مرکز پژوهش‌های مجلس شورای اسلامی
دفتر مطالعات انرژی، صنعت و معدن
مسلسل: ۲۱۷۰۴ ■ تیر ۱۴۰۵

مروری بر چالش‌ها و راهکارهای سیاستی ارتقای امنیت سایبری در ایران با رویکرد تطبیقی (با تمرکز بر موضوع نقض داده)

تاریـــخ انتشـــار: ۱۴۰۵/۴/۳۰
Publish Date : 2026/07/21

عنـوان: مروری بـر چالش‌هـا و راهکارهـای سیاسـتی ارتقای امنیـت سـایبری در ایران بـا رویکرد تطبیقی (با تمرکز بر موضوع نقض داده)

تهیـه و تدوین کنندگان (Authors) : سیدمسـعود شـریفی، امیـد زند کریمخانی، محمدحسـن هدایتی (گروه مخابرات و فناوری اطلاعات)

واژه‌های کلیدی: امنیت سایبری، حفاظت از داده‌های شخصی، اقتصاد دیجیتال

ناشـر: مرکزپژوهش‌های مجلس شـورای اسلامی

DOI: https://doi.org/10.22034/mrc.report.21704
Permanent Link:
Publisher : Islamic Parliament Research Center of Iran

شماره مسلسل: ۲۱۷۰۴
کد موضوعی: ۳۱۰

عنوان: مروری بر چالش‌ها و راهکارهای سیاستی ارتقای امنیت سایبری در ایران با رویکرد تطبیقی (با تمرکز بر موضوع نقض داده)

نوع گـزارش: طرح☐ لایحه☐، نظارتی☐، راهبردی■، پیش‌نویس قانونی☐

نام دفتر: مطالعات انرژی، صنعت و معدن (گروه مخابرات و فناوری اطلاعات)

اظهار نظر کنندگان: بهادر غلامی (مدیر گروه امنیتی)، سیدمحسن علوی‌منش (مشاور معاونت پژوهش های تولیدی و زیربنایی)

همکار: حسین عزیزی (گروه مخابرات و فناوری اطلاعات)

ناظران علمی: میلاد بیگی، حبیب‌اله ظفریان

گرافیک و صفحه آرایی: نفیسه حاجی‌صفری

ویراستارادبی: زهرا کریمی

تاریخ شروع مطالعه: ۱۴۰۲/۱۰/۰۱

دفترمطالعات‌انرژی، صنعت‌ومعدن

فهرست مطالب

فهرست جداول

مروری بر چالش‌ها و راهکارهای سیاستی ارتقای امنیت سایبری در ایران با رویکرد تطبیقی

(با تمرکز بر موضوع نقض داده)

چکیده

امنیت سایبری در دنیای دیجیتالی امروز یکی از مهم‌ترین چالش‌های پیش روی دولت‌ها، سازمان‌ها و کاربران است. در ایران، حمله‌های سایبری و نشت داده‌های گسترده در سال‌های اخیر به یکی از معضلات اساسی تبدیل شده که نه تنها حریم خصوصی میلیون‌ها کاربر، بلکه امنیت اطلاعات سازمان‌ها و زیرساخت‌های حیاتی کشور را به‌شدت تهدید کرده است. این گزارش، نمونه‌های برجسته‌ای از حمله‌های سایبری به سازمان‌ها و شرکت‌های ایرانی مانند اسنپ‌فود، تپسی، شبکه بانکی و شرکت‌های بیمه را تحلیل می‌کند. در این بررسی‌ها، علاوه‌بر پیامدهای اقتصادی، اجتماعی و اعتباری این حمله‌ها، به ضعف‌های زیرساختی، قانونی و مدیریتی در حوزه امنیت سایبری کشور نیز توجه شده است. مهم‌ترین یافته‌های این گزارش نبود قوانین جامع و نهادهای نظارتی مستقل، ضعف در اطلاع‌رسانی شفاف، نبود استانداردهای اجباری برای حفاظت از داده‌ها و کمبود نیروی انسانی متخصص است. همچنین، مشکلاتی مانند هزینه بالای سرمایه‌گذاری در امنیت سایبری برای شرکت‌های کوچک و متوسط، ضعف زیرساخت‌های فناوری اطلاعات و آسیب‌پذیری در برابر تحریم‌ها و فیلترینگ نیز در این تحلیل‌ها برجسته شده است.

برای مقابله با این چالش‌ها و کاهش آثار مخرب حمله‌های سایبری، پیشنهادهایی مانند ایجاد قانون جامع حفاظت از داده‌ها، تقویت نظارت و الزام‌های امنیتی، توسعه برنامه‌های آموزشی برای تربیت نیروی کار متخصص، ارائه مشوق‌های مالی برای ارتقای زیرساخت‌های امنیتی و الزام به بیمه امنیت سایبری ارائه شده است. علاوه‌بر این، گزارش بر اهمیت همکاری‌های بین‌المللی، ایجاد شفافیت در اطلاع‌رسانی نقض‌های داده و تقویت آگاهی عمومی کاربران نسبت به حفاظت از اطلاعات شخصی تأکید دارد.

خلاصه مدیریتی

بیان / شرح مسئله

در عصر دیجیتال کنونی، امنیت سایبری یکی از مهم‌ترین الزام‌های حفظ ثبات اقتصادی، اجتماعی و سیاسی جوامع است. این اهمیت به‌ویژه در کشورهایی مانند ایران که زیرساخت‌های فناوری اطلاعات آنها به‌سرعت در حال گسترش است، دوچندان می‌شود. طی سال‌های اخیر، حمله‌های سایبری متعدد به شرکت‌ها، نهادهای دولتی و زیرساخت‌های حیاتی ایران، به نشت داده‌های حساس میلیون‌ها شهروند و کاربر منجر شده است. ازجمله این حمله‌ها هک سامانه‌های بانکی، شرکت‌های بیمه، ثبت احوال، پلتفرم‌های تاکسی اینترنتی و خدمات سفارش غذاست.

این حمله‌ها نه‌تنها اطلاعات شخصی کاربران، بلکه امنیت اقتصادی و ملی را نیز تحت تأثیر قرار داده است. برای مثال، در هک یکی از سکوهای خدمات، اطلاعات بیش از ۲۰ میلیون کاربر شامل جزئیات سفارش‌ها و شماره تماس افراد درز پیدا کرد. در حمله به شبکه بانکی و صرافی‌های رمزارز طی جنگ ۱۲ روزه رژیم صهیونیستی بر علیه ایران، اطلاعات مالی میلیون‌ها مشتری تهدید شد و پیش از این نیز شرکت‌های بیمه با افشای داده‌های حساس مربوط به بیمه‌گذاران مواجه شدند. چنین حوادثی باعث کاهش اعتماد عمومی به سیستم‌های دیجیتالی، تضعیف اعتبار سازمان‌ها و حتی آسیب به زیرساخت‌های اقتصادی کشور می‌شود.

بر این اساس، بسیاری از سازمان‌ها و شرکت‌ها در ایران، زیرساخت‌ها و سیاست‌های مناسبی برای مقابله با حمله‌های سایبری ندارند. ضعف نظارت قانونی، نبود قوانین جامع حفاظت از داده‌ها، کمبود نیروی انسانی متخصص در حوزه امنیت سایبری و نبود شفافیت در اطلاع‌رسانی نقض‌های داده از دلایل اصلی گسترش این معضل هستند. در بسیاری از موارد، سازمان‌ها حتی پس از وقوع حمله، اقدام‌های لازم برای تقویت امنیت سایبری خود را انجام نمی‌دهند.

نقطه‌نظرات / یافته‌های کلیدی

در این گزارش، چندین نمونه از حمله‌های سایبری گسترده در ایران و جهان بررسی شـــده که نتایج زیر را به‌عنوان یافته‌های کلیدی ارائه می‌دهد:

- **وسعت و پیامد حمله‌های سایبری**: حمله‌های اخیر در ایران دامنه گسترده‌ای داشـــته و باعث آسیب سازمان‌های دولتی و خصوصی متعددی شده است. حمله به سامانه ثبت احوال و هک سامانه‌های بانکی که اطلاعات هویتی و داده‌های حساس میلیون‌ها نفر را در معرض خطر قرار داد، نشان‌دهنده آسیب‌پذیری شدید زیرساخت‌های امنیتی در کشور اســـت. در مواردی مانند حمله به شرکت‌های بیمه، حتی اطلاعات پزشکی و بیمه‌ای افراد نیز درز پیدا کرده است.
- **ضعف در اطلاع‌رسانی و پاسخگویی**: بسیاری از سازمان‌ها پس از حمله‌های سایبری، اطلاع‌رسانی شفافی درباره جزئیات نقض داده‌ها و اقدام‌های انجام شده ندارند. در موارد متعددی، کاربران نهایی حتی از وقوع حمله آگاه نشده و نمی‌توانند اقدام‌های لازم را برای حفاظت از اطلاعات خود انجام دهند.
- **نبود قوانین جامع و نهادهای نظارتی مستقل**: یکی از دلایل اصلی گسترش این مشکلات، فقدان قوانین جامع حفاظت از داده‌ها در ایران است. در بسیاری از کشورها، قوانینی مانند GDPR در اتحادیه اروپا یا CCPA در ایالات متحده، شرکت‌ها را ملزم به رعایت استانداردهای سخت‌گیرانه امنیت داده‌ها می‌کنند و در صورت نقض، جریمه‌های سنگینی در نظر می‌گیرند. در ایران، چنین قوانین جامعی وجود ندارد و نهادهای نظارتی نیز قدرت و اختیار کافی برای مقابله با تخلف‌ها را ندارند.
- **کمبود نیروی انسانی متخصص**: امنیت سایبری به نیروی انسانی متخصص و آموزش‌دیده نیاز دارد. در ایران، کمبود چنین افرادی باعث

شده که بسیاری از سازمان‌ها نتوانند به‌درستی با تهدیدهای ســـایبری مقابله کنند. این مشکل به‌ویژه در سازمان‌های دولتی و شرکت‌های کوچک و متوسط به‌وضوح دیده می‌شود.

- **عدم مسئولیت‌پذیری سازمان‌ها:** بسیاری از شرکت‌ها و سازمان‌ها پس از حمله‌های سایبری، هیچ‌گونه اقدام مؤثری برای جبران خسارت کاربران انجام نمی‌دهند. در کشورهای دیگر، شرکت‌ها موظف به پرداخت خسارت یا ارائه خدمات اضافی به کاربران آسیب‌دیده هستند، اما در ایران، این مسئولیت‌پذیری وجود ندارد.

پیشنهاد راهکارهای تقنینی، نظارتی یا سیاستی

برای مقابله با مشکل‌های امنیت سایبری و بهبود وضعیت حفاظت از داده‌ها در ایران، مجموعه‌ای از راهکارهای تقنینی، نظارتی و سیاستی پیشنهاد می‌شود:

۱. ایجاد قانون جامع حفاظت از داده‌ها: با تصویب یک قانون جامع و شـــفاف در خصوص کاربران، شرکت‌ها و نهادهای نظارتی حقوق و مسئولیت‌های تمامی ذی‌نفعان مشخص می‌شود. این قانون باید شامل الزام‌هایی برای حفاظت از داده‌ها، جریمه‌های سنگین برای تخلف‌ها و استانداردهای سخت‌گیرانه برای ذخیره و پردازش داده‌ها باشد.

۲. ایجاد نهاد مستقل حفاظت از داده‌ها: تأسیس یک نهاد مستقل برای نظارت بر حفاظت از داده‌ها و تحقیق درباره نقض‌های امنیتی، بسیار ضروری است. این نهاد باید قدرت اجرایی کافی برای تحقیق، جریمه و تعقیب قانونی متخلفان داشته باشد.

۳. افزایش شفافیت در اطلاع‌رسانی: الزام سازمان‌ها در اطلاع‌رسانی سریع و شفاف به کاربران و نهادهای نظارتی در صورت وقوع نقض داده‌ها، یکی از اقدام‌های ضروری است. این اطلاع‌رسانی باید شامل جزئیات نوع داده‌های فاش‌شده، اقدام‌های انجام‌شده و توصیه‌های حفاظتی برای کاربران باشد.

۴. الزام به ممیزی‌های امنیتی: سازمان‌ها باید به انجام ممیزی‌های منظم امنیت سایبری توسط شرکت‌های شخص ثالث معتبر ملزم شوند. این ممیزی‌ها باید شامل ارزیابی زیرساخت‌های امنیتی، پروتکل‌های مدیریت داده و استانداردهای رمزنگاری باشد.

۵. ترویج بیمه امنیت سایبری: شرکت‌ها باید ملزم به خرید بیمه امنیت سایبری شوند تا در صورت وقوع حمله‌ها، بتوانند خسارت‌های مالی و حقوقی کاربران را جبران کنند. همچنین ارائه تخفیف‌های بیمه برای شرکت‌هایی که اقدام‌های امنیتی پیشرفته‌تری را اجرا می‌کنند، می‌تواند مشوقی برای بهبود امنیت سایبری باشد.

۶. آموزش و توسعه نیروی انسانی: سرمایه‌گذاری در آموزش و تربیت نیروی کار متخصص در حوزه امنیت سایبری ضروری است. دولت باید با همکاری دانشگاه‌ها و بخش خصوصی، برنامه‌های آموزشی جامع و مشوق‌های مالیاتی برای شرکت‌ها ارائه دهد.

۷. مشوق‌های مالی برای شـــرکت‌ها: ارائه کمک‌های مالی، وام‌های کم‌بهره و معافیت‌های مالیاتی برای شـــرکت‌هایی که در ارتقای زیرساخت‌های امنیتی خود سرمایه‌گذاری می‌کنند، نقش مهمی در بهبود امنیت سایبری دارند.

۸. تقویت همکاری‌های بین‌المللی: همکاری با سازمان‌ها و نهادهای بین‌المللی در حوزه امنیت سایبری می‌تواند به اشتراک‌گذاری دانش، تجربه‌ها و فناوری‌های پیشرفته کمک کند. این همکاری‌ها باید بر رفع موانع ناشی از تحریم‌ها و فیلترینگ تمرکز داشته باشد.

۹. استفاده از فناوری‌های پیشرفته: الزام سازمان‌ها به استفاده از فناوری‌هایی مانند هوش مصنوعی برای شناسایی و پاسخگویی سریع به تهدیدهای سایبری، می‌تواند به بهبود امنیت دیجیتالی کمک کند.

۱۰. ایجاد برنامه‌های واکنش به حوادث: طراحی و پیاده‌ســـازی برنامه‌هـــای جامع واکنش به حوادث ســـایبری و برگزاری تمرین‌ها و رزمایش‌های دوره‌ای برای آمادگی در برابر حمله‌های احتمالی ضروری است.

۱. مقدمه

پس از هک داده‌های یکی از سکوهای ارائه خدمات برخط در حوزه سفارش غذا و دزدیده‌شدن اطلاعات بیش از ۲۰ میلیون کاربر و حدود ۸۸۰ میلیون سفارش [۱]، باید توجه کرد که اطلاعات هر یک از افراد و سازمان‌ها مانند نام، شماره تلفن، نشانی، سابقه تراکنش‌های مالی، پیام‌های شخصی، تاریخچه پزشکی، خریدهای اینترنتی، سفرها، فهرست مشتریان و اسرار شرکت در پایگاه‌های داده گوناگون ذخیره شده است. تهدیدهای سایبری برای دسترسی به این داده‌ها با اهداف گوناگون مالی، جاسوسی، سیاسی، ایجاد اختلال و... بیش از گذشته این حجم داده را تهدید می‌کند. امروزه میلیاردها رکورد از اطلاعات گوناگون در معرض خطر و در دسترس عموم قرار گرفته است که هرکدام می‌توانند تهدیدی بالقوه باشند. تأمین امنیت و محافظت از داده‌ها به یکی از اقدام‌های مهم و ضروری برای اشخاص، سازمان‌ها و دولت‌ها تبدیل شده است.

نقض داده[1] و نشت داده[2] از مهم‌ترین تهدیدهای امنیتی هستند که می‌توانند نتیجه حمله‌های مخرب مجرمان سایبری، تهدیدها و افشای اطلاعات کارمندان یا حتی خطاهای ساده انسانی باشند. درنتیجه بر اثر آن‌ها فرد، افراد یا سازمان‌های غیرمجاز به داده‌های حساس، محافظت‌شده یا محرمانه دسترسی پیدا می‌کنند و در معرض مشاهده، کپی، انتقال، حذف یا انتشار قرار می‌گیرند.

پیامدهای نقض و نشت داده دارای ابعاد متفاوتی است. برای افراد، می‌تواند به سرقت هویت، ضرر مالی، تهدید، اخاذی و تجاوز به حریم شخصی منجر شود؛ در سازمان‌ها می‌تواند با کاهش ارزش سهام و اعتبار همراه باشد و برای دولت‌ها نیز خطرهای زیرساختی و امنیتی در پی خواهد داشت. جبران این خسارت‌ها و غرامت‌های نظارتی و بازیابی دوباره اعتبار و اعتماد مشتریان و کاربران (تا حدی که امکانش وجود دارد) می‌تواند هزینه‌های هنگفتی در پی داشته باشد و نیازمند سال‌ها زمان بوده که گاهی از توان برخی سازمان‌ها خارج است به کوچک‌شدن سهم آن‌ها از بازار یا فروش اجباری به رقبا منجر می‌شود.

هر مورد نقض و نشت داده میلیون‌ها نفر را تحت تأثیر قرار می‌دهد و امنیت یا اعتماد به نهادها و دولت‌ها را تضعیف می‌کند و پایه و اساس یک جامعه دیجیتالی را که برمبنای اعتماد و امنیت ساخته شده، از بین می‌برد. بنابراین، توجه به افشای داده، پیشگیری و جبران آن اهمیت دارد که باید در دستور کار سیاستگذاران و تنظیم‌گران، نه فقط به‌صورت واکنشی و پسینی، بلکه به‌صورت پیش‌دستانه و پیشینی باشد زیرا برای تأمین امنیت کشور، نهادها و شهروندان ضروری است.

در این گزارش، با مرور برخی از بزرگ‌ترین نمونه‌های نقض و نشت داده در دنیا و ایران، به دلایل، تأثیرات، شیوه‌های مواجهه با آن‌ها و اقدام‌های قانونی صورت گرفته پرداخته می‌شود تا با مقایسه این رخدادها در ایران و دیگر کشورها، درس‌هایی برای محافظت از داده و حریم خصوصی کاربران، سازمان‌ها و امنیت زیرساخت‌های ملی حاصل شود.

1. Data Breach
2. Data Leak

۲. نقض و نشست داده، بررسی تفاوت‌های فنی و حقوقی

برخلاف اینکه اصطلاح نقض داده (Data Breach) و نشـــت داده (Data Leak) در کشـــور ما اغلب به یک معنا و به‌جای یکدیگر استفاده می‌شوند، این دو مورد پدیده‌های متمایزی هستند که هر دو به فاش‌شدن اطلاعات حساس منجر می‌شوند و از لحاظ فنی و حقوقی تفاوت‌های مهمی دارند و علل و پیامدهای آن‌ها متفاوت است. درک این تفاوت‌ها برای پیاده‌سازی اقدام‌های امنیتی و همچنین مواجهه با این رخدادها حیاتی است.

نقض داده یک نفوذ عمدی و ناشی از حمله سایبری است و زمانی رخ می‌دهد که افراد غیرمجاز از راه هک، فیشینگ یا دیگر فعالیت‌های مخرب به سیستم‌های کامپیوتری، شبکه‌ها یا پایگاه‌های داده نفوذ کرده و به اطلاعات محرمانه و محافظت‌شده دسترسی پیدا می‌کنند. تمرکز اصلی در نقض داده، دسترسی غیرمجاز به داده است.

در نشت داده، معمولاً داده‌ها به‌طور غیرعمدی یا تصادفی فاش می‌شوند و در دســـترس افراد غیرمجاز قرار می‌گیرند. در اینجا، خطای انسانی، تنظیمات و پیکربندی اشتباه سیستم‌ها و پایگاه‌های داده یا حتی گم‌شدن دستگاه حاوی اطلاعات یا رمزهای عبور می‌تواند از دلایل نشت باشد. برای مثل ممکن است ایمیل حاوی اطلاعات حساس به نشانی اشتباه ارسال شود، یا یک سند حساس در یک سرور ابری عمومی در دسترس قرار گیرد. عواقب نشـــت داده می‌تواند به اندازه نقض داده مضر باشد و به سرقت هویت، خسارت‌های مالی و آسیب به اعتبار منجر شود.

در این گزارش با بررسی چندین مورد از بزرگ‌ترین نمونه‌های نقض و نشت داده، به بررسی دلایل، پیامدها، شیوه‌های مواجهه و اقدام‌های قانونی در قبال آن‌ها می‌پردازیم.

چند مورد از بزرگ‌ترین نمونه‌های نقض و نشت داده عبارت‌اند:

۱. یاهو (اکتبر ۲۰۱۷):[1] یاهو پس از چهار سال اعلام کرد که یک نقض داده در اوت ۲۰۱۳ توسط گروهی از هکرها انجام شده و ۳ میلیارد حساب را تهدید کرده اســـت. این رخداد یکی از بزرگ‌ترین نقض‌های داده در تاریخ بود که اعتماد کاربران به این سرویس را به‌شدت خدشه‌دار کرد.

۲. نقض داده ادهار[2] هند (مارس ۲۰۱۸): جزئیات اطلاعات شـــخصی بیش از یک میلیارد شهروند هندی که در بزرگ‌ترین پایگاه داده بیومتریک جهان ذخیره شده بود، به‌صورت آنلاین در معرض فروش قرار گرفت.

۳. ادوارد اسنودن (۲۰۱۳):[3] افشـــای اطلاعات محرمانه آژانس امنیت ملی آمریکا (NSA) توسط کارمند سابق، ادوارد اسنودن، یکی از گسترده‌ترین نشت‌های اطلاعات طبقه‌بندی‌شده در تاریخ بود. این افشـــاگری بحث‌های گسترده‌ای را درباره حقوق حریم خصوصی و نظارت دولتی برانگیخت.

۴. فیس‌بوک (۲۰۱۹):[4] در این نقض، اطلاعات شخصی حدود ۵۴۰ میلیون کاربر فیس‌بوک مانند نام، شماره تلفن و نشانی افشا شد. این رخداد به تحقیقات گسترده، جریمه‌های سنگین و انتقادهای شدید از این رسانه اجتماعی بزرگ منجر شد.

۵. اکوئیفکس (۲۰۱۷):[5] نقض اطلاعات اعتباری شرکت اکوئیفکس تقریباً ۱۴۷ میلیون آمریکایی را تحت تأثیر قرار داد و شامل شماره‌های تأمین اجتماعی، تاریخ تولد و نشـــانی بود. این رخداد پیامدهای مالی عظیمی برای افراد داشت و باعث نگرانی‌های جدی در مورد امنیت داده‌های مالی شد.

1. Yahoo
2. Aadhaar
3. Edward Snowden
4. Facebook
5. Equifax

۶. ماریوت اینترنشنال (۲۰۱۸):[1] در این نقض، اطلاعات شخصی بیش از ۳۳۹ میلیون مهمان از هتل‌های زنجیره‌ای ماریوت مانند نام، نشانی، شماره پاسپورت و اطلاعات کارت اعتباری به سرقت رفت. این رخداد نشان‌دهنده آسیب‌پذیری سیستم‌های رزرواسیون هتل‌ها در برابر حمله‌های سایبری بود.

۷. کپیتال وان (Capital One) (۲۰۱۹): در این نقض، اطلاعات شخصی بیش از ۱۰۰ میلیون نفر از مشتریان این شرکت خدمات مالی مانند شماره‌های تأمین اجتماعی و اطلاعات حساب بانکی به خطر افتاد. این رخداد نگرانی‌ها در مورد ایمنی سیستم‌های مالی آنلاین را افزایش داد.

۸. کم ۴ (مارس ۲۰۲۰):[2] این وب‌سایت مخصوص پخش ویدیوی جنسی بزرگسالان بود که نه به‌دلیل حمله سایبری بلکه بر اثر یک اشتباه در پیکربندی سرور خود، نزدیک به ۱۱ میلیارد رکورد از اطلاعات آن فاش شد و باعث رسوایی‌های فراوان و بزرگی شد و اطلاعات حساسی مانند نام کامل، نشانی ایمیل، تمایل‌های جنسی، سابقه چت و گزارش پرداخت افراد منتشر شد.

۹. ترلو (ژانویه ۲۰۲۴):[3] داده‌های ۱۵ میلیون کاربر از پلتفرم مدیریت پروژه ترلو در دارک‌وب منتشر شد.

۱۰. مایکروسافت پاور اپز (۲۰۲۱):[4] یک اشتباه در پیکربندی این نرم‌افزار، به دسترسی غیرمجاز به منابع حساس منجر شد و حجم زیادی از داده‌ها را فاش کرد.

۱۱. پاناما پیپرز (۲۰۱۶):[5] نشت بیش از ۱۱ میلیون سند از یک شرکت حقوقی پانامایی، فعالیت‌های مالی برون‌مرزی افراد ثروتمند و قدرتمند در سراسر جهان را به نمایش گذاشت. این اسناد به افزایش فساد و نظارت بر پناهگاه‌های مالیاتی چندین کشور منجر شد.

۱۲. پارادایز پیپرز (۲۰۱۷):[6] با نشت ۱۳٫۴ میلیون سند از دو شرکت خدمات مالی، جزئیات سرمایه‌گذاری‌های برون‌مرزی بسیاری از شخصیت‌های مشهور، سیاستمداران و شرکت‌های چندملیتی فاش شد. این نشت نشان داد که چگونه افراد و سازمان‌های ثروتمند می‌توانند از قوانین مالی برای کاهش مالیات و پنهان کردن دارایی‌هایشان استفاده کنند.

۱۳. فیس‌بوک کمبریج آنالیتیکا (۲۰۱۸):[7] نشت اطلاعات شخصی میلیون‌ها کاربر فیس‌بوک به شرکت مشاوره سیاسی کمبریج آنالیتیکا، نگرانی‌هایی را در مورد استفاده از داده‌های شخصی برای مقاصد سیاسی و دستکاری انتخابات ایجاد کرد.

۱۴. ویکی‌لیکس (۲۰۱۰ تاکنون):[8] وب‌سایت افشاگر ویکی‌لیکس طی سال‌های گذشته اسناد و اطلاعات محرمانه دولتی و سازمانی متعددی را منتشر کرده که به افزایش آگاهی عمومی از فعالیت‌های دولت‌ها و شرکت‌ها شده است. با این حال، منتقدان ویکی‌لیکس استدلال می‌کنند که انتشار این اطلاعات می‌تواند به امنیت ملی و منافع عمومی کشور آسیب برساند.

1. Marriott International
2. CAM4
3. Trello
4. Microsoft Power Apps
5. Paradise Papers
6. Paradise Papers
7. Facebook Cambridge Analytica
8. WikiLeaks

۳. بررسی نمونه‌های خارجی

۳-۱. گزارش موردی: فیس‌بوک

فیس‌بوک در درجه اول به‌عنوان یک پلتفرم رسانه اجتماعی شناخته می‌شد. در ۳ آوریل ۲۰۲۱، گزارشی مبنی‌بر انتشار اطلاعات شخصی کاربران فیس‌بوک در یک فروم هک سطح پایین اعلام شد. این نشـــت داده مربوط به سال ۲۰۱۹ بوده و داده‌های افشاشده شامل اطلاعات شخصی بیش از ۵۳۳ میلیون کاربر فیس‌بوک از ۱۰۶ کشور جهان است که شـــامل بیش از ۳۲ میلیون کاربر در ایالات متحده، ۱۱ میلیون کاربر در بریتانیا و ۶ میلیون کاربر در هند است. این داده‌ها شامل شماره تلفن، شناسه فیس‌بوک، نام کامل، مکان، تاریخ تولد، و در برخی موارد آدرس ایمیل آن‌هاست.

یکی از سخن‌گویان فیس‌بوک اعلام کرده بود که داده‌ها به‌دلیل یک آسیب‌پذیری که این شرکت در سال ۲۰۱۹ اصلاح کرده بود، استخراج شده است [۲]. به گفته آلون گال، مدیر ارشد فناوری شرکت اطلاعات جرائم سایبری هادسون راک که اطلاعات فاش شده را کشف کرد [۳]، با اینکه چند سال از عمر داده‌های لو رفته می‌گذشت، هکرها می‌توانستند از داده‌ها برای جعل هویت افراد و ارتکاب کلاهبرداری استفاده کنند. تا اکتبر ۲۰۲۳ این آخرین نشت داده برای این شرکت بود [۴]. هرچند که پیش از آن بارها دچار نقض حریم خصوصی کاربران و نشت داده شده بود.

۳-۱-۱. اعلامیه‌های رسمی [۵]

سه روز بعد از گزارش رسانه اینسایدر،[1] فیس‌بوک طی اطلاعیه‌ای تأیید کرد که اطلاعات بیش از ۵۳۰ میلیون کاربر افشا شده است. فیس‌بوک تصریح کرد که داده‌ها از طریق هک سیستم به دست نیامده‌اند، بلکه قبل از سپتامبر ۲۰۱۹ از این پلتفرم استخراج شده‌اند.

استخراج داده تاکتیکی است که طی آن سیستم خودکار، اطلاعات موجود در یک پلتفرم را برمی‌دارد. این آسیب‌پذیری در سال ۲۰۱۹ کشف و گزارش شد [۶]. فیس‌بوک در همان سال تغییرهایی اعمال کرد و سپس اطمینان داد که در نتیجه اقدامی که انجام داده این آسیب دیگر وجود ندارد.

در ادامه اطلاعیه، این شرکت به شرح اتفاق، منبع آسیب‌پذیری (سرویس واردکننده مخاطب که کمک می‌کرد افراد دوستان خود را با استفاده از فهرســـت مخاطبین خود پیدا کنند)، اقدام‌های خود در قبال این اتفاق، نوع اطلاعات فاش‌شده (که فاقد اطلاعات مالی یا رمز عبور بوده)، توصیه‌هایی برای ایمن نگه داشتن حساب کاربری (به‌روزکردن تنظیمات حریم خصوصی، احراز هویت دومرحله‌ای) پرداخته است. فیس‌بوک بر تعهد خود برای رسیدگی به چنین مسائلی تأکید کرد، و اظهار داشت که فعالانه برای حذف داده‌های افشاشده و پیگیری اقدام‌های قانونی علیه سوءاستفاده‌کنندگان، تلاش می‌کند.

۳-۱-۲. تعداد افراد تحت تأثیر

اطلاعات ۵۳۳ میلیون کاربر فیس‌بوک در ۱۰۶ کشور، شامل: بیش از ۳۲ میلیون کاربران در ایالات متحده، ۱۱ میلیون کاربر در بریتانیا و ۶ میلیون کاربر در هند افشا شده است.

۳-۱-۳. داده‌های لورفته

داده‌ها شامل شماره تلفن، نام کامل، مکان، برخی از آدرس‌های ایمیل، سایر جزئیات از پروفایل کاربر مانند تاریخ تولد و اطلاعات بیوگرافی هستند. این اطلاعات شامل اطلاعات مالی، سلامت یا رمز عبور نیست [۷].

۳-۱-۴. اقدام‌های سازمان

فیس‌بوک تغییراتی در سرویس واردکننده مخاطب اعمال کرد و تکنیک‌هایی را برای جلوگیری از دسترسی غیرمجاز و استخراج اطلاعات کاربر از پلتفرم به‌کار گرفت. همچنین این شرکت نظارت بر تهدیدهای احتمالی و تطبیق اقدام‌های امنیتی خود را در دستور کار قرار داد. این

1. Insider

شرکت اعلام کرد همکاری‌های لازم را با نهادهای قانونی انجام داده است.

یکی از انتقادهای واردشده به فیس‌بوک پس از این اتفاق، عدم اطلاع‌رسانی به تک‌تک کاربران بود. طبق گفته سخنگوی این شرکت، فیس‌بوک برای اطلاع‌رسانی به کاربران، این واقعیت را می‌سنجد که اطلاعات به‌صورت عمومی در دسترس است و این مشکلی نیست که کاربران بتوانند خودشان آن را برطرف کنند[۸].

۵-۱-۳. اثر اتفاق بر شرکت

پس از افشای این نشت داده، نگرانی کاربران از امنیت خود در این پلتفرم افزایش یافت و صحبت‌هایی برای پاک‌کردن این شبکه اجتماعی و ترک آن انجام شد[۹]. همچنین پس از اعلام این نشت، ترافیک سایتی[۱۰] نشان‌دهنده نگرانی کاربران بود تا بفهمند آیا داده‌های آنها نیز افشا شده است یا خیر؟[۱۱]

نشت اخیر داده‌ها از فیس‌بوک، به‌علت خلف وعده این شرکت در مهار استخراج انبوه اطلاعات (پس از رسوایی کمبریج آنالیتیکا)،[1] بازتاب گسترده‌ای داشت. با توجه به سابقه استخراج اطلاعات ۸۰ میلیون کاربر در پرونده مذکور برای اهداف سیاسی، این اتفاق مجدداً بحث‌ها درباره امنیت داده‌های کاربران را به کانون توجه بازگردانده و نگرانی‌ها از بهره‌برداری غیرمجاز از اطلاعات شخصی را افزایش داده است[۲].

رسوایی فیس‌بوک در این مورد به‌شدت بر محبوبیتش تأثیر گذاشت به‌نحوی که به گفته شرکت تحلیلی- تجاری میکس‌پنل،[2] از آوریل ۲۰۱۸، اولین ماه کامل پس از انتشار خبر رسوایی کمبریج آنالیتیکا، لایک (پسندیدن) و اشتراک‌گذاری پست‌ها در فیس‌بوک تقریباً ۲۰ درصد کاهش یافت[۱۲]. همچنین ای‌مارکتر،[3] کاهش استفاده از فیس‌بوک در ایالات متحده را گزارش کرد و گفت که کاربران معمولی فیس‌بوک ۳۸ دقیقه در روز را در سایت می‌گذرانند که نسبت به سال ۲۰۱۷ که این مقدار ۴۱ دقیقه بوده، کاهش یافته است[۱۳] [۱۲]. حرکت جمعی با هشتگ #DeleteFacebook از جمله دیگر آثار این اتفاق بود[۱۴].

برای این رسوایی داده‌ای، در ۲۶ مارس ۲۰۱۸، یک هفته پس از انتشار اولیه ماجرا، سهام فیس‌بوک حدود ۲۴ درصد معادل ۱۳۴ میلیارد دلار کاهش یافت[۱۵].

پس از این رخداد، فیس‌بوک مجموعه‌ای از اقدام‌های فنی فوری و ساختاری را برای ارتقای امنیت پیاده‌سازی کرد. این اقدام‌ها شامل غیرفعال‌سازی قابلیت آسیب‌پذیر «View As»، بازنشانی توکن‌های دسترسی حدود ۹۰ میلیون کاربر و خارج کردن آنها از حساب و اجبار به واردشدن مجدد بود. در ادامه، فیس‌بوک سیاست‌های دسترسی توسعه‌دهندگان به APIها را به‌ویژه در ارتباط با اطلاعات گروه‌ها محدود و بازنگری کرد. همچنین برنامه پاداش‌یابی باگ‌ها[4] توسعه یافت تا گزارش آسیب‌پذیری‌ها در حوزه‌های جدید، شامل خدمات ثالث را پوشش دهد[۱۶] [۱۷].

۶-۱-۳. دعاوی جمعی

فیس‌بوک در طول سالیان فعالیتش دچار نشت داده‌های متعددی شده و پرونده‌های دعاوی جمعی متعددی علیه این شرکت مطرح شده است. در خصوص نشت داده‌ها در سال ۲۰۱۹ از طریق بخش واردکننده مخاطب، که در سال ۲۰۲۱ رسانه‌ای شد، شکایت جمعی صورت نگرفت اما این شرکت از سوی قانونگذاران جریمه مالی شد.

در پرونده نقض حریم خصوصی مربوط به رسوایی کمبریج آنالیتیکا، از سوی سهام‌داران یک دعوی جمعی انجام شد که در آن مدعی بودند قیمت سهام این شرکت طی دو هفته بیش از ۱۸ درصد کاهش داشته و بیانیه‌هایی که توسط فیس‌بوک و مدیران آن منتشر شده بر قیمت سهام تأثیرگذار بوده است. این دعوی از سمت قاضی به‌دلیل کمبود ادله شاکیان در اثبات ادعایشان مبنی بر آگاه‌بودن مدیران از این اتفاق، رد شد[۱۸].

1. Cambridge Analytica
2. Mixpanel
3. EMarketer
4. Bug Bounty

پرونده دیگری علیه فیس‌بوک و مدیران این شرکت به اتهام سهل‌انگاری در محافظت از حریم خصوصی داده‌های کاربران به جریان افتاد[۱۹][۲۰]. در کانادا نیز پرونده‌ای متشکل از همه افرادی که در کانادا زندگی می‌کردند، تشکیل شد و حساب فیس‌بوک آن‌ها در نتیجه نقض داده در معرض خطر بود[۲۱].

پیرو افشای نشت داده در آوریل ۲۰۲۱، برای کسانی که در اتحادیه اروپا یا منطقه اقتصادی اروپا زندگی می‌کردند، امکانی ایجاد شد که بتوانند از فیس‌بوک خسارت مالی دریافت کنند. قوانین کلی حفاظت از داده‌های اروپا (GDPR)[1] این حق را می‌دهد که درصورت نقض حقوق حفاظت از داده‌ها، افراد غرامت پولی نیز دریافت کنند[۲۲] [۲۳] [۲۴] [۲۵] [۲۶] [۲۷]. جالب اینجاست که برخی از این پرونده‌ها هنوز به پایان نرسیده‌اند.

۳-۱-۷. نتیجه دعاوی

در پرونده‌ای دیگر، شرکت مِتا[2] (شرکت مادر فیس‌بوک) به‌منظور حل‌وفصل یک دعوی جمعی، با پرداخت ۷۲۵ میلیون دلار موافقت کرد. شاکیان در این پرونده، فیس‌بوک را به اشتراک‌گذاری غیرمجاز داده‌های کاربران با شرکت‌های ثالث، از جمله کمبریج آنالیتیکا، و همچنین اهمال در نظارت بر نحوه دسترسی و استفاده این شرکت‌ها از داده‌ها متهم کرده بودند؛ اتهامی که مِتا ضمن پذیرش پرداخت مبلغ مذکور، آگاهانه بودن آن را رد کرد. طبق شـــرایط این توافق، غرامت مقرر به تمامی کاربرانی که در بازه زمانی «مه ۲۰۰۷ تا دسامبر ۲۰۲۲» حساب کاربری فعال داشته‌اند، تعلق می‌گیرد. میزان نهایی این پرداخت‌ها با توجه به شاخص‌هایی نظیر تداوم عضویت در پلتفرم و مستندات ارائه‌شده از سوی متقاضیان، متغیر بوده است[۲۸] [۲۹] [۳۰] [۳۱] [۳۲]. در نهایت حدود ۱۷٫۷ میلیون کاربر فیس‌بوک ادعاهای معتبری را ارائه کردند. به گفته وکلای دخیل در این دعوا، ممکن است این بیشترین تعداد ادعاهایی باشد که تاکنون در یک پرونده دعوی دسته‌جمعی در ایالات متحده ثبت شده است[۳۳].

۳-۱-۸. اقدام‌های توافق‌نامه

این توافق همچنین مِتا را ملزم کرد تا رویکرد خود به حفظ حریم خصوصی را اصلاح کرده و دسترسی شخص ثالث به داده‌های کاربر را محدود کند.

۳-۱-۹. تبعات قانونی و نظارتی

۳-۱-۹-۱. کمیسیون حفاظت از داده‌ها (DPC)

کمیسیون حفاظت از داده‌ها (DPC) اتحادیه اروپا پس از افشای اطلاعات در آوریل ۲۰۲۱، مِتا را به ۲۶۵ میلیون یورو جریمه (حدود ۲۷۶ میلیون دلار) محکوم کرد. DPC مدت کوتاهی پس از انتشار اخبار، تحقیق‌ها را آغاز و بررسی کرد که آیا فیس‌بوک با قوانین کلی حفاظت از داده‌های اروپا (GDPR) مطابقت دارد یا خیر[۳۴]. پس از بررسی‌های انجام شده، DPC اعلام کرد مِتا دو ماده از قوانین حفاظت از داده اتحادیه اروپا را پس از وقوع استخراج جزئیات از پروفایل‌های عمومی کاربران فیس‌بوک در سراسر جهان نقض کرده است. DPC علاوه‌بر جریمه، مِتا را ملزم کرد «با انجام طیفی از اقدام‌های اصلاحی مشخص در یک بازه زمانی خاص، خود را با ملزوم‌ها مطابقت دهد». این مجازات مجموع جریمه‌های تحمیلی مِتا توسط DPC را به نزدیک یک میلیارد یورو رساند. با این حال، این سؤال حقوقی مطرح شد که آیا اجرای قوی GDPR اثر بازدارندگی مورد نظر آن را دارد یا خیر؟ البته رئیس بخش حفاظت از داده‌ها در دفتر ایرلند این اقدام‌ها را در بازدارندگی مؤثر می‌داند[۳۵] [۳۶].

گفتنی است که این مرجع در پرونده دیگری درمورد تبلیغ‌ها نیز مِتا را جریمه کرده است[۳۷]. در دستور دیگری، DPC، مِتا، مالک فیس‌بوک را به‌دلیل سوءاستفاده از اطلاعات کاربران، به میزان بی‌سابقه ۱٫۲ میلیارد یورو جریمه کرد. این جریمه مربوط به نقض GDPR بزرگ‌ترین مجازات اعمال‌شده از زمان اجرای این مقررات بود. علاوه‌بر این، DPC به مِتا دستور داد تا انتقال داده‌های کاربران از اتحادیه اروپا به ایالات متحده را متوقف کند که این تعلیق انتقال داده‌ها فوری نبود و به مِتا برای اجرای این دستور مهلت داده شد[۳۸] [۳۹].

1. General Data Protection Regulation
2. META

۲-۹-۱-۳. کمیسیون تجارت فدرال ایالات متحده (FTC)

رسوایی کمبریج آنالیتیکا موجب خشم جهانی شد و تنظیمگران را به بررسی دقیق شیوه‌های محافظت داده توسط فیس‌بوک واداشت. در پی این اتفاق، کمیسیون تجارت فدرال ایالات متحده (FTC)،[1] این شرکت را ملزم کرد هنگام اشتراک‌گذاری داده‌های کاربران با اشخاص ثالث، اعلان‌های واضحی را به آن‌ها ارائه دهد. فیس‌بوک در سال ۲۰۱۹ با تسویه حساب ۵ میلیارد دلاری با FTC موافقت کرد. همچنین موافقت کرد که ۱۰۰ میلیون دلار برای حل‌وفصل پرونده‌ای با کمیسیون بورس و اوراق بهادار ایالات متحده، برای گمراه‌کردن سرمایه‌گذاران در مورد خطرهای ناشی از سوءاستفاده از داده‌های کاربران بپردازد[۴۰] [۴۱] [۴۲] [۴۳].

این نشت‌های داده توسط فیس‌بوک پیامدهای قانونی بالقوه را خاطر نشـــان کرد که می‌تواند توسط سایر شرکت‌ها و در سایر نشت‌ها به آن توجه شود. نکات قابل‌توجه و تأمل پس از این اتفاق، می‌تواند شامل نقض قوانین حفظ حریم خصوصی داده‌ها در ایالات متحده و اتحادیه اروپا و عواقب آن، اطلاع‌رسانی درصورت نشت داده‌ها و جریمه‌های مالی احتمالی آن و تأثیر بر آسیب‌پذیری شهرت شرکت در نتیجه نشت داده و اهمیت یادگیری از چنین حوادثی برای جلوگیری از نشت اطلاعات در آینده و محافظت از حریم خصوصی کاربران باشد[۴۴].

۲-۳. گزارش موردی: یاهو

یاهو، یکی از شرکت‌های بزرگ ارائه‌دهنده خدمات اینترنتی، پس از افشای دو حمله جداگانه به داده‌های کاربران خود، به‌شدت مورد انتقاد واقع شد. این حمله‌ها در اواخر ۲۰۱۳ و ۲۰۱۴ رخ داده و اطلاعات حساب کاربری بیش از ۱,۵ میلیارد نفر را تحت تأثیر قرار داد. در ادامه به بررسی جزئیات این دو نشت داده، تأثیرات آن‌ها بر کاربران، و پاسخ‌های یاهو در برابر آن‌ها می‌پردازیم.

۲-۳-۱. اعلامیه‌های رسمی

اعلامیه شماره ۱ (۲۲ سپتامبر ۲۰۱۶)

در این اعلامیه[۴۵]، یاهو اطلاع داد که متوجه شده اطلاعات خاصی از حساب کاربرانش در اواخر ۲۰۱۴ توسط حمله‌ای دزدیده شده است. یاهو پس از دو سال از این نشـــت داده خبر داد که احتمالاً توسط مجرمان سایبری تحت حمایت ســـایر دولت‌ها رخ داده است. (در ادامه با تحقیق‌های کمیسیون اوراق بهادار آمریکا اثبات شد که برخلاف ادعای یاهو، این شرکت در این دو سال از این موضوع آگاه بوده است)[۴۶].

اعلامیه شماره ۲ (۱۴ دسامبر ۲۰۱۶)

یاهو در این اعلامیه[۴۷] اطلاع داد که در نوامبر ۲۰۱۶ توسط ضابطین قانون مطلع شده فایل‌های داده‌ای در دسترس وجود دارد که شخص ثالثی ادعا کرده داده‌های کاربران یاهو است. یاهو پس از بررسی، درســـتی این ادعا را تأیید کرد. در ادامه این اطلاعیه یاهو بیان کرد که این نشت داده در یک حمله جداگانه در اواخر ۲۰۱۳ رخ داده و اطلاعات بیش از یک میلیارد کاربر دزدیده شده است. تحقیقات نشان می‌دهد که اطلاعات بانکی در سیستم ذخیره نمی‌شدند.

در هر دو اطلاعیه، یاهو به بیان جزئیات اتفاق (اینکه اطلاعات دزدیده‌شده شامل چه بوده‌اند و چه اطلاعاتی در امان بوده‌اند) و توضیح جزئیات فنی به زبان ساده برای کاربران، اینکه چه کسانی تحت تأثیر این حادثه امنیتی بوده‌اند و نحوه اطلاع‌رسانی به آن‌ها و اینکه آیا ایرادهای موجود برطرف شده یا خیر؛ همچنین شرح کامل اقدام‌های خود و توصیه‌هایی برای کاربران پرداخته است. یاهو همچنین به کاربران اطمینان داده که کاملاً با مجریان قانون همکاری دارد. در این اطلاعیه‌ها در مورد دامنه نشت داده نیز به کاربران اطلاع‌رسانی شده که برای نمونه به داده‌های سایر سرویس‌های یاهو که مورد استفاده کاربران بوده، مانند تامبلر،[2] آسیبی نرسیده است.

1. U.S. Federal Trade Commission
2. Tumblr

۲-۲-۳. تعداد افراد تحت تأثیر

بیش از یک میلیارد نفر [۴۷] در سال ۲۰۱۳ و ۵۰۰ میلیون نفر [۴۸] در سال ۲۰۱۴ تحت تأثیر این حمله‌ها قرار گرفتند.

۳-۲-۳. داده‌های لورفته

یاهو در اعلامیه شماره ۱ [۴۵] بیان کرد که اطلاعات حساب کاربری به‌سرقت رفته شامل نام، آدرس ایمیل، شماره تلفن، تاریخ تولد، رمزهای عبور هش‌شده[۱] (اکثریت قریب‌به‌اتفاق با bcrypt) و در برخی موارد، سؤال‌ها و پاسخ‌های امنیتی رمزگذاری شده یا نشده است. همچنین یاهو مدعی شد که اطلاعات دزدیده شده شامل رمزهای عبور محافظت نشده، داده‌های کارت پرداخت یا اطلاعات حساب بانکی نیست.

۴-۲-۳. اقدام‌های سازمان

یاهو در پاسخ به این نشت داده‌ها اقدام‌های مختلفی انجام داده است [۴۵] [۴۷]:

- اطلاع‌رسانی به کاربران در مورد وقوع حمله‌ها،
- پیشنهاد اقدام‌های امنیتی لازم به کاربران،
- ابطال سؤال‌های امنیتی و کوکی‌ها،
- تشویق به تغییر رمزهای عبور،
- بهبود سیستم‌های امنیتی،
- شناسایی دسترسی غیرمجاز به حساب کاربر و جلوگیری از آن.

۵-۲-۳. اثر اتفاق بر شرکت

نشت داده‌های یاهو، که در سال ۲۰۱۳ رخ داده، یکی از بزرگ‌ترین نقض اطلاعات در تاریخ محسوب می‌شود [۵۰] و تأثیرات عمیق و پایداری بر خوش‌نامی و آینده مالی شرکت گذاشت. همچنین این رخدادها پیامدهای گسترده‌تری برای صنعت فناوری داشته و بر نیاز به افزایش اقدام‌های امنیت سایبری و مسئولیت‌پذیری در مدیریت داده‌های کاربران تأکید داشت زیرا علاوه‌بر کاربران عادی، اطلاعات افراد در سطوح نظامی و دولتی نیز تهدید شد (بیش از ۱۵۰ هزار کارمند دولت و ارتش ایالات متحده از ایمیل‌های یاهو استفاده می‌کردند) [۵۱].

کاهش قیمت سهام، یکی از عواملی بود که بر طولانی‌ترشدن مذاکره‌ها، فروش و قیمت نهایی این شرکت در هنگام خرید توسط Verizon تأثیر گذاشت که با کاهش ۳۵۰ میلیون دلاری یا ۷٫۲۵ درصدی قیمت همراه بود [۵۲]. قیمت سهام یاهو، پس از اعلام هر یک از این نشت داده‌ها نزولی شد به‌گونه‌ای که در ۲۳ سپتامبر ۲۰۱۶ یک روز پس از اعلامیه اول ۳٫۰۶ درصد و در ۱۵ دسامبر ۲۰۱۶ پس از انتشار اعلامیه دوم ۶٫۱۱ درصد کاهش یافت [۵۳] [۵۴].

۶-۲-۳. دعاوی جمعی

در چنین مواقعی، معمولاً تک‌تک کاربران اقدام به شکایت‌های فردی نمی‌کنند زیرا عموم افراد دانش و تخصص کافی در این زمینه را ندارند، هزینه پیگیری شکایت بالاست و خسارتی که به آن‌ها وارد شده چندان بزرگ و حساس نبوده و معمولاً شکایت فردی برای افراد بهینه نیست. در این مواقع دعاوی جمعی جایگزین شکایت اشخاص می‌شود تا منافعی بیش از منافع تک‌تک افراد را نمایندگی کند. کارآمدی مقررات عمومی آیین دادرسی و نبود تناسب میان سود سرشار عرضه‌کنندگان کالا و خسارت‌های اندک مصرف‌کنندگان باعث شده تا نظام‌های حقوقی به‌دنبال راه‌حلی برای پرکردن خلأ اجرای عدالت برای مصرف‌کنندگان باشند. دعاوی جمعی یکی از این راهکارهاست که نخست در نظام حقوق آمریکا پیش‌بینی شده و اینک به اروپا رسیده و حتی برخی از کشورهای در حال توسعه نیز اقسامی از آن را پذیرفته‌اند. با این حال، نظام حقوقی ایران به‌رغم درگیری با همان مشکل‌ها و موانع احقاق حقوق مصرف‌کنندگان، راه‌حل جدی و قابل‌قبول ندارد [۵۵].

---

۱. هش‌کردن (Hashing) فرایندی است که در آن یک داده، مانند گذرواژه، با استفاده از یک تابع ریاضی به رشته‌ای با طول ثابت تبدیل می‌شود. این فرایند یک‌طرفه است و به‌طور معمول امکان بازیابی داده اصلی از روی مقدار هش وجود ندارد؛ به همین دلیل از آن برای ذخیره‌سازی امن گذرواژه‌ها و بررسی یکپارچگی داده‌ها استفاده می‌شود.

در همین راستا چندین دعوی جمعی علیه یاهو مطرح شـــد. به خطر انداختن اطلاعات حساس حساب شخصی میلیون‌ها کاربر و تأثیر آن بر قیمت سهام از موضوع‌های اصلی در این روند قانونی بود. در این شکایت‌ها ادعا شـــد که یاهو نتوانسته به اندازه کافی از اطلاعات شخصی کاربران محافظت کند و اظهارهای نادرست و گمراه‌کننده‌ای در مورد امنیت سیستم‌های خود ارائه کرده است. کانادا یکی از کشورهایی بود که شکایتی را مطرح کرد زیرا این نشت داده‌ها باعث نقض حریم خصوصی بیش از ۵ میلیون کانادایی شد[۵۶] [۵۷] [۵۸] و ایالات متحده نیز شکایت‌هایی را آغاز کرد[۵۹] [۶۰] [۶۱]. حکم نهایی دادگاه کشور آمریکا افراد ساکن در سرزمین‌های اشغالی را نیز دربرمی‌گرفت[۶۰].

۷-۲-۳. نتیجه دعاوی

با امضای توافق‌نامه، یاهو متعهد شد که مبلغی حداکثر به ارزش ۳۷۷,۹۵ دلار به هر فرد که تحت تأثیر این حوادث بوده پرداخت کند[۵۹].

۸-۲-۳. اقدام‌های توافق‌نامه

براساس شروط توافق‌نامه، یاهو به موارد زیر ملزم شد[۶۰] [۶۲] [۶۳]:

- بهبود خط‌مشی کسب‌وکار در راستای حفظ امنیت اطلاعات شخصی ذخیره‌شده کاربران در پایگاه‌های داده خود،
- پرداخت مبلغ ۱۱۷,۵۰۰,۰۰۰ دلار به صندوق تسویه،
- ارائه حداقل دو سال خدمات نظارت بر اعتبار یا پرداخت نقدی جایگزین به افراد،
- پرداخت جبران خسارت‌ها به افرادی که زیان‌های اقتصادی دیده‌اند شامل پرداخت افراد برای تبلیغ در یاهو، خدمات ویژه یا خدمات ایمیل تجاری،
- پرداخت هزینه‌ها ازجمله اطلاع‌رسانی، حق‌الزحمه وکلا و دادرسی، و غرامت شاکیان،
- سلب ادعای شاکیان (پس از این توافق‌نامه) علیه متهمان در رابطه با نقض داده‌ها.

۹-۲-۳. تبعات قانونی و نظارتی

الف) کمیسیون اوراق بهادار و بورس ایالات متحده[1] (SEC)

این پرونده اولین پرونده دعوی جمعی سهامداران به‌دلیل نقض قوانین اوراق بهادار مرتبط به داده بوده که اهمیت قانونگذاری در این حوزه برای سایر موارد مطرح و حس شد[۶۴]. سرانجام یاهو به‌علت عدم اطلاع‌رسانی به‌موقع در مورد این حمله‌ها و گمراه‌ساختن سهامداران، موظف به پرداخت جریمه ۳۵ میلیون دلاری به کمیسیون اوراق بهادار و بورس ایالات متحده شد[۴۶].

ب) کمیسیون حفاظت از داده‌ها[2] (DPC) [۶۵]

کمیسیون حفاظت از داده‌های ایرلند (DPC) مرجع نظارتی مسئول اجرای مقررات عمومی حفاظت از داده‌ها (GDPR) است و علاوه بر آن، وظایف و اختیاراتی در ارتباط با سایر چارچوب‌های نظارتی مهم، از جمله مقررات حریم خصوصی ایرلند[3] (۲۰۱۱) و دستورالعمل‌های اتحادیه اروپا نیز بر عهده دارد[۶۶]. GDPR از تاریخ ۲۵ مه ۲۰۱۸ لازم‌الاجرا شد و به DPC این اختیار را می‌دهد که در صورت تخلف، جریمه‌ای تا سقف ۲۰ میلیون یورو یا ۴ درصد از کل گردش مالی سالیانه جهانی شرکت در سال مالی قبل ـ هرکدام که بیشتر باشد ـ اعمال کند.

در خصوص تخلف‌های واقع‌شده پیش از ۲۵ مه ۲۰۱۸، قانون ۱۹۸۸[4] حاکم بود؛ ازاین‌رو، نشت داده‌های سال ۲۰۱۳ از منظر حقوقی مورد بررسی قرار نگرفت، زیرا یاهو در زمان وقوع این نشت، با توجه به تعاریف قانونی موجود، «کنترل‌کننده داده» محسوب نمی‌شد[۶۵]. نظرات این مرجع به شکل زیر بود:

1. Securities and Exchange Commission
2. Data Protection Commission

۳. شرکت یاهو به‌منظور مدیریت فعالیت‌ها و ارائه خدمات خود در مناطق اروپا، خاورمیانه و آفریقا، از طریق نهاد حقوقی «Yahoo EMEA Limited» مستقر در ایرلند اقدام می‌کرد؛ ازاین‌رو، این شرکت تحت نظارت نهادهای حفاظت از داده‌های این کشور قرار داشت.

۴. قانون حفاظت از داده‌های ایرلند (مصوب ۱۹۸۸)، به‌عنوان چارچوب حاکم بر صیانت از داده‌های شـــخصی در این کشـــور پیش از اجرای مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR)، وظیفه تعیین استانداردهای نظارتی را بر عهده داشت.

- عدم نظارت کافی یاهو بر داده‌ها با استانداردهای اتحادیه اروپا مطابقت نداشته و DPC اقدام‌های اجباری برای رفع این نقض را اعلام کرده است. این اقدام‌ها شامل به‌روزرسانی سیاست‌های حفاظت از داده‌ها، قراردادها و رویه‌های مرتبط با پردازش داده‌هاست.
- موفقیت در اعمال تغییرها و رفع نقض‌ها توسط یاهو تحت نظر DPC و تحت تعهدهای توافق‌نامه قرار خواهد گرفت.
- امکان صدور اخطاریه اجرایی در صورت لزوم و نظارت مداوم بر شرکت یاهو.

به‌طور کلی این نشت داده اهمیت بیش از پیش قانونگذاری در این حوزه را برای حمایت از حقوق مصرف‌کنندگان، سهام‌داران و... نشان داد. ازجمله این موارد اطلاع‌رسانی به‌موقع نشت داده است زیرا عدم اجرای این موضوع ازسوی یاهو باعث بروز مشکل‌هایی ازجمله چندین مورد کلاه‌برداری از کاربران شده بود که اگر اطلاع‌رسانی و اقدام‌های مناسب آن زودتر صورت می‌گرفت، تا حد زیادی از آن جلوگیری می‌شد.

پس از این اتفاق، تنظیم‌گران به اهمیت بیش از پیش ایجاد پایه و اساس اقدام‌های اجرایی شدید با مجازات‌های واقعی پی بردند و سایر شرکت‌ها نیز متوجه شدند که چه اقدام‌هایی می‌تواند خطرهای اجرایی برای آن‌ها داشته باشد.

پیرو این اتفاق، نقش کلیدی وکلا در تحقیق و پاسخ به حوادث سایبری و نیاز سازمان‌ها به استخدام وکلای داخلی با تجربه و متخصص در امنیت سایبری و تحقیق‌های این‌گونه حوادث پررنگ شد.

همچنین نقش و صلاحیت مدیران ارشد در واکنش به حوادث سایبری به بحث گذاشته شد، زیرا مدیران ارشد یاهو به‌خوبی قبل از فاش شدن از این نقض‌ها اطلاع داشتند. این پرسش‌ها پابرجاست که چرا آن‌ها در اطلاع‌رسانی تأخیر کردند و چه کسی تصمیم گرفت این نقض‌ها به‌موقع فاش نشود؟ شکست‌های مدیران ارشد یاهو نشان داد که چرا هیئت مدیره باید نقش مهمی را نه‌تنها در امنیت سایبری، بلکه در نظارت بر واکنش بعد از حادثه سایبری ایفا کند [۶۷].

SEC[1] قوانینی را در مورد مدیریت ریسک امنیت سایبری، استراتژی، حکمرانی و افشای حوادث توسط شرکت‌های عمومی تصویب کرد و از شرکت‌ها می‌خواهد که چنین نشت داده‌هایی را ظرف چهار روز پس از کشف افشا کنند. در صورتی که دادستان کل ایالات متحده تشخیص دهد که افشای فوری، خطرهای قابل توجهی برای امنیت ملی یا عمومی به‌همراه دارد، با اطلاع این تصمیم به‌صورت کتبی به کمیسیون، ممکن است زمان اعلان به تأخیر بیفتد [۶۸].

اِی‌جِی یائن[2] از مدیران شرکت آرمانینو[3] که جزو شرکت‌های بزرگ آمریکا درزمینه حسابداری، مشاوره و فناوری است، می‌گوید: «اقدام‌های اخیر SEC و تحول‌های نظارتی، امنیت سایبری را از یک موضوع فنی به یک نگرانی در سطح هیئت‌مدیره با عواقب واقعی برای سهل‌انگاری آن ارتقا می‌دهد. بنابراین، درحالی‌که برخی از جزئیات ممکن است قدیمی باشد، میراث نشت داده یاهو پابرجاست و نقش جدایی‌ناپذیر امنیت سایبری در مدیریت شرکت را برجسته می‌کند» [۶۹].

۳-۳. گزارش موردی: ماریوت اینترنشنال

ماریوت اینترنشنال[4] یک شرکت اقامتی جهانی است که دفتر مرکزی آن در بتزدا، مریلند[5] قرار دارد. اولین هتل این شرکت در سال ۱۹۷۵ تأسیس شد. ماریوت اینترنشنال، به‌عنوان بزرگ‌ترین و جهانی‌ترین شرکت اقامتگاهی در جهان، یک شرکت سهامی عام است که در بورس نیویورک معامله می‌شود. این شرکت با حضور در کشورهای متعدد در سراسر جهان به یک نام پیشرو در صنعت هتل‌داری و مهمان‌داری تبدیل شد. در سال ۲۰۱۶، ماریوت اینترنشنال با خرید شرکت Starwood Hotels & Resorts Worldwide مجموعه‌ای از برندهای بزرگ

1. U.S. Securities and Exchange Commission
2. AJ Yawn
3. Armanino LLP
4. Marriott International
5. Bethesda, Maryland

هتل‌داری مانند Sheraton و Westin را به ساختار خود اضافه کرد. با این حال، ارزیابی‌های پس از ادغام نشان داد که برخی ضعف‌های امنیتی در زیرساخت‌های سامانه‌های رزرو اســـتاروود وجود داشته که به‌طور کامل اصلاح یا یکپارچه‌ســـازی نشده بود و همین امر سطح ریسک‌پذیری امنیتی را در این سامانه‌ها افزایش داد [۷۰] [۷۱].

در اواخر سال ۲۰۱۸، شـــرکت هتل‌های زنجیره‌ای ماریوت اعلام کرد که یکی از سیستم‌های رزرواسیون آن به خطر افتاده و صدها میلیون رکورد سوابق مشتریان ازجمله شماره کارت اعتباری و شماره پاسپورت توسط مهاجمان کشف شده است.

در ۸ سپتامبر ۲۰۱۸، یک ابزار امنیتی داخلی، تلاش برای دسترسی به پایگاه داده رزرو مهمان داخلی را به‌عنوان اقدام مشکوک علامت‌گذاری کرد. بعد از دسترسی مشـــکوک، ماریوت طی تحقیق‌های داخلی خود پی برد که پایگاه داده سیستم رزرو مهمان با خطرهایی مواجه شده است. پس از بررسی‌ها مشخص شد اطلاعات و سوابق ۵۰۰ میلیون مهمان مانند شماره کارت اعتباری و پاسپورت در معرض خطر قرار گرفته است. درنتیجه عدم فروش داده‌های این شرکت است که می‌تواند نشان‌دهنده تلاش برای کسب این اطلاعات ارزشمند به سفارش نهادهای غیرتجاری باشد.

۱-۳-۳. اعلامیه‌های رسمی

در تاریخ ۳۰ نوامبر ۲۰۱۸، ماریوت طی اعلامیه‌ای به تشریح اتفاق پیش‌آمده و اقدام‌های خود پرداخت. این شرکت اعلام کرد که این نقض امنیتی مرتبط با پایگاه داده رزرو مهمان در یکی از زیرمجوعه‌هایش ایجاد شده است. طی این بیانیه اعلام شد که اخطار دسترسی مجاز در ۸ سپتامبر بوده و در ۱۹ نوامبر تحقیق‌ها مشخص کرد که دسترسی قبل از ۱۰ سپتامبر بوده است. براساس تحقیق‌ها یک شخص غیرمجاز اطلاعات را کپی و رمزگذاری کرده و اقدام‌هایی را برای حذف آن انجام داده است. در ۱۹ نوامبر ۲۰۱۸، ماریوت توانست اطلاعات را رمزگشایی و تأیید کند که محتواها از پایگاه داده رزرو مهمان استاروود است. شرکت بیان داشت بررسی‌هایش را ادامه می‌دهد اما تاکنون به نشت داده‌های بیش از ۵۰۰ میلیون نفر، پی برده که برای حدود ۳۲۷ میلیون آنان اطلاعات جزئی‌تری نیز بوده اســـت. در این بیانیه آمده که این اتفاق به مراجع قانونی اطلاع‌رسانی شده و در حال همکاری با این مراجع هستند. رئیس و مدیر اجرایی ضمن ابراز تأسف و اعلام حمایت از کاربران، به مشتریان اطمینان دادند که در تلاش برای برطرف‌کردن مشکل‌های موجود هستند [۷۲].

۲-۳-۳. تعداد کاربران تحت تأثیر قرار گرفته شده

در بیانیه اولیه، اطلاعاتی درمورد حدود ۵۰۰ میلیون مهمان تخمین زده شده بود که شرکت پس از مدتی طی بیانیه‌ای تعداد را تصحیح کرد و گفت: «این شـــرکت با اطمینان نســـبی به این نتیجه رسیده که اطلاعات کمتر از ۳۸۳ میلیون مهمان منحصربه‌فرد درگیر بوده است» [۷۳].

۳-۳-۳. نوع داده‌ها

برای حدود ۳۲۷ میلیون نفر از این مهمانان، ترکیبی از اطلاعات شامل نام، آدرس پستی، شماره تلفن، آدرس ایمیل، شماره پاسپورت، تاریخ تولد، جنسیت، اطلاعات ورود و خروج، تاریخ رزرو و اولویت‌های ارتباطی است. برای برخی، اطلاعات بیش‌تری شامل شماره کارت پرداخت و تاریخ انقضای کارت پرداخت نیز می‌شود. برای مهمانان باقیمانده، اطلاعات منتشر شده محدود به نام و گاهی آدرس پستی و ایمیل می‌شده است [۷۲].

در ژانویه ۲۰۱۹، شرکت ماریوت فاش کرد که بیش از ۵ میلیون شماره پاســـپورت رمزگذاری‌نشده و بیش از ۲۰ میلیون شماره پاسپورت رمزگذاری‌شده در این نشت داده وجود داشته اســـت. ماریوت همچنین فاش کرد که این حمله شامل اطلاعات ۸,۶ میلیون کارت اعتباری رمزگذاری‌شده بود که از این تعداد ۳۵۴۰۰۰ کارت اعتباری منقضی شـــده بود. با این حال، گفته می‌شود که کمتر از ۲۰۰۰ شماره کارت رمزگذاری‌نشده هنوز ممکن است در معرض خطر باشند [۷۴] [۷۵] [۷۶].

۴-۳-۳. آثار

بعد از افشای نشت داده، قیمت سهام این شرکت با کاهش ۵٫۶ درصدی همراه بود [۷۷] [۷۸]. همچنین پس از این حادثه انتقادهای گسترده‌ای به ماریوت به‌علت نقض‌های امنیتی وارد شد. به‌ویژه، رسانه‌ها و کارشناسان فناوری اطلاعات، شکست‌های ماریوت را در انجام بررسی‌های لازم روی آسیب‌پذیری‌های امنیتی موجود استاروود قبل از فرایند خرید و ادغام، بررسی کردند. آسیبی که برای نزدیک به چهار سال به مجرمان سایبری اجازه می‌داد به اطلاعات شخصی مشتریان دسترسی داشته و از آن‌ها استفاده کنند. علاوه‌بر این، تخمین زده می‌شود که این شرکت به‌علت کاهش وفاداری مشتریان پس از این حادثه، بیش از ۱ میلیارد دلار از درآمد خود را از دست داده باشد [۷۹]. همچنین باعث کاهش نمره‌های رضایت مشتری در سال ۲۰۱۹ و میزان اعتماد مردم به این شرکت شد [۸۰].

نگرانی‌های بسیاری از نشت داده‌های مرتبط با کارت بانکی و شماره پاسپورت به وجود آمد، زیرا می‌توانست به کلاه‌برداری و جعل هویت منجر شود [۸۱]. همچنین با داشتن شماره پاسپورت افراد می‌توان برنامه‌های سفر قربانیان حمله‌های سایبری را ردیابی کرد، که بسیاری از آن‌ها ممکن است مقام‌های دولتی یا مدیران تجاری باشند [۷۵]. کارشناسان رمزگذاری به ماریوت انتقادهایی در مورد نحوه و نوع اطلاع‌رسانی در مورد رمزنگاری اطلاعات وارد کردند که به آن‌ها پاسخی نداد [۸۲].

۵-۳-۳. اقدام‌های سازمان

- شرکت از ۳۰ نوامبر ۲۰۱۸ شروع به ارسال ایمیل اطلاع‌رسانی به مهمانانی کرد که اطلاعاتشان افشا شده بود.
- یک وب‌سایت و مرکز تماس اختصاصی با پشتیبانی چند زبانه برای سؤال‌های کاربران ایجاد شد. این وب‌سایت به‌روزشونده اطلاعات و سؤال‌های مرتبط را به کاربران ارائه داده و به‌مرور پرسش‌های پرتکرار را در دسترس عموم قرار می‌داد.
- ارائه یک سال عضویت رایگان در سرویس Web Watcher به ساکنان ایالات متحده، کانادا و بریتانیا (سرویس نظارتی بر سایت‌هایی که دزدان اطلاعات را می‌فروشند و اطلاع‌رسانی به افراد در صورت فروش اطلاعات آن‌ها و همچنین دسترسی به خدمات مشاوره کلاه‌برداری و پوشش بازپرداخت).
- تشکیل پرونده SEC: ماریوت ارسال فرم K-8[1] به SEC را آغاز کرد و بیانیه مطبوعاتی و اطلاعات اضافی درباره این حادثه را ارائه داد [۷۲] [۸۳].
- قرار شد که این شرکت هزینه جایگزینی گذرنامه با شماره جدید را بپردازد یا هزینه‌های کارت اعتباری را «اگر کلاهبرداری صورت گرفته باشد» پرداخت کند [۸۴].
- این شرکت، سیستم رزرو مهمان استاروود، که آسیب‌پذیر بود را از دسترس خارج کرد و سیستم یکپارچه ماریوت در تمامی هتل‌ها استفاده شد [۷۳].
- ماریوت در پی این نشت داده، وارد برخی فرایندهای حقوقی شد که جرائم مالی و عملکردی را که در زیر بیان خواهد شد، در پی داشت.

۶-۳-۳. دعاوی حقوقی

شکایت‌های دسته‌جمعی متعددی علیه این شرکت مطرح شد که دلیل آن شکست ماریوت در انجام بررسی‌های لازم روی سیستم‌های فناوری اطلاعات استاروود بود.

در یک مورد، بیش از ۱۵۰ نفر که قبلاً در املاک شرکت ماریوت اقامت داشتند، از این شرکت شکایت کردند و مدعی شدند که ماریوت به اندازه کافی برای محافظت از آن‌ها در برابر نقض داده‌ها، اقدام نکرده است [۸۵].

در پرونده دیگری، افرادی با به خطر افتادن اطلاعات شخصی‌شان و بی‌توجهی ۲ ساله شرکت ماریوت در تأمین امنیت سامانه‌های زیرمجموعه

---

۱. فرم K-8 یکی از گزارش‌های رسمی شرکت‌های بورسی به U.S. Securities and Exchange Commission (SEC) است که برای افشای رویدادهای مهم و بااهمیت، از جمله رخدادهای امنیت سایبری، به سرمایه‌گذاران و بازار سرمایه ارائه می‌شود.

خود، که نشان‌دهنده نقض قوانین حمایت از مصرف‌کننده است، از این شرکت شکایت کردند[۸۶] و در جریان شکایت دیگری نیز، شاکیان ۱۲,۵ میلیارد دلار زیان خواستند[۸۷].

بسیاری از این دعاوی با یکدیگر ادغام شدند تا روند دادگاه را ساده کنند. چنین دعاوی دسته‌جمعی معمولاً سال‌ها طول می‌کشد تا به محاکمه برسد و در بیشتر موارد توافق می‌کنند. طی این توافق‌نامه‌ها، متهم ملزم به پرداخت مبلغ و یا انجام تغییراتی در شرکت نیز می‌شود.

روند بررسی شکایت‌ها در دادگاه در مراحل اولیه به‌علت پیوستن مشتریان به برنامه‌های وفاداری ماریوت روند پیچیده‌تری را در پی خواهند داشت. این برنامه‌ها مزایای زیادی را برای مشـــتریان وفادار تبلیغ می‌کنند اما در مقابل هزینه‌هایی (مانند کاهش یا سلب امکان شکایت از شرکت) را در قالبی توافق‌نامه‌ای که معمولاً خوانده نمی‌شود ، در پی دارد. وکلای شاکیان مدعی هستند که مشتریان آگاهانه این حق را از خود سلب نکرده‌اند[۸۸] [۸۹] [۹۰]. پس از اینکه ماریوت سعی کرد از سلب حق مشتریان، که در انتهای چندین صفحه قوانین و مقررات، آن را تأیید کرده بودند، استفاده کند، دادگاه آن را رد و روند دادرسی را به جریان انداخت[۹۱].

۷-۳-۳. نتیجه دعاوی

هنوز نتیجه نهایی اعلام نشده است.

۸-۳-۳. تبعات حقوقی و نظارتی

دفتر کمیسر اطلاعات بریتانیا [۱] (ICO) که یک سازمان دیده‌بان حقوق مصرف‌کننده است، ماریوت را ۲۳.۸ میلیون دلار (کمتر از جریمه اولیه ۱۲۳ میلیون دلاری) جریمه کرد. ICO می‌گوید که این شرکت به‌علت انجام ندادن اقدام‌های فنی یا سازمانی مناسب هنگام پردازش داده‌ها، اســـتانداردهای امنیتی موردنیاز GDPR را برآورده نکرده و به این ترتیب، این شرکت الزام‌های حفاظت از داده‌ها را که اکنون از طریق مقررات GDPR اجرا می‌شود، نقض کرده است. با این حال، سازمان دیده‌بان اذعان کرد که ماریوت پس از فاش‌شدن حادثه امنیت سایبری، بلافاصله با مشـــتریان و ICO تماس گرفت، و برای کاهش خطر آسیب وارده به مشتریان اقدام کرد. میزان جریمه اولیه در نظر گرفته شده بیش از مقدار تصویب‌شـــده بود اما به‌علت هزینه‌های پیش روی ماریوت برای بهبود امنیت خود و سایر هزینه‌ها، این جریمه کاهش پیدا کرد[۹۲] [۹۳].

نشت داده در شرکت ماریوت، اهمیت امنیت سایبری در هنگام ادغام شرکت‌ها را نشان داد. در بسیاری از موارد، اتخاذ فرایندهای دیجیتالی مشترک و سیاست‌های امنیتی برای حفظ استراتژی‌های دفاعی یکســـان در برابر مجرمان سایبری، می‌تواند برای شرکت‌های ادغام‌شده مفید باشد.

از دیگر درس‌های این نشت داده، اهمیت بسیار نرم افزارهای مؤثر امنیتی و تشخیص تهدید و آسیب‌پذیری است. ممکن است این سرویس‌ها در ابتدا گران باشند اما با کاهش احتمال نشت داده و نقض حریم خصوصی از آسیب‌های بزرگ‌تر جلوگیری می‌کنند.

ماریوت یک شرکت غیرفناوری است که شهرت آن یک دارایی ضروری در تجارت هتل‌داری است. شهرت ماریوت براساس کیفیت خدمات مهمان‌نوازی آن‌هاست، نه براساس استحکام امنیت سایبری. این اتفاق اثر مشـــهود و ملموس حفاظت اطلاعات و امنیت داده را بر شرکتی که ارزش آن به فناوری اطلاعات مربوط نیست آشکار کرد. همچنین این نشـــت داده، تأثیرات بالقوه‌ای بر صنعت بیمه داشت. بیمه در برابر حمله‌های سایبری یک بیمه نسبتاً جدید است زیرا ابعاد ضرر و زیان شرکت‌ها در حمله‌های سایبری باید سنجیده شود (بیمه سایبری این شرکت بسیاری از هزینه‌های اولیه مرتبط با بحران را پوشش می‌داد). پس از این اتفاق صحبت‌هایی در این زمینه میان متخصصان این حوزه به‌وجود آمد[۷۹] [۹۴] [۹۵].

1. Information Commissioner's Office

۴-۳. گزارش موردی: ادهار، ثبت احوال هند

بین اوت ۲۰۱۷ و ژانویه ۲۰۱۸، به‌طور غیررسمی اعلام شد که اطلاعات بیش از ۱ میلیارد شهروند هندی در Aadhaar دچار نشت شده و در معرض خطر قرار گرفته است. فروشندگان ناشناس ازطریق واتس‌اپ[1] برای دسترسی به مرجع شناسایی منحصربه‌فرد هند که سوابق تقریباً هر شهروندی در آن موجود است، حدود ۵۰۰ روپیه و کمتر را دریافت می‌کردند.

ادهار یک شماره شناسایی ۱۲ رقمی به‌عنوان مدرکی هویتی توسط سازمان شناسایی منحصربه‌فرد هند (UIDAI)[2] که یک مرجع قانونی ایجاد شده توسط دولت هند و زیر نظر وزارت الکترونیک و فناوری اطلاعات است، برای ساکنان هند به‌صورت داوطلبانه و براساس اطلاعات بیومتریک (۱۰ اثر انگشت، ۲ اثر عنبیه و عکس صورت) و داده‌های جمعیتی (نام، تاریخ تولد، سن، جنسیت، نشانی و...) صادر می‌کرد.

این شماره در جهت تأیید هویت و نشانی عمل کرده و به روشی آنلاین و مقرون‌به‌صرفه قابل تأیید است و از جعل هویت جلوگیری می‌کند. ازجمله کاربردهای آن می‌توان به این موارد اشاره کرد: دسترسی به خدمات دولتی و مزایای رفاهی (به‌عنوان یک شناسه اصلی برای ارائه خدمات)، تسهیل دسترسی به خدمات و امور مالی بخش‌های محروم جامعه، جلوگیری از سرقت هویت و کلاهبرداری از منافع ساکنان فقیر و حاشیه‌نشین که اغلب فاقد اسناد هویتی سنتی هستند[۹۶].

یکی از اشکال‌های مهمی که به این سامانه وارد شده بود، این بود که افراد حتی برای خرید سیم‌کارت یا ثبت‌نام در مدرسه نیز مجبور به استفاده از آن بودند و این موجب انباشت حجم انبوهی از داده‌های شهروندان شده بود[۹۷].

در سال ۲۰۲۳، این سامانه برای چندمین بار دچار نشت داده شد و گزارشی از شرکت امنیت سایبری ایالات متحده Resecurity فاش کرد که اطلاعات شخصی ۸۱۵ میلیون هندی شامل نام، شماره تلفن، آدرس، اطلاعات ادهار و پاسپورت آن‌ها در دارک‌وِب منتشر شده است. براساس گزارشی که در Standard Business منتشر شده است، هکرها در ازای ۸۰۰۰۰ دلار حاضر به فروش داده‌های ادهار و پایگاه داده گذرنامه هستند. پلیس هشدارهایی را در پلتفرم X (توییتر سابق) صادر کرد و از افراد خواست ورود از طریق روش بیومتریک ادهار خود را قفل کنند تا در برابر فعالیت‌های کلاهبرداری در امان باشند[۹۸].

۱-۴-۳. اعلامیه‌های رسمی

در ۱۹ نوامبر ۲۰۱۷ گزارش‌هایی از نگرانی‌ها درباره امنیت این سیستم مطرح شد[۹۹] که واکنش مراجع رسمی را در پی داشت. UIDAI در ۲۰ نوامبر در بیانیه‌ای گفت که داده‌های ادهار کاملاً ایمن و امن است و هیچ‌گونه نشت یا نقض داده وجود ندارد. UIDAI گفت که به نظر می‌رسد روزنامه مدعی تنها از طریق یک مرکز جست‌وجو که در اختیار مقام‌های دولتی قرار گرفته به جزئیات محدودی دسترسی داشته باشد. این مرکز مدعی شد که اقدام‌های پیشگیرانه‌ای را برای رسیدگی به نمایش شماره‌های ادهار در وب‌سایت‌های دولتی انجام داده است؛ و امنیت و یکپارچگی سیستم احراز هویت ادهار را مجدداً تأیید و تأکید کرده که هیچ موردی از نقض داده‌های بیومتریک وجود ندارد[۱۰۰].

بعد از انکار چندباره نشت داده توسط UIDAI، که سیستم ادهار را مدیریت می‌کند، گزارشی تحقیقی در ۳ ژانویه ۲۰۱۸ با عنوان «۵۰۰ روپیه، ۱۰ دقیقه، و شما به جزئیات میلیاردی ادهار دسترسی دارید» توسط روزنامه تریبون فاش کرد که جزئیات ادهار تنها با پرداخت ۵۰۰ روپیه به‌راحتی قابل‌دسترس است[۱۰۱].

در پی انتشار این گزارش، UIDAI در ۴ ژانویه گفت که به‌دنبال طرح اتهام علیه افرادی است که از سیستم «سوءاستفاده» کرده‌اند، است اما تأکید کرد که هیچ اثر انگشت یا اسکن شبکیه چشم در دسترس دیگران قرار نگرفته است[۱۰۲]. در بیانیه‌ای آمده است: «نمایش صرف اطلاعات جمعیتی را نمی‌توان بدون بیومتریک مورد سوءاستفاده قرار داد. ادعاهای دور زدن یا فریب دادن سیستم ثبت‌نام ادهار کاملاً بی‌اساس است. داده‌های ادهار کاملاً ایمن و مطمئن هستند»[۱۰۳] [۱۰۴] [۱۰۵].

۲-۴-۳. تعداد افراد تحت تأثیر

بیش از ۱ میلیارد نفر است[۱۰۱].

1. WhatsApp
2. The Unique Identification Authority of India

۳-۴-۳. داده‌های لورفته

شماره ادهار، نام، ایمیل و نشانی فیزیکی، کد پستی، شماره تلفن، عکس‌ها و اطلاعات پاسپورت، داده‌های بیومتریک و تمام مشخصاتی که ممکن است یک فرد به UIDAI ارسال کرده باشد.

۴-۴-۳. اقدام‌های سازمان

UIDAI، دو روز پس از گزارش روزنامه تریبون، علیه این روزنامه و روزنامه‌نگار آن شـــکایتی را مطرح کرد[۱۰۶]. این امر توســـط اتحادیه روزنامه‌نگاران محکوم شد[۱۰۷] و این شکایت به‌عنوان شاهدی علیه ادعای آنان در وخامت وضع موجود شد. در کمتر از یک سال، این چهارمین مورد گزارش شده از حمله به آزادی بیان در زمینه ادهار بود[۱۰۸]. در تمامی موارد این سازمان اتهام و گزارش‌ها را تکذیب می‌کرد[۱۰۹].

پیرو این گزارش، یک مقام دولتی بیان کرد که تمامی امتیازهایی که به افراد تعیین‌شده برای دســـترسی داده شده بود فوراً لغو شده‌اند. او همچنین افزود که این سیستم اکنون فقط با بیومتریک فردی که جزئیات آن باید تأیید شود، امکان دسترسی را به افراد می‌دهد. همچنین مقامات ارشد پلیس دهلی گفته بودند که در حال بررسی دخالت افراد خودی در UIDAI پس از ادعای نقض اطلاعات هستند[۱۱۰].

۵-۴-۳. اثر اتفاق بر شرکت

در ژانویه ۲۰۱۸ بار دیگر اخطارهایی در مورد اپلیکیشن‌های مرتبط با این سازمان توسط محققان امنیتی داده شد[۱۱۱]. پس از یک سال از این حادثه در گزارشی به اشکال‌های وارده به سیستم این سازمان و برنامه‌های مرتبط با آن پرداخته و مدعی شد که در طول یک سال گذشته، موارد متعددی از نشت داده‌های ادهار به‌صورت آنلاین از طریق وب‌سایت‌های دولتی وجود داشته است[۱۱۲]. این گزارش نشان می‌دهد که با وجود انتقادهای فراوان اقدام مؤثر و درستی برای امنیت کاربران این سازمان در طول یک سال انجام نشده است.

۶-۴-۳. دعاوی جمعی

دعوی جمعی علیه دولت صورت نگرفت.

۷-۴-۳. نتیجه دعاوی

مشخص نیست.

۸-۴-۳. اقدام‌های توافق‌نامه

مشخص نیست.

۹-۴-۳. تبعات قانونی و نظارتی

چندماه پس از این اتفاق، گزارش‌های متعدد UIDAI را مجبور کرد طی بیانیه‌ای از مردم بخواهد که شماره ادهار خود را در انظار عمومی فاش نکنند[۱۱۳]. یکی از مسائل اصلی مدنظر منتقدان سیستم ادهار، حریم خصوصی بود. ادهار از مشکل‌های امنیتی بی‌شماری رنج می‌برد و سیستم بارها ثابت کرده بود که هم در برابر نشت‌های داخلی و هم سوءاستفاده خارجی از داده‌ها آسیب‌پذیر است. ادهار به‌عنوان یک ایده جدید برای کاهش بوروکراسی و کلاهبرداری آغاز شد، اما خود حریم شخصی همه کاربران را تهدید و حقوق قانونی شهروندان هند را محدود می‌کرد. علاوه‌بر این منتقدان معتقد بودند ارتباط و پتانسیل ادهار در کمک به برنامه‌های یادگیری ماشینی تحت کنترل دولت، اصول دمکراتیک را نیز تضعیف خواهند کرد. پس از آنکه دادگاه بر ادامه استفاده از این سیستم تأکید کرد و لغو و تعطیلی آن را مطرح نکرد، از دولت خواست هرچه سریع‌تر قوانین مناسب و قدرت‌مندی را برای حفظ و امنیت داده‌ها معرفی کند[۱۱۴] [۱۱۵] [۹۷].

انتشار پیش‌نویس لایحه قانون حفظ حریم خصوصی برای هند در همان سال کمک شایانی به بهبود شرایط کرد. هرچند که پیش‌نویس لایحه تا حد زیادی در مورد ادهار بی‌اثر بود؛ با این حال، پیشنهاد کرد که قانون ادهار برای تقویت حفاظت از داده‌ها اصلاح شود[۱۰۹].

این حادثه، نیاز به نوسازی چارچوب‌های امنیتی و اجرای اصلاح‌های نظارتی را برای رفع آسیب‌پذیری‌های سیستم شناسایی منحصربه‌فرد هند برجسته کرد. دولت یک بازنگری جامع را آغاز کرد و فناوری‌های پیشرفته رمزگذاری را برای محافظت از داده‌های حساس پیاده‌سازی کرد. اجرای سخت‌گیرانه دســـترسی مبتنی‌بر نقش، برای محدودکردن و نظارت بر دسترسی به پایگاه داده اعمال شد و تضمین می‌کرد که افراد فقط به اطلاعات لازم برای مسئولیت‌های خود دسترسی دارند.

پروتکل‌های پیشرفته احراز هویت معرفی شدند که شامل اجرای احراز هویت چندعاملی و رمزگذاری بیومتریک برای خنثی کردن تلاش‌ها در دسترسی غیرمجاز بودند. برای تشویق سازمان‌ها در اولویت‌دادن به امنیت سایبری، دولت مجازات‌های سخت‌تری را برای رعایت نکردن مقررات حفاظت از داده‌ها در نظر گرفت که شامل جریمه‌های سنگین و عواقب قانونی برای نهادهایی است که به‌اندازه کافی از اطلاعات حساس محافظت نمی‌کنند.

دولت با درک اهمیت آگاهی از امنیت سایبری، کمپین‌های آگاهی عمومی را راه‌اندازی کرد. هدف این کمپین‌ها آموزش افراد در مورد بهترین شیوه‌ها برای امنیت آنلاین، خطرهای مرتبط با اشتراک‌گذاری اطلاعات شخصی و اقدام‌های لازم برای محافظت از داده‌های آن‌ها بود [۱۱۶].

قانون محافظت از داده‌های شخصی دیجیتال هند سال ۲۰۲۳، اولین قانون عرضه‌شده در حوزه محافظت از داده‌های شخصی در هند است [۱۱۷]. هدف این قانون ایجاد دستورالعمل‌های روشن برای جمع‌آوری، ذخیره و استفاده از داده‌های شخصی است و سازمان‌ها را در قبال نقض داده‌ها مسئول می‌داند. در سال‌های ۲۰۱۷ و ۲۰۱۸، چند عامل محرک وجود داشت که به نسخه‌های اولیه این لایحه منجر شد. دادگاه عالی اخیراً حریم خصوصی را یک حق اساسی اعلام کرده و قرار بود در مورد مطابقت یا مغایرت ادهار با قانون اساسی تصمیم بگیرد. علاوه‌بر این، یک بحث جهانی در مورد قوانین حفاظت از داده‌ها وجود داشت که با اجرای قریب‌الوقوع GDPR آغاز شد. این قوانین که در سال ۲۰۱۶ تصویب و در سال ۲۰۱۸ لازم‌الاجرا شد، در آن مقطع زمانی، به‌عنوان یک الگوی قابل‌قبول برای تصویب در نظر گرفته شد و بر مذاکره‌های هند تأثیر فراوانی گذاشت [۱۱۸].

۴. جریمه‌های نقض داده

جریمه‌ها بسته به ماهیت و شدت حادثه می‌تواند متفاوت باشد. در اینجا به برخی از نمونه‌های آن اشاره می‌کنیم:

درحالی‌که نقض و نشت داده‌ها نگرانی‌هایی را ایجاد می‌کنند، عواقب و مجازات‌های بالقوه بر اساس عمدی یا غیرعمدی‌بودن حادثه متفاوت است. نقض داده‌ها به‌طور معمول به‌دلیل سوءنیت درگیرشده، مجازات‌های سنگین‌تری را به‌همراه دارند. اما در نشت داده به‌دلیل غیرعمدی بودن، مجازات‌ها نسبت به نقض داده‌ها کمتر است. با این حال، عواقب آن هنوز می‌تواند قابل توجه باشد. مجازات‌ها می‌توانند با توجه به چندین عامل به‌طور قابل توجهی متفاوت باشند:

- **نوع داده‌های افشاشده:** سوابق پزشکی، اطلاعات مالی و شماره‌های تأمین اجتماعی مجازات‌های سنگین‌تری نسبت به داده‌های حساس دارند.
- **تعداد افراد تحت تأثیر:** نقض‌های بزرگ‌تر احتمال محکومیت به جریمه‌های بالاتری دارند.
- **حوزه قضایی:** کشورهای مختلف دارای مقررات حریم خصوصی داده‌های متفاوتی هستند و جریمه‌های متفاوتی در ارتباط با آن دارند.
- **عمدی یا تصادفی بودن:** نقض‌های داده به‌دلیل عمدی‌بودن اغلب مجازات‌های شدیدتری دارند. همچنین این موضوع بسیار مهم است که آیا شرکت در مسئولیت‌های حفاظت از داده‌های خود سهل‌انگاری کرده یا خیر؟
- **نقض مقررات خاص:** تخطی از قوانین مشخص حوزه حریم خصوصی داده، نظیر مقررات عمومی حفاظت از داده‌ها (GDPR) یا قانون حفاظت از حریم خصوصی مصرف‌کنندگان کالیفرنیا[1] (CCPA)، می‌تواند به اعمال جرائم و مجازات‌های اضافی منجر شود.

برای نمونه:

الف) جریمه‌ای که GDPR یا همان مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا در نظر می‌گیرد، عبارت است از تا ۲۰ میلیون یورو یا ۴ درصد از گردش مالی سالیانه جهانی شرکت، هر کدام که بیشتر باشد.

ب) قانون CCPA یا قانون حریم خصوصی مصرف‌کننده کالیفرنیا، جریمه‌ای تا ۷۵۰۰ دلار برای هر رکورد مصرف‌کننده که به خطر افتاده باشد در نظر می‌گیرد.

ج) قانون HIPAA آمریکا نیز جریمه‌های مدنی تا ۵۰۰۰۰ دلار برای هر تخلف پیش‌بینی کرده است.

1. California Consumer Privacy Act

گاهی مجازات نقض داده‌ها می‌تواند بسیار شدید باشد. برای مثال، Equifax موافقت کرد که حداقل ۵۷۵ میلیون دلار برای نقض داده خود در سال ۲۰۱۷ بپردازد. شرکت چینی دیدی گلوبال به‌علت نقض قوانین حفاظت از داده این کشور ۱.۱۹ میلیارد دلار جریمه شد و آمازون نیز با نقض مقررات حفاظت از داده‌های عمومی (GDPR) در اروپا ۸۷۷ میلیون دلار جریمه شد.

همچنین شایان ذکر است که شـــرکت‌ها علاوه‌بر جریمه‌های مالی، ممکن است با آسیب‌های اعتباری، از دســـت‌دادن اعتماد مشتریان و شکایت‌های احتمالی از سوی افراد آسیب‌دیده مواجه شوند.

باید توجه داشته باشیم که پیشگیری از افشای داده‌ها، بسیار مهم است، زیرا هر دو نوع حادثه می‌توانند عواقب قابل توجهی برای سازمان‌ها داشته باشند.

۵. نمونه‌های نقض و نشت داده در ایران

در سال‌های اخیر، نشت داده‌ها و حمله‌های سایبری به زیرساخت‌ها و سازمان‌های مختلف در ایران به یکی از چالش‌های جدی حوزه امنیت اطلاعات تبدیل شده اســـت. این حمله‌ها، که دامنه آن‌ها از سامانه‌های دولتی تا ســـکوهای خصوصی و بانک‌ها گسترده است، بارها حریم خصوصی کاربران را در معرض خطر قرار داده و اعتماد عمومی را متزلزل کرده‌اند. ضعف در زیرساخت‌های امنیت سایبری، عدم شفافیت در اطلاع‌رسانی و نبود قوانین جامع برای حفاظت از داده‌ها، دلایل عمده تداوم و گسترش این معضل هستند. در این بخش به بررسی مهم‌ترین موارد نشت داده‌ها و حمله‌های سایبری در ایران، پیامدهای آن‌ها، و زمینه‌های آسیب‌پذیری می‌پردازیم.

در جدول زیر فقط برخی از نقض و نشت داده‌های اخیر را مشاهده می‌کنید:

جدول ۱. مهم‌ترین موارد نقض و نشت داده در دو سال اخیر در ایران

تاریخ	نهاد
تیر ۱۴۰۲	هک سرورهای بنیاد شهید
شهریور ۱۴۰۲	هک تپسی
شهریور ۱۴۰۲	هک اطلاعات شرکت‌های بیمه
شهریور ۱۴۰۲	هک سامانه ثبت احوال
مهر ۱۴۰۲	هک سایت وزارت علوم
آذر ۱۴۰۲	حمله به شبکه سوخت
دی ۱۴۰۲	هک اسنپ‌فود
بهمن ۱۴۰۲	هک سایت مجلس و خانه ملت
اسفند ۱۴۰۲	هک سامانه قوه قضائیه
اسفند ۱۴۰۲	هک وب‌سایت بنیاد مستضعفان
شهریور ۱۴۰۳	هک ۲۰ بانک ایرانی
اسفند ۱۴۰۳	هک بانک سپه
خرداد ۱۴۰۴	هک بانک سپه طی جنگ ۱۲ روزه
خرداد ۱۴۰۴	هک بانک پاسارگاد طی جنگ ۱۲ روزه
خرداد ۱۴۰۴	هک صرافی نوبیتکس طی جنگ ۱۲ روزه

مأخذ: گردآوری‌شده توسط نگارنده.

۵-۱. گزارش موردی: اسنپ‌فود

در تاریخ ۱۰ دی ماه ۱۴۰۲، پلتفرم اسنپ‌فود، یکی از بزرگ‌ترین ارائه‌دهندگان خدمات سفارش غذا در ایران، هدف یک حمله سایبری قرار گرفت که به دسترسی غیرمجاز هکرها به بخشی از اطلاعات کاربران منجر شد. این رخداد، که در ادامه موجی از حمله‌های مشابه به شرکت‌های دیگر رخ داد، نگرانی‌های گسترده‌ای درباره امنیت سایبری و حفظ حریم خصوصی کاربران در کشور ایجاد کرد.

۵-۱-۱. اعلامیه‌های رسمی

شرکت اسنپ‌فود در همان روز طی یک بیانیه رسمی، هک شدن بخشی از داده‌های کاربران را تأیید کرد. این شرکت اعلام کرد که به‌محض شناسایی حمله، اقدام‌های لازم برای مهار دسترسی هکرها انجام شد و موضوع به پلیس فتا و نهادهای امنیتی گزارش شد. همچنین اسنپ‌فود اظهار داشت که هیچ‌گونه اطلاعات حساس مانند رمز عبور کاربران در این حمله درز پیدا نکرده است.

۵-۱-۲. تعداد افراد تحت تأثیر

براساس اعلامیه‌های غیررسمی و اطلاعات منتشرشده توسط گروه هکری، حدود ۲۰ میلیون کاربر تحت تأثیر این حمله قرار گرفتند. این عدد شامل اطلاعات کاربران فعال و غیرفعال در پلتفرم بوده است.

۵-۱-۳. داده‌های لو رفته

هکرها مدعی شدند که اطلاعاتی مانند شماره تلفن، موقعیت مکانی سفارش‌ها، سوابق سفارش‌ها، و جزئیات کارت‌های بانکی (بدون CVV2 و رمز) را به‌دست آورده‌اند. با این حال، اسنپ‌فود تأکید کرد که اطلاعات حساس بانکی کاربران در دسترس قرار نگرفته است؛ زیرا این داده‌ها در سامانه‌های جداگانه و امن نگهداری می‌شوند.

۵-۱-۴. اقدام‌های سازمان

پس از وقوع حمله، اسنپ‌فود مدعی شد تیم‌های امنیتی را برای ارزیابی و تقویت زیرساخت‌های امنیتی خود به کار گرفته است.

۵-۱-۵. دعاوی جمعی و توافق‌ها

پس از وقوع حمله سایبری، دعاوی جمعی علیه اسنپ‌فود مطرح نشده و تاکنون جزئیات دقیقی درباره هرگونه توافق‌نامه رسمی میان اسنپ‌فود و کاربران یا نهادهای نظارتی منتشر نشده است. گزارش‌ها نشان می‌دهد که هکرها برای بازگرداندن اطلاعات، درخواست مبلغی در حدود ۳۰ هزار دلار کرده بودند. اسنپ‌فود هرگز تأیید نکرد که این باج پرداخت شده است. با این حال، بخشی از داده‌ها برای نمونه توسط هکرها در فضای مجازی منتشر شد که اسم و مشخصات سفارش برخی از کاربران نیز در آن‌ها قابل مشاهده بود.

حمله به اسنپ‌فود، علاوه‌بر تأثیرات منفی بر اعتبار شرکت، بار دیگر ضعف‌های موجود در زیرساخت‌های امنیت سایبری کشور را برجسته کرد. این رخداد ضرورت بازنگری در سیاست‌های امنیتی و تقویت قوانین مربوط به حفاظت از داده‌های شخصی در ایران را بیش از پیش نمایان ساخت. بنابراین برخلاف مواردی که در کشورهای دیگر رخ داد و نمونه‌های آن‌ها را بررسی کردیم، در کشور ما دعاوی جمعی علیه شرکت شکل نگرفت و هیچ‌گونه اطلاعی در دست نیست که سازمان‌های مربوطه نیز شرکت را متهم و جریمه کرده باشند.

۵-۱-۶. پیام پلیس فتا

این حادثه توجه جدی نهادهای نظارتی به ضعف‌های امنیت سایبری در کشور را جلب کرد. پلیس فتا ضمن تأیید وقوع حمله به اسنپ‌فود، اعلام کرد که تیم‌های امنیت سایبری به‌طور مداوم در حال بررسی این موضوع هستند و تمام اقدام‌های لازم برای شناسایی و تعقیب هکرها انجام شده است. همچنین از کاربران خواسته شد که اقدام‌های امنیتی فردی خود را جدی‌تر بگیرند.

۵-۲. گزارش موردی، تپسی

در شهریور ماه ۱۴۰۲، حمله سایبری به تپسی، یکی از سرویس‌های بزرگ تاکسی اینترنتی کشور، رخ داد. این حمله امنیت اطلاعات کاربران

و راننده‌ها را در معرض خطر قرار داد و واکنش‌های بسیاری را در پی داشت. گروه هکری مدعی شد به داده‌های گسترده‌ای شامل اطلاعات مسافران، رانندگان، و جزئیات سفرها دسترسی پیدا کرده است.

۵-۲-۱. اعلامیه‌های رسمی

میلاد منشی‌پور، مدیرعامل وقت تپسی، در بیانیه‌ای اعلام کرد که این شرکت به‌محض شناسایی نفوذ، اقدام‌های لازم را برای جلوگیری از دسترسی بیشتر انجام داده و موضوع را به پلیس گزارش کرده است. وی همچنین تصریح کرد که شرکت تصمیم گرفته حتی با وجود تهدیدها به انتشار اطلاعات با هکرها وارد مذاکره نشود.

۵-۲-۲. تعداد افراد تحت تأثیر

گزارش‌های غیررسمی نشان می‌دهد داده‌های بیش از ۲۷ میلیون مسافر و ۶ میلیون راننده در این حمله به خطر افتاده است. هکرها مدعی شدند اطلاعات مربوط به ۱۳۶ میلیون سفر را نیز در اختیار دارند[۱۱۹].

۵-۲-۳. داده‌های لورفته

داده‌های لورفته شامل نام، شماره تماس، اطلاعات دستگاه‌های همراه کاربران و جزئیات سفرها بود. گروه هکری همچنین نمونه‌ای از این داده‌ها را در فضای مجازی منتشر کرد و برای عدم افشای کامل اطلاعات، مبلغی معادل ۳۵ هزار دلار درخواست کرد[۱۱۹].

۵-۲-۴. اقدام‌های سازمان

تپسی پس از شناسایی حمله، دسترسی هکرها را مسدود و با اعلام این رخداد، از کاربران عذرخواهی کرد. این شرکت تأکید کرد که باج‌خواهی را نمی‌پذیرد و تمام اقدام‌های لازم برای پیشگیری از حمله‌های مشابه در آینده را در دستور کار قرار داده است.

۵-۲-۵. اثر اتفاق بر شرکت

حمله سایبری تأثیرهای منفی بر اعتبار تپسی داشت. کاربران نسبت به امنیت داده‌های خود نگران شدند، و این موضوع باعث کاهش اعتماد عمومی به خدمات این شرکت شد. در روزهای پس از این حادثه، واکنش‌های کاربران در شبکه‌های اجتماعی نیز گسترده بود. اما مانند مورد اسنپ، در بلند مدت، برخلاف اینکه هیچ‌گونه خسارتی به کاربران پرداخت نشد، این واکنش‌های منفی کاهش یافت و فراموش شد.

۵-۲-۶. دعاوی جمعی و توافق‌ها

در این مورد نیز نه توسط مردم و نه سازمان‌های مربوطه (مانند پلیس فتا و دادستانی کل کشور)، دعاوی حقوقی علیه تپسی شکل نگرفت. تپسی رسماً اعلام کرد که حاضر به پرداخت باج به هکرها نیست. با وجود این، گروه هکری اطلاعات محدودی را برای اثبات ادعای خود منتشر کرد، اما داده‌های گسترده‌تر به‌طور عمومی منتشر نشد.

۵-۳. گزارش موردی: حمله هکری به ۲۰ بانک ایرانی

حمله سایبری به ۲۰ بانک ایرانی در شهریور ماه ۱۴۰۳ توسط گروه هکری IRLeaks یکی از بزرگ‌ترین رخدادهای امنیتی در حوزه بانکی ایران محسوب می‌شود. این حمله باعث افشای حجم زیادی از اطلاعات حساس مشتریان و تهدید امنیت اطلاعات مالی شد. در ادامه، ابعاد مختلف این حادثه به تفصیل بررسی می‌شود.

در شهریورماه ۱۴۰۳، گروه هکری IRLeaks با نفوذ به سامانه‌های ۲۰ بانک ایرانی، اطلاعات حساس میلیون‌ها مشتری را به سرقت برد. این حمله، که به‌عنوان یکی از پیچیده‌ترین حمله‌های سایبری علیه زیرساخت‌های بانکی ایران شناخته می‌شود، نگرانی‌هایی در خصوص امنیت داده‌ها و حفاظت از اطلاعات شخصی شهروندان ایجاد کرد. در پی این حادثه، شرکت تأمین‌کننده خدمات الکترونیکی بانکی توسن متهم به عدم رعایت استانداردهای امنیتی شد [۱۲۰].

۵-۳-۱. اعلامیه‌های رسمی

ابتدا هیچ‌یک از بانک‌های هدف و نهادهای نظارتی به‌صورت رسمی این حمله را تأیید نکردند. اما پس از انتشار گزارش‌هایی ازسوی رسانه‌ها، بانک مرکزی ایران و شرکت توسن[1] مجبور به ارائه توضیحات شدند. با این حال هیچ‌گاه پاسخ‌گویی و اطلاعیه‌ای رسمی در این زمینه منتشر نشد.

۵-۳-۲. تعداد افراد تحت تأثیر

گزارش‌ها نشان می‌دهد اطلاعات بیش از ۲۰ میلیون مشتری، شـــامل داده‌های حساب‌های بانکی، کارت‌های اعتباری و اطلاعات شخصی کاربران در این حمله به خطر افتاده است.

۵-۳-۳. داده‌های لورفته

اطلاعات منتشر شده در این حمله شامل نام و نام خانوادگی، شماره کارت بانکی و تاریخ انقضا، شماره شناسنامه و کد ملی، موجودی حساب و جزئیات تراکنش‌ها، اطلاعات تماس شامل شماره تلفن و آدرس است.

۵-۳-۴. اقدام‌های سازمان

هیچ‌گاه شفاف نشد.

۵-۳-۵. اثر اتفاق بر شرکت

به‌علت اینکه تمام بستر بانکی تهدید شد، کاربران تقریباً امکان جایگزینی نداشتند و نمی‌توانستند فعالیت‌های مالی خود را به بستر دیگری منتقل کنند، به همین دلیل ازسوی کاربران اثر خاصی رخ نداد.

۵-۳-۶. دعاوی جمعی و توافق‌نامه‌ها

مانند هک اسنپ و تپسی، و برخلاف خصوصی بودن این دو شرکت، بانک‌ها جزو بخش دولتی محسوب می‌شدند، هیچ اقدامی درباره دعاوی فردی و جمعی و توافق با کاربران انجام نشد.

۵-۳-۷. آیا باج پرداخت شد؟

طبق گزارش‌ها، شرکت توسن برای جلوگیری از افشای بیشتر اطلاعات، مبلغی معادل ۳ میلیون دلار به گروه هکری پرداخت کرد. این گروه هکری پس از دریافت این مبلغ، بخشی از اطلاعات را حذف کرد، اما مشخص نیست که آیا تمام داده‌ها بازگردانده شده یا امکان سوءاستفاده از آن‌ها همچنان وجود دارد[۱۲۰].

این حمله سایبری بار دیگر ضعف‌های جدی در زیرساخت‌های امنیت سایبری ایران را آشکار کرد. اگرچه شرکت توسن تلاش کرد تا آثار این حمله را کاهش دهد، اما افشای اطلاعات میلیون‌ها مشتری ضربه‌ای جدی به اعتبار نظام بانکی کشور وارد کرد. همچنین، عدم شفافیت و واکنش نهادهای مسئول به این حمله، به نگرانی‌های عمومی افزود. این پرسش پیش می‌آید که چرا در چنین مواقعی، از نظر قانونی، سازمان‌ها ملزم به پاسخ‌گویی نیستند؟ و همچنین کاربران نیز حساسیت چندانی نسبت به داده‌های خود ندارند.

۵-۴. گزارش موردی: هک اطلاعات شرکت‌های بیمه در ایران

در شهریورماه ۱۴۰۲، حمله‌ای سایبری به شبکه اطلاعاتی ۱۸ شرکت بیمه در ایران رخ داد که به‌عنوان یکی از گسترده‌ترین حمله‌های سایبری به صنعت بیمه کشور شناخته شد. این حمله به افشای اطلاعات میلیون‌ها بیمه‌گذار منجر شد. اطلاعات منتشر شده شامل داده‌های هویتی و بیمه‌ای کاربران بود که نگرانی‌های زیادی در مورد حفظ حریم خصوصی و سوءاستفاده از داده‌ها ایجاد کرد.

۱. شرکت توسن (TOSAN) یکی از شرکت‌های ایرانی در حوزه نرم‌افزارهای بانکی و پرداخت اســـت که راهکارهای بانکداری الکترونیک و سامانه‌های مالی را برای بانک‌ها و مؤسسات مالی ارائه می‌دهد.

۵-۴-۱. اعلامیه‌های رسمی

شرکت بیمه مرکزی ایران و برخی شرکت‌های بیمه‌ای ابتدا وقوع حمله را تکذیب کردند یا آن را به «شبه‌افکنی» رسانه‌ها نسبت دادند. با این حال، بعداً گزارش‌هایی منتشر شد که نشان می‌داد اطلاعات حساس کاربران به دست هکرها افتاده و در فضای مجازی برای فروش گذاشته شده است. بیمه مرکزی تأیید کرد که به برخی شرکت‌ها درباره ضعف‌های امنیتی هشدار داده شده بود، اما به صراحت مسئولیت این رویداد را نپذیرفت[۱۲۱].

۵-۴-۲. تعداد افراد تحت تأثیر و داده‌های لورفته

براساس ادعاهای هکرها، اطلاعات بیش از ۱۱۵ میلیون بیمه‌گذار شامل نام، نام خانوادگی، تاریخ تولد، نام پدر، شماره تلفن/موبایل، شماره شناسنامه، کد ملی، کد ملی شرکت و... لورفته است. این اطلاعات شـــامل بیمه‌های شخص ثالث، عمر و سلامت بوده و حجم گسترده‌ای از داده‌ها را دربر می‌گیرد[۱۲۱].

۵-۴-۳. اقدام‌های سازمان

اقدام‌های سازمان مشخص نیست. حمله به شـــرکت‌های بیمه ایران، زنگ خطری جدی برای صنعت مالی و بیمه‌ای کشور بود. این رویداد نشان داد که علی‌رغم اهمیت داده‌های کاربران، اقدام‌های کافی برای حفاظت از آن‌ها انجام نشده و برای جلوگیری از حمله‌های مشابه، نیاز به سرمایه‌گذاری در امنیت سایبری، تدوین قوانین جدید و شفاف‌سازی در برخورد با چنین رویدادهایی لازم است.

۶. مروری بر قوانین حفاظت از داده در دنیا

در ادامه، خلاصه‌ای از مهم‌ترین قوانین مربوط به نقض داده را مرور خواهیم کرد:[۱۲۲] [۱۲۳] [۱۲۴] [۱۲۵] [۱۲۶] [۱۲۷] [۱۲۸] [۱۲۹] [۱۳۰] [۱۳۱] [۱۳۲].

الف) ایالات متحده آمریکا: در ایالات متحده، ۴۸ ایالت و ناحیه کلمبیا دارای قوانین نقض داده و امنیت اطلاعات هستند که سازمان‌ها و نهادهای دولتی را ملزم به اطلاع‌رسانی درباره نقض‌های امنیتی در صورت تأثیر بر اطلاعات شخصی شناسایی‌شده می‌کنند. شرکت‌ها نیز ممکن است ملزم به اقدام برای کاهش آثار نقض شـــوند. کمیسیون تجارت فدرال (FTC) می‌تواند شرکت‌هایی را که سیاست‌های حفظ حریم خصوصی اعلام شـــده خود را رعایت نمی‌کنند و از اطلاعات مشتریان محافظت نمی‌کنند، بررسی کند. با این حال، هیچ قانون فدرال جامع برای اطلاع‌رسانی نقض‌ها وجود ندارد.

قوانین و مقررات امنیت داده‌ای که در سطح فدرال اجرا می‌شوند شامل موارد زیر هستند:

- **قانون** Gramm-Leach-Bliley (GLB): مؤسسات مالی را ملزم به حفظ امنیت و محرمانگی اطلاعات شخصی می‌کند.
- **قانون** FTC Safeguards Rule: مؤسسات مالی مشخصی را به ایجاد تدابیر امنیتی برای حفاظت از اطلاعات مشتریان ملزم می‌کند.
- **قانون** HIPAA Breach Notification Rule: نهادهای تحت پوشش HIPAA را به اطلاع‌رسانی درباره نقض اطلاعات بهداشتی محافظت‌شده ملزم می‌کند.
- **قانون** FTC Health Breach Notification Rule: شرکت‌های مرتبط با سلامت (که تحت HIPAA نیستند) را به اطلاع‌رسانی درباره نقض اطلاعات سلامت الکترونیکی ملزم می‌کند.

ب) اتحادیه اروپا: اتحادیه اروپا دارای یکی از جامع‌ترین و سخت‌گیرانه‌ترین قوانین حفاظت از داده در جهان است که تحت مقررات عمومی حفاظت از داده‌ها (GDPR) اجرا می‌شود. این مقررات تمامی شرکت‌ها و سازمان‌هایی را که داده‌های شهروندان اتحادیه اروپا را پردازش می‌کنند، صرف نظر از محل استقرار آن‌ها، ملزم به رعایت الزام‌های سخت‌گیرانه می‌کند.

براساس GDPR، سازمان‌ها موظفند هرگونه نقض داده را ظرف ۷۲ ساعت به مقام‌های نظارتی مربوطه اطلاع دهند، مگر اینکه این نقض خطر جدی برای حقوق و آزادی افراد نداشته باشد. همچنین، در صورت تأثیرگذاری زیاد نقض بر افراد، شرکت‌ها باید به آن‌ها اطلاع دهند. مجازات‌های عدم رعایت می‌تواند تا ۲۰ میلیون یورو یا ۴ درصد از درآمد سالیانه جهانی شرکت باشد.

مهم‌ترین اصول GDPR شامل موارد زیر است:

- **شفافیت:** سازمان‌ها باید کاربران را از نحوه جمع‌آوری و پردازش داده‌هایشان آگاه کنند.
- **مسئولیت‌پذیری:** سازمان‌ها باید اقدام‌های لازم برای حفاظت از داده‌ها را انجام دهند و در برابر نهادهای نظارتی پاسخگو باشند.
- **حقوق افراد:** شامل حق دسترسی، اصلاح، حذف و انتقال داده‌ها به سایر ارائه‌دهندگان خدمات است.

در سراسر اتحادیه اروپا، نهادهای نظارتی مانند دفتر کمیساریای اطلاعات بریتانیا (ICO) و کمیسیون ملی اطلاعات و آزادی‌های فرانسه (CNIL) وظیفه اجرای این مقررات را برعهده دارند.

جدول ۲. مقایسه قوانین حفاظت از داده‌ها، مهلت‌ها، جرائم و نهادهای نظارتی در کشورهای مختلف TopofForm

کشور	نام قانون	مهلت اطلاع‌رسانی	جریمه‌ها و مجازات‌ها	مرجع نظارتی	الزام‌های اطلاع‌رسانی	دامنه اجرایی
اتحادیه اروپا	مقررات عمومی حفاظت از داده‌ها (GDPR)	۷۲ ساعت	تا ۲۰ میلیون یورو یا ۴ درصد از درآمد جهانی	کمیسیون اروپا (EDPB)	به تنظیم‌کننده و افراد آسیب‌دیده	جهانی (فراتر از مرزهای اتحادیه اروپا)
ایالات متحده	CCPA و CPRA	بدون زمان مشخص	تا ۷,۵۰۰ دلار به ازای هر تخلف	دادستان کل کالیفرنیا	به مصرف‌کنندگان و دادستان کل	ایالت کالیفرنیا
کانادا	PIPEDA	زمان معقول	تا ۱۰۰,۰۰۰ دلار کانادا	کمیسیون حفظ حریم خصوصی کانادا	به OPC و افراد آسیب‌دیده	سراسری
بریتانیا	قانون حفاظت از داده (DPA)	۷۲ ساعت	مطابق با GDPR	کمیساریای اطلاعات (ICO)	به ICO و افراد آسیب‌دیده	سراسری
چین	قانون حفاظت از اطلاعات شخصی (PIPL)	بدون زمان مشخص	جریمه‌های سنگین برای عدم رعایت	اداره فضای مجازی چین (CAC)	به CAC	سراسری
هند	قانون حفاظت از داده‌های شخصی (DPDP)	بدون زمان مشخص	جریمه‌های سنگین برای عدم اطلاع‌رسانی	هیئت حفاظت از داده‌ها	به هیئت حفاظت از داده‌ها	سراسری
ژاپن	قانون حفاظت از اطلاعات شخصی (APPI)	بدون زمان مشخص	جریمه‌های مالی برای عدم رعایت	کمیسیون حفاظت از اطلاعات شخصی (PIPC)	به PIPC	سراسری
عربستان سعودی	قانون حفاظت از داده‌ها (PDPL)	۷۲ساعت	تا ۵ میلیون ریال سعودی	سازمان ملی امنیت سایبری	به نهاد نظارتی و افراد آسیب‌دیده	سراسری

کشور	نام قانون	مهلت اطلاع‌رسانی	جریمه‌ها و مجازات‌ها	مرجع نظارتی	الزام‌های اطلاع‌رسانی	دامنه اجرایی
آفریقای جنوبی	قانون حمایت از اطلاعات شخصی (POPIA)	بدون زمان مشخص	جریمه‌های مالی و احتمال زندان	تنظیم‌کننده اطلاعات	به نهاد نظارتی و افراد آسیب‌دیده	سراسری
برزیل	قانون LGPD	بدون زمان مشخص	۲ درصد از درآمد ناخالص، حداکثر ۵۰ میلیون ریال	سازمان ملی حفاظت از داده‌ها (ANPD)	به ANPD	سراسری
مکزیک	قانون فدرال حفاظت از داده (LFPDPPP)	۵ روز	جریمه‌های مالی	مؤسسه شفافیت و حمایت از داده	به نهاد نظارتی	سراسری

مأخذ: گردآوری‌شده توسط نویسنده.

۷. چالش‌های امنیت سایبری

با توجه به مطالعات موردی بررسی شده می‌توان چالش‌های امنیت سایبری را موارد ذیل دانست: ۱. ضعف زیرساخت‌های امنیت سایبری ۲. ضعف مدیریت داده‌ها ۳. اطلاع‌رسانی ناکارآمد نقض‌ها ۴. کمبود نیروی انسانی متخصص ۵. عدم مسئولیت‌پذیری شرکت‌ها و سازمان‌ها ۶. هزینه بالای امنیت سایبری ۷. ضعف در واکنش به حوادث سایبری ۸. ضعف نظارت و قوانین جامع ۹. آثار تحریم‌ها و فیلترینگ و ۱۰. پیامدهای گسترده نقض‌ها. در جدول ۳ شرح این چالش‌ها و شیوه‌های مواجه پیشنهادی برای مقابله با آنها تلخیص شده است.

جدول ۳. مشکل‌ها و شیوه‌های مواجهه پیشنهادی در امنیت سایبری ایران

چالش	شرح مشکل	شیوه‌های مواجهه پیشنهادی
۱. ضعف زیرساخت‌های امنیت سایبری	زیرساخت‌های فناوری اطلاعات در شرکت‌ها و سازمان‌ها به‌طورکلی برای مقابله با حمله‌های سایبری طراحی نشده‌اند و از استانداردهای بین‌المللی فاصله دارند.	• ممیزی‌های اجباری امنیت سایبری: الزام شرکت‌ها به انجام ممیزی‌های منظم توسط شرکت‌های معتبر شخص ثالث برای ارزیابی زیرساخت‌ها و شیوه‌های امنیتی. • گواهینامه‌های استاندارد: الزام به دریافت گواهینامه‌های بین‌المللی مانند ISO/IEC ۲۷۰۰۱ که نشان‌دهنده رعایت استانداردهای امنیتی باشد. • به‌روزرسانی سیستم‌ها: الزام به به‌روزرسانی منظم نرم‌افزارها و سخت‌افزارهای امنیتی برای جلوگیری از آسیب‌پذیری‌ها. • توسعه نرم‌افزار ایمن: استفاده از اصول توسعه نرم‌افزار امن شامل تست نفوذ و بررسی کد.
۲. ضعف مدیریت داده‌ها	داده‌های کاربران اغلب بدون امنیت مناسب ذخیره شده یا در حجم زیاد نگهداری می‌شوند که خطر افشا یا سوءاستفاده را افزایش می‌دهد.	• حداقل‌سازی داده‌ها: الزام شرکت‌ها به جمع‌آوری فقط داده‌های ضروری و حذف داده‌های قدیمی یا غیرضروری. • ناشناس‌سازی داده‌ها: استفاده از تکنیک‌های ناشناس‌سازی و مستعارسازی برای کاهش خطر افشای داده‌های حساس. • پاکسازی دوره‌ای: الزام به پاکسازی دوره‌ای داده‌ها برای کاهش حجم اطلاعات ذخیره‌شده. • رمزگذاری داده‌ها: استفاده از رمزگذاری قوی برای داده‌ها در حالت استراحت و انتقال.

چالش	شرح مشکل	شیوه‌های مواجهه پیشنهادی
۳. اطلاع‌رسانی ناکارآمد نقض‌ها	شرکت‌ها و سازمان‌ها اغلب نقض‌های امنیتی را به‌موقع یا به‌صورت شفاف اطلاع نمی‌دهند، که به بی‌اعتمادی کاربران و گسترش آسیب‌ها منجر می‌شود.	• قوانین اطلاع‌رسانی اجباری: الزام شرکت‌ها به گزارش نقض داده‌ها ظرف حداکثر ۷۲ ساعت به کاربران و مقام‌های نظارتی. • شفافیت عمومی: الزام شرکت‌ها به ارائه گزارش عمومی درباره نوع نقض، داده‌های تحت تأثیر و اقدام‌های انجام‌شده. • جریمه‌های تأخیر: اعمال جریمه‌های سنگین برای تأخیر در اطلاع‌رسانی یا ارائه اطلاعات ناقص.
۴. کمبود نیروی انسانی متخصص	کمبود نیروی کار ماهر در زمینه امنیت سایبری، مدیریت داده‌ها و فناوری اطلاعات باعث افزایش خطر نقض داده‌ها و ضعف پاسخگویی به تهدیدها می‌شود.	• سرمایه‌گذاری در آموزش: ارائه برنامه‌های آموزشی جامع برای تربیت نیروی کار متخصص در امنیت سایبری. • مشوق‌های دولتی: اعطای کمک‌های مالی یا مشوق‌های مالیاتی به شرکت‌ها برای آموزش کارکنان. • همکاری دولتی و خصوصی: تشویق شرکت‌ها به همکاری با نهادهای دولتی و دانشگاه‌ها برای توسعه نیروی کار متخصص.
۵. عدم مسئولیت‌پذیری شرکت‌ها و سازمان‌ها	بسیاری از شرکت‌ها و سازمان‌ها در قبال نقض داده‌ها پاسخگو نیستند و تمایلی به اجرای سیاست‌های امنیتی سخت‌گیرانه ندارند.	• جریمه‌های مالی سنگین: اعمال جریمه‌های قابل توجه براساس درصدی از درآمد سالیانه برای نقض‌های امنیتی. • مسئولیت‌پذیری قانونی: ارائه مجازات کیفری برای مدیران اجرایی در موارد بی‌توجهی شدید به امنیت. • مسئولیت شرکت‌های بیمه: الزام شرکت‌های بیمه به ارائه پوشش مالی برای خسارت‌های ناشی از نقض داده‌ها.
۶. هزینه بالای امنیت سایبری	شرکت‌های کوچک و متوسط (SMEs) به‌علت محدودیت بودجه نمی‌توانند از فناوری‌های پیشرفته امنیتی استفاده کنند.	• مشوق‌های مالیاتی: ارائه معافیت‌های مالیاتی برای شرکت‌هایی که در امنیت سایبری سرمایه‌گذاری می‌کنند. • کمک‌های دولتی: اعطای وام‌ها یا کمک‌های مالی به شرکت‌های کوچک برای ارتقای زیرساخت‌های امنیتی. • بیمه امنیت سایبری: الزام به خرید بیمه امنیت سایبری برای جبران هزینه‌های خسارت و غرامت.
۷. ضعف در واکنش به حوادث سایبری	بسیاری از شرکت‌ها و سازمان‌ها فاقد برنامه‌های مؤثر برای شناسایی، مهار و رفع نقض‌های امنیتی هستند.	• برنامه‌های واکنش به حوادث: الزام به طراحی و پیاده‌سازی برنامه‌های جامع واکنش به حوادث سایبری. • مانورهای سایبری: برگزاری دوره‌ای تمرین‌ها و رزمایش‌های شبیه‌سازی برای آماده‌سازی تیم‌ها. • استفاده از هوش مصنوعی: توسعه سیستم‌های مبتنی‌بر هوش مصنوعی برای شناسایی و مهار سریع تهدیدها.
۸. ضعف نظارت و قوانین جامع	نبود چارچوب قانونی یکپارچه و نهاد نظارتی قوی به عدم هماهنگی در مدیریت امنیت سایبری منجر شده است.	• قانون جامع حفاظت از داده‌ها: تصویب قانونی که حقوق و مسئولیت‌های تمامی ذی‌نفعان را مشخص کند. • نهاد حفاظت از داده‌ها: ایجاد یک نهاد مستقل با اختیارات قانونی برای نظارت، تحقیق و اعمال جریمه. • قدرت‌های اجرایی: اعطای اختیار به نهاد نظارتی برای تعقیب قانونی نقض‌کنندگان.

چالش	شرح مشکل	شیوه‌های مواجهه پیشنهادی
۹. آثار تحریم‌ها و فیلترینگ	تحریم‌ها و فیلترینگ باعث محدودیت در دسترسی به فناوری‌ها، تجهیزات و اطلاعات به‌روز شده و شرکت‌ها را آسیب‌پذیرتر کرده است.	• حمایت از تولید داخلی: سرمایه‌گذاری در تولید تجهیزات و نرم‌افزارهای امنیتی بومی. • همکاری بین‌المللی: ایجاد مسیرهایی برای همکاری با سازمان‌های بین‌المللی مانند ITU و UN در حوزه امنیت سایبری مانند آموزش‌های امنیتی و رفتاری، ارتقای استانداردهای امنیتی و... • برطرف‌سازی موانع فیلترینگ: ایجاد استثناهایی در سیاست فیلترینگ برای تسهیل دسترسی به ابزارها و خدمات امنیتی.
۱۰. پیامدهای گسترده نقض‌ها	نقض داده‌ها می‌تواند پیامدهای مالی، حقوقی و اعتباری گسترده‌ای برای شرکت‌ها به‌همراه داشته باشد.	• بیمه مصرف‌کنندگان: الزام شرکت‌ها به ارائه بیمه برای کاربران در برابر سرقت هویت یا خسارت مالی. • دعاوی جمعی: ایجاد سازوکارهایی برای پیگیری حقوقی توسط کاربران آسیب‌دیده. • شفافیت بیشتر: الزام شرکت‌ها به همکاری کامل با تحقیقات نهادهای نظارتی و ارائه جزئیات نقض‌ها.

مأخذ: همان.

۸. جمع‌بندی و پیشنهادها

امنیت سایبری و حفاظت از داده‌ها در جوامع مدرن به یکی از دغدغه‌های اصلی تبدیل شده است، به‌ویژه در کشورهایی مانند ایران که وابستگی آن‌ها به فناوری دیجیتال و زیرساخت‌های اطلاعاتی روزبه‌روز افزایش می‌یابد. در سال‌های اخیر، مجموعه‌ای از حمله‌های سایبری گسترده به زیرساخت‌های دولتی و خصوصی ایران، مانند سیستم‌های بانکی، ثبت احوال، شرکت‌های بیمه و سکوهای خدماتی، نقاط ضعف جدی در مدیریت امنیت داده‌ها را نمایان می‌کند.

این حمله‌ها تأثیرهای مخربی بر امنیت اطلاعات کاربران و اعتبار سازمان‌ها داشته و ضعف زیرساخت‌های امنیتی، نبود قوانین جامع حفاظت از داده‌ها، کمبود شفافیت در اطلاع‌رسانی و پاسخگویی و همچنین کمبود نیروی انسانی متخصص در حوزه امنیت سایبری را برجسته کرده است. پیامدهای این حمله‌ها تنها محدود به خسارت‌های اقتصادی نیست، بلکه باعث تضعیف اعتماد عمومی به نهادها، افزایش آسیب‌پذیری امنیت ملی و کاهش رقابت‌پذیری شرکت‌های ایرانی در بازارهای جهانی نیز شده است.

درنتیجه سیاستگذاری مؤثر، تصویب قوانین جامع و نظارت دقیق می‌تواند نقشی کلیدی در کاهش این تهدیدها و حفاظت از داده‌ها داشته باشد. طبق بررسی تجربه‌های بین‌المللی تدوین چارچوب‌های قانونی منسجم، ایجاد نهادهای نظارتی قدرتمند و اجرای برنامه‌های آموزشی جامع می‌تواند اثر قابل توجهی بر ارتقای امنیت سایبری داشته باشد.

پیشنهادها

برای مقابله با تهدیدهای امنیت سایبری و بهبود حفاظت از داده‌ها در ایران، مجموعه‌ای از اقدام‌های تقنینی، سیاستگذاری و نظارتی پیشنهاد می‌شود:

تقنینی

ایران نیازمند تصویب قوانین جامع حفاظت از داده‌هاست. یک قانون جامع، مشابه مقررات حفاظت از داده‌های عمومی (GDPR) در اتحادیه اروپا، باید تدوین شود که شامل حقوق کاربران، مسئولیت سازمان‌ها، الزام‌های شفافیت و جریمه‌های سنگین برای تخلف‌ها باشد. این قانون

باید تمامی ذی‌نفعان، مانند سازمان‌های دولتی و خصوصی را ملزم به رعایت اصول شـــفافیت و حفاظت از داده‌ها کند. البته شفافیت برای نهادهای امنیتی و نظامی ملزم به ملاحظه‌هایی متفاوت از دیگر سازمان‌های دولتی و خصوصی است. بنابراین برای شفافیت در این حوزه‌ها می‌توان نهاد ناظری مانند ستاد کل نیروهای مسلح را پیشنهاد کرد.

علاوه‌بر این، تدوین ســـازوکارهایی برای طرح دعاوی جمعی، که به کاربران امکان می‌دهد در صورت نقض امنیت داده‌هایشان اقدام قانونی انجام دهند، ضروری است. این اقدام‌ها می‌توانند باعث تقویت پاسخگویی سازمان‌ها شوند و کاربران را برای مطالبه حقوق خود توانمند کند.

سیاستگذاری

ایجاد یک نهاد مستقل حفاظت از داده‌ها با اختیارهای اجرایی می‌تواند نقطه عطفی در مدیریت امنیت سایبری باشد. این نهاد باید مسئول نظارت بر حفاظت از داده‌ها، تحقیق در مورد نقض‌ها و اعمال جریمه‌های لازم باشد.

همچنین، اجرای ممیزی‌های سالیانه توسط شرکت‌های معتبر برای ارزیابی زیرساخت‌های امنیتی و مدیریت داده‌ها ضروری است.

علاوه‌بر این، شرکت‌ها باید تشویق به خرید بیمه امنیت سایبری شوند تا هزینه‌های مالی ناشی از حمله‌های سایبری جبران شود. دولت می‌تواند ازطریق ارائه تخفیف‌های مالیاتی یا کمک‌های مالی، شرکت‌های کوچک و متوسط را به سرمایه‌گذاری در امنیت سایبری تشویق کند.

همچنین، توسعه برنامه‌های آموزشی برای تربیت نیروی انسانی متخصص در حوزه امنیت سایبری، از اولویت‌های مهم سیاستگذاری است. این برنامه‌ها باید در سطح مدارس، دانشگاه‌ها و سازمان‌ها پیاده‌سازی شوند تا کمبود نیروی کار متخصص کاهش یابد.

نظارت و اجرا

الزام سازمان‌ها به شفافیت در اطلاع‌رســـانی نقض‌های امنیتی یکی از گام‌های مهم در بهبود اعتماد عمومی است. سازمان‌ها باید ظرف ۷۲ ساعت پس از وقوع نقض، آن را به کاربران و نهادهای نظارتی اطلاع دهند. این اقدام می‌تواند به کاهش آسیب‌ها و پیشگیری از سوءاستفاده بیشتر کمک کند.

تقویت نظارت بر زیرساخت‌ها ازطریق پیاده‌سازی سیستم‌های پیشرفته شناسایی تهدیدها، به‌ویژه مبتنی‌بر هوش مصنوعی، از دیگر اقدام‌های ضروری است.

همچنین برگزاری رزمایش‌های سایبری دوره‌ای می‌تواند آمادگی سازمان‌ها را برای مقابله با حمله‌های سایبری افزایش دهد.

علاوه‌بر این، الزام سازمان‌ها به طراحی و پیاده‌ســـازی تکنیک‌های ناشناس‌سازی داده‌ها می‌تواند خطرهای ناشی از افشای اطلاعات را کاهش دهد.

منابع و مآخذ

[۱] ادعای هک اسنپ‌فود و افشای اطلاعات کاربران؛ اسنپ‌فود بیانیه داد.
https://digiato.com/iran-technology-news/snapfood-issued-statement-hacking-platform.
[2] Stolen Data of 533 Million Facebook Users Leaked Online - Business Insider. https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.
[3] https://twitter.com/UnderTheBreach/status/1378314424239460352.
[4] Facebook Data Breaches: Full Timeline Through 2023.
[5] The Facts on News Reports About Facebook Data. https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/.
[6] Amazon Ring No Longer Sharing Home Security Footage With Police, Company Says - CNET. https://www.cnet.com/home/ring-will-stop-sharing-video-with-police-with-some-exceptions-heres-what-it-means-for-you/.
[7] 533 million Facebook users' phone numbers and personal data have been leaked online.
[8] After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users : NPR. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.
[9] Everything You Need to Know About the 2021 Facebook Data Breach. https://heimdalsecurity.com/blog/everything-you-need-to-know-about-the-2021-facebook-data-breach/.
[10] Have I Been Pwned: Check if your email address has been exposed in a data breach. https://haveibeenpwned.com/.
[11] The FB breach has certainly generated some interest, currently doing 40k-45k requests per min on... https://twitter.com/troyhunt/status/1378802860939309056.
[12] Facebook usage falling after privacy scandals, data suggests | Facebook | The Guardian. https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows.
[13] Declines in Facebook Usage Drive Down Average Time Spent on Social Media. https://www.emarketer.com/content/average-social-media-time-spent.
[14] #DeleteFacebook. https://web.archive.org/web/20250425112056/https://moveme.studentorg.berkeley.edu/project/deletefacebook/.
[15] Facebook stock recovers all $134B lost after Cambridge Analytica data scandal - CBS News. https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-in-after-cambridge-analytica-datascandal.
[16] ICT Institute | Facebook Personal Data Breach, the aftermath. https://ictinstitute.nl/facebook-personal-data-breach-the-aftermath/.
[17] Facebook was repeatedly warned of security flaw that led to biggest data breach in its history. https://www.telegraph.co.uk/technology/2020/02/09/facebook-repeatedly-warned-security-flaw-led-biggest-data-breach/.
[18] Investor class action over Facebook's Cambridge Analytica breach DOA. https://www.reuters.com/legal/litigation/investor-class-action-over-facebooks-cambridge-analytica-breach-doa-2021-12-21/.
[19] Court Denies Dismissal Motion in Facebook User Data Privacy Derivative Suit. https://www.dandodiary.com/2023/05/articles/shareholders-derivative-litigation/court-denies-dismissal-motion-in-facebook-user-data-privacy-derivative-suit/.
[20] Facebook paid billions extra to the FTC to spare Zuckerberg in data suit, shareholders allege. https://www.politico.com/news/2021/09/21/facebook-paid-billions-extra-to-the-ftc-to-spare-zuckerberg-in-data-suit-shareholders-allege-513456.
[21] Facebook Data Breach Class Action. https://kmlaw.ca/cases/facebook-data-breach-class-action/.
[22] Digital Rights Ireland agrees settlement with Irish Data Protection Commission over data breach complaint - Digital Rights Ireland. https://www.digitalrights.ie/digital-rights-ireland-agrees-settlement-with-irish-data-protection-commission-over-data-breach-complaint.
[23] Facebook data breach mass action – Digital Freedom Fund. https://digitalfreedomfund.org/facebook-data-breach-mass-action.
[24] Mass legal action against Facebook over data breach. https://www.rte.ie/news/2021/0416/1210188-facebook-data-case.

[25] DRI Facebook Action - Digital Rights Ireland. https://www.digitalrights.ie/facebook/.
[26] Dutch court finds Facebook misused data in class action suit. https://www.reuters.com/technology/dutch-court-finds-facebook-used-dutch-personal-data-incorrectly-2023-03-15/.
[27] Digital Rights Ireland to sue for damages for Facebook users over dark web data leak. https://www.irishexaminer.com/news/arid-41064308.html.
[28] How to Claim Your Share of Facebook's $725 Million Privacy Settlement. https://www.nytimes.com/2023/04/20/business/facebook-settlement-apply.html.
[29] Facebook parent Meta to settle Cambridge Analytica scandal case for $725 million. https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/.
[30] In re: Facebook, Inc. Consumer Privacy User Profile Litigation. https://facebookuserprivacysettlement.com/.
[31] Facebook parent Meta agrees to pay $725 million to settle privacy lawsuit. https://www.cnbc.com/2022/12/23/facebook-parent-meta-agrees-to-pay-725-million-to-settle-privacy-lawsuit-prompted-by-cambridge-analytica-scandal.html.
[32] Meta to Pay $725 Million to Settle Cambridge Analytica Lawsuit. https://www.wsj.com/articles/meta-to-pay-725-million-to-settle-cambridge-analytica-lawsuit-11671797385.
[33] Facebook Privacy Settlement Payouts: Here's How Much Money You'll Get – Forbes Advisor. https://www.forbes.com/advisor/legal/facebook-class-action-lawsuit-settlement/.
[34]Digital Rights Ireland takes DPC to Court Over Facebook's 530 Million Users' Data Leak - Digital Rights Ireland. https://www.digitalrights.ie/dri-takes-dpc-to-court-over-facebook-data-leak/.
[35] Meta fined €265m over data protection breach that hit more than 500m users | Meta | The Guardian. https://www.theguardian.com/technology/2022/nov/28/meta-fined-265m-over-data-breach-affecting-more-than-500m-users.
[36] Meta fined $276 million over Facebook data leak involving more than 533 million users. https://www.theverge.com/2022/11/28/23481786/meta-fine-facebook-data-leak-ireland-dpc-gdpr.
[37] Meta fined over $400 million by top EU regulator for forcing users to accept targeted ads. https://www.cnbc.com/2023/01/04/meta-fined-more-than-400-million-in-ireland-over-eu-privacy-breaches.html.
[38] Facebook owner Meta fined €1.2bn for mishandling user information | Data protection | The Guardian. https://www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta.
[39] Meta Was Just Fined a Record-Breaking $1.3 Billion by E.U. Regulators. https://time.com/6281713/meta-facebook-fine-eu/.
[40] Facebook settles with FTC: $5 billion and new privacy guarantees | TechCrunch. https://techcrunch.com/2019/07/24/facebook-settles-with-ftc-5-billion-and-new-privacy-guarantees/.
[41] FTC slaps Facebook with record $5 billion fine, orders privacy oversight. https://www.cnbc.com/2019/07/24/facebook-to-pay-5-billion-for-privacy-lapses-ftc-announces.html.
[42] Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data. https://www.sec.gov/news/press-release/2019-140.
[43] Facebook Data Breaches: Full Timeline Through 2023. https://firewalltimes.com/facebook-data-breach-timeline/.
[44] Legal Implications of the Facebook Data Breach. https://web.archive.org/web/20240417050324/https://www.kelleykronenberg.com/category/blog/technology-data-privacy-and-social-media/legal-implications-of-the-facebook-data-breach/.
[45] Yahoo Security Notice September 22, 2016. https://help.yahoo.com/kb/account/sln28092.html.
[46] Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million. https://www.sec.gov/news/press-release/2018-71.
[47] Yahoo Security Notice December 14, 2016. https://help.yahoo.com/kb/account/SLN27925.html#cont10.
[48] Yahoo Says Hackers Stole Data on 500 Million Users in 2014. https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.
[49] Yahoo Security Notice December 14, 2016 Account Help | Yahoo Help. https://help.yahoo.com/kb/account/SLN27925.html#cont4.
[50] 10Biggest Data Breaches in History Revealed. https://web.archive.org/web/20241107205254/

https://tech.co/news/10-biggest-data-breaches.
[51] Stolen Yahoo Data Includes Government Employee Information. https://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-government-employee-information.
[52] SECURITIES ACT OF 1933
Release No. 10485 / April 24, 2018. https://www.sec.gov/files/litigation/admin/2018/33-10485.pdf.
[53] SHAREHOLDER ALERT: Pomerantz Law Firm Announces the Filing of a Class Action against Yahoo Inc. and Certain Officers - YHOO. https://finance.yahoo.com/news/shareholder-alert-pomerantz-law-firm-032600940.html.
[54] Yahoo shares fall after latest security breach. https://www.reuters.com/article/idUSKBN144238.
[۵۵] دعاوی جمعی و نقش آن‌ها در احقاق حقوق مصرف کنندگان.
https://jplr.atu.ac.ir/article_2220.html.
[56] Yahoo Data Breach Class Action. https://www.yahooclassaction.com.
[57] Yahoo! Privacy Breach Class Action | Home. https://www.charneylawyers.com/yahoo!-class-action.
[58] Yahoo Email Data Breach Class Action | Merchant Law Group LLP. https://www.merchantlaw.com/class-actions-recours-collectif-canada/yahoo-email-data-breach.
[59] Yahoo Data Breach Class Action Settlement. https://topclassactions.com/lawsuit-settlements/closed-settlements/yahoo-data-breach-class-action-settlement.
[60] Yahoo! Inc. Customer Data Security Breach Litigation Settlement. https://yahoodatabreachsettlement.com.
[61] Yahoo! Settles Data Breach Securities Class Action for $80 Million | ISS. https://www.issgovernance.com/yahoo-settles-data-breach-securities-class-action-80-million.
[62] Yahoo strikes $117.5 million data breach settlement after earlier accord rejected. https://www.reuters.com/article/idUSKCN1RL1GX.
[63] Yahoo data breach: $117.5 million settlement reached - CBS News. https://www.cbsnews.com/news/yahoo-data-breach-117-5-million-settlement-reached.
[64] For $80 Million, Yahoo! Settles Shareholder Class Action Claiming Stock Price Losses from Data Breaches. https://web.archive.org/web/20230204193800/https://www.pbwt.com/data-security-law-blog/for-80-million-yahoo-settles-shareholder-class-action-claiming-stock-price-losses-from-data-breaches/.
[65] Data Protection Commission concludes investigation into Yahoo Data Breach. https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-concludes-investigation-into-Yahoo-Data-Breach.
[66] Who we are. https://www.dataprotection.ie/en/who-we-are.
[67] The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far). https://www.ballardspahr.com/insights/alerts-and-articles/2018/05/yahoo-data-breach.
[68] SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2023-139.
[69] 10Years After Yahoo Breach, What's Changed? (Not Much). https://www.darkreading.com/cyberattacks-data-breaches/10-years-after-yahoo-whats-changed-not-much.
[70] Marriott International Inc. | Encyclopedia.com. https://www.encyclopedia.com/economics/economics-magazines/marriott-international-inc.
[71] Marriott International History: Founding, Timeline, and Milestones - Zippia. https://www.zippia.com/marriott-international-careers-7125/history.
[72] Marriott Announces Starwood Guest Reservation Database Security Incident. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident.
[73] Marriott News Center. https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/.
[74] Marriott Provides Update on Starwood Database Security Incident | Marriott International. https://marriott.gcs-web.com/news-releases/news-release-details/marriott-provides-update-starwood-database-security-incident.
[75] Passport information stolen as part of massive Marriott International data breach | Nixon Peabody LLP. https://www.nixonpeabody.com/insights/articles/2019/01/08/passport-information-stolen-as-part-of-massive-marriott-international-data-breach.

[76] Marriott reveals 5 million unencrypted passport numbers were leaked in 2018 data breach. https://www.nbcnews.com/tech/tech-news/marriott-reveals-5-million-unencrypted-passport-numbers-were-leaked-2018-n954791.
[77] Marriott's stock sinks after disclosing data breach affecting up to 500 million guests. https://www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30.
[78] Massive Data Breach at Marriott Pulls Shares Down. https://www.thestreet.com/investing/stocks/marriott-massive-data-breach-may-put-500-million-guests-information-at-risk-14796827.
[79] Cyber Case Study: Marriott Data Breach - CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/case-study/marriott-data-breach/.
[80] Marriott Data Breach FAQ: What Really Happened? https://hoteltechreport.com/news/marriott-data-breach.
[81] Marriott breach: Here's the risk of a compromised passport number. https://www.cnbc.com/2018/11/30/passports-compromised-in-the-marriott-breach-could-lead-to-fraud.html.
[82] Marriott Hackers Stole Data On 500 Million Guests -- Passports And Credit Card Info Included. https://www.forbes.com/sites/thomasbrewster/2018/11/30/marriott-admits-hackers-stole-data-on-500-million-guests/.
[83] SEC Filing | Marriott International. https://marriott.gcs-web.com/node/28301/html.
[84] Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.
[85] Marriott's data breach may be the biggest in history. Now it's facing multiple class-action lawsuits. https://www.vox.com/the-goods/2019/1/11/18178733/marriott-starwood-hack-lawsuit.
[86] Class Action Lawsuit Filed On Behalf Of Plaintiffs Whose Sensitive Personal Information Was Stolen In Breach Of Marriott Servers. https://www.prnewswire.com/news-releases/class-action-lawsuit-filed-on-behalf-of-plaintiffs-whose-sensitive-personal-information-was-stolen-in-breach-of-marriott-servers-300758440.html.
[87] Marriott sued hours after announcing data breach | ZDNET. https://www.zdnet.com/article/marriott-sued-hours-after-announcing-data-breach/.
[88] Fourth Circuit Decision in Marriott Data Breach Case Kicks the Can Down the Road | Electronic Frontier Foundation. https://www.eff.org/deeplinks/2023/08/fourth-circuit-decision-marriott-data-breach-case-kicks-can-down-road.
[89] Recent Marriott Data Breach Class Action Decision Underscores the Importance of Class Action Waivers. https://www.privacyworld.blog/2023/10/recent-marriott-data-breach-class-action-decision-underscores-the-importance-of-class-action-waivers/.
[90] Marriott privacy class decertification decision highlights proper 'order of business'. https://www.reuters.com/legal/litigation/column-marriott-privacy-class-decertification-decision-highlights-proper-order-2023-08-22/.
[91] Marriott MDL Class Action and Waiver Impacts. https://www.natlawreview.com/article/district-court-quickly-reinstates-class-certification-marriott-data-breach.
[92] Marriott fined £18.4 million by UK watchdog over customer data breach | ZDNET. https://www.zdnet.com/article/marriott-fined-gbp18-4-million-by-uk-watchdog-over-customer-data-breach/.
[93] UK watchdog reduces Marriott data breach fine to $23.8M, down from $123M | TechCrunch. https://techcrunch.com/2020/10/30/uk-watchdog-reduces-marriott-data-breach-fine-to-23-8m-down-from-123m.
[94] Marriott and Dell data breaches: what consequences on stock prices and intangible assets? https://www.linkedin.com/pulse/marriott-dell-data-breaches-what-consequences-stock-prices-project.
[95] Marriott data breach FAQ: How did it happen and what was the impact? | CSO Online. https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.
[96] About your Aadhaar. https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html.
[97] Initial analysis of Indian Supreme Court decision on Aadhaar | Privacy International. https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar.
[98] Massive Aadhaar Data Breach Of 815 Million Indians: Here's How To Keep Your Details Safe. https://web.archive.org/web/20231130021838/https://business.outlookindia.com/news/massive-

aadhaar-data-breach-of-815-million-indians-heres-how-to-keep-your-details-safe.
[99] UIDAI reveals 210 govt websites made Aadhaar details public, did not specify when breach took place â□□ Firstpost. https://www.firstpost.com/india/uidai-reveals-210-govt-websites-made-aadhaar-details-public-did-not-specify-when-breach-took-place-4217597.html.
[100] Aadhaar Data is Never Breached or Leaked: UIDAI. https://pib.gov.in/newsite/PrintRelease.aspx?relid=173667.
[101] Rs 500, 10 minutes, and you have access to billion Aadhaar details - The Tribune. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.
[102] UIDAI denies biometric data breach, points to misuse of grievance redressal search facility | Outlook India. https://www.outlookindia.com/website/story/uidai-denies-biometric-data-breach-points-to-misuse-of-grievance-redressal-searc/306403.
[103] The Tribune reports Aadhaar data breach using Rs 500, 10 minutes, UIDAI says info fully secure. https://scroll.in/latest/863787/uidai-claims-the-tribune-misreported-article-on-aadhaar-data-breach.
[104] "Not Shooting Messenger": Aadhaar Authority's Defence After Police Case. https://www.ndtv.com/india-news/not-shooting-messenger-aadhaar-authoritys-defence-after-police-case-1796955.
[105] India investigating alleged breach in citizen database Aadhaar | The Straits Times. https://www.straitstimes.com/asia/south-asia/india-investigating-alleged-breach-in-citizen-database-aadhaar.
[106] UIDAI Files Case In Aadhaar-Data-For-Rs 500 Report, Journalist Named. https://www.ndtv.com/india-news/uidai-files-case-for-aadhaar-data-for-rs-500-report-journalist-named-1796899.
[107] Storm of protest after FIR on Tribune Aadhaar expose - The Tribune. https://www.tribuneindia.com/news/archive/nation/storm-of-protest-after-fir-on-tribune-aadhaar-expose-524922.
[108] Aadhaar breach report: Reactions on freedom and privacy | CSO Online. https://www.csoonline.com/article/567915/aadhaar-breach-report-reactions-on-freedom-and-privacy.html.
[109] In a year of data breaches, India's massive biometric programme finally found legitimacy. https://qz.com/india/1501568/in-2018-supreme-court-backed-indias-aadhaar-despite-data-leaks.
[110] UIDAI blocks Aadhaar data access from officials, after The Tribune report: Economic Times. https://scroll.in/latest/864347/after-data-breach-report-uidai-blocks-all-officials-from-accessing-aadhaar-portal-economic-times.
[111] Twitter user highlights security flaws in UIDAI's mAadhaar app for Android devices, user data could be compromised â□□ Firstpost. https://www.firstpost.com/business/twitter-user-highlights-potential-security-flaws-in-uidais-maadhaar-app-for-android-devices-user-data-could-be-compromised-4298719.html.
[112] Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected â□□ Firstpost. https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html.
[113] 'Don't Share Aadhaar Number Online': UIDAI After RS Sharma's Dare. https://www.thequint.com/news/india/aadhaar-number-uidai-trai-chief-rs-sharma-challenge.
[114] Aadhaar breach is serious, but bigger challenge is a data and privacy protection law. https://www.orfonline.org/expert-speak/aadhaar-breach-serious-bigger-challenge-data-privacy-protection-law.
[115] The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/.
[116] Aadhar Data Breach: Protecting India's Digital Identity. https://www.linkedin.com/pulse/aadhar-data-breach-protecting-indias-digital-identity-digialert-smlhc.
[117] India Passes Digital Personal Data Protection Act. https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/.
[118] Understanding India's New Data Protection Law. https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624.
[۱۱۹] تپسی هک شد و بخشی از اطلاعات کاربران به‌دست هکرها افتاد - زومیت.
https://www.zoomit.ir/tech-iran/408696-tapsi-hacked-user-data-leaked/.
[۱۲۰] بزرگ‌ترین حمله هکری به کشور اتفاق افتاد/ خطری کاربران بانک‌ها را تهدید می‌کند؟ - خبرآنلاین.
https://www.khabaronline.ir/news/1954552/.

[۱۲۱] اطلاعات ۱۸ شرکت بیمه با ۱۱۵ میلیون رکورد هک شد/رئیس بیمه مرکزی برکنار شد / پایگاه خبری تحلیلی انصاف نیوز. https://ensafnews.com/435496/.
[122] Data Privacy Laws and Regulations Around the World. https://securiti.ai/privacy-laws/.
[123] Personal Information Protection and Electronic Documents Act. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html.
[124] Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-33-gdpr/.
[125] Art. 34 GDPR – Communication of a personal data breach to the data subject - General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-34-gdpr/.
[126] Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[127] What is Data Breach and Data Security Law? | Winston & Strawn Law Glossary | Winston & Strawn. https://www.winston.com/en/legal-glossary/data-breach-and-data-security.
[128] Personal data breaches: a guide | ICO. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/.
[129] bakermckenzie. https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/china/topics/breach-notification-requirements.
[130] Breach notification in China - Data Protection Laws of the World. https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=CN.
[131] Data breach notification laws. https://en.wikipedia.org/wiki/Data_breach_notification_laws.
[132] Baker McKenzie. https://insightplus.bakermckenzie.com/bm/investigations-compliance-ethics/japan-enacts-amendments-to-the-act-on-the-protection-of-personal-information.

عنوان: مروری بر چالش‌ها و راهکارهای سیاستی ارتقای امنیت سایبری در ایران با رویکرد تطبیقی (با تمرکز بر موضوع نقض داده)

DOI: https://doi.org/10.22034/mrc.report.21704
Permanent Link:
Publisher : Islamic Parliament Research Center of Iran

گزیده سیاستی

امروزه امنیت سایبری همان امنیت ملی است. حفظ اطلاعات شهروندان، زیرساخت‌های حیاتی و داده‌های دولتی در برابر تهدید سایبری پایه‌ای اساسی برای حفظ تمامیت و اقتدار ملی است. ازاین‌رو تصویب قانون جامع حفاظت از داده‌ها و ایجاد نهاد مستقل نظارتی ضروری است.

مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاســـداران، روبروی پـــارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۵۸۵۵-۱۵۸۷۵ پست الکترونیک: mrc@majles.ir

وب‌سایت: rc@majles.ir