Volume 16, Number 4, Winter 2024

Journal of
Science & Technology Policy

# Analysis of the Requirements for User Data Security on Service Provider Platforms

**Behnaz Ahmadvand[*1], Artin Jahanshahi [2]**

1- Assistant Professor, National Research Institute for Science Policy, Tehran, Iran.
(Corresponding Author: ahmadvand@nrisp.ac.ir)
2- Ph.D. student in Private Law, Univeristy of Shiraz, Shiraz, Iran.

**Abstract**

One of the most crucial issues in information security is the protection of user data from unauthorized access. In this regard, the privacy policy of almost every platform asserts that the company's protocol, server, security layers, and data management techniques will ensure data security. However, the precise mechanism and criteria for implementing security measures remain unspecified. Existing laws, except for the e-commerce law, fail to provide guidance on securing user data in electronic commerce, resulting in a significant gap in regulatory oversight. This article uses descriptive and analytical methods within Iranian law to examine the requirements for securing users' data. Data processors must consider the type of data, implementation costs, processing nature, geographical location, subject and purposes of processing, potential risks, and their impact on individuals' rights to ensure adequate security. Therefore, data processors must adopt appropriate technical and organizational measures to ensure the security of users' data at an adequate level. Periodic review and assessment and reporting of the level of consumer data protection on platforms and providing a regulatory artery have been regarded as data protection requirements. The Supreme Commission for the Regulation of Cyberspace has obliged all service providers to encrypt the data that leads to the identification of users within two months, through the amendment of their privacy policies, and to recognize the "right to delete" information for users. The result is that due to the shortcomings of the directive, including generalities, the lack of identification of the special platform for compensation, and the ambiguity and silence of the provisions of the directive in some cases, as well as the reliance of the implementation guarantee on civil and criminal liability, the approval of the law on the protection of personal data, along with encouraging The self-regulating system of the platforms seems to be a practical solution.

***Keywords:*** Personal Data, Sensitive Data, Encryption, Right to Delete, Privacy, National Center for Cyberspace.

**How to Cite this Paper:**

Ahmadvand, B. & Jahanshahi, A. (2023). **Analysis of the Requirements for User Data Security on Service Provider Platforms.** *Journal of Science & Technology Policy*, 16(4), 83-98. {In Persian}.
Doi: 10.22034/jstp.2024.11526.1708



Publisher: National Research Institute for Science Policy

فصلنامه علمی-پژوهشی
سیاست علم و فناوری

سال شانزدهم، شماره ٤، زمستان ١٤٠٢

مقاله پژوهشی

# بررسی الزامات حاکم بر تأمین امنیت داده‌های کاربران توسط پلتفرم‌های ارائه‌دهنده خدمات

بهناز احمدوند[1*]، آرتین جهانشاهی[2]

۱- استادیار، مرکز تحقیقات سیاست علمی کشور، تهران، ایران.

(نویسنده عهده‌دار مکاتبات: ahmadvand@nrisp.ac.ir)

۲- دانشجوی دکتری حقوق خصوصی، دانشگاه شیراز، شیراز، ایران.

## چکیده

تأمین امنیت داده‌های کاربران از دسترسی غیرمجاز یکی از چالش‌های اساسی در حفاظت از اطلاعات است. در اغلب خط‌مشی‌های حریم خصوصی پلتفرم‌های ارائه‌دهنده خدمات، اعلام شده که پروتکل، سرور و لایه‌های امنیتی پلتفرم و روش‌های مناسب مدیریت داده‌ها، تلاش حداکثری برای امنیت داده‌ها خواهند کرد؛ بااین‌حال، سازوکار و معیاری جهت اتخاذ تدابیر امنیتی شناسایی نشده است. در قوانین لازم‌الاجرا تنها قانون تجارت الکترونیک است که مقررات کلی در این حوزه مقرر کرده است. نوشتار حاضر با روش توصیفی-تحلیلی در بستر حقوق ایران صورت گرفته و درصدد بررسی الزامات حاکم بر امنیت داده کاربران است. نتیجه پژوهش نشان می‌دهد پردازشگران داده باید ضمن مسئول بودن در برابر امنیت داده، با در نظر گرفتن نوع داده، هزینه‌های اجرا و ماهیت، قلمرو، موضوع و اهداف پردازش و همچنین خطرات متنوع و آثار آن بر حقوق افراد، معیارهای فنی و سازمانی متناسبی را برای تضمین سطح مناسبی از امنیت در نظر بگیرند. بررسی دوره‌ای و ارزیابی و تنظیم گزارش از وضعیت سطح حفاظت از داده‌های مصرف‌کنندگان در پلتفرم‌ها و نیز ارائه شریان نظارتی برای مرکز ملی فضای مجازی از الزامات حفاظت از داده است. کمیسیون عالی تنظیم مقررات فضای مجازی کلیه ارائه‌دهندگان خدمات را مکلف کرده که از طریق اصلاح سیاست‌های حریم خصوصی خود، داده‌هایی که منجر به شناسایی هویت کاربران می‌شوند را طی دو ماه رمزنگاری کرده و «حق حذف» اطلاعات را برای کاربران شناسایی کنند. نتیجه آن که با توجه به نواقص دستورالعمل، از جمله کلی گویی، عدم شناسایی بستر ویژه جبران خسارت، و ابهام و سکوت مفاد دستورالعمل در برخی موارد و نیز اتکای ضمانت اجرا به مسئولیت مدنی و کیفری، تصویب قانون حفاظت از داده‌های افراد در کنار تشویق نظام خودتنظیم‌گری پلتفرم‌ها، از جمله راهکارهای عملی به‌نظر می‌رسند.

**کلیدواژه‌ها**: داده شخصی، داده حساس، رمزگذاری، حق حذف، حریم خصوصی، مرکز ملی فضای مجازی.

برای استنادات بعدی به این مقاله، قالب زیر به نویسندگان محترم مقالات پیشنهاد می‌شود:

احمدوند، بهناز.، جهانشاهی، آرتین. (١٤٠٢). **بررسی الزامات حاکم بر تأمین امنیت داده‌های کاربران توسط پلتفرم‌های ارائه‌دهنده خدمات**. *سیاست علم‌وفناوری*، (٤)١٦، ٨٣-٩٨.

Doi: 10.22034/jstp.2024.11526.1708

**۱- مقدمه**

با توسعه اینترنت و فناوری‌های اطلاعات و ارتباطات در کشور، تجارت‌ها از شکل سنتی خود گذر کرده و در بستر الکترونیک و برخط (آنلاین) جای گزیده‌اند. در وضعیت کنونی، با توجه به اهمیت و کاربرد داده‌ها[۱] در ارائه خدمات لحظه‌ای، انواع و اقسام پلتفرم‌ها در مقیاس کوچک و بزرگ به جمع‌آوری، پردازش[۲] و نگهداری انواع داده‌های شخصی کاربران متکی هستند و متقابلاً کاربران و مصرف‌کنندگان برای دریافت خدمات ناچار به ارائه داده‌های خود می‌باشند. حسب حوزه فعالیت و خدمات پلتفرم‌ها، ممکن است داده‌های گوناگونی از جمله «داده‌های شخصی[۳]» از شخص جمع‌آوری و پردازش گردد؛ برخی از داده‌ها به گونه‌ای هستند که به تنهایی یا با ترکیب با سایر داده‌ها می‌توانند منجر به شناسایی یک شخص حقیقی زنده گردند[۴] که این داده‌ها در اصطلاح داده شخصی نامیده می‌شوند. در واقع داده شخصی عبارت است از «هر نمادی از واقعه، اطلاعات یا مفهوم که به تنهایی یا در ترکیب با داده‌های دیگر می‌تواند به شناسایی یک شخص حقیقی زنده منجر شود مانند شماره‌های ملی، شناسنامه، حساب‌های بانکی، ژنتیک، بیمه نامه و گذرنامه»[۵].

در نظام‌های حقوقی پیشرو از جمله اتحادیه اروپا در زمینه حفاظت از اطلاعات، تنها داده‌های اخیر است که از جهت رابطه آن با حریم خصوصی اطلاعاتی افراد مورد حمایت مضاعف قانونگذار قرار گرفته است [۱]. در سیاست‌های حریم خصوصی پلتفرم‌های بزرگ که ارائه خدمات از سوی آنها مستلزم جمع‌آوری و پردازش اطلاعات متنوع و گسترده است، انواع اطلاعاتی که از کاربر جمع‌آوری و پردازش می‌شود و نیز شیوه‌های تأمین امنیت داده احصاء شده و به اطلاع کاربر می‌رسد؛ شیوه‌ای که در نظام حقوقی آمریکا رایج است. در نظام حقوقی آمریکا، به علت پیروی از الگوی مبتنی بر بازار در خصوص داده و تجارت آن، قانونگذار فدرال بی آنکه در قالب حق، حمایت‌هایی برای افراد موضوع داده یا مصرف کنندگان شناسایی کند، اقدام به مقررات‌گذاری در حوزه‌های مختلف کرده است، از جمله حوزه بهداشت و درمان، اینترنت، ارائه‌دهندگان خدمات اینترنتی، حریم خصوصی آنلاین کودکان و غیره. قانونگذاران ایالتی جهت ارائه حمایت‌های قانونی مؤثرتر برای حفاظت از حریم خصوصی اطلاعاتی افراد، قوانین مشابهی با مقررات عمومی حفاظت از داده تصویب کرده‌اند، از جمله قانون حریم خصوصی مصرف‌کننده کانادا مصوب ۲۰۱۸ [۲].

با پیچیده‌تر شدن نیازهای کاربران و افزایش تعداد داده‌های تولید شده، پلتفرم‌های بزرگ ناگزیر از تأسیس «مرکز داده[۶]» می‌باشند. مرکز داده، مکانی اختصاصی است که در آن مجموعه‌ای از سرورها، کامپیوترها، زیرساخت‌های امنیتی و ارتباطی و دیگر تجهیزات شبکه و الکترونیکی قرار دارند و هدف اصلی این مرکز ارائه، نگهداری و پشتیبانی از انواع سرویس‌های تحت شبکه اینترنت است. مرکز داده ممکن است شامل مرکز ذخیره داده، مرکز پردازشی یا مرکز جمع‌آوری داده یا هر سه باشد. از آنجا که حجم داده‌ها به طور تصاعدی در حال رشد است و نقض داده‌ها بیشتر از هر زمان دیگری اتفاق می‌افتد، شناسایی و جلوگیری از از دست دادن داده‌ها به یکی از مهم‌ترین نگرانی‌های امنیتی برای شرکت‌های مبتنی بر داده تبدیل شده است. یکی از چالش‌های اساسی کشور در حوزه فناوری اطلاعات و ارتباطات در بخش عمومی و خصوصی تأمین امنیت داده است؛ اهمیت و آثار زیان‌بار سوء استفاده از اطلاعات شهروندان از جمله نقض حریم خصوصی، و در خطر بودن جان و مال افراد، بر کسی پوشیده نیست. با ترکیب و پردازش اطلاعات مربوط به نام، شماره تماس، موقعیت مکانی و زمانی و اطلاعات رستوران‌های مورد علاقه یک فرد می‌توان به جزئی‌ترین لایه‌های خصوصی زندگی یک فرد پی برد و از آن اطلاعات

[۱] مطابق بند ث ماده ۱ قانون مدیریت داده و اطلاعات ملی مصوب ۱۴۰۱، منظور از داده «مجموعه‌ای از اعداد و حروف و علائم و نشانه‌هایی هستند که به صورت قراردادی در ابزارهای الکترونیکی یا رقومی یا توسط هر نوع فناوری جدید ارتباطاتی و اطلاعاتی تولید می‌شوند». به طور کلی، داده‌ها علایمی هستند که می‌توان از طریق آنها به وقایع، اشیا، رخدادها و مفاهیم پی برد.

[۲] در پیش‌نویس لایحه حمایت از داده‌ها، پردازش اینگونه تعریف شده است: «هر نوع عملیاتی که توسط کنترلگر یا پردازشگر در مورد داده‌های شخصی و داده‌های شخصی حساس به صورت خودکار یا دستی صورت می‌گیرد مانند جمع‌آوری، ذخیره، استفاده، توزیع، تجزیه و تحلیل، ترکیب با داده‌های دیگر و انتقال».

[3] Personal Data

[۴] ماده ۲ طرح صیانت و حفاظت از داده و اطلاعات شخصی

[۵] ماده ۱ پیش‌نویس لایحه حمایت از داده‌ها

[6] Data Center

برای اهداف متعدد استفاده یا سوءاستفاده کرد. در بخش خصوصی، نشت اطلاعاتی پلتفرم‌ها امنیت اطلاعات شامل سه جزء مرتبط به هم است؛ محرمانه بودن، یکپارچگی و در دسترس بودن داده‌ها. نقض امنیت اطلاعات در درجه اول شامل دو جزء اول می‌شود و زمانی رخ می‌دهد که اطلاعات حساس و قابل شناسایی شخصی بدون مجوز قابل دسترسی باشد [۳].

در تاریخ ۱۱ دی ۱۴۰۲، اسنپ‌فود[1]، سرویس آنلاین سفارش غذا متعلق به شرکت آوا نگار اطلس تجارت که در حوزه تجارت الکترونیک غذا فعالیت می‌کند، در بیانیه‌ای خبر از هک و نشت داده‌های ۲۰ میلیون کاربر مشتمل بر ۸۸۰ میلیون داده خبر داد [٤]. پیش از آن گروه هکری داخلی موسوم به آی.آر لیکس[2] اعلام کرد داده‌های ذیل را در اختیار دارد و به قیمت ۳۵ هزار دلار به فروش گذاشته است:

– اطلاعات بیش از ۲۰ میلیون کاربر شامل: نام کاربری، رمز عبور، ایمیل، نام و نام خانوادگی، شماره موبایل، تاریخ تولد. –اطلاعات بیش از ۵۱ میلیون آدرس کاربر شامل: موقعیت مکانی، آدرس کامل، شماره تلفن.

–اطلاعات بیش از ۱۸۰ میلیون دستگاه همراه شامل: نوع و مدل دستگاه، پلتفرم، توکن، فروشگاه نصب برنامه.

–اطلاعات بیش از ۳٦۰ میلیون سفارش شامل: آی.پی سفارش دهنده، آدرس دریافتی، تلفن دریافتی، شهر، مدت زمان دریافت، نام و نام خانوادگی، مشخصات فروشگاه یا رستوران، قیمت، محصول.

–اطلاعات بیش از ۳۵ هزار پیک شامل: نام، نام خانوادگی، شماره تماس، کد ملی، شهر.

–اطلاعات بیش از ٦۰۰ هزار پرداخت سفارش شامل: نام صاحب کارت، نام کامل مشتری، شماره تماس، شماره کارت، نام بانک.

–اطلاعات بیش از ۱٦۰ میلیون سفر انجام شده توسط پیک شامل: نام کامل مبدا و مقصد، آدرس مبدا و مقصد، تلفن مبدا و مقصد، موقعیت جغرافیایی مبدا و مقصد، تاریخ.

– اطلاعات بیش از ۲٤۰ هزار وندور[3] شامل: نام کامل، آدرس، تلفن، ایمیل، موقعیت مکانی، نام مدیریت مجموعه.

–اطلاعات بیش از ۸۸۰ میلیون سفارش محصول.

علی‌رغم مذاکره این شرکت با هکرها مبنی بر عدم فروش اطلاعات و اثربخش بودن این مذاکره، امنیت داده این قبیل شرکتها کماکان یک مسئله اساسی است و بیش از پیش باید مورد توجه قرار گیرد. با نظر به گسترش حملات سایبری بر مراکز داده شرکت‌های بزرگ، تأمین امنیت داده کاربر برای جلب اطمینان و اعتماد کاربر و رعایت حریم خصوصی او و نیز رشد کسب و کار اهمیت حیاتی دارد. با توجه به نوپدید بودن موضوع و فقدان مقررات در این زمینه، رابطه کاربر و شرکت از طریق سیاست‌های حریم خصوصی تنظیم می‌گردد. با عنایت به موارد اشاره شده و با توجه به اهمیت داده‌های شهروندان ایرانی در سطح ملی و نیز امکان سوءاستفاده از آنها توسط عناصر بیگانه، لازم است الزامات و سیاست‌های حاکم بر تأمین امنیت داده توسط پلتفرم‌های ارائه‌دهنده خدمات بررسی گردد. از جهت اینکه حسب حوزه و دامنه فعالیت پلتفرم‌هاممکن است الزامات متفاوتی رعایت گردد، مطالعه حاضر به طور موردی به اسنپ‌فود پرداخته و با روش توصیفی–تحلیلی و با مطالعه قوانین و پیش‌نویس لوایح و طرح‌های مرتبط، در مقام پاسخ به این پرسش می‌باشد که چه الزاماتی در خصوص امنیت داده توسط سیاست حریم خصوصی اسنپ‌فود و مقررات قانونی وجود دارد؟

در ضمن لازم است الزامات و آثار دستورالعمل اجرایی اخیر مرکز ملی فضای مجازی (از این پس مرکز) بر کاربران و پلتفرم‌ها تبیین گردد. با نظر به این که حفاظت از داده در کشور نوپدید بوده و مرکز ملی فضای مجازی پس از انتشار خبر نشت اطلاعاتی کاربران اسنپ‌فود اقدام به تصویب دستورالعمل مرقوم کرده است، لذا نوشتارهای مرتبط با پژوهش محدود است. محبوب افراسیاب و مهدی ناصر (۱۳۹۹) در مقاله‌ای تحت عنوان «چارچوب‌های حقوقی حفظ امنیت پردازش داده‌های خصوصی(مطالعه تطبیقی در حقوق ایران و اتحادیه اروپا» به بررسی سازوکارهای سیاستی و تقنینی جهت تأمین امنیت داده‌های خصوصی پرداخته است؛ باوجوداین، دامنه موضوعی مقاله اخیر محدود به اینترنت اشیا بوده و در بستر حقوق ایران و اتحادیه اروپا به طور تطبیقی نگاشته شده است. انصاری (۱٤۰۲) در کتاب «حقوق داده: اصول پردازش داده‌های شخصی» ذیل عنوان اصل تمامیت و

[1] Snapfood
[2] IRleaks
[3] در زنجیره تأمین، به شرکت بازرگانی معتبر اطلاق می‌شود، که تأمین‌کننده کالا یا خدمات است و در زمان نیاز به یک کالا یا خدمات خاص، در کوتاه‌ترین زمان می‌توانند به نیاز متقاضیان پاسخ دهند.

محرمانگی داده‌ها، اتخاذ تدابیر امنیتی، ارزیابی ریسک و تدابیر فنی حفاظتی، به عنوان الزامات تأمین امنیت داده معرفی شده که نوشتار حاضر ضمن عنایت به موارد اشاره شده، به الزامات سازمانی و معیارهای عینی و همچنین مسئول حفاظت از داده تأکید خواهد داشت.

لطیف‌زاده و همکاران (۱۴۰۲) در مقاله‌ای تحت عنوان «تعهدات پردازش‌کنندهٔ داده شخصی در اتحادیه اروپا و امکان‌سنجی پذیرش آن در حقوق ایران» در خصوص امنیت داده به تعهدات پردازشگر داده در حقوق اتحادیه اروپا اشاره کرده که مقاله حاضر با تکیه بر مصوبات اخیر کمیسیون عالی تنظیم مقررات شورای عالی فضای مجازی و همچنین پیش‌نویس لوایح موجود به تحلیل موضوع خواهد پرداخت.

نوشتار حاضر در دو بخش تنظیم شده است؛ در بخش اول، الزامات امنیتی و معیارهای تأمین امنیت داده همراه با تحلیل و نقد قوانین و پیش‌نویس‌های موجود بررسی خواهد شد و بخش دوم به بررسی دستورالعمل جدید کمیسیون عالی تنظیم مقررات فضای مجازی و آثار آن اختصاص یافته است.

## ۲- الزامات‌حاکم بر تأمین امنیت داده‌های مصرف‌کننده

اشخاص برای دریافت خدمات عمومی و خصوصی متنوع ناچارند داده‌های خود را در اختیار سازمان‌ها و شرکت‌های خصوصی قرار دهند. سازمان‌ها و پلتفرم‌ها به عنوان امین داده‌ها و متولی آنها، مسئولیت نگهداری و حفظ داده‌های کاربران می‌باشند. حفاظت از حریم خصوصی داده کاربران، مستلزم شناسایی تکالیف برای متولیان داده در قالب اصول پردازش داده‌های شخصی و حقوق کاربر [۵] و یکی از مصادیق اصلی آن تکلیف پردازشگران داده بر تأمین امنیت داده کاربر است [٦]. تهدیدات سایبری و امنیت اطلاعات از مسائلی است که با دیجیتالی شدن اقتصاد و روابط اجتماعی در کانون توجه قرار گرفته است. خطرات سایبری ناشی از استفاده از فناوری اطلاعات و ارتباطات است که محرمانه بودن، در دسترس بودن یا یکپارچگی داده‌ها و خدمات دیجیتال را تهدید می‌کند و منجر به وقفه در کسب و کار، نقض حریم خصوصی کاربر، خرابی زیرساخت یا سایر خسارات مادی می‌شود [۷]. نقض داده «به عنوان یک حادثه امنیتی که در آن، داده‌های حساس، محافظت شده یا محرمانه توسط شخصی غیر مجاز برای انجام این کار کپی، انتقال، مشاهده، سرقت یا استفاده می‌شود» تعریف می‌شود [۸]. اصطلاح امنیت سایبری معمولاً برای اشاره به مجموعه‌ای از شرایط یا رویدادهای مرتبط با بهبود یکپارچگی یک سیستم یا زیرساخت مدیریت اطلاعات و رسیدگی به چالش‌های موجود و نوظهور مرتبط استفاده می‌شود. از آنجا که افراد، نهادها، پلتفرم‌هاو سازمان‌ها به صورت روزمره با داده‌ها سر و کار دارند، این داده‌های انباشته شده در طول زمان باید در برابر افراد غیرمجاز با قصد سوء استفاده از این داده‌ها محافظت شوند. بنابراین هدف از تأمین امنیت داده‌ها، حفاظت از عناصر سه‌گانه محرمانه بودن[1]، یکپارچگی[2] و در دسترس بودن[3] داده‌ها است [۹]. تأمین امنیت محرمانه بودن داده به اقداماتی اشاره دارد که برای اطمینان از اینکه داده‌ها، به ویژه داده‌های حساس، از دسترسی غیرمجاز و افشاء محافظت می‌شوند انجام می‌گردد. به عبارت دیگر، محرمانه بودن داده‌ها به جلوگیری از حمله فعال اشخاص غیرمجاز به داده‌های کاربران و اطمینان از اینکه اطلاعات دریافتی توسط گیرنده داده کاملاً با اطلاعات ارسال شده توسط فرستنده مطابق باشد، اشاره دارد؛ به این معنی که فقط افراد مجاز حق دسترسی و دریافت داده‌ها را دارند [۱۰]. سطح محرمانه بودن داده می‌تواند بر اساس نوع داده و یا دسته‌بندی‌های مقرر شده در قوانین متفاوت باشد. یکپارچگی به محافظت از تمامیت و صحت داده‌ها در جریان حیات داده[4] اشاره دارد. براین‌اساس، باید تدابیر امنیتی اتخاذ شود تا داده‌ها در برابر حذف یا تغییر و تحریف غیرمجاز محافظت شوند [۱۲] و در صورت نقض داده، اقدامات فوری لازم برای جلوگیری یا کاهش آسیب انجام گردد. در دسترس بودن به معنای ارائه دسترسی یکپارچه و مستمر به کاربران از طریق سرورهای قوی و زیرساخت شبکه با سازوکارهای در دسترس بودن بالا است

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Lifecycle of data

برای نشان دادن جریان اطلاعات یا به عبارتی، سرنوشت اطلاعات، می‌توان آن را به چهار مرحله تقسیم کرد: تولید، جمع‌آوری و ذخیره، پردازش، استفاده و حذف یا انتقال [۱۱]

که در طراحی سیستم تعبیه می‌شود. در دسترس بودن داده تأکید می‌کند که داده‌ها می‌توانند به طور معمول در هر زمان دسترسی داشته باشند، یعنی کاربر می‌تواند به محض نیاز به داده‌ها در فضای ابری دسترسی داشته باشد، آنها را بارگذاری کند یا برخی تغییرات در آنها انجام دهد.

**۲-۱ الزامات فنی تأمین امنیت داده**

اسنَپ‌فود یک سرویس سفارش آنلاین غذا است که با همکاری رستوران‌ها و پیک‌های موتوری، غذا را به مشتریان تحویل می‌دهد. اسنپ‌فود اولین برنامه سفارش آنلاین غذا در کشور است که از سال ۱۳۸۸ فعالیت خود را با نام زودفود آغاز کرد و سپس با ادغام به گروه اسنپ، به اسنپ‌فود تغییر نام داد. اسنپ‌فود در سیاست‌های حریم خصوصی خود [۱۳] در مورد شیوه‌های امنیت داده کاربران اعلام داشته که «اسنپ‌فود همانند سایر وب سایت‌ها از جمع‌آوری آی.پی و کوکی‌ها استفاده می‌کند، اما پروتکل، سرور و لایه‌های امنیتی اسنپ‌فود و روش‌های مناسب مدیریت داده‌ها حداکثر تلاش را به عمل می‌آورد که اطلاعات کاربران را محافظت و از دسترسی‌های غیرقانونی جلوگیری کند». از جمله خلاءهای اساسی سیاست حفظ اطلاعات و حریم خصوصی اسنپ‌فود، عدم اشاره صریح به شیوه‌های امنیتی متناسب با نوع داده‌های جمع‌آوری شده است. نظر به این که ارائه خدمات مستلزم جمع‌آوری و پردازش داده‌های متنوعی از جمله داده‌های شخصی و غیرشخصی است، لازم است معیارهای عینی برای تأمین مناسب انواع داده و اقدامات و تدابیر امنیتی-حفاظتی موجود به اطلاع مصرف‌کننده برسد. از دیگر خلاءهای سیاست‌های امنیتی-حفاظتی اسنپ‌فود، عدم اشاره به موارد مسئولیت شرکت در برابر نقض داده‌های کاربران می‌باشد. در ادامه سیاست حریم خصوصی این سرویس ارائه دهنده غذا در خصوص مسئولیت شرکت مقرر شده است «مسئولیت هرگونه سوء استفاده به شخص یا اشخاص متخلف مربوط بوده و اسنپ‌فود حق اعتراض و پیگیری را از طریق قانونی بنابر صلاحدید خود محفوظ می‌دارد». در مجموع می‌توان گفت در خصوص مسئولیت ناشی از امنیت اطلاعات، تمرکز اصلی سیاست حریم خصوصی این شرکت، احاله مسئولیت (ناشی از عدم رعایت مفاد سیاست حریم خصوصی، حفظ و نگهداری رمز عبور و نام کاربری) به کاربر است.

با نظر به این که حوزه فعالیت شرکت اسنپ‌فود ارائه برخط سفارش و عرضه خدمات غذا در بستر الکترونیک است، قانون تجارت الکترونیک در این باره حکم‌فرماست. در کنار این قانون می‌توان به پیش‌نویس لایحه حمایت از داده‌ها و پیش‌نویس حمایت و حفاظت از داده و اطلاعات شخصی نیز اشاره کرد؛ فصل دوم و سوم پیش‌نویس لایحه حمایت از داده‌ها نیز به اصول پردازش داده‌های شخصی و حقوق کاربر پرداخته است. ماده ۵۹ قانون تجارت الکترونیکی به اصول حاکم بر پردازش داده‌پیام‌های شخصی (اصل تحصیل قانونی، اصل تحصیل مضیق و مرتبط داده، اصل صحت داده، اصل دسترسی به داده) در بستر تجارت الکترونیک و حقوق کاربر(حق دسترسی، حق تصحیح و حق حذف) اختصاص یافته است. هدف از شناسایی اصول پردازش داده و حقوق کاربر، ایجاد چارچوبی برای حفاظت از حریم خصوصی داده‌های اشخاص است [١٤]. در خصوص سایر مقررات و الزامات جزئی، ماده ٦١ قانون تجارت الکترونیکی مقرر داشته است: «سایر موارد راجع به دسترسی موضوع «داده پیام»، از قبیل استثنائات،افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسؤول دیدبانی وکنترل جریان «داده پیام»های شخصی به موجب مواد مندرج در باب چهارم این قانون وآئین‌نامه مربوطه خواهد بود».با وجود این، تاکنون آیین‌نامه مزبور تهیه و تصویب نشده است. قانون اخیر نقض هر یک از موارد اشاره شده را با قید مجازات کیفری ممنوع کرده و لذا می‌توان گفت رویکرد ضمانت اجرای نقض داده‌های شخصی کاربر در قانون تجارت الکترونیکی ایران یک رویکرد کیفری و همچنین مبتنی بر مسئولیت مدنی است. در خصوص مسئولیت کیفری لازم به اشاره است که مطابق ماده ۷۱ عدم رعایت شرایط مقرر در ماده ۵۸ و ۵۹ یک تا سه سال حبس است و جریمه نقدی نیز تنها در صورت بی-احتیاطی یا بی مبالاتی دفاتر خدمات صدور گواهی‌الکترونیکی به میزان پنجاه میلیون ریال که جریمه سبکی است مقرر شده است. این رویکرد مخالف با رویکرد حمایت از پلتفرم‌های ارائه‌دهنده خدمات است. در خصوص مسئولیت ناشی از خسارات وارده به افراد، ماده (۷۸) مقرر داشته است مسئولیت

مدنی مؤسسات عمومی و خصوصی در مورد نقص یا ضعف سیستم‌ها، به جز خساراتی که در نتیجه قطع فیزیکی ارتباط الکترونیکی پدید می‌آید، یعنی فرض مسئولیت را پذیرفته است که با مسئولیت مدنی عرضه‌کنندگان خدمات در فقه امامیه نیز مطابق است [۱۵]؛ بااین‌حال، با توجه به سکوت قانون، در سایر موارد مسئولیت مبنی بر قواعد عام (تقصیر) است. خلاء اصلی قانون تجارت الکترونیکی سکوت درباره مسئول بودن مشمولان قانون در حفاظت از امنیت داده‌پیام‌های مبادله شده است؛ بنابراین با توجه به قانون فعلی لازم‌الاجرا، تکلیف مبنی بر رعایت تدابیر امنیتی–حفاظتی برای جلوگیری از دسترسی غیرمجاز و نقض داده کاربر با ابهام مواجه است، لذا شناسایی ضمانت اجراهای قانونی غیرکیفری متناسب ضروری است [۱۶] [۱۷]. در راستای رفع نقیصه‌های قانون اخیر، در پیش‌نویس لوایح و طرح‌های مرتبط با صیانت از داده شخصی تکالیفی در راستای اتخاذ تدابیر امنیتی–حفاظتی مقرر شده است. در این راستا، ماده ۱۹ پیش‌نویس لایحه حمایت از داده‌ها مقرر داشته است «هر کنترل‌گر و پردازشگری...موظف است با توجه به اهداف، زمینه‌ها، هزینه‌ها و خطرات احتمالی پردازش داده‌های شخصی، اقدامات امنیتی لازم را برای حفاظت از داده‌های شخصی با توجه به میزان حساسیت داده‌های مورد پردازش انجام دهد». در پیش‌نویس لایحه حمایت از داده‌ها، اصل تکلیف تأمین امنیت داده‌ها توسط متولیان داده مورد شناسایی قرار گرفته و لذا نوع و سطح امنیت را در سنجه ماهیت و حساسیت داده (از حیث شخصی یا غیر شخصی بودن داده و نیز از حیث داده‌های شخصی حساس و داده‌های شخصی غیرحساس) اهداف پردازش داده، هزینه‌های اتخاذ تدابیر امنیتی–حفاظتی، به عهده متولی داده گذاشته است.

از نقاط قوت این پیش‌نویس لایحه می‌توان به موارد زیر اشاره کرد:

–اولاً؛ با بررسی ماده اخیر و سایر مواد مرتبط به خوبی می‌توان برداشت کرد که در تأمین امنیت داده‌ها باید به ماهیت داده‌ها توجه شود؛ تمام داده‌هایی که توسط بخش عمومی و خصوصی جمع‌آوری می‌گردد الزاماً داده شخصی محسوب نمی‌شوند و برخی داده‌ها وجود دارد که اگرچه منجر به شناسایی هویت فرد نمی‌شود، باوجوداین، برای ارائه خدمات لازم است. چنین داده‌هایی نیازمند سطح بالایی از امنیت نیستند و در صورت دسترسی غیرمجاز به آنها خسارتی وارد نمی‌گردد یا در مقایسه با نقض داده‌های شخصی خسارات به مراتب کمتری در پی دارد [۱۸]. در مقابل، برای داده‌های شخصی بایستی تدابیر امنیتی–حفاظتی بالایی در نظر گرفته شود چرا که نقض این داده‌ها منجر به نقض حقوق و منافع افراد، به ویژه حریم خصوصی آنها می‌گردد و ممکن است خسارات مالی، جانی و معنوی به دنبال داشته باشد. از طرفی دیگر از داده‌های اشخاص می‌توان برای صدمه به امنیت ملی سوءاستفاده کرد. داده‌های شخصی خود بر اساس ماهیت ممکن است غیرحساس یا حساس باشند. منظور از داده‌های شخصی حساس داده‌های مبین ریشه‌های‌قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌های مربوط به وضعیت جسمانی، روانی و یا جنسی اشخاص است. داده‌های اخیر مستلزم حمایت بیشتری هستند و تدابیری امنیتی بالاتری در مقایسه با داده‌های شخصی غیرحساس باید برای آن در نظر گرفت.

– ثانیاً؛ از آنجا که حسب اهمیت ماهیت داده، حوزه و دامنه فعالیت پلتفرم‌ها و نیز ساختار آنها از حیث بزرگ یا کوچک بودن کسب و کار، ممکن است داده‌های گوناگونی در مقیاس متنوع پردازش گردد لذا نمی‌توان برای تمامی پلتفرم‌ها نسخه واحدی برای تأمین امنیت داده تنظیم کرد. تحول دائمی روش‌های تأمین امنیت اطلاعات بر این استدلال صحه می‌گذارد.

– ثالثاً؛ در خصوص تأمین امنیت داده کاربران باید معیار هزینه‌های اتخاذ چنین تدابیری نیز در نظر گرفته شود زیرا گاه ممکن است نامعقول بودن اتخاذ برخی تدابیر امنیتی منجر به عدم تمایل شرکت به فعالیت و خدمات‌رسانی باشد.

با وجود نقاط قوت معیارهای شناسایی شده در پیش‌نویس لایحه حمایت از داده برای امنیت، اشاره‌ای به فناوری‌های روز در تأمین امنیت داده نشده است. واضح است که روش‌های تأمین امنیت داده‌های شخصی از جمله

ناشناس‌سازی[1] و رمزگذاری[2] هر روز در حال توسعه و تحول هستند؛ بر اساس معیار «استفاده از فناوری‌های روز» پلتفرم‌های ارائه‌دهنده خدمات بایستی با در نظر داشتن فعالیت‌ها و ساختار سازمانی و نیز هزینه‌ها، از روش‌های جدید امنیت داده استفاده کنند. اشاره به این معیار از این جهت حائز اهمیت است که پلتفرم‌ها ممکن است با استفاده از روش‌های قدیمی امنیت سعی در کاهش هزینه‌های خود کنند و از سوی دیگر در صورت نقض امنیت داده ممکن است به تدابیر اتخاذ شده استناد کرده و مدعی تبری از مسئولیت شوند. بااین‌حال، لازم به ذکر است ملزم نمودن بخش خصوصی به استفاده از آخرین پیشرفت‌های حاصله در امنیت اطلاعات ممکن است برای بسیاری از پلتفرم‌هانامعقول و هزینه‌های گزاف به دنبال داشته باشد؛ ازاین‌رو، معیار «معقول بودن[3]» تدابیر امنیتی به عنوان یک استاندارد حقوقی مطرح شده است [۲۱]؛ طبق این معیار در قوانین و مقررات به جای آنکه به مصادیق امنیت (دیوار آتش، رمزنگاری و...) اشاره گردد، پلتفرم‌ها ملزم می‌شوند تا در یک فرایند مداوم اقدام به شناسایی خطرات احتمالی کنند و تناسب تدابیر امنیتی با خطرات را ارزیابی کنند.

طرح صیانت و حفاظت از داده و اطلاعات شخصی که با هدف حمایت از حیثیت و کرامت اشخاص موضوع داده‌ها تدوین شده است، یکی از راه‌های حفاظت از حقوق افراد را اصل مسؤلیت پذیری کنشگران پردازش داده‌ها و اطلاعات شخصی اعلام کرده است (ماده ۱) و در ماده ۳۵ مقرر داشته است «هریک از کارکردها و مراحل پردازش، باید از تمهیدات ایمنی و امنیتی ویژه خود برخوردار باشد. این تمهیدات باید هر سه سطح ذیل را در برگیرند: الف) ایمنی و امنیت فیزیکی، شامل زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری مرتبط ب) ایمنی و امنیت اطلاعات، شامل انواع پردازنده‌های سخت‌افزاری و نرم‌افزاری پ) ایمنی و امنیت انسانی، شامل همه کنترل گران و پردازش گران اصلی و مرتبط» و ماده ۳۶ مقرر داشته «ساز و کارها و ابزارهای سخت‌افزاری و نرم‌افزاری ایمنی و امنیتی مقرر یا پیشنهادی باید با شرایط ذیل سازگار باشد: الف) نوع و میزان آسیب‌زایی تهدیدهای بالقوه و بالفعل از نگاه اشخاص موضوع داده ب) تأمین‌پذیری آنها پ) توانمندی فنی و اجرایی».

نقطه قوت این طرح در خصوص امنیت داده تقسیم آن به دسته امنیت فیزیکی، اطلاعاتی و انسانی اشاره کرد. نشت اطلاعاتی از طرق مختلفی ممکن است رخ دهد؛ گاه ممکن است ایراد و خطای سخت‌افزاری راه ورود اشخاص غیرمجاز را تسهیل کند و گاه ممکن است عدم نظارت بر نیروی انسانی در دسترسی به اطلاعات و مراکز داده باعث نشت اطلاعات توسط افراد داخل سازمانی یا خارجی رخ دهد [۲۲]؛ ازاین‌رو، بایستی امنیت داده‌ها در لایه‌های مختلف نرم‌افزاری و سخت‌افزاری و انسانی در پلتفرم‌های ارائه‌دهنده خدمات الزاماً شناسایی شده و رعایت گردند. از محتوای ماده اخیر به خوبی می‌توان برداشت کرد که تأمین امنیت در لایه‌های فیزیکی، اطلاعاتی و انسانی مستلزم بررسی دوره‌ای وضعیت موجود و رفع خلاءهای احتمالی می‌باشد. مطابق ماده ۳۶ تدابیر امنیتی باید سازگار با نوع و میزان تهدیدات از نگاه کاربران و نیز قابلیت تأمین امنیت و امکان اتخاذ آنها از حیث فنی و اجرایی است. چنان که اشاره شد داده‌ها با توجه به نوع و حساسیت نیازمند سطوح گوناگون و متناسب با ماهیت هر یک می‌باشند، لذا مطابق بند الف ماده ۳۶ با توجه به اینکه معیار، نگاه کاربران است، در مورد اسنپ‌فود باید اظهار داشت که داده‌های مختلف کاربران از جمله موقعیت مکانی و جغرافیایی، اطلاعات حساب بانکی، اطلاعات تماس اطلاعات مربوط به سخت‌افزار مورد استفاده کاربران که حساسیت بالایی دارند باید از سطح امنیت بالاتری برخوردار باشند. مطابق ماده اخیر، لازمهٔ تأمین امنیت داده‌های کاربران، امکان‌پذیر بودن تدابیر مورد نظر از حیث فنی و اجرایی است. هر شرکتی بایستی بر اساس ظرفیت‌های درونی و ساختاری خود اقدام به اتخاذ تدابیر امنیتی کند؛ در مورد اسنپ‌فود، با توجه به اینکه فعالیت گسترده‌ای در این بستر اتفاق می‌افتد و

[1] ناشناس‌سازی یا بی‌نام‌سازی، فرآیندی است که به موجب آن شناسه‌های کلیدی که ممکن است باعث شناسایی افراد شود به طور دائمی و غیرقابل بازگشت از داده‌ها در فرآیند پردازش حذف و یا پنهان می‌گردد تا در عین حال که از داده‌های اشخاص استفاده می‌شود هویت آنان نامعلوم بداند [۱۹].

[2] از لحاظ فنی رمزگذاری روشی است که در آن به کمک الگوریتم‌های ریاضیاتی، داده‌های قابل فهم به داده‌های غیرقابل درک تبدیل می‌شوند تا تنها اشخاص مجاز با در دست داشتن کلید آن به داده‌ها دسترسی داشته باشند [۲۰].

[3] Reasonable

اطلاعات سه طرف (رستوران‌ها، پیک‌های موتوری و کاربران) درگیر می‌باشد لازم است با توجه به ظرفیت‌های مالی و ساختاری خود اقدام به بازبینی تدابیر امنیتی خود کند. از جمله خلاءهای طرح اخیر، عدم اشاره به هزینه‌های احتمالی برای بخش خصوصی در مورد تأمین امنیت داده و نیز عدم اشاره به تکلیف پلتفرم‌ها مبتنی بر استفاده از شیوه‌های نوین معقول در امنیت داده است.

**۲-۲ الزامات نظارتیِ درون‌سازمانی برای تأمین امنیت داده**

حفاظت معقول از داده‌های کاربران در برابر دسترسی غیرمجاز و نشت اطلاعات و ارائه خدمات مطلوب به مصرف‌کنندگان در کنار آن، مستلزم بررسی دوره‌ای و ارائه گزارش از وضعیت زیرساخت‌ها، سازه‌ها و سامانه‌های نرم‌افزاری و سخت‌افزاری از حیث به‌روز بودن و متناسب بودن آن با نوع و حساسیت داده‌ها و اقدام جهت رفع خلاءها و رخنه‌های امنیتی است. عدم تأمین متناسب داده‌های کاربران در برابر تهدیدات امنیتی نه تنها منجر به کاهش اعتماد مصرف‌کنندگان می‌گردد بلکه هزینه‌هایی از جهت جبران خسارات وارده بر مصرف‌کنندگان و نیز جریمه‌های عدم حفاظت از داده بر پلتفرم‌های ارائه‌دهنده خدمات تحمیل می‌گردد [۲۳]؛ بنابراین لازم است پیش از بروز تهدیدات امنیتی، امنیت داده‌های کاربران به طور معقول حفاظت گردد. بررسی دوره‌ای و ارزیابی وضعیت باعث می‌شود که پلتفرم‌های ارائه‌دهنده خدمات در برابر خطرات احتمالی از پیش آمادگی داشته و از وقوع خسارات مالی به شرکت و نقض حریم خصوصی اطلاعاتی افراد جلوگیری گردد. لازمهٔ اتخاذ چنین تدبیری شناسایی مسئولی تحت عنوان «مسئول یا ناظر حفاظت از داده» برای ارزیابی و تنظیم گزارش و اطلاع‌رسانی به نهادهای تصمیم‌گیرنده شرکت و نهادهای قانونی ذی‌ربط است. در واقع با پیچیده‌تر شدن فعالیت پلتفرم‌های ارائه‌دهنده خدمات از یکسو و احتمال بسیار قوی تصویب قوانین مربوط به حفاظت از داده‌های اشخاص و وضع ضمانت اجراهای ناظر بر فعالیت شرکت‌ها، بیش از پیش نیاز به شناسایی مسئول حفاظت از داده احساس خواهد شد [۲٤]. گرچه پلتفرم‌ها می‌توانند بدون وجود الزام قانونی در این خصوص با روی آوردن بر قواعد خودتنظیمی می‌توانند برای مطابقت با مقررات، مسئول حفاظت از داده تعیین کنند، بااین‌حال، وجود الزام قانونی باعث خواهد شد حقوق افراد موضوع داده به نحو مطلوب تأمین گردد. اشاره به این نکته نیز حائز اهمیت است که با شناسایی قانونی و مکلف کردن متولیان داده به انتصاب مسئول حفاظت از داده، نظارت مراجع قانونی بر متولیان با سهولت بیشتری صورت خواهد گرفت. به عبارت دیگر، می‌توان مقرر نمود که مسئول حفاظت داده با انجام بررسی‌های دوره‌ای و مداوم و تنظیم گزارش درباره وضعیت فعلی در مورد حفاظت از داده‌های کاربران، ضمن گزارش به نهادهای تصمیم‌گیرنده درون‌سازمانی، گزارش‌های خود و اقدامات صورت گرفته برای رفع خلاءهای بالقوه و بالفعل را به مراجع قانونی صالح ارسال کند. در پیش‌نویس لایحه حمایت از داده‌ها علی‌رغم ارائه معیارهای مطلوب در زمینه تأمین امنیت داده، چنین امری پیش‌بینی نشده است. باوجوداین، در ماده ۳۰ پیش‌نویس کمیسیونی در سطح نظارت کلان شناسایی شده که می‌توان نمونه کوچک‌تر آن را در سطح خرد در پلتفرم‌ها شناسایی کرد. مطابق ماده ۳۰ کمیسیون وظایف و اختیارات زیر را برعهده دارد و می‌تواند برای انجام آنها کارگروه‌های لازم تشکیل شود : ۱- نظارت بر متابعت کنترلگرها و پردازشگرهای داده‌های شخصی با الزامات مقرر در این قانون از جمله با دریافت و بررسی گزارش‌ها و اعاملات کنترلگرها؛ ۲- رسیدگی به شکایت‌های اشخاص موضوع داده از جهت نقض حقوق خود علیه کنترلگرها از طریق هیئت موضوع ماده (۳۱) ۳- تصویب دستورالعمل‌های مقرر در این قانون و سایر دستورالعمل‌های لازم برای اجرای مطلوب قانون؛ ٤- فرهنگ سازی، آموزش و اطلاع رسانی لازم در خصوص چگونگی اجرای قانون و ارائه نظرات مشورتی به مجریان قانون؛ ۵- تصویب فهرست داده‌هایی که انتقال آنها به کنترلگرها یا پردازشگرهای خارجی ممنوع است؛ ٦- تصویب دستورالعمل کیفیت استاندارد صیانت از داده‌ها؛ ۷- تصمیم‌گیری درباره تعلیق اجرای برخی از الزامات قانونی مذکور در این قانون نظیر اخذ رضایت شخص موضوع داده در وضعیت‌های اضطراری.

در پیش‌نویس طرح صیانت و حفاظت از داده و اطلاعات شخصی نیز به ناظر یا مسئول حفاظت از داده درون‌سازمانی

توجهی نشده و تنها در ماده ۲۳ به موارد انتصاب ناظر ویژه اشاره شده است. در این طرح منظور از ناظر ویژه کسی است که «که پیرو حکم صادره از سوی کمیسیون(کمیسیون صیانت از داده‌ها و اطلاعات شخصی)، صلاحیت نظارت بر پردازش داده‌ها و اطلاعات شخصی را می‌یابد». مطابق ماده مرقوم در موارد ذیل ناظر ویژه تعیین می‌شود: الف) پردازش داده‌ها و اطلاعات شخصی حیاتی و حساس ب) پردازش کلان‌داده‌ها و اطلاعات شخصی پ) زیان‌ها و آسیب‌های جدی یا پرشمار بالقوه و بالفعل پردازش‌ها به داده‌ها و اطلاعات شخصی ت) سایر موارد به تشخیص هیأت نظارت و تأیید کمیسیون. ناظر ویژه در این طرح از طرف هیأت نظارتی که به موجب این طرح تشکیل می‌گردد منصوب می‌گردد تا بر فرایند پردازش داده‌ها در موارد معین نظارت کند. همچنین مطابق ٤٥ طرح، پردازشگران موظفند در مواردی که پردازش داده برای حقوق افراد موضوع داده، زیان‌بار است از ناظر ویژه کسب تکلیف کنند. چنان که در ابتدای مقاله اشاره گردید، نظام‌های پیشرو در حوزه حفاظت از داده‌های شخصی، از جمله اتحادیه اروپا، مقررات جامعی در مورد شیوه‌های حفاظت و نظارت بر امنیت داده‌های شخصی افراد وضع کرده‌اند. از جمله شیوه‌های ارزیابی امنیت داده‌ها که در مقررات عمومی حفاظت[1] از داده در ماده ۲۵ و ۳۵ منعکس شده است ارزیابی دوره‌ای امنیت داده‌ها توسط مسئولان حفاظت از داده است. طبق ماده ۲۵ مقررات عمومی حفاظت از داده، با توجه به آخرین وضعیت موجود، هزینه پیاده‌سازی و ماهیت، قلمرو، موضوع و اهداف پردازش و همچنین خطرات متنوع ازنظر احتمال و شدت برای حقوق و آزادی‌های فردی در مقابل پردازش، کنترلگر باید هم در زمان معرفی ابزارهای پردازش و هم خودِ پردازش، معیارهای فنی و سازمانی مناسبی را اجرا کند، ازجمله مستعار سازی. مطابق ماده ۳۵ زمانی که نوعی از پردازش با استفاده از فناوری‌های جدید، با در نظر گرفتن ماهیت، قلمرو، موضوع و اهداف پردازش، منجر به خطر بالا برای حقوق و آزادی‌های اشخاص حقیقی شود، کنترلگر باید پیش از انجام پردازش، ارزیابی اثرات عملیات پردازشی را باهدف حفاظت داده‌های شخصی، در نظر داشته باشد. ارزیابی دوره‌ای شامل موارد زیر است: ۱) توصیف سیستماتیک عملیات پردازشی و اهداف پردازش ۲) ارزیابی ضرورت و تناسب عملیات پردازشی نسبت به اهداف پردازش ۳) ارزیابی خطرات مربوط به حقوق و آزادی‌های اشخاص موضوع داده ٤) معیارهای پیشبی‌نیشده برای حل خطرات، شامل معیارها و سازوکارهای امنیتی برای تضمین حفاظت از داده‌های شخصی. مطابق ماده ۳۹ مقررات عمومی حفاظت از داده، مسئول حفاظت از داده باید از جریان ارزیابی دوره‌ای عملیات پردازش اطلاع داشته و در صورت نیاز در مورد شیوه‌ها و سازوکارهای امنیتی نظر او جلب گردد [۲٦].

## ۳- سند سیاست‌ها و الزامات حفاظت از داده‌ها مصوب کمیسیون عالی تنظیم مقررات فضای مجازی کشور

مرکز ملی فضای مجازی، زیر نظر شورای عالی فضای مجازی کشور تأسیس شده تا اشراف کامل و به روز نسبت به فضای مجازی در سطح داخلی و جهانی و تصمیم‌گیری نسبت به نحوه مواجهه فعال و خردمندانه کشور با این موضوع از حیث سخت‌افزاری، نرم‌افزاری و محتوایی در چارچوب مصوبات شورای عالی و نظارت بر اجرای دقیق تصمیمات در همه سطوح تحقق یابد. این مرکز در چارچوب مصوبات شورای عالی فضای مجازی، بالاترین سطح حاکمیتی را در میان کلیه‌ی دستگاه‌های کشور در حوزه فضای مجازی دارد. مطابق ماده ۹ اساسنامه مرکز ملی فضای مجازی، جهت تصمیم‌سازی و تحقق مصوبات شورای عالی، مرکز در زمان تأسیس دارای سه کمیسیون عالی زیر می‌باشد: ۱- کمیسیون عالی تنظیم مقررات فضای مجازی کشور ۲- کمیسیون عالی ارتقای تولید محتوای فضای مجازی کشور ۳-کمیسیون عالی امنیت فضای مجازی کشور. کمیسیون عالی تنظیم مقررات فضای مجازی کشور جهت تنظیم سیاست‌ها، نظارت، هدایت، هماهنگی و تصویب مقررات و آیین‌نامه‌های کلان در همه ابعاد فضای مجازی در چارچوب مصوبات شورای عالی فضای مجازی تشکیل شده است. از جمله مهم‌ترین وظایف شورا موارد زیر

[1] General Data Protection Regulations (G.D.P.R.)
این مقرره توسط پارلمان و شورای اتحادیه اروپا در سال ۲۰۱۶ به تصویب رسید و از ۲۵ ماه مه سال ۲۰۱۸ در کشورهای عضو اتحادیه اروپا لازم‌الاجرا شده است.

است: تصویب معیارها، سیاست‌ها و نظام‌های کنترل کیفی و فنی در همه زمینه‌های فضای مجازی از جمله امنیتی و محتوایی و همچنین سیاست‌ها و معیارهای ارائه محتوا، خدمات، توسعه و بهره‌برداری در فضای مجازی کشور در چارچوب مصوبات شورای عالی؛ سیاستگذاری، هماهنگی و تصویب ضوابط کلی صدور مجوز فعالیت و بهره‌برداری در چارچوب مصوبات شورای عالی برای ارائه هر گونه فعالیت در فضای مجازی شامل محتوا (اعم از داده، متن، صوت و تصویر)، خدمات و زیرساخت‌های فنی و ارتباطی؛ تدوین سیاست‌ها و تصویب مقررات کلان مورد نیاز فضای مجازی کشور از جمله توافقنامه های درجه و سطح خدمات، حمایت از حقوق کاربران فضای مجازی و تنظیم روابط فعالان فضای مجازی در چارچوب مصوبات شورای عالی. مطابق مصوبه مربوط به شرح وظایف و اختیارات کمیسیون عالی تنظیم مقررات، کمیسیون عالی تنظیم مقررات فضای مجازی کشور برای تنظیم سیاست‌ها، نظارت، هدایت، هماهنگی و تصویب مقررات و آیین‌نامه‌های کلان در همه ابعاد فضای مجازی و تنظیم‌گری تنظیم‌گران بخشی، تشکیل و وظایف و اختیارات آن به شرح زیراست: «تهیه و پیشنهاد نظامات و مقررات برای تصویب در شورای عالی فضای مجازی کشور در زمینه‌ها و ابعاد مختلف از قبیل: معماری کلان تنظیم‌گری فضای مجازی با نظر به جایگاه و مسئولیت‌های هر یک از تنظیم‌گران بخشی؛ تعیین یا ایجاد تنظیم‌گران بخشی خدمات جدید؛ اصلاح مأموریت و شرح وظایف تنظیم‌گران بخشی؛ تصویب دستورالعمل‌ها، ضوابط، الزامات اجرایی و فنی، نظارتی و هماهنگی ملی برای تحقق مصوبات شورای عالی فضای مجازی کشور؛ تصویب الزامات کلان پیشنهادی تنظیم‌گران بخشی در زمینه صدور مجوز؛ تصویب معیارها، ضوابط و نظام‌های کنترل کیفی و فنی در همه زمینه‌های فضای مجازی؛ ایجاد هماهنگی و نظارت بر عملکرد دستگاه‌های صادرکننده مجوزهای حوزه فضای مجازی؛ تنظیم مقررات جمع‌آوری، فرآوری داده‌ها و حفظ حریم خصوصی کاربران در سکوهای فضای مجازی».

کمیسیون تنظیم مقررات شورای عالی فضای مجازی در مصوبات خود به اهمیت حفاظت از حریم خصوصی داده‌های افراد تأکید کرده است. مصوبه جلسه شماره ۸۷ کمیسیون عالی تنظیم مقررات تحت عنوان «سیاست‌ها و الزامات کلان حمایت از رقابت و مقابله با انحصار سکوهای فضای مجازی» در بند ۳ ماده ٤ به رعایت الزامات صیانت از داده‌ها توسط ارائه دهندگان خدمات اشاره کرده است. همچنین به موجب بند ۳ ماده ۹ مصوبه اخیر، مرکز ملی رقابت به صورت سالانه اختیار اصلاح معیارهای دخیل در استاندارد «رفاه مشتری» متناسب با ویژگی‌های متمایز بازارهای دو یا چندسویه خدمات و کالاهای فضای مجازی با در نظر گرفتن معیارهایی چون حفظ حریم خصوصی کاربران، قدرت انتخاب، صیانت از داده‌های شخصی، هزینه‌های جابه‌جایی و تأثیرات وابستگی به سکوهای مسلط یافته است. به دنبال انتشار اخبار مربوط به هک اسنپ‌فود و نشت اطلاعاتی کاربران آن، کمیسیون عالی تنظیم مقررات فضای مجازی کشور مرکز ملی فضای مجازی، دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی مصوب ۱٤۰۲/۱۰/۱۱ را ابلاغ کرد. مطابق دستورالعمل اخیر، با هدف کاهش بخشی از مخاطرات مرتبط با نقض حریم خصوصی کاربران، اشخاص حقوقی غیردولتی و دستگاه‌های اجرایی کشور (دستگاه های اجرایی موضوع ماده ۲۹ قانون برنامه پنج ساله ششم توسعه) به رعایت شرایط مرتبط با شیوه های جمع‌آوری، پردازش و نگهداری داده های کاربران در سامانه ها و سکوهای فضای مجازی مکلف شده‌اند: « ۱- کلیه ارائه دهندگان خدمات از طریق سامانه‌ها و سکوهای فضای مجازی موظف‌اند حداکثر ظرف مدت دو ماه (۲ ماه) از تاریخ ابلاغ این دستور العمل: ۱-۱- سیاست‌های حفظ حریم خصوصی مرتبط با جمع آوری، پردازش و نگهداری داده‌های کاربران را به صورت شفاف شامل موارد زیر اعلام و رضایت صریح آنان مبنی بر پذیرش شرایط را اخذ نمایند: ۱-۱-۱- کدام اقلام داده‌ای را و برای چه منظوری از کاربران دریافت و یا جمع آوری می‌کنند. در این زمینه و در زمان دریافت و جمع‌آوری، اقلام ضروری را از اقلام اختیاری تفکیک نموده و قابلیت انتخاب را برای کاربر در ارائه اطلاعات اختیاری فراهم کنند؛ -۲-۱-۱- شیوه دریافت و جمع آوری اعم از دریافت

مستقیم از کاربران و یا به صورت غیر مستقیم و از طریق مشخصات تجهیزات و سامانه‌های در اختیار کاربران را مشخص کنند؛ ۳-۱-۱- نحوه و ابزار اطلاع رسانی تغییر سیاست‌ها را مشخص نموده و مجدداً رضایت صریح کاربران را اخذ و تغییرات لازم را اعمال نمایند؛ ۲-۱ -داده‌ها باید صرفاً در حد اقلام مورد نیاز برای انجام تکالیف قانونی یا ادامه کسب و کار و متناسب با اهدافی که در بند "۱-۱-" برای کاربر شرح داده شده و اجازه و رضایت صریح وی اخذ گردیده است، جمع آوری، پردازش و ذخیره سازی شود». با توجه به اینکه حق حریم خصوصی ایجاب می‌کند فرد تصمیم بگیرد چه اطلاعاتی از او در دسترس دیگران باشد و در صورت تمایل درخواست حذف اطلاعات خودد دهد، بند ۳-۱ دستورالعمل مقرر داشته است «در صورت درخواست کاربران برای حذف داده‌های مرتبط از قبیل حذف حساب کاربری، تمام و یا بخشی از داده‌های مرتبط با فعالیت آنان در سامانه و سکو (مشروط به عدم مغایرت با قوانین و مقررات کشور و مأموریت ها و تکالیف دستگاه های اجرایی)، بلافاصله انجام پذیرفته و داده‌های حذف شده از سامانه و سکوی برخط، به منظور رعایت مقررات قانونی به پایگاه‌های داده پشتیبان مستقر در بخش غیر بر خط و منفصل از شبکه های ارتباطی عمومی منتقل و تنها برای انجام تکالیف مقرر در قانون نگهداری یا پردازش شود و پس از خاتمه مواعد قانونی یا قضایی، به طور کامل امحاء شوند». حق بر حریم خصوصی ایجاب می‌کند که افراد بتوانند در فضای مجازی ناشناس بمانند و خود تصمیم بگیرند که کدام یک از اطلاعاتشان در دسترس عموم قرار گیرد. این حق، با مشکل اساسی افراد یعنی حق تصمیم‌گیری درباره این که کدام یک از اطلاعات آنها در اینترنت قابل دسترسی باشد، مرتبط است [۲۵]

در خصوص پردازش داده‌هایی که منجر به شناسایی هویت افراد می‌شوند، در دستورالعمل مقرر شده است که «داده‌های مربوط به هویت و اطلاعات شخصی کاربران که منجر به شناسایی هویت ایشان می‌شود، صرفاً باید به صورت رمزنگاری شده ذخیره شود. دستورالعمل‌های مرتبط با سطوح و شیوه‌های رمزنگاری بر اساس وظایف تعیین شده در اسناد مصوب شورای عالی فضای مجازی کشور، توسط دستگاه های مسئول ابلاغ می‌شود». براین‌اساس، پلتفرم‌های مشمول دستورالعمل کمیسیون عالی تنظیم مقررات فضای مجازی کشور بایستی مطابق با مصوبات شورای عالی فضای مجازی که در آن شیوه‌ها و سطوح امنیتی مقرر شده است، ساختار سازمانی خود در خصوص تأمین امنیت داده‌های کاربران را بازبینی کنند. مدت زمان اجرای مقررات دستورالعمل به مدت ۲ ماه از زمان ابلاغ دستورالعمل تعیین شده است؛ با توجه به پیچیدگی رمزنگاری داده‌ها، به ویژه در مواردی که مراکز داده حاوی تعداد فراوانی داده است، از نظر عملی و اجرایی به سختی امکان‌پذیر است و در صورت امکان نیز هزینه‌های نامعقولی برای مشمولان دستورالعمل به بار خواهد آورد. در دستورالعمل به اخذ رضایت از کاربر اشاره شده لیکن در خصوص ویژگی‌های آزادانه و آگاهانه در رضایت و یا چگونگی اخذ رضایت از کاربری که کودک است سخنی به میان نیامده است. در خصوص ماهیت داده مورد حفاظت که الزاماً باید داده شخصی باشد و معیارهای تشخیص داده شخصی از غیرآن، ماده‌ای وجود ندارد. اصول پردازش داده به روشنی تصریح نشده است. حقوق افراد موضوع داده به درستی و با جزئیات احصاء نشده است. دستورالعمل فوق، حاوی نکات کلی برای بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات است و ضمانت اجرای نقض هر کدام از مفاد، در متن دستورالعمل مشخص نشده است. واضح است که یک دستورالعمل چهار بندی که پس از هک اسنپ‌فود به صورت شتابزده به تصویب رسیده‌است نواقص زیادی دارد و جوابگوی معضلات ارائه‌دهندگان خدمات در سامانه‌ها و پتلفرم‌ها در فضای مجازی نیست.

از انتقادات اساسی وارد بر دستورالعمل شورای عالی فضای مجازی، کلی گویی و به عبارت دیگر تأکید موکد بر مقررات قانون تجارت الکترونیکی بدون نوآوری و تغییر است. به عبارت دیگر پیش از مصوبه شورای عالی فضای مجازی نیز مطابق قانون تجارت الکترونیکی ارائه دهندگان خدمات در بستر تجارت الکترونیکی بایستی امکان حذف داده‌ها را فراهم آورند. در حالی که این مصوبه ترتیب و شیوه جدیدی مطرح نکرده و اتخاذ تصمیم به تنظیم‌گران بخشی واگذار شده است.

در خصوص تأمین امنیت داده نیز با توجه به عدم تصویب آیین‌نامه مربوط به تدابیر حفاظتی و امنیتی در حفاظت از داده‌پیام‌ها، مصوبه شورای عالی فضای مجازی نوعی شناسایی حق و تلکیف بر ارائه دهندگان خدمات است، در حالی که این امر باید به مراجع صالح تصویب آیین‌نامه قانون تجارت محول گردد. اقدام به شناسایی حق و تکلیف برای بخش خصوصی که تنها در انحصار مراجع صالح تقنینی است با هدف وجودی شورای عالی فضای مجازی که سیاست‌گذاری و راهبرد بر اساس قوانین مصوب است مغایرت دارد. عدم شناسایی ضمانت اجرای غیرکیفری برای نقض امنیت داده‌های شخصی توسط ارائه دهندگان خدمات در بستر تجارت الکترونیک از دیگر ضعف‌های نظام حقوقی فعلی است. با نظر به این که حتی با رعایت تدابیر امنیتی و حفاظتی امکان نشت اطلاعات وجود دارد، ضمانت اجرای کیفری معقول و متناسب نمی‌باشد. شناسایی جریمه مالی به نفع کاربران بر اساس شاخصی همچون درصدی از کل درآمد خالص سالانه می‌تواند به عنوان پیشنهاد مطرح گردد.

### ۳-۱ حق حذف و شرایط اعمال آن توسط کاربر

حق حذف داده‌های شخصی که با حق بر فراموش شدن به طور مترادف استعمال می‌شود در حقوق اروپا بـه عنوان یک حق مرتبط با شخصیت افراد می‌باشد کـه عناصـر مختلفـی از جملـه احتـرام بـه کرامت انسانی و حق بر حریم خصوصی را در بر مـی‌گیـرد و همچنـین ریشـه در حـق افـراد برای تعیین سرنوشت زندگی و اطلاعـات مربـوط بـه آن (خودمختـاری اطلاعاتی) بـه نحـو دلخواه و بدون دخالت دیگـران دارد [۲۶]. حـق حذف داده‌های شخصی در رویه قضـایی دیـوان دادگسـتری اتحادیـه اروپـایی نیـز در پرونـده‌هـای مشهوری مثل دعوی کاستژا گونزالس علیه شرکت گوگل اعمال شده منعکس شده است. مقررات عمـومی حفاظت از داده در ماده ۱۷ ذیل عنوان حق حذف [حق بر فرامـوش شـدن]» ضـمن بـه رسمیت شناختن این حق، متولی داده را موظف کرده که تحت شرایطی داده‌هـای فـرد موضـوع داده را حذف نماید. بر اساس بندهای شش‌گانه این مـاده در صورتی کـه داده‌هـای شخصـی دیگر برای دستیابی به اهداف اصلی جمع‌آوری و پردازش ضرورت نداشته باشند یا به صورت غیرقانونی پردازش شده باشند یا فرد موضوع داده به فرایند پردازش اعتراض کرده باشد و یا هنگامی که فرد رضایت خود نسبت به پردازش را پس گرفته باشد و دیگر مبنایی قـانونی برای پردازش وجود نداشته باشد در این صورت متولی داده بایـد داده‌هـای شخصـی وی را حذف نماید. علاوه بر موارد گفته شده متولی داده ممکن اسـت جهـت سـازگاری بـا تعهدات قانونی داده‌های شخصی فرد موضـوع داده را حذف نماید.

در حقوق ایران حق حذف داده برای اولین بار در قانون تجارت الکترونیکی مطرح شده و بند د ماده ۵۹ قانون تجارت الکترونیکی مقرر داشته است «شخص موضوع «داده پیام» باید به پرونده‌های رایانه‌ای حاوی «داده پیام»های‌شخصی مربوط به خود دسترسی داشته و بتواند «داده پیام»های ناقص و یا نادرست را محو یا اصلاح کند». در این قانون نیز همچون حقوق اتحادیه اروپا حق حذف ریشه در صحت و دقیق بودن داده‌ها دارد؛ با این حال قانون تجارت الکترونیک در خصوص حق حذف به درخواست فرد موضوع داده و تعهد قانونی متولی داده در خصوص حذف در شرایط قانونی ابهام دارد. در واقع، با توجه به این که متولی داده باید تنها داده‌های مربوط به ارائه خدمات خود را جمع‌آوری و ذخیره نماید، در مواردی که داده‌های دیگری غیر از آن چه در سیاست حریم خصوصی شرکت آمده است جمع‌آوری گردد، متولی داده بایستی این داده‌ها را حذف کند. این مورد در ماده ۱۷ مقررات عمومی حفاظت از داده نیز اشاره شده است، با این حال به نظر می‌رسد طبق قوانین فعلی، متولیان داده با چنین الزامی روبرو نمی‌باشند.

مطابق دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی، کلیه ارائه‌دهندگان خدمات از طریق سامانه‌ها و سکوهای فضای مجازی بایستی ضمن شناسایی گزینه اختیار حذف اطلاعات برای کاربران، پس از دریافت تقاضای حذف، داده‌ها را از سامانه‌ها و سکوهای برخط خارج کرده و آن ها را به پایگاه‌های غیربرخط منتقل نمایند. مطابق ذیل بند ۳-۱- از

داده‌های نگهداری شده در سامانه‌ها و سکوهای غیربرخط تنها برای انجام تکالیف قانونی استفاده خواهد شد و پس از خاتمه مواعد قانونی یا قضایی، به طور کامل باید امحاء گردد. از جمله انتقادات اساسی وارد به دستورالعمل اخیر این است که امحای داده‌های مستقر در پایگاه‌های داده پشتیبان به گذشتن مواعد قانونی مشروط شده است. به نظر می‌رسد ملزم کردن ارائه دهندگان خدمات برای نگهداری داده‌ها به این شیوه معقول نمی‌باشد چرا که مواعد قانونی متعددی در قوانین شناسایی شده است که مطابقت با تمام آنها برای ارائه دهندگان خدمات معقول نخواهد بود. انتقاد دیگری که به دستورالعمل اخیر وارد است عدم شناسایی مواردی است که ارائه دهندگان خدمات بایستی بدون درخواست کاربر نیز حذف نمایند. با توجه به اهمیت اطلاع به موقع مقامات قانونی و نظارتی ذی‌ربط هنگام نقض داده‌های شخصی، لازم است سازوکاری مشخص گردد تا ارائه‌دهندگان خدمات در مواقع نشت اطلاعاتی هشدارهای لازم را به مقامات دهند تا اقدامات پس از حادثه امنیتی و عنداللزوم اتخاذ تدابیر لازم برای پیشگیری از وقوع خسارات شدیدتر صورت پذیرند. مقررات عمومی حفاظت از داده در راستای تقویت امنیت داده‌های شخصی بـرای کنترلگر مقرر کرده است که هنگام وقوع نقض داده‌های شخصی بلافاصله نهاد نظارتی را مطلع نماید. ماده ۳۳در این بـاره اعلام می‌دارد:«در صـورت وقـوع نقض داده‌های شخصـی، کنترلگر باید در صورت امکان بدون تاخیر غیرضروری و حداکثر ظرف ۷۲ ساعت از زمان آگاهی از نقض داده مراتب را بر اساس ماده ۵۵ به اطلاع نهاد نظارتی برساند مگر اینکه بعید باشد نقض داده خطری برای حقوق و آزادی‌های اشخاص حقیقی داشته باشد. علاوه بر این اگر اعلام به نهاد نظارتی ظرف ۷۲ساعت انجام نشود بایـد دلایل تأخیر نیز گزارش شود. با توجه به اینکه پردازشگر نیز یکی از بازیگران اصلی در حوزه پـردازش داده می‌باشد به موجب بند ۲همین ماده باید هنگام وقوع نقض داده شخصی مراتب را به طور فوری بـه اطلاع کنترلگر برساند.

با این حال مصوبه کمیسیون تنظیم مقررات شورای فضای مجازی در این مورد، سیاست‌های لازم را مقرر نکرده و مانند قانون تجارت الکترونیکی طرح جزئیات را به تنظیم‌گران بخشی محول کرده است. عدم تخصص لازم تنظیم‌گران بخشی به ابهامات موجود در مصوبه شورای عالی فضای مجازی دامن زده و موجب تشتت رویکردها در شناسایی الزامات لازم در خصوص تأمین امنیت داده‌ها خواهد شد.

### ۳-۲ آیین دادخواهی ناشی از نقض داده‌های شخصی کاربران

شناسایی مجاری قانونی و قضایی برای دادخواهی ناشی از نقض داده‌های شخصی از جمله چالش‌های اساسی کاربران در تجارت الکترونیک می‌باشد. با توجه به صلاحیت عام مراجع دادگستری در رسیدگی به تظلمات، و با عنایت به فقدان بستر متناسب دادخواهی ناشی از نشت اطلاعات ، لازم است قانونگذار به موضوع ورود پیدا کرده و کمیسیونی متشکل از نمایندگان ذی‌ربط برای رسیدگی به امر نقض داده‌های شخصی و تصمیم‌گیری درباره ضمانت‌اجرای قابل اعمال تأسیس کند. همچنین شورای عالی فضای مجازی می‌تواند این نهاد را در درون ساختار خود فراهم کند تا کاربران در مواقع نقض داده برای دادخواهی به آن مراجعه کنند. نظر به تخصصی بودن موضوع، تعداد بالای زیان‌دیدگان در نشت‌های اطلاعاتی و نیز با عنایت به این که تأمین امنیت به طور مطلق امکان‌پذیر نیست، ایجاد مرجعی ویژه برای دریافت شکایات، گزارش‌ها و درخواست‌های کاربران مبنی بر ارزیابی خسارات وارد شده و عنداللزوم جریمه ارائه دهندگان خدمات متخلف جهت حفاظت از حقوق کاربران لازم است. در راستای تشویق ارائه دهندگان خدمات به ارائه حمایت‌های مؤثر و اتخاذ تدابیر کارآمد برای داده‌های کاربران، پیشنهاد می‌شود شورای عالی فضای مجازی سیاست‌های لازم برای اتکا به شیوه خودتنظیمی توسط ارائه دهندگان خدمات اقدام کند. در صورت تشویق بخش خصوصی به خودتنظیمی از طریق ارائه معافیت‌های مالی یا درجه‌بندی اعتبار ارائه‌دهندگان خدمات، ضمن تمایل بخش خصوصی به ایفای نقش فعال‌تر جهت کسب اعتبار، از داده‌های کاربران به نحو مطلوب‌تری حفاظت خواهد شد. همچنین ارائه‌دهندگان خدمات می‌توانند ذیل ساختار سازمانی خود مرجع مشخصی برای دریافت شکایات کاربران و رسیدگی به درخواست آنان مبنی بر نقض داده‌های شخصی و ارزیابی میزان خسارات وارده به مدیریت

مسئول حفاظت از داده شرکت تأسیس کنند [۲۸].

به منظور نظارت بر حسن اجرای این قانون، تصویب دستورالعمل‌ها و شیوه‌نامه‌های اجرایی، فرهنگ‌سازی و ایجاد رویه‌های واحد در حمایت از داده‌های شخصی، مطابق ماده ۲۶ لایحه حمایت از داده‌ها کمیسیون حمایت از داده‌های شخصی زیر نظر شورای عالی فضای مجازی ایجاد خواهد شد. مطابق ماده ۳۰ لایحه مرقوم کمیسیون وظایف و اختیارات زیر را بر عهده دارد و می‌تواند برای انجام آنها کارگروه‌های لازم را تشکیل شود : ۱. نظارت بر متابعت کنترلگرها و پردازشگرهای داده‌های شخصی با الزامات مقرر در این قانون از جمله با دریافت و بررسی گزارش‌ها و اعلامات کنترلگرها؛ ۲. رسیدگی به شکایت‌های اشخاص موضوع داده از جهت نقض حقوق خود علیه کنترلگرها از طریق هیئت رسیدگی به تخلفات (موضوع ماده ۳۱) ۳. تصویب دستورالعمل‌های مقرر در این قانون و نیز سایر دستورالعمل‌های لازم برای اجرای مطلوب قانون؛ ٤. فرهنگ سازی، آموزش و اطلاع رسانی لازم در خصوص چگونگی اجرای قانون و ارائه نظرات مشورتی به مجریان قانون؛ ۵. تصویب فهرست داده‌هایی که انتقال آنها به کنترلگرها یا پردازشگرهای خارجی ممنوع است؛ ٦. تصویب دستورالعمل کیفیت استاندارد صیانت از داده‌ها؛ ۷. تصمیم گیری درباره تعلیق اجرای برخی از الزامات قانونی مذکور در این قانون نظیر اخذ رضایت شخص موضوع داده در وضعیت های اضطراری. مطابق ماده ۳۱ لایحه حمایت از داده‌ها رسیدگی به کلیه شکایت‌ها و گزارش‌های مربوط به تخلف از این قانون در هیأتی با عنوان هیأت رسیدگی به تخلفات متشکل از اعضای زیر انجام خواهد شد : ۱–چهار نماینده ثابت و تام‌الاختیار که دو نفر از آنان باید حقوقدان باشند، از سوی کمیسیون از میان اعضا یا خارج از اعضا انتخاب خواهند شد. ۲–یک نماینده ثابت از اتاق بازرگانی، صنایع و معادن ایران و برای مدت دو سال انتخاب خواهد شد؛ ۳–یک نماینده ثابت که از سوی سازمان نظام صنفی رایانه‌ای کشور ازمیان اعضا یا خارج از اعضا و برای مدت ۲ سال انتخاب خواهد شد. ٤– یک نماینده ثابت که از سوی اتحادیه کشوری کسب و کارهای مجازی از میان اعضا یا خارج از اعضا و برای مدت دو سال انتخاب خواهد شد.

## ٤– نتیجه‌گیری

اسنپ‌فود داده‌های گوناگونی از کاربران خود در اختیار دارد که در غالب موارد در زمره داده‌های شخصی قرار می‌گیرند و حساسیت بالایی برای مصرف‌کننده دارند. در سیاست حفظ اطلاعات و حریم خصوصی اسنپ‌فود اعلام داشته که پروتکل، سرور و لایه‌های امنیتی اسنپ فود و روش‌های مناسب مدیریت داده‌ها حداکثر تلاش را به عمل می آورد که اطلاعات کاربران را محافظت و از دسترسی‌های غیر قانونی جلوگیری کند. طبیعتا مسئولیت هرگونه سوء استفاده به شخص یا اشخاص متخلف مربوط بوده و اسنپ فود حق اعتراض و پیگیری را از طریق قانونی بنابر صلاحدید خود محفوظ می‌دارد. در سیاست حریم خصوصی این سرویس ارائه دهنده خدمات غذا اشاره‌ای به معیارها و ضوابط امنیتی که شرکت در قبال امنیت داده‌های دارد نشده است. در پیش‌نویس لایحه حمایت از داده‌ها ارائه دهندگان خدمات ملزم شده‌اند با توجه به اهداف، زمینه‌ها، هزینه‌ها و خطرات احتمالی پردازش داده‌های شخصی، اقدامات امنیتی لازم را برای حفاظت از داده‌های شخصی با توجه به میزان حساسیت داده‌های مورد پردازش انجام دهند. در پیش‌نویس طرح صیانت و حفاظت از داده و اطلاعات شخصی نیز اشخاص مذکور بایستی اقدامات و تدابیر امنیتی–حفاظتی را در لایه‌های فیزیکی، اطلاعاتی و انسانی مقرر داشته و معیار را تأمین‌پذیری و قابلیت پیاده‌سازی از حیث فنی و اجرایی قرار داده است. کمیسیون عالی تنظیم مقررات فضای مجازی کشور در دستورالعمل اخیر خود، به عنوان بخش اول سند سیاست‌ها و الزامات حفاظت از داده‌ها، ارائه‌دهندگان خدمات را مکلف کرده است از طریق اصلاح و بازبینی سیاست‌های حریم خصوصی خود، اطلاعاتی که از کاربر دریافت و نگهداری می‌شود را به طور شفاف بیان کرده و برای کاربر حق حذف داده‌های خود را شناسایی کنند و در صورتی که داده‌های جمع‌آوری شده منجر به شناسایی هویت کاربر گردد آنها را رمزگذاری کنند. ارائه‌دهندگان خدمات مکلف هستند ظرف ۲ ماه از ابلاغ این دستورالعمل دستورات اجرایی مقررشده را اتخاذ کنند. با پیچیده‌تر شدن عملیات پردازش و افزایش

حجم داده و هزینه‌های بالای نقض امنیت داده از یکسو و لزوم انطباق با مقررات از سوی دیگر، در این نوشتار پیشنهاد شده است ارائه دهندگان خدماتش ملزم به شناسایی مسئول حفاظت از داده در ساختار خود شوند تا ضمن بررسی و تنظیم گزارش از وضع و سطح امنیت داده‌ها، دستورات اجرایی نهادهای نظارتی را اعلام و اجرای آن را گزارش دهند. اجرای این راهکار به سیاست خودتنظیم‌گری منجر می‌شود. توضیح بیشتر آنکه کاربران با مطالعه سیاست‌های حریم خصوصی پلتفرم‌ها و مقایسه آنها با یکدیگر بهترین و امن‌ترین پلتفرم را برای دریافت خدمت انتخاب نمایند و این وضعیت باعث ایجاد رقابت و بهبود کیفیت در بین پلتفرم‌ها خواهد شد. از سوی دیگر وضع قانون یا مقرره متناسب نیز از ضروریات خدمات پلتفرم‌ها و سامانه‌ها در فضای مجازی قلمداد می‌شود. یک دستورالعمل چهاربندی که با شتابزدگی تصویب و ابلاغ شده، معضل موجود را حل نمی‌کند. با توجه به نواقص دستورالعمل، از جمله کلی گویی، عدم شناسایی بستر ویژه جبران خسارت، و ابهام و سکوت مفاد دستورالعمل در برخی موارد و نیز اتکای ضمانت اجرا به مسئولیت مدنی و کیفری، ایجاب می‌کند مجلس شورای اسلامی برای وضع قانون در زمینه حفاظت از داده‌ها در بستر تجارت الکترونیک و تحدید اختیارات مراجعی که فاقد شأن تقنینی می‌باشند به طور جدی وارد شود.

## تعارض منافع

نویسندگان تعهد می‌کنند که هیچ تعارض منافعی در این مقاله وجود نداشته است.

## References


[1] Ahmadvand B., & Jahanshahi, A. (2023). **Comparative Studying the Personal Data in the European Union and Iranian Legal System**. *CLR*, 27 (1) :105-132

[2] Buresh, D. L. (2019). **A Comparison between the European and the American Approaches to Privacy**. *Indon. J. Int'l & Comp. L.*, *6*, 257.

[3] Riedy, M. K., & Hanus, B. (2016). **Yes, Your Personal Data Is at Risk: Get over It**. *SMU Sci. & Tech. L. Rev.*, *19*, 3.

[4] https://twitter.com/snappfood?lang=en

[5] Ansari, B. (2007). *Privacy Law*. Tehran: Samt Publication{In Persian}

[6] Latifzadeh, M., Qabuli Dorafshan, S. M. M., Mohseni, S., & Abedi, M. (2023). **The Obligations of the Personal Data Processor in the European Union and the Feasibility of Its Acceptance in Iranian** Law. *Civil Jurisprudence Doctrines*, *15*(27), 245-286. Https://doi.org/10.30513/cjd.2022.3094.1541 {In Persian}

[7] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). **Cyber risk and cybersecurity: a systematic review of data availability**. *The Geneva Papers on risk and insurance-Issues and practice*, *47*(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

[8] Freeha, K., K.J. Hwan, M. Lars, and M. Robin. 2021. **Data breach management: An integrated risk model**. *Information & Management*, 58(1): 103392. https://doi.org/10.1016/j.im.2020.103392.

[9] Yee, C. K., & Zolkipli, M. F. (2021). **Review on Confidentiality, Integrity, and Availability in Information Security**. *Journal of ICT in Education*, 8(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021

[10] Nisha Dhanraj Dewani, Zubair Ahmed Khan, Agarwal, A., Sharma, M., & Shaharyar Asaf Khan. (2022). *Handbook of research on cyber law, data protection, and privacy*. Information Science Reference. An Imprint Of Igi Global.

[11] Lambert, P. (2020). *A User's Guide to Data Protection: Law and Policy*. In Library Genesis. Bloomsbury Professional.

[12] Badini, H., & Karami, H. (2021). **Comparative study of responsibility of the processing Applicant institution, the controller, and the Processor under gdpr and the Bill "Preservation and protection Personal Data"**. *Legal Research Quarterly*, *24*(95), 137-158. https://doi.org/10.29252/jlr.2021.184069.1396 {In Persian}

[13] https://snappfood.ir/privacy-policy

[14] Taghavifard, M. T., Taghva, M., Faghihi, M., & Jamshidi, M. (2017). **A Comparative Study on Information Privacy Protection Acts in Iran and Selected Countries.** *Majlis and Rahbord*, *24*(89), 301-333. {In Persian}

[15] Badini, H., & Kandsari, H. S. (2018). **A Comparative Analysis of the Foundations of Civil Responsibility of Service Suppliers in Islamic, Iranian and French Law**. *J. Compar. L.*, *5*, 177. https://doi.org/10.22096/law.2019.34496

[16] Ghanad, F., & Aligholi, A. (2020). **The Notion and Importance of Personal Data and Privacy and Their Various Protections in Cyber Space**. *ModernTechnologies Law*, *1*(1), 297-322. https://doi.org/10.22133/clj.2020.243290.1016.{In Persian}

[17] Latifzadeh, M., Qabuli Dorafshan, S. M. M., Mohseni, S., & Abedi, M. (2023). **Protection of Personal Data in EU Law and its Feasibility in the Iranian Legal System**. *Public Law Studies Quarterly*, *53*(2), 981-1005.

*Knowledge Discovery*, 7(5), e1211. Wiley. https://doi.org/10.1002/widm.1211
[23] Lambert, P. (2016). *The Data Protection Officer*. CRC Press.
[24] Šidlauskas, A. (2021). **The Role and Significance of the Data Protection Officer in the Organization**. *Socialiniai Tyrimai*, 44(1), 8–28. https://doi.org/10.15388/soctyr.44.1.1
[25] Zamani, S. G., & Attar, S. (2017). **Human Rights and the Right to Be Forgotten in the Age of New Information**. Technologies. *International Law Review*, *33*(55), 81-108. doi: 10.22066/cilamag.2016.23525 {In Persian}
[26] European Union Agency for Fundamental Rights and Council of Europe. (2018). *Handbook on European data protection law*. Luxembourg, Publications Office of the European Union
[27] Ansari, B. (2023). *Rights of Virtual Space Users*. Tehran: Sahami Enteshar Co.
[28] Giurgiu, A., & Larsen, T. A. (2016). **Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More'European'DPAs as Guardians of Consistency?**. *Eur. Data Prot. L. Rev.*, *2*, 342. Https://doi.org/10.22059/jplsq.2021.324694.2786 {In Persian}
[18] Li, Y., & SaxunovÃ, D. (2020). **A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations**. *Procedia Computer Science*, *170*, 1110-1115. https://doi.org/10.1016/j.procs.2020.03.060
[19] Smedinghoff, T. J. (2015). **An Overview of Data Security Legal Requirements for All Business Sectors**. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2671323
[20] Stam, A., & Kleiner, B. (2020). **Data anonymisation: legal, ethical, and strategic considerations**. *Swiss Centre of Expertise in the Social Sciences*, 1-15 https://doi.org/10.24449/FG-2020-00011
[21] Koo, J., Kang, G., & Kim, Y.-G. (2020). **Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges**. *Sustainability*, 12(24), 10571. MDPI. https://doi.org/10.3390/su122410571
[22] Cheng, L., Liu, F., & Yao, D. D. (2017). **Enterprise data breach: causes, challenges, prevention, and future directions.** *Wiley Interdisciplinary Reviews: Data Mining and*