داشته است. کیفر تخلف انتظامی تناسب و ارتباط با شغل مرتکب تخلف دارد؛ از قبیل توییح، تعلیق موقت، انفصال موقت یا دائم از شغل و... در این حالات خطا نوع خاصی است که اساس آن انضباط شغلی و مسلکی است و از چارچوب مسئولیت مدنی خارج بوده و مرتکب تخلف انتظامی فقط مسئولیت انتظامی دارد.

مبانی مصونیت مدنی و مسئولیت دولت با توجه به مبانی مسئولیت مدنی

اگر به پیروی از اندیشمندان حقوق، هدف اصلی قواعد مسئولیت مدنی را جبران خسارت زیان‌دیده و ترمیم زیان وارده بدانیم، دولت نیز از این قاعده مستثنی نخواهد ماند؛ بویژه با توجه به نقشی که دولت‌های امروزی در جامعه ایفا می‌کنند، و به مقتضای آن در تمامی شئون اجتماعی به‌طور همه‌جانبه مداخله می‌ورزند و احتمال انجام اعمال ضمان‌آور برای آن‌ها بسیار است. به عنوان نمونه، «باید خسارت مادی ناشی از بازماندن از فعالیت اقتصادی اشخاص و یا خسارات معنوی ناشی از کسر حیثیت و اعتبار اجتماعی اشخاص را جبران نمایند» (Zargoush, 2011).

مسئولیت حکومت به جای کارمند

به گفته نویسندگان مسئولیت دولت نسبت به اعمال کارکنان خود مسئولیتی مستقیم است. به این ترتیب که هرگاه کارمند دولت مرتکب عمل زیانبار شود، دولت نه به سبب خطا یا مسئولیت کارمند که به دلیل خطای خود مستقیماً عهده‌دار مسئولیت خواهد بود. در این معنا مسئولیت دولت تابع مسئولیت کارمند نیست، بلکه به صرف صدور خطای زیانبار از کارمند، اداره مسئول جبران خسارت است. به عبارت دیگر، عمل به دولت منسوب می‌گردد بدون آنکه ابتدا آن را به کارمند عامل ورود زیان نسبت دهیم.

نظریه مسئولیت حکومت یا به تعبیری دولت به معنی اعم یا به تعبیری بیت‌المال به جای مستخدم دولت، نظریه‌ای است که در آثار نویسندگان درباره کارمندان دولت و قضات دیده می‌شود.

به عقیده نویسندگان ضابطه مسئولیت حکومت به جای کارکنان را در حقوق ما می‌توان در مسئولیت مدنی قضات که به موجب اصل ۱۷۱ قانون اساسی پیش‌بینی گردیده است و یکی از بارزترین جلوه‌های مسئولیت مدنی دولت (به معنی اعم) نسبت به اعمال کارکنان خود به شمار می‌رود، مشاهده نمود. اصل ۱۷۱ مقرر می‌دارد: «هرگاه در اثر تقصیر یا اشتباه قاضی در موضوع یا در حکم یا در تطبیق حکم بر مورد خاص ضرر مادی یا معنوی متوجه کسی گردد، در صورت تقصیر، مقصر طبق موازین اسلامی ضامن است و در غیر این صورت، خسارت به وسیله دولت جبران می‌شود؛ البته حقوقدانان تصریح کرده‌اند که اگر تقصیر در حکم عمد باشد. یعنی برای مثال، قاضی بدون خواندن کتاب‌ها و رویه قضایی و بدون مشورت با همکاران، شتابزده تصمیم ناروایی بگیرد و یا آنکه حقیقت را فدای انگیزه‌ها و آمال سیاسی و اخلاقی خود گرداند، اینگونه اعمال را که عرف قضایی نمی‌پسندد، نیز باید در حکم عمد دانست (Katouzian, 2001).

مطالعه آثار فقهای امامیه نیز به خوبی موید این معناست که مسئولیت جبران خسارات ناشی از خطای قاضی به عقیده مشهور از بیت‌المال است (Ibn Babawayh, 1355). بنابراین، قاضی

به سازمان یا مؤسسه دولتی برگزیده‌اند، نظریه مسئولیت اشخاص حقوقی است. گفته می‌شود که هر اداره یا ارگان یا نهادی چون مجلس، یک شخص حقوقی عمومی است و مانند هر شخص حقوقی مسئول اعمال زیانبار خود است. اعمالی که کارمندان اداره به نام شخص حقوقی انجام می‌دهند، اعمال منسوب به این شخص به شمار می‌آید زیرا کارمندان به مثابه اندام‌های این شخص به شمار می‌روند، پس خطای کارمند در هنگام انجام وظیفه خطای شخص حقوقی است. این قاعده از مفهوم شخصیت حقوقی نشأت گرفته است (Aalipour, 2011).

البته منطق حقوقی ایجاب می‌کند که برای تامین هرچه بهتر عدالت در مورد خطاهای شخصی، نماینده در حین انجام وظیفه. یعنی تقصیرهای عمدی و سنگین او به جای آنکه تنها حکومت مسئول باشد، نماینده و حکومت به صورت جمعی مسئول خواهند بود. برخی دیگر با تاکید بر اینکه شخص حقوقی نباید از نتایج اعمال کارکنان خود برکنار بماند، معتقدند که مسئولیت شخص حقوقی نسبت به اعمال کارمندانش به مواردی اختصاص دارد که کارمندی در اجرای عملی که به نمایندگی از شخص حقوقی انجام می‌دهد، خسارت را در نتیجه خطای خود به بار آورده باشد. بنابراین، در خصوص اعمالی که نیابت‌بردار نیست، اگر عمل کارمند منتهی به خسارت شود، هر چند که در حین انجام وظیفه‌اش باشد، مسئولیت شخصی او را در پی خواهد داشت (Zeraat, 2013). چنین عملی به شخص حقوقی منسوب نمی‌گردد زیرا اگر قانونگذار شخصی را مسئول دیگران قرار دهد، این تضمین باعث از بین رفتن مسئولیت خطاکار در چنین مواردی نمی‌شود. به طور مثال، در اتلاف و تسبیب، نمایندگی راه ندارد. پس اگر کارمندی در هنگام کار مال متعلق به دیگری را تلف کند، شخصاً مسئول خواهد بود (Katouzian, 2001).

عده‌ای دیگر - فارغ از این مباحث - مسئولیت مستقیم دولت را بیشتر متکی بر نظریه تضمین حق می‌دانند، حمایت از حقوق

مسئول خطاهای عمدی و یا در حکم عمد خود است که در قانون اساسی به تقصیر تعبیر شده است. این نکته را نیز باید افزود، که ملاک و ضابطه سنجش تقصیر قاضی و شیوه رفتار یک قاضی متعارف است که خطای حرفه‌ای نامیده می‌شود. به گفته نویسندگان، تعبیر تقصیر دادرس بر مبنای خطای حرفه‌ای وسیله‌ای است برای تعدیل مسئولیت او و سازگار کردن آن با خطرهای احترازناپذیر شغل قضاوت (Katouzian, 2001).

با توجه به اینکه شغل نمایندگی مجلس نیز شغلی پرمسئولیت است، شاید بتوان با تنقیح مناط و الغاء خصوصیت از اصل ۱۷۱ این مطلب را در خصوص کارمندان نیز بیان داشت. یعنی اگر خطای حرفه‌ای کارمند در چارچوب وظایف باشد و عمدی یا در حکم عمد نباشد، دولت (به معنی اعم) مسئول جبران خسارت است. چنانکه مقتضای قاعده «صاحب غنیمت صاحب غرامت است» این است که خسارات وارد باید از مال دولت و نه از مال کارمند پرداخت شود (Hashemi, 2007).

مقتضای قاعده «مال هیچ فردی بی‌ارزش نیست» نیز این است که چون حکومت به منظور رعایت جامعه و نظام اسلامی تخلف و اضرار کارمند به دیگران را تجویز نموده و برخی از مشاغل دولت را که مستلزم وقوع تخلف است، پذیرفته که بایستی خساراتی را که به واسطه عمل آنها به افراد وارد می‌شود، جبران کند. اگر تجویز ارتکاب برخی تخلفات برای نماینده و اعطای حق مصونیت به او یک نوع قانونگذاری در جهت مصالح نماینده - و نه عنوان نمایندگی - باشد، در این صورت، نماینده ضامن ضرر و زیان ناشی از استفاده از حق مزبور است و دولت هیچ‌گونه ضمانتی نخواهد داشت. بدون شک، تجویز ارتکاب برخی افعال ضرری برای دیگران توسط کارمندان در صورتی است که آن افعال از لوازم شغل آنها باشد.

در حقوق موضوعه، مبنایی که برخی از نویسندگان و بویژه پیروان نظریه تقصیر برای انتساب مستقیم مسئولیت عمل زیانبار کارمند

شهروندی که از عمل کارمند یک سازمان عمومی زیان دیده است، اقتضا می‌کند که آسان‌ترین طریق برای جبران خسارت او برگزیده شود. اعتقاد و التزام به مسئولیت مستقیم دولت بهترین راه‌حل برای حصول این نتیجه است. البته به عقیده ریورواستاد فرانسوی، مبنای عمومی مسئولیت مدنی دولت نه بر تقصیر که تنها بر خطر ایجادشده از اعمال او قرار دارد.

در قوانین داخلی رگه‌های از مسئولیت حکومت یا بیت‌المال دیده می‌شود. مثلاً، ماده ۳۲۳ قانون مجازات اسلامی مقرر می‌دارد: «هرگاه ثابت شود که مأمور نظامی یا انتظامی در اجرای دستور آمر قانونی تیراندازی نموده و هیچ‌گونه تخلف از مقررات نکرده است، ضامن دیه مقتول نخواهد بود و جز مواردی که مقتول و یا مصدوم مهدورالدم نبوده، دیه بر عهده بیت‌المال خواهد بود. نظر به اینکه دیه علاوه بر جنبه کیفری ماهیتی مدنی نیز دارد، خاصه آنجا که از سوی دولت پرداخت می‌شود، به منظور جبران خسارت است. بنابراین این ماده یک مسئولیت بدون تقصیر برای دولت مقرر داشته که مبتنی بر نظریه خطر است. یعنی عمل تیراندازی مأمور دولت خطری نامتعارف ایجاد نموده که در نتیجه آن به دیگران خسارت وارد شده است. لذا دولت باید تاوان ایجاد این خطر را بپردازد. زیرا به وجود آوردن این محیط خطرناک منسوب به او است. البته لازم به ذکر است که به گفته حقوقدانان با توجه به ماده ۱۲ قانون مسئولیت مدنی برای کارفرمایان فرض تقصیر نموده است. در این باره نیز می‌توان گفت: که نظام حقوقی ما از نظریه تقصیر پیروی کرده است و نظریه ایجاد خطر در نظام حقوقی ایران مورد استعمال نیست (Mir Mohammad Sadeghi, 2009).

اینترنت و مسئولیت مدنی دولت

اینترنت و رایانه مشکلات خاص خود را ایجاد کرده است. نقض حریم زندگی خصوصی افراد و دستبرد به محتوای رایانه‌ها و همچنین ارسال نامه‌های الکترونیکی ناخواسته و تبلیغاتی، از جمله این مشکلات است. در روزگاران گذشته آگهی‌های تبلیغاتی از

طریق پست معمولی ارسال می‌شد و نامه‌های اداری نیز دست به دست می‌گشت. کاربران اینترنت هنگام استفاده از این فن‌آوری جدید، خواه ناخواه، اطلاعات وسیعی را در اختیار شکارچیان می‌گذارند؛ اطلاعاتی همچون شماره کارت اعتباری، شماره حساب بانکی و فهرست اسامی دوستان و همچنین اطلاعات پزشکی و البته محصولات مصرفی مورد علاقه افراد. امکان دستیابی حکومت‌ها، کارفرمایان و بویژه تبهکاران به این اطلاعات باعث نگرانی کاربران شده است. این احساس که دیگران به این آسانی می‌توانند از اعتقادات، احساسات، سلامت جسمی و همچنین میزان موجودی حساب بانکی دیگران مطلع شوند، برای هیچ کس خوشیند نیست (Hel-Foroush, 2003).

نباید حقوق اینترنت را در زمره شاخه‌های علم حقوق آورد. حقوق اینترنت اصطلاحی غیررسمی است که به تطبیق قواعد شاخه‌های سستی علم حقوق همچون حقوق مدنی و حقوق جزا با فعالیت‌هایی که از طریق اینترنت صورت می‌گیرد، اطلاق می‌شود. حقوق اینترنت شاخه‌ای خاص از حقوق نیست؛ قواعد مطرح در آن، در حقیقت، همان قواعد سستی است که برای تطابق با وضعیت خاص اینترنت به لباسی نو در آمده است. با این حال، قوانین متعددی برای حل معضله‌های از اینترنت وضع گردیده است (Desbois, 1966).

فعالیت در زمینه اقتصاد بدون آگاهی از نحوه اعمال قواعد قوانین و مقررات قدیم و جدید فعالیت‌های اینترنتی امکان‌پذیر نیست؛ فعالیت‌هایی همچون تبلیغات، عقد قرارداد، بانکداری، ارسال مکاتبات به محاکم و ادارات دولتی، استخدام و معاملات گوناگون. این گفته که حقوق اینترنت و رایانه پدیده‌ای جدید است بدان معنی نیست که باید همه چیز را از نو فرا گرفت بلکه بسیاری از اصول و قواعد عمومی برای حل مسائل این شاخه از حقوق نیز. نقض حریم زندگی خصوصی افراد و بویژه دست‌اندازی به اطلاعات موجود در نامه‌های الکترونیکی اولین مسئله‌ای است که

گذار از مصونیت مطلق حاکمیت به پاسخگویی مبتنی بر وظیفه مراقبت است.

در نظام حقوقی ایران، مبانی مسئولیت مدنی دولت در این حوزه را باید از قواعد کلی استنباط کرد، زیرا هنوز قانون خاصی در زمینه «مسئولیت دیجیتال دولت» وجود ندارد. قانون مسئولیت مدنی ۱۳۳۹، اصل کلی جبران خسارت ناشی از فعل یا ترک فعل را مقرر داشته است و قانون انتشار و دسترسی آزاد به اطلاعات (۱۳۸۸) نیز تکلیف دولت را در فراهم‌سازی دسترسی به داده‌ها تصریح می‌کند. بر اساس این دو مبنا، می‌توان گفت ممانعت از دسترسی‌پذیری - چه بر اثر تصمیم اداری، چه به دلیل سهل‌انگاری در نگهداری سامانه‌ها - نقض وظیفه دولت در قبال شهروندان است. با این حال، چالش اساسی در ایران تمایز میان اعمال حاکمیتی و تصدی‌گری است. دادگاه‌ها معمولاً اعمال حاکمیتی را از شمول مسئولیت مدنی خارج می‌دانند و این امر باعث می‌شود که بسیاری از خسارات ناشی از تصمیمات مدیریتی دولت در حوزه سایبری، غیرقابل مطالبه تلقی شود. همچنین فقدان نهادهای تخصصی برای رسیدگی به دعاوی مربوط به اختلالات سامانه‌های عمومی، بر این مشکل افزوده است.

در مقابل، حقوق انگلیس سیر تاریخی متفاوتی را پشت سر گذاشته است. این نظام که قرن‌ها تحت سلطه اصل «The King can do no wrong» قرار داشت، از نیمه قرن بیستم به وسیله Crown Proceedings Act 1947 عملاً این مصونیت را محدود کرد و زمینه طرح دعا علیه مقامات و نهادهای عمومی را فراهم آورد. در ادامه، دکترین‌های مهمی چون Misfeasance in Public Office (قصور در انجام وظیفه عمومی) و Negligence (بی‌احتیاطی اداری) توسعه یافتند که اکنون ستون فقرات مسئولیت مدنی دولت در حقوق کامن‌لا محسوب می‌شوند. در چارچوب «قصور در انجام وظیفه عمومی»، اگر مقام دولتی از اختیارات خود آگاهانه و برخلاف منافع عمومی استفاده کند یا با

در زمینه مسئولیت مدنی باید مورد بررسی قرار گیرد. هر کارگر یا کارمند آمریکایی، روزانه به طور متوسط ۱۹۰ نامه الکترونیکی ارسال می‌کند. این عدد بدون محاسبه نامه‌های خصوصی است. آمار فوق بیانگر اهمیت مسئله است. از سویی، هنگامی که در عالم اینترنت به گشت و گذار می‌پردازید، شکارچیان با دنبال کردن مسیرتان به علائق شخصی شما پی می‌برند و ممکن است حتی اطلاعات مربوط، به فروش نیز برسند (Samuelson, 1989). استفاده از تصویر و اسامی افراد برای کسب منافع تجاری نیز از لحاظ مسئولیت مدنی در محیط اینترنت قابل بررسی است. افترا، صرف‌نظر از جنبه جزایی، از لحاظ مسئولیت مدنی نیز می‌تواند مسئولیت به بار آورد. با توجه به شیوع پدیده اینترنت و سهولت دستیابی به اطلاعات از طریق آن، افترا به این شیوه حتی می‌تواند خطرناک‌تر از شیوه‌های معمول باشد. نامه‌های الکترونیکی ناخواسته یا تبلیغاتی نیز از لحاظ مسئولیت مدنی، آثار حقوقی عدیده‌ای را به بار می‌آورند (Zourden, 2003) مطالعه قواعد مسئولیت مدنی در رابطه با اینترنت گسترده‌تر و با اهمیت‌تر از قواعد دیگر زمینه‌های حقوقی است.

تطبیق مسئولیت مدنی دولت در ممانعت از دسترسی‌پذیری به

داده و سامانه‌ها در حقوق ایران و انگلیس

پدیده دولت الکترونیک در سال‌های اخیر، ساختار سنتی اداره امور عمومی را متحول کرده و مفاهیمی چون «حق دسترسی‌پذیری دیجیتال» را به سطح حقوق بنیادین شهروندان ارتقا داده است. اگر در گذشته مسئولیت دولت عمدتاً ناظر بر اعمال فیزیکی و تصمیمات اداری بود، امروز عملکرد دیجیتال دولت - از جمله تداوم، امنیت و بی‌تبعیضی در دسترسی به داده‌ها و سامانه‌های الکترونیکی - نیز می‌تواند منشأ تعهدات مدنی باشد. بررسی تطبیقی میان حقوق ایران و حقوق انگلیس، تفاوت نگاه دو نظام حقوقی به این مسئولیت را روشن می‌سازد و بیانگر مسیر تکاملی

بی‌اعتنایی شدید نسبت به حقوق اشخاص عمل نماید، دولت مسئول جبران خسارت تلقی می‌شود. کاربرد این دکتین در حوزه دسترسی دیجیتال بدین معناست که هرگاه مقام یا نهاد عمومی عمداً سامانه‌ای را مسدود کند یا از علم به آسیب حاصل از این مسدودسازی غفلت ورزد، شرط سوءنیت یا بی‌اعتنایی فاحش محقق و امکان طرح دعوا فراهم است.

در حوزه «بی‌احتیاطی اداری» نیز، مفهوم *Duty of Care* یا «وظیفه مراقبت» نقش اساسی دارد. نهادهای عمومی، همچون سایر اشخاص، در قبال افرادی که به نحوی پیش‌بینی‌پذیر از اقدامات آنان متأثر می‌شوند، وظیفه احتیاط و دقت دارند. چنانچه دولت یا کارگزاران آن در طراحی، نگهداری، یا نظارت بر سامانه‌های دیجیتال قصور ورزند و شهروندان از این رهگذر متضرر شوند، تقصیر اداری محقق و مسئولیت مدنی برقرار است. پرونده‌هایی نظیر *Anns v Merton London Borough Council* (1978) و *Caparo Industries plc v Dickman* (1990)، حدود و معیارهای این وظیفه را ترسیم کرده‌اند و امروزه این مبنا به حوزه فناوری و داده نیز تسری یافته است.

تفاوت بنیادین حقوق ایران و انگلیس در رویکرد به «تقصیر دولت» قابل مشاهده است. در ایران، بار اثبات تقصیر بر عهده زیان‌دیده است و مفهوم تقصیر عموماً محدود به نقض صریح قانون یا عدم انجام وظیفه قانونی تلقی می‌شود. اما در انگلیس، مفهوم گسترده‌تری از تقصیر پذیرفته شده که شامل بی‌مبالاتی ساختاری و قصور در اعمال دقت متعارف نیز می‌گردد. به بیان دیگر، در حالی که در نظام ایران، زیان‌دیده باید نقض قانون یا آیین‌نامه را اثبات کند، در نظام انگلیسی کافی است نشان دهد که دولت نتوانسته استاندارد مراقبت متعارف را رعایت کند. این تفاوت موجب می‌شود که شهروندان در انگلیس راهکارهای مؤثرتری برای احقاق حق خود در برابر ممانعت از دسترسی دیجیتال داشته

باشند، در حالی که در ایران، دعوا در اغلب موارد به استناد فقدان مسئولیت حاکمیتی رد می‌شود.

از سوی دیگر، در ایران مفهوم «حق دسترسی به داده» بیشتر ماهیت سیاسی و اطلاع‌رسانی دارد، ولی در انگلیس به‌طور فزاینده‌ای در قالب «حق مدنی» و حتی «حق انسانی» تحلیل می‌شود. مقرراتی نظیر *Freedom of Information Act 2000*، نهادهای عمومی را ملزم ساخته که نه تنها اطلاعات، بلکه زیرساخت‌های لازم برای دسترسی دیجیتال را به شکلی پایدار و منصفانه فراهم کنند. تخطی از این الزامات، در رویه دادگاه‌های اداری و مدنی، به عنوان نقض تعهد عمومی تلقی و قابل پیگرد است. در ایران نیز هرچند قانون انتشار و دسترسی آزاد به اطلاعات گامی مهم در این راستا بوده، اما ضعف ضمانت اجراها و عدم تصریح مسئولیت جبرانی برای ممانعت از دسترسی، همچنان چالش‌برانگیز است.

از نظر نظریه حقوقی، حقوق انگلیس به سمت پاسخگویی حاکمیت بر پایه وظیفه مراقبت گرایش یافته، در حالی که حقوق ایران هنوز در چارچوب حاکمیت اقتدار و مصونیت اعمال حاکمیتی حرکت می‌کند. در نتیجه، در انگلیس، دولت نه تنها به عنوان قدرت حاکم، بلکه به عنوان ارائه‌دهنده خدمت عمومی (*Public Service Provider*) دیده می‌شود که مانند هر شخص دیگر تابع الزامات دقت، احتیاط و انصاف است. این دیدگاه عملی، موجب توسعه سیاست‌های *open data*، تضمین دسترسی‌پذیری دیجیتال برای گروه‌های آسیب‌پذیر، و شکل‌گیری مسئولیت‌های ویژه در قبال نقض عمدی یا غیرعمدی این دسترسی شده است.

البته باید توجه داشت که حقوق انگلیس نیز مصونیت مطلق دولت را به‌طور کامل کنار نگذاشته است. در برخی حوزه‌های حساس حکومتی — مانند امنیت ملی یا تصمیم‌های مرتبط با منافع راهبردی دولت — دادگاه‌ها همچنان به اصل استقلال تصمیم‌گیری احترام می‌گذارند. با این حال، حتی در این موارد نیز معیار «تناسب و

ضرورت اقدام» مورد بررسی قرار می‌گیرد؛ امری که در حقوق ایران کمتر دیده می‌شود و تصمیمات حاکمیتی غالباً غیرقابل تعرض باقی می‌مانند.

در نتیجه این مقایسه، روشن می‌شود که حقوق انگلیس با تعدیل تاریخی مصونیت حاکمیت و توسعه‌ی مسئولیت مدنی دولت، الگویی واقع‌گرایانه برای پاسخگویی در حوزه‌های نوپدید، از جمله دسترسی دیجیتال ارائه کرده است. این تجربه نشان می‌دهد که پاسخگویی الزاماً به معنای تضعیف اقتدار دولت نیست، بلکه سازوکار حقوقی اطمینان از کارآمدی، شفافیت و اعتماد عمومی است. نظام حقوقی ایران نیز برای تطبیق با الزامات دولت الکترونیک و حفاظت از حقوق دیجیتال شهروندان، ناگزیر از بازتعریف حدود مصونیت و تقویت ضمانت‌های اجرایی در این زمینه است. تصویب قوانین خاص در باب مسئولیت مدنی دولت در فضای داده‌محور، ایجاد مرجع قضایی تخصصی و پذیرش معیار «تقصیر سازمانی» به جای مصونیت حاکمیتی مطلق، می‌تواند گامی مؤثر در جهت همگرایی با تجربه حقوق انگلستان و تحقق عدالت دیجیتال باشد.

نتیجه‌گیری

پژوهش حاضر با تمرکز بر مسئولیت مدنی دولت در ممانعت از دسترسی‌پذیری به داده‌ها و سامانه‌های عمومی، نشان داد که تحول دیجیتال در حکمرانی، صرفاً یک تغییر فناورانه نیست، بلکه مستلزم بازاندیشی در مفاهیم بنیادین حقوق عمومی و مسئولیت دولت است. دسترسی‌پذیری دیجیتال در شرایط کنونی به یکی از ابزارهای تحقق حقوق شهروندی، شفافیت اداری و برابری در بهره‌مندی از خدمات عمومی تبدیل شده و هرگونه اختلال، انسداد یا محدودسازی غیرموجه آن می‌تواند آثار حقوقی قابل توجهی برای اشخاص و جامعه به همراه داشته باشد.

یافته‌های پژوهش بیانگر آن است که در حقوق ایران، اگرچه قواعد عام مسئولیت مدنی و برخی قوانین خاص ظرفیت نظری لازم برای

شناسایی مسئولیت دولت را دارند، اما این ظرفیت در عمل به دلیل غلبه برداشت سنتی از «اعمال حاکمیتی» و استمرار نوعی مصونیت گسترده دولت، به‌طور مؤثر فعال نشده است. در بسیاری از موارد، ممانعت از دسترسی به سامانه‌های دولتی یا داده‌های عمومی — حتی اگر ناشی از سوءمدیریت، ضعف فنی یا تصمیمات اداری غیرمتناسب باشد — در زمره اعمال حاکمیتی تلقی شده و از شمول مسئولیت مدنی خارج می‌شود. این رویکرد، موجب تضعیف حمایت حقوقی از شهروندان و کاهش کارآمدی نظام جبران خسارت در حوزه حقوق دیجیتال شده است.

در مقابل، حقوق انگلیس با عبور تدریجی از نظریه مصونیت مطلق حاکمیت، الگوی متفاوتی از پاسخگویی دولت را ارائه می‌دهد. توسعه نهادهایی مانند *Misfeasance in Public Office* و پذیرش گسترده مفهوم *Duty of Care* نشان می‌دهد که دولت در این نظام حقوقی، نه تنها در قبال اعمال عمدی و سوءاستفاده از قدرت، بلکه در برابر بی‌احتیاطی و قصور در اداره خدمات عمومی دیجیتال نیز مسئول شناخته می‌شود. این امر به‌ویژه در حوزه دسترسی‌پذیری دیجیتال اهمیت دارد؛ زیرا بسیاری از خسارات وارده نه ناشی از تصمیمات صریح، بلکه حاصل ضعف ساختاری، نبود استانداردهای فنی یا عدم پیش‌بینی آثار اقدامات اداری است. تحلیل تطبیقی انجام‌شده در این پژوهش نشان می‌دهد که تفاوت اصلی میان دو نظام حقوقی، در «سطح شناسایی تعهد دیجیتال دولت» نهفته است. در حقوق ایران، تعهد دولت به دسترسی‌پذیری داده و سامانه‌ها بیشتر ماهیتی برنامه‌ای و سیاست‌گذارانه دارد، در حالی که در حقوق انگلیس این تعهد به‌عنوان یک وظیفه حقوقی الزام‌آور با ضمانت اجرای مدنی تلقی می‌شود. نتیجه این تفاوت آن است که شهروندان در نظام حقوقی انگلیس از ابزارهای مؤثرتری برای مطالبه حق و جبران خسارت برخوردارند، در حالی که در ایران، مسیرهای احقاق حق محدود و اغلب ناکارآمد است.

حوزه سامانه‌ها و زیرساخت‌های دیجیتال، به‌طور مطلق از شمول مسئولیت مدنی خارج نشود. ایجاد شعب یا مراجع تخصصی برای رسیدگی به دعاوی مرتبط با دولت الکترونیک و حقوق داده، می‌تواند به وحدت رویه و افزایش کارآمدی نظام جبران خسارت کمک کند.

از منظر سیاست‌گذاری، پیشنهاد می‌شود دولت با تدوین استانداردهای فنی و حقوقی دسترسی‌پذیری دیجیتال و الزام نهادهای عمومی به رعایت آن‌ها، از بروز خسارات پیشگیری کند. آموزش حقوق دیجیتال به مدیران و کارگزاران دولتی و شفاف‌سازی حقوق شهروندان در این حوزه، نقش مهمی در کاهش تعارضات و افزایش اعتماد عمومی خواهد داشت.

در نهایت، برای پژوهش‌های آتی، بررسی تطبیقی مسئولیت دولت در ممانعت از دسترسی‌پذیری دیجیتال با نظام‌های حقوقی اتحادیه اروپا یا تحلیل رویه‌های قضایی داخلی در دعاوی مرتبط با سامانه‌های الکترونیکی، می‌تواند افق‌های جدیدی در توسعه ادبیات حقوق عمومی و حقوق فناوری اطلاعات بگشاید.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافی وجود ندارد.

EXTENDED ABSTRACT

The rapid expansion of digital governance has fundamentally transformed the structure and operation of public administration, rendering access to governmental data and digital systems an indispensable condition for the realization of contemporary citizenship rights. In modern administrative states, digital platforms are no longer auxiliary tools but constitute the primary interface through which individuals exercise legal entitlements, receive public services, and participate in administrative procedures. Consequently, any obstruction, suspension, or restriction of access to these systems—whether resulting

در نهایت، می‌توان گفت که چالش اساسی حقوق ایران در این حوزه، نه فقدان مبانی نظری مسئولیت، بلکه عدم تطبیق ساختار حقوقی با اقتضائات حکمرانی دیجیتال است. ادامه رویکرد سنتی به اعمال حاکمیتی در فضای داده‌محور، موجب فاصله گرفتن حقوق عمومی از واقعیت‌های اجتماعی و فناوری شده و اعتماد عمومی به خدمات الکترونیکی دولت را تضعیف می‌کند. تجربه حقوق انگلیس نشان می‌دهد که بازتعریف مسئولیت مدنی دولت در حوزه دسترسی‌پذیری دیجیتال، نه تهدیدی برای اقتدار حاکمیت، بلکه شرط لازم برای تحقق دولت پاسخگو، شفاف و کارآمد در عصر دیجیتال است.

پیشنهادهات

در پرتو نتایج به‌دست‌آمده، پیشنهاد می‌شود قانون‌گذار ایرانی با تصویب مقررات خاص در حوزه مسئولیت مدنی دولت در فضای دیجیتال، تکلیف نهادهای عمومی را در قبال دسترسی‌پذیری پایدار، ایمن و غیرتبعیض‌آمیز به داده‌ها و سامانه‌ها به‌صورت صریح مشخص کند. شناسایی «تقصیر سازمانی» و «بی‌احتیاطی اداری دیجیتال» به‌عنوان مبنای مستقل مسئولیت، می‌تواند خلأهای موجود را تا حد زیادی جبران کند.

همچنین ضروری است در رویه قضایی، بازنگری جدی در مفهوم اعمال حاکمیتی صورت گیرد و تصمیمات مدیریتی دولت در

from administrative decisions, security policies, technical failures, or institutional negligence—can generate tangible material and moral harm. From a legal perspective, such harm raises complex questions concerning the civil liability of the state, particularly where traditional doctrines of sovereign immunity continue to exert influence. Within this context, access to data must be understood not merely as a technical facility but as a legally protected interest rooted in broader principles of transparency, equality, and human dignity. The right of individuals to access their personal and administrative data has been widely

recognized as an essential component of informational self-determination, implying that data subjects must retain continuous and effective access to information concerning the nature, scope, purpose, and duration of data processing (Aslani, 2005; Banisar, 2000). Any unjustified interference with this access therefore constitutes a potential breach of legal duty capable of triggering state responsibility.

From a conceptual standpoint, the legal analysis of state liability for obstructing digital accessibility requires a careful examination of the foundations of civil responsibility and its distinction from moral, criminal, and disciplinary liability. In classical legal theory, civil liability arises where an unlawful act or omission causes compensable harm and imposes upon the injuring party an obligation to make reparation (Jafari Langroudi, 1999). Unlike moral responsibility, which remains confined to conscience and ethical accountability, civil liability is enforced through coercive legal mechanisms and is contingent upon the existence of actual damage (Khorram-Abadi, 2012). Within Iranian legal thought, the concept of responsibility has historically been articulated through the notion of “guarantee” (ḍamān), emphasizing the obligation to restore loss irrespective of intent in certain circumstances (Gorji, 2001). This framework allows for the theoretical inclusion of governmental entities within the scope of civil liability, particularly where harm arises from the actions or omissions of public officials acting in an institutional capacity. The doctrinal separation between contractual and non-contractual liability further underscores that harm caused by digital obstruction—typically occurring outside any contractual relationship—falls squarely within the domain of tortious state responsibility.

The issue becomes more intricate when state immunity and the attribution of wrongful acts

are considered. Traditional approaches have often shielded governmental bodies from liability by categorizing harmful conduct as “sovereign acts,” thereby excluding them from judicial scrutiny. However, modern theories increasingly reject absolute immunity in favor of functional accountability. In Iranian law, although no comprehensive statute specifically addresses digital-era state liability, various legal provisions implicitly endorse governmental responsibility for harm caused by officials in the course of their duties. The constitutional model of judicial liability, particularly the principle that compensatory responsibility may shift to the state treasury where harm is not attributable to intentional misconduct, illustrates this evolving approach (Ibn Babawayh, 1355; Katouzian, 2001). From this perspective, the state may bear direct responsibility for systemic failures in digital infrastructure or administrative negligence that deprives individuals of lawful access to data. Such responsibility is reinforced by jurisprudential principles emphasizing that public benefit entails public burden, thereby requiring the state to compensate losses resulting from risks generated by public administration (Hashemi, 2007; Zargoush, 2011).

A comparative examination of English law reveals a more explicit and structured evolution away from sovereign immunity toward enforceable governmental accountability. Historically encapsulated in the maxim “the Crown can do no wrong,” English law gradually dismantled this doctrine through statutory and judicial developments, culminating in the recognition of civil actions against public authorities. Central to this transformation is the doctrine of misfeasance in public office, which establishes liability where public officials knowingly abuse power or act with reckless indifference to the rights of individuals. Alongside this, the expansion of administrative negligence and the concept of

duty of care has enabled courts to hold governmental bodies liable for failures to meet reasonable standards of care in the provision of public services. When applied to digital governance, these doctrines imply that unjustified disruption of access to data systems—whether through deliberate policy choices or negligent system management—may constitute actionable wrongdoing. The English approach thus frames digital accessibility as an operational obligation rather than a discretionary privilege, aligning liability with foreseeable harm and institutional responsibility.

The relevance of these principles becomes particularly evident in the context of the internet and information technologies, where the scale and sensitivity of data amplify the consequences of obstruction. Digital environments expose individuals to risks such as privacy violations, unauthorized data exploitation, and economic loss, all of which intensify the legal significance of access continuity (Hel-Foroush, 2003). Legal scholarship has consistently emphasized that internet-related harms must be addressed through the adaptation of traditional civil liability rules rather than the creation of entirely new legal categories (Desbois, 1966). The proliferation of electronic communications, online transactions, and automated administrative processes renders access disruptions potentially more damaging than analogous disruptions in the physical world. Moreover, the circulation of unsolicited electronic communications, reputational harm through online defamation, and the commodification of personal data demonstrate that digital harm often transcends national boundaries and temporal limitations (Samuelson, 1989; Zourden, 2003). Within this environment, state-imposed or state-enabled barriers to access acquire heightened legal relevance, as they may

exacerbate vulnerability and undermine trust in public administration.

The comparative analysis of Iranian and English legal frameworks therefore highlights a critical divergence in the treatment of state liability for digital obstruction. While Iranian law possesses doctrinal resources capable of supporting governmental responsibility, these resources remain underdeveloped in practice due to the persistence of broad immunity doctrines and the absence of explicit regulatory standards for digital accessibility. English law, by contrast, demonstrates a more mature integration of accountability mechanisms, grounding liability in duty of care and institutional fault rather than formal classifications of sovereign action. This contrast underscores the need for legal systems confronting digital transformation to recalibrate traditional doctrines in light of new modes of governance. Ensuring effective access to data and digital systems is no longer merely a matter of administrative efficiency but a legal imperative closely linked to civil liability, public trust, and the protection of fundamental rights.

In conclusion, the obstruction of access to data and digital systems represents a legally significant harm that challenges conventional boundaries between sovereign authority and civil accountability. As public administration becomes increasingly data-driven, the legal responsibility of the state must evolve accordingly, recognizing that digital accessibility is integral to the exercise of citizenship and the legitimacy of governance. The comparative insights drawn from English law illustrate that limiting state immunity and embracing liability grounded in duty of care does not undermine governmental authority but rather strengthens transparency, accountability, and public confidence in the digital age.

References

- Aalipour, H. (2011). *Criminal Law of Information Technology* (1st ed.). Khorsandi.
- Aghaeinia, H. (2008). *Crimes Against Persons* (4th ed.). Mizan Publishing.
- Aslani, H. R. (2005). *Information Technology Law* (1st ed.). Mizan Publishing.
- Baheri, M. (2005). *An Outlook on General Criminal Law* (2nd ed.).
- Banisar, D. (2000). *Privacy and Human Rights*. Electronic Information Center.
- Desbois, H. (1966). *Le Droit d'auteur en France* (2nd ed.). Dalloz.
- Gorji, A. (2001). *Fundamental Concepts of Civil and Criminal Law*. Majd Publications.
- Hashemi, M. (2007). *Constitutional Law of the Islamic Republic of Iran* (18th ed., Vol. 2). Mizan Publishing.
- Hel-Foroush, F. (2003). *Computer Crimes* Islamic Azad University, Science and Research Branch]. Tehran.
- Ibn Babawayh. (1355). *Man La Yahduruhu al-Faqih*. Islamiyah Publications.
- Jafari Langroudi, M. J. (1999). *Mabsut*. Ganj-e-Danesh.
- Katouzian, N. (2001). *General Rules of Contracts* (Vol. 4). Borna Publications.
- Khorram-Abadi, A. (2012). *Criminal Liability of Internet Service Providers (ISPs)* (1st ed.). Dadyar.
- Mir Mohammad Sadeghi, H. (2009). *Crimes Against Persons and Physical Integrity* (2nd ed., Vol. 1). Mizan Publishing.
- Saffar, M. J. (1994). Legal Personality. *Journal of personality*. <https://doi.org/10.1111/j.1467-6494.1994.tb00294.x>
- Samuelson, P. (1989). Can hackers be sued for damage caused by computer viruses? *Communications of the Acm*, 32(6), 666-700.
- Zargoush, M. (2011). *An Analytical-Comparative Study of the State's Civil Liability* (1st ed.). Mizan Publishing.
- Zeraat, A. (2013). *A Concise Commentary on the Islamic Penal Code 2013* (1st ed.). Ghoghnoos Publishing.
- Zourden, P. (2003). *Principles of Civil Liability*. Mizan Publishing.