Journal of Islamic Human Rights
Volum 1, Consecutive Number 1, 2024
Journal Homepage: https://islamichumanrights.ir/

Protecting Non-Public Cyber Data: A Critical Reflection on Two Bills in Iran's Criminal Policy

Mahdi Khaghani Esfahani*

Assistant Professor of Criminal Law and Criminology, The Institute for Research and Development in Humanities (SAMT), Tehran, Iran. khaghani@samt.ac.ir

Abstract

Unauthorized processing of personal data leads to violations of the rights of their owners, and the criminal nature of most instances of violations necessitates the provision of the right to file a criminal lawsuit for the person who owns the rights (data subject). Therefore, the government is obliged to protect the rights of personal data owners as victims; therefore, adopting an efficient criminal policy to protect such data and prevent and punish illegal data processing is the subject of research from the perspective of criminal policy to promote the security of national and international cyber rights. The approval of the "General Data Protection Regulation of the European Union" (2016) and its implementation since 2018, on the one hand, and the formulation of the "Data Protection and Privacy in Cyberspace Bill" in Iran in 2017, as well as the "Personal Data Protection and Protection Bill" in 2018, and of course the approval of the "National Data Management and Information Law" in 2022, are manifestations of the Iranian legislator's firm decision to update the country's laws and regulations in this area and to partially model them on the regulations mentioned in the European Union. However, the shortcomings of Iran's legislative criminal policy in preventive and punitive protection of personal data are the subject of criticism in this article. This qualitative article was written through a critical analysis of the discourse governing the articles of the two bills, within the framework of a critical approach to legislative criminal policy and with an interdisciplinary nature of criminal law and information technology law, and includes reform proposals for Iranian legislative criminal policymakers in the field of cyber regulation.

Keywords: Criminal policy, data security, personal data, cyber rights, data protection bill

- Khaghani Esfahani, M. (2024). Protecting Non-Public Cyber Data: A Critical Reflection on Two Bills in Iran's Criminal Policy, *Journal of Islamic Human Rights*, 1(1), 1-22.

مجله حقوق بشر اسلامی
دورۀ اول ـ شمارۀ اول ـ ۱۴۰۳
صفحات ۱-۲۲ (مقاله پژوهشی)
تاریخ: دریافت ۱۴۰۳/۰۹/۰۱ـ پذیرش ۱۴۰۳/۱۱/۰۲ ـ انتشار ۱۴۰۳/۱۲/۱۵

صیانت از داده‌های سایبری غیرعمومی، تأملی انتقادی بر دو لایحه در سیاست جنایی ایران

مهدی خاقانی اصفهانی *

استادیار حقوق جزا و جرم‌شناسی پژوهشکده تحقیق و توسعه علوم انسانی (سمت)، تهران، ایران.
khaghani@samt.ac.ir

چکیده

پردازش غیرمجاز داده‌های شخصی به نقض حقوق صاحبان آن‌ها منجر می‌شود و مجرمانگیِ ماهیت اغلب مصادیق نقض، مقتضیِ پیش‌بینی حق اقامه دعوای کیفری برای شخص صاحب حق (موضوع داده) است. لذا حاکمیت موظف به حمایت از حقوق مالکان داده‌های شخصی به‌عنوان بزه‌دیدگان است؛ لذا اتخاذ یک سیاست جنایی کارآمد جهت حمایت از این‌گونه داده‌ها و پیشگیری و کیفرگذاری پردازش غیرقانونیِ داده‌ها، موضوع پژوهش از منظر سیاست جنایی جهت ارتقای امنیت حقوق سایبری ملی و بین‌المللی است. تصویب «مقررات عمومیِ حفاظت از داده اتّحادیه اروپا» (۲۰۱۶) و اجرای آن از سال ۲۰۱۸ از یک‌سو و تدوین «لایحه حفاظت از داده‌ها و حریم خصوصی در فضای مجازی» در ایران در سال ۱۳۹۶ و همچنین «لایحه صیانت و حفاظت از داده‌های شخصی» در سال ۱۳۹۷ و هم البته تصویب «قانون مدیریت داده‌ها و اطلاعات ملّی» در سال ۱۴۰۱، نمود تصمیم راسخ مقنّن ایرانی در روزآمدساختن قوانین و مقررات کشور در این حیطه و الگوبرداریِ نسبی از مقررات مورد اشاره در اتّحادیه اروپا است. اما نارسایی‌های سیاست جنایی تقنینی ایران در حمایت پیشگیرانه و کیفرگذارانه در قبال داده‌های شخصی، مورد نقد مقاله حاضر است. این مقاله کیفی، به روش تحلیل انتقادی گفتمانِ حاکم بر موادی از دو لایحه مزبور، در چارچوب رویکرد انتقادی به سیاست جنایی تقنینی و با ماهیت میان‌رشته‌ایِ حقوق کیفری و حقوق فناوری اطلاعات تألیف یافته و دربرگیرندۀ پیشنهادهای اصلاحی برای سیاستگذاران جنایی تقنینی ایران در حوزه مقررات‌گذاری سایبری می‌باشد.

کلیدواژه: سیاست جنایی، امنیت داده، داده‌های شخصی، حقوق سایبری، لایحه حفاظت از داده‌ها

- خاقانی اصفهانی، مهدی. (۱۴۰۳). صیانت از داده‌های سایبری غیرعمومی، تأملی انتقادی بر دو لایحه در سیاست جنایی ایران، مجله حقوق بشر اسلامی، ۱(۱)، صفحات ۱-۲۲.

مقدمه

اگرچه ظرفیت‌های قانونی و به‌تبع آن قضایی در حمایت کیفری از داده‌های شخصی وجود دارد، لیکن خلأهای تقنینی با توجه به عدم تصویب لایحه صیانت و حفاظت از داده‌های شخصی وجود دارد، از طرفی خود لایحه نیازمند بررسی دقیق علمی است تا آسیب‌شناسی صورت گیرد و نقاط قوت و ضعف آن شناسایی شود. بررسی کارکرد دستگاه‌های اجرایی در قبال حمایت از داده‌های شخصی امری است که نیازمند بررسی است، این نهادها نیز به آسیب‌شناسی نیاز دارند. مهم‌تر از همه ارائه طرحی است که هماهنگی متقابل بین دو نظام تقنینی ـ قضایی و اداری ـ اجرایی برقرار کند.

از این رو، تبیین سیاست جنایی ایران در حمایت از داده‌های شخصی و آسیب‌شناسی آن، که از طریق بررسی تحلیلی ـ انتقادی قوانین موضوعه در رابطه با داده‌های شخصی و نقد رویه حاکم در رسیدگی به پرونده‌های مرتبط میسر است، در کنار تبیین کارکرد و اقدامات نهادهای اداری، انتظامی و اجرایی در حمایت از داده‌های شخصی، می‌تواند زمینه مطالعه جهت ترسیم و ارائه الگوی مطلوب در حمایت از داده‌های شخصی با نگاهی به مقررات بین‌المللی و اروپایی را به دست دهد. هم‌راستا با این مهم، تبیین و تحلیل اصول کیفری حاکم بر پردازش داده‌های شخصی و تبیین چارچوب قانونی و غیرقانونی پردازش این داده‌ها و شناسایی ظرفیت‌ها و خلأهای قانونی حقوق ایران در زمینه حمایت کیفری از داده‌های شخصی، همپای استفاده از ابزارهای حقوقی، کیفری، انتظامی و آموزشی در اصلاح ساختارها و نهادها و بخش‌های اداری، زمینه‌ساز امکان ارائه طرح و الگو مبنی بر چگونگی ایجاد تعامل و هماهنگی بین دو نظام کیفری و اجرایی در قبال حمایت کیفری از داده‌های شخصی خواهد بود.

میزان جمع‌آوری و پردازش این داده‌ها توسط شرکت‌های خصوصی و نهادهای حاکمیتی تا حد بسیار زیادی افزایش یافته است. تحول سریع و روزافزون فناوری و نیز پدیده جهانی شدن، چالش‌های جدیدی درخصوص حمایت از داده‌های شخصی ایجاد کرده است. پردازش داده‌های شخصی به‌ویژه داده‌های شخصی حساس در موارد غیرضرور، حقوق و آزادی‌های افراد را در معرض خطر قرار می‌دهد. به‌منظور حمایت از حق بنیادین افراد در برابر پردازش غیرمجاز داده‌های شخصی و به‌ویژه داده‌های شخصی حساس، شاهد تکوین و توسعه یک رویکرد در حقوق ایران و اتحادیه اروپا هستیم. این رویکرد در جهت رعایت موازنه بین حق بنیادین افراد نسبت به حمایت از داده‌های

شخصی خود و ضرورت‌های ملی و منافع اجتماعی مرتبط با پردازش داده‌های شخصی اتخاذ شده است.

یک سیاست جنایی مطلوب در زمینه حمایت از داده‌های شخصی سه رهیافت پیشگیری، نظارت و پاسخ‌دهی را هم‌زمان در نظر می‌گیرد. این سیاست جنایی در مقام پاسخ‌دهی به پردازش غیرمجاز داده‌ها دو رویکرد تنظیم‌گری اداری و سرکوب کیفری را با هم هماهنگ می‌سازد و نسبت به حمایت از داده‌های شخصی حساس رویکردی افتراقی اتخاذ می‌کند. همچنین باید توجه داشت که اصل رضایت از ذخیره، پردازش و توزیع داده شخصی، اصل آگاهی و اطلاع دادن درخصوص اهداف پردازش، اصل جمع‌آوری و استفاده از داده‌ها به اندازه ضرورت و متناسب با اهداف تعیین‌شده، اصل صحیح و روزآمد بودن داده‌های مورد پردازش، اصل دسترسی و مشارکت در کنترل صحت داده‌ها و امکان حذف آن‌ها، اصل امکان درخواست حذف داده‌های شخصی توسط شخص موضوع داده، بر داده‌های شخصی حاکم است. سیاست تقنینی ایران بر سرکوب کیفری پردازش غیرمجاز داده‌ها متمرکز است. با وجود این، سیاست قضایی در زمینه حمایت از داده‌ها فعال نیست.

وانگهی رویکرد صرفاً کیفری در حمایت از داده‌های شخصی مؤثر نیست. نظام حقوقی ایران از سازوکارهای نظارت کافی در حمایت از داده‌های شخصی و مکانیسم‌های اداری برای رسیدگی به تخلفات این حوزه و جبران خسارت از صاحبان داده‌های شخصی برخوردار نیست. ارتقای سیاست جنایی در حمایت از داده‌های شخصی مستلزم قانون‌گذاری مناسب و ایجاد نهادی تنظیم‌گر جهت پیشگیری، نظارت و پاسخ‌دهی است. تکمیل و اصلاح جرم‌انگاری‌ها و ایجاد هماهنگی متقابل میان دو نظام اداری و کیفری ازجمله عوامل مؤثر در انطباق سیاست جنایی با نیازهای مربوط به این حوزه است.

۱. پیشینه پژوهش

در سال ۲۰۱۸ مقاله‌ای فرانسوی تحت عنوان "Traitement illicite de données relatives à la santé" توسط *پیر دسماریاس* و *میل برتو* تألیف شده است. در این مقاله نویسندگان از یک‌سو به تبیین چارچوب قانونی پردازش داده‌های شخصی در حوزه سلامت می‌پردازند و از سوی دیگر با توجه به رویه قضایی، حمایت کیفری از پردازش غیرمجاز داده‌های شخصی در حوزه سلامت را مورد بررسی قرار می‌دهند. در این مقاله، رأی صادرشده در تاریخ ۷ ژوئن ۲۰۱۷ توسط دادگاه مارسی در مورد محکومیت یک

پزشک شاغل در بیمارستان مارسی به جهت پردازش غیرمجاز داده‌های شخصی به پرداخت ۵۰۰۰ یورو جزای نقدی، تحلیل می‌شود.

برت کاسترز و دیگران در سال ۲۰۱۸ مقاله‌ای با عنوان "A comparison of data protection legislation and policies across EU" را منتشر کرده‌اند. این مقاله کشورهای آلمان، سوئد، بریتانیا، ایرلند، فرانسه، هلند، رومانی و ایتالیا را در حوزه حمایت و حفاظت از داده‌ها از منظر وضعیت کلی حفاظت از داده‌ها، سیاست‌های ملی حفاظت از داده‌ها (ازجمله میزان کنترل بر داده‌های شخصی و میزان آگاهی از شیوه‌های کنترل بر داده‌های شخصی)، نحوه اجرای مقررات این حوزه (رویکردهای مختلف کشورهای مذکور به حمایت از داده‌های شخصی) و کنترل‌گران (ازجمله تعداد و وضعیت سازمان‌های مستقل از دولت و میزان شفافیت در اهداف) مورد بررسی قرار داده است. استنتاج این مقاله چنین است که هرچند رهنمود سال ۱۹۹۵ اتحادیه اروپا و از آن مهم‌تر GDPR (General Data Protection Regulation) سال ۲۰۱۶ درصدد یکسان‌سازی شرایط حمایت از داده‌ها در سراسر اتحادیه اروپا بوده و کماکان نیز هستند، لیکن هنوز هم میان کشورهای این اتحادیه ازهم‌گسیختگی قانونی وجود دارد.

در سال ۱۳۹۷ پایان‌نامه‌ای تحت عنوان بررسی تطبیقی سیاست کیفری ایران و سوریه در حمایت از داده‌های شخصی با نگاهی به حقوق انگلستان توسط آقای عبدالغنی عتقی به نگارش درآمده است. در این پایان‌نامه نظام‌های حقوقی ایران، سوریه و انگلستان از منظر مفهوم داده‌های شخصی و تفکیک آن از مفاهیم مشابه، انواع و اشکال داده‌های شخصی و اهمیت حمایت از آن‌ها، سیاست کیفری ماهوی حمایت از داده‌های شخصی (تعیین مصلحت حمایت‌شده در جرایم داده‌های شخصی، سیستم‌های جرم‌انگاری اعمال ضد داده‌های شخصی و جرایم علیه داده‌های شخصی)، مسئولیت کیفری و ماهیت مجازات و سیاست کیفری شکلی در حمایت از داده‌های شخصی مورد بررسی قرار گرفته‌اند. در پایان نیز نگارنده چنین نتیجه گرفته که ایران و سوریه در زمینه حمایت کیفری از داده‌های شخصی در قیاس با کشور انگلستان، در جایگاهی نازل‌تر قرار دارند.

دکتر باقر انصاری کتابی با عنوان حقوق حریم خصوصی را در سال ۱۳۹۳ به رشته تحریر درآورده است. ایشان پس از پرداختن به مفهوم و تعریف حریم خصوصی، نسبیت حریم خصوصی، عوامل مؤثر بر حریم خصوصی، مبنا و ماهیت حریم خصوصی، حمایت از این حریم در اسناد بین‌المللی و حقوق اسلام، مطالعه تطبیقی حریم خصوصی و حمایت

از حریم خصوصی در حقوق موضوعه ایران، گفتار پنجم از بخش سوم کتاب خود را به حریم اطلاعات شخصی اختصاص داده‌اند. ایشان در این گفتار ارتباط میان داده‌های شخصی و حریم خصوصی، مفهوم داده‌های شخصی، اصول حاکم بر داده‌های شخصی (ازجمله اصل جمع‌آوری، اصل استفاده از داده‌های شخصی، اصل به گردش انداختن داده‌های شخصی، اصل جریان فرامرزی داده‌ها و اصل دسترسی به داده‌های شخصی و تصحیح داده‌های نادرست) را به‌صورت تطبیقی و با لحاظ قوانین و مقررات بین‌المللی موجود در این حوزه، تبیین نموده است.

۲. مفاهیم و نظریات اساسی پژوهش

در این بخش، پس از تبیین مقدمه و ضرورت پژوهش، مقاله به تعریف و تشریه اصطلاحات و نظریه‌های اساسیِ منشأ تأثیر در بدنه مقاله می‌پردازد.

۲-۱. محرمانگی داده‌ها

محرمانگیِ داده، به حق شهروندان در کنترل اطلاعات شخصی آن‌ها و تصمیم در مورد (افشاء یا عدم افشا آن) گفته می‌شود. محرمانگیِ داده و حفاظت از آن، دو موضوع مرتبط با یکدیگر هستند. به‌طورکلی، حفاظت از داده، سازوکاری حقوقی است که محرمانگیِ آن را تضمین می‌کند. به بیان دیگر، محرمانگیِ داده تعریف می‌کند که چه کسی به داده دسترسی داشته باشد؛ در حالی که حفاظت از داده، ابزارها و سیاست‌هایی را برای محدودکردن بالفعل دسترسی به داده‌ها وضع می‌کند. یکی از مهم‌ترین شاخصه‌های ماهوی در حمایت از داده‌های شخصی، حفاظت از محرمانگیِ آن‌ها است. این موضوع در ماده ۸ منشور حقوق اساسی اتحادیه اروپا مورد توجه قرار گرفته است: «هرکس حق حفاظت از داده‌های شخصی مربوط به خود را دارد. چنین داده‌هایی باید به‌طور منصفانه، برای اهداف مشخص و براساس رضایت فرد و یا برخی مبانی قانونی دیگر که توسط قانون وضع‌شده‌اند، پردازش شوند ...». قانون اساسی ایران نیز در اصول ۲۲، ۲۳، ۲۵ و ۳۹، به انحاء مختلف از حریم خصوصی حمایت کرده است؛ بنابراین قانون اساسی ایران، اگرچه به‌طور غیرمستقیم، صراحت بالایی در حمایت از داده‌های شخصی افراد دارد (رجبی، ۱۴۰۲: ۹-۸).

شایان ذکر است داده‌ها زمانی شخصی قلمداد می‌شوند که به یک شخص حقیقی، مربوط یا قابل ربط باشند. این عنصر در تعیین قلمرو داده‌های شخصی و تأثیر استفاده از فناوری‌های جدید برای پردازش داده‌ها، در شخصی یا غیرشخصی قلمداد شدن آن‌ها، نقش تعیین‌کننده‌ای دارد. اگر فردی از طریق داده‌هایی که پردازش می‌شود شناسایی یا قابل‌شناسایی شود، باز داده شخصی نخواهد بود مگر اینکه آن داده‌ها به او مربوط باشد (رجبی، ۱۴۰۲: ۸۸). بنابراین داده‌ها ممکن است به یک فرد قابل‌شناسایی ارجاع دهند ولی به دلیل مربوط نبودن به او، داده‌ها در مورد آن فرد، شخصی نمی‌باشد. در بسیاری از موقعیت‌ها این ارتباط به‌راحتی برقرار می‌شود؛ به‌عنوان مثال داده‌های ثبت‌شده در پرونده کارگزینی به وضوح مربوط به وضعیت شخصی به‌عنوان کارمند است. همچنین اطلاعات مربوط به نتایج آزمایش پزشکی یک بیمار که در پرونده پزشکی وی موجود است یا تصویر شخصی که در یک مصاحبه ویدئویی از او فیلم‌برداری شده است. با وجود این گاهی مربوط بودن به‌صورت غیرمستقیم است، برای مثال، ارزش یک خانه می‌تواند داده شخصی باشد (عزیزی، ۱۳۹۸: ۱۰۸). درواقع ارزش یک خانه خاص اطلاعات مربوط به یک شیء است نه یک شخص اگر از این اطلاعات برای تعیین میزان تعهدات یک شخص نسبت به پرداخت برخی مالیات‌ها استفاده شود در این صورت مسلم است که چنین اطلاعاتی باید به‌عنوان داده‌های شخصی در نظر گرفته شود.

یکی از تقسیم‌بندی‌های به عمل آمده از داده‌ها، تفکیک آن‌ها به حاکمیتی و غیرحاکمیتی است. در ارتباط با داده حاکمیتی، بایستی گفت که حکومت‌ها، حجم گسترده‌ای از داده را تولید، نگهداری و مدیریت می‌کنند که دارای ارزش سیاسی، اقتصادی و اجتماعی بالایی است. طبیعتاً بخشی از این داده‌ها بنا به یکی از اقتضائات سه‌گانهٔ امنیت ملی، اسرار تجاری و حریم خصوصی، انحصاراً در اختیار حاکمیت است و در اصطلاح به آن، داده حاکمیتی گفته می‌شود. در مقابل، هر داده‌ای که مشمول امتیازات و همچنین محدودیت‌های داده حاکمیتی نباشد را می‌توان داده غیرحاکمیتی قلمداد نمود (انصاری، ۱۴۰۲: ۱۵۵-۱۴۵).

تقسیم داده بر مبنای نوع و هدف پردازش به عمل آمده نیز از دیگر تقسیم‌بندی‌های آن است و در این خصوص، داده‌ها را می‌توان به داده‌های پردازش شده بر مبنای رضایت، داده‌های پردازش شده بر مبنای ضرورت قراردادی، داده‌های پردازش شده به‌منظور

تعهدات قانونی کنترل‌گر، داده‌های پردازش شده به‌منظور حفاظت از منافع حیاتی اشخاص، داده‌های پردازش شده برای نفع عمومی و انجام وظیفه رسمی و داده‌های پردازش شده برای منافع مشروع کنترل‌گر یا شخص ثالث اشاره نمود (همان، ۱۹۱-۱۶۵).

۲-۲. پردازش داده‌ها

پردازش دارای تعریفی بسیار گسترده در قانون است و اساساً به معنای هر آن چیزی است که ممکن است با داده‌ها انجام گیرد و این، شامل پیاده کردن اطلاعات از اینترنت، ارسال اطلاعات به کمک پست الکترونیکی و خواندن یک قسمت از اطلاعات بر روی صفحه یک رایانه می‌باشد عباسی کلیمانی و اکبری، ۱۳۹۸: ۸۷). به عبارت دیگر پردازش به هرگونه فعالیت یا مجموعه‌ای از فعالیت‌ها گفته می‌شود که بر روی داده‌های شخصی یا مجموعه‌ای از داده‌های شخصی، توسط ابزارهای خودکار یا غیرخودکار انجام می‌شوند؛ همانند جمع‌آوری، ثبت، سازماندهی، ساختاردهی، ذخیره‌سازی[1]، انطباق یا تغییر بازیابی، مشورت، استفاده، افشا از طریق خبررسانی، انتشار یا قابل دسترس ساختن، هماهنگی یا ترکیب، محدود ساختن، پاک‌کردن یا تخریب (بند ۲ ماده ۴ مقررات عمومی اتحادیه اروپا).

در لایحه صیانت و حفاظت از داده‌های شخصی منظور از پردازش داده‌ها عبارت است از هرگونه عملیات دستی یا خودکار بر داده‌های شخصی، شامل و نه محدود به ایجاد، ثبت، دریافت، گردآوری، نگهداری، جداسازی، تغییر، تجزیه و تحلیل، طبقه‌بندی، ساختاربندی، تطبیق، ذخیره‌سازی، اشتراک‌گذاری، فرستادن، توزیع و عرضه، انتشار و در دسترس قرار دادن و پاک کردن آن‌ها (باب یکم، بخش دوم، ماده ۲، بند ب)؛ درواقع، به محض ثبت داده‌ها یک رابطه حقوقی و اخلاقی بین پردازشگر و پردازنده ایجاد می‌شود و پردازشگر مسئولیت حفاظت از داده‌ها را بر عهده دارد.

---

۱. ذخیره داده (Data Saving) به معنای اقدامی است که جهت نگهداری و حفاظت از داده و با ابزارهای مخصوص دارای حافظه انجام می‌گیرد. در مورد ذخیره داده پیام‌های شخصی حساس، پرونده شرکت فرانسوی SKF نمونه جالبی است. این شرکت بدون اطلاع به کمیسیون ملی اطلاعات و آزادی‌های فرانسه، اطلاعاتی را در مورد زندگی خصوصی، عقاید سیاسی متقاضیان کار و عضویت آنان در اتحادیه‌های کارگری در یک دستگاه دستی ذخیره داده‌ها نگهداری می‌کرد. این عمل نقض ماده ۴۲ قانون پردازش داده‌ها و آزادی‌های فردی ۱۹۸۷ محسوب می‌شد. کمیسیون اطلاعات و آزادی‌ها پرونده را به دادستان کل ارسال کرد که خواستار جریمه‌ای معادل درآمد یک سال شرکت بود (زیبر، ۱۳۹۰: ۵۶)

مقررات حفاظت از داده اروپا و همچنین لایحه صیانت و حفاظت از داده‌های شخصی به تعریف پردازش داده به‌طور مطلق پرداخته‌اند اما نظر به ادامه تعریف واضح می‌شود که مراد هر دو سند، ارائه تعریف از پردازش داده شخصی است نه مطلق پردازش داده. نکته دیگر این که برخی از اقداماتی که ذیل تعریف پردازش داده چه در لایحه و چه در مقررات اروپایی مطرح‌شده است در تعریف سند مقابل وجود ندارد اما در لایحه صیانت با وجود عبارت «شامل نه محدود به» همه موارد مذکور در مقررات اروپایی ذیل تعریف لایحه قابل فرض است و حتی مواردی که در هر دو سند مورد ذکر قرار نگرفته نیز در این تعریف مفروض خواهد بود. در نهایت، پردازش داده‌های شخصی هرگونه عملیات یا مجموعه عملیاتی است که صرف نظر از روش‌های به کار گرفته شده، موضوع آن‌ها داده‌های شخصی باشد. بی‌شک، نوع تعریف، بر الگوی سیاست جنایی مواجهه با این رایم تأثیر می‌گذارد؛ آنچنان که سیاست جنایی امنیت‌گرا با شعار تأمین حداکثری امنیت شهروندان، بیشتر دچار نوعی بحران، خصوصاً در عرصهٔ نظام حقوق بشری گردیده است. (فرهادی آلاشتی و جوان‌جعفری، ۱۳۹۶: ۶۹)

۳-۲. سیاست جنایی امنیت سایبری

پس از پیروزی انقلاب اسلامی و از اواخر دهه ۱۳۶۰ خورشیدی، اصطلاح سیاست کیفری مورد توجه برخی از اساتید حقوق جنایی قرار گرفت. از دهه ۱۳۷۰، کتاب‌ها و مقاله‌های مورد ترجمه و تحقیق به قلم «دکتر علی‌حسین نجفی ابرندآبادی» ـ استاد پیشکسوت عرصه سیاست جنایی و جرم‌شناسی ـ خوانش دلماس‌مارتی و کریستین لازرژ[1] از سیاست جنایی در کلاس‌های تحصیلات تکمیلی حقوق جزا و جرم‌شناسی، رساله‌ها، کتاب‌ها و مقاله‌ها و به‌طورکلی در نوشتگان و گفتمان سیاست جنایی در ایران رواج یافت.

مارک آنسل اولین ارائه‌کننده تعریف موسّع از سیاست جنایی است. او سیاست جنایی را «واکنش سازمان‌یافته و سنجیدهٔ جامعه در مقابل اعمال مجرمانه یا ضد اجتماعی» تعریف کرد (آنسل، ۱۳۹۱: ۴۲). پس از او، کریستین لازرژ در تعریف سیاست جنایی نوشت: «غور و تفحص انتقادانه و علت‌آبانه پیرامون پدیده مجرمانه، رمزیابی پدیده مجرمانه و وسایل به

۱. دو استاد شهیر فرانسوی حوزه سیاست جنایی که دو کتاب و چند مقاله از آن‌ها مورد برگردان و بحث و تفصیل توسط استاد دکتر علی‌حسین نجفی ابرندآبادی قرار گرفته است.

کار گرفته شده برای مبارزه علیه رفتارهای انحرافی یا مجرمانه» و نیز «یک استراتژی حقوقی و اجتماعی مبتنی بر مبانی برگزیده ایدئولوژیک یا هدف پاسخ‌دهی واقع‌گرایانه به مسائل و مقتضیات پیشگیری و سرکوبی پدیده مجرمانه به معنای وسیع کلمه» (لازرژ، ۱۴۰۰: ۳۱). اما مهم‌ترین تعریف از سیاست جنایی در میان تعاریف موسّع ـ که بر ادبیات دانشگاهیِ ایران نیز چیرگی دارد ـ تعریف میری دلماس‌مارتی است: «مجموعه روش‌هایی که به وسیله آن، بدنه اجتماعی (هیئت اجتماع: دولت و ملت) پاسخ‌های خود را به پدیده مجرمانه سازماندهی می‌کند.» (دلماس مارتی، ۱۳۸۱: ۳۴)

امنیت حقوق سایبری بر پایه اصولی مانند حریم خصوصی، امنیت اطلاعات و مسئولیت‌پذیری و پاسخگویی استوار است و در دو مفهوم مضیق و موسع کار برد دارد. مفهوم مضیق اتخاذ تدابیر فنی و پیشگیرانه برای تأمین امنیت شبکه و اطلاعات است. مفهوم موسع اصلی، کلیه تدابیر فنی و قانونی برای تأمین داده، اطلاعات، سیستم، شبکه‌های رایانه‌ای و مخابراتی است و مفهوم موسع واسطه‌ای، تدابیری است در پی تنظیم مقررات مناسب برای این فضا تا امنیت فضای واقعی را تأمین کند (شاملو، ۱۴۰۱: ۴۳۷). امنیت جامعه در گرو امنیت فضای سایبر است. بنابراین برای امنیت سایبر باید به اقدامات پیشگیرانه دست زد. حفاظت دقیق از داده‌ها، هم از طریق دولت و هم از طریق سازمان‌های خدمت‌رسان و هم از طریق خود افراد، در کاهش ناامنی بسیار مؤثر است. از طرف دیگر لازم است اقدامات و رویه‌های حقوقی برای مقابله با تهدیدات سایبری و جرایم مرتبط با فناوری اطلاعات اعمال شود. قوانین سایبری برای جرایم هک، کلاهبرداری، سرقت و انتشار بدافزار ایجاد و مجازات متناسب برای آن تعیین شود. با تنظیم قوانین از حریم خصوصی افراد حفاظت شود و مانند اتحادیه اروپا (GDPR) سازمان‌ها به رعایت مقررات حریم خصوصی ملزم شوند. استانداردهای امنیتی برای ذخیره‌سازی و انتقال داده‌ها ایجاد شود و سازمان‌ها به استفاده از فناوری رمزنگاری و امنیتی ملزم شوند (وطنی و اسدی، ۱۳۹۵: ۱۰۳). همچنین مکانیزمی برای گزارش‌دهی حوادث و پاسخ به حملات سایبری ایجاد شود و برای مقابله با جرایم فرامرزی همکاری‌های بین‌المللی برقرار گردد. شهروندان و سازمان‌ها با خطرات سایبر آشنا و نحوه محافظت از خود در فضای سایبر را آموزش ببینند. درباره حقوق دیجیتال و مسئولیت‌های مرتبط با فضای مجازی آگاهی داده شود. نهادهای نظارتی بر فعالیت‌های

سایبری نظارت داشته و مجرمان سایبری تعقیب شوند و برای مقابله با جرایم سایبری در معاهدات و توافق‌نامه‌های بین‌المللی مشارکت شود و اطلاعات و تجربیات دیگر کشورها در زمینه امنیت سایبری استفاده شود.

۳. نقد لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی

لایحه «حمایت از داده‌ها و حریم خصوصی در فضای مجازی» به همت سازمان فناوری اطلاعات ایران و پژوهشگاه قوه قضاییه و دانشگاه علم و فرهنگ تدوین و در دهم دی‌ماه ۱۳۹۶ منتشر شده است، یکی از مهم‌ترین لوایح درخصوص حفظ حریم خصوصی و صیانت از داده‌ها و اطلاعات کاربران در حوزه فضای سایبر است. با وجود کوشش فراوانی که در تهیه متن پیش‌نویس صورت گرفته، همچنان دارای اشکالات شکلی و ماهوی ازجمله عدم حفاظت از اطلاعات مخصوصاً اطلاعات مالی است. پژوهشگران (حیدری و جعفری، ۱۳۹۹: ۵۲) بحث کرده‌اند که به جهت اشکالات فراوان پیش‌نویس، زمان بیشتری جهت نقد آن از سوی صاحب‌نظران لازم بوده و تاکنون هیچ‌گونه اقدام رسمی درخصوص آن صورت نگرفته است و چه‌بسا در صورت قانون شدن لایحه «صیانت و حفاظت از داده‌های شخصی» از اهمیت و ضرورت تصویب آن کاسته شود.

در دولت هشتم پیش‌نویس لایحه‌ای تحت عنوان «حمایت از حریم خصوصی» در نهاد ریاست جمهوری آماده شد که تقریباً تمامی ابعاد حقوق حریم خصوصی را دربرداشت. این پیش‌نویس که در حال حاضر به صورت طرح در مجلس شورای اسلامی مطرح است و دورنمای مقنن در این زمینه را تشکیل می‌دهد در ۱۲۱ ماده و هفت فصل به ترتیب زیر تدوین شده است: تعاریف، حریم خصوصی منازل و اماکن خصوصی، حریم خصوصی جسمانی، حریم خصوصی در محل کار، حریم خصوصی اطلاعات، حریم خصوصی ارتباطات و مسئولیت‌های ناشی از نقض حریم خصوصی.

درخصوص تجارت الکترونیکی، مواد ۱۰۳ تا ۱۱۰ لایحه (مبحث سوم از فصل ششم) تحت عنوان حریم خصوصی در اینجا قابلیت بررسی دارند؛ تدقیق در مواد فوق الاشاره نشان‌دهنده این است که سمت و سوی محتوایی آن‌ها عمدتاً قواعد ناظر بر تکالیف ارائه‌دهندگان خدمات اینترنتی (اعم از داخلی و بین‌المللی) است تا قواعد مرتبط به داده‌های شخصی و طبیعی است.

در لایحه صیانت و حفاظت از داده‌های شخصی شرایط رضایت به پردازش عبارت‌اند از: پردازش داده‌های شخصی مربوط به وضعیت‌ها یا موقعیت‌های غیرعمومی، منوط به رضایت شخص موضوع آن‌هاست (ماده ۴)، اعلام رضایت اشخاص موضوع داده باید با رعایت شرایط ذیل باشد: الف) پیش از پردازش باشد؛ ب) بیانگر آگاهی شخص موضوع داده باشد؛ و پ) استنادپذیر باشد (ماده ۵). پردازش داده‌های شخصی مربوط به وضعیت‌ها یا موقعیت‌های عمومی، بدون رضایت شخص یا اشخاص موضوع آن‌ها در صورتی بلامانع است که: الف) خودش داده‌ها را در معرض پردازش قرار داده باشد؛ یا ب) پردازش داده‌های خود را منع یا محدود نکرده باش. (ماده ۶). رضایت حاصل از فریب یا تهدید یا اکراه شخص موضوع داده معتبر نیست و در صورت عدم اهلیت وی، رضایت ولی یا قیم او الزامی است. حالات اغما و مانند آنکه بر نبود قصد و اراده وی دلالت دارند، موجب عدم اهلیت‌اند (ماده۷ بخش یکم از باب دوم حقوق اشخاص موضوع داده‌ها.)

در ماده ۱۲ و ۱۳ این لایحه استثنائات اصل رضایت آمده است به این ترتیب در موارد ذیل، طبق ماده ۱۲ پردازش داده‌های شخصی در چارچوب قوانین مربوط، بدون رضایت اشخاص موضوع آن‌ها بلامانع است: الف) برای صیانت از حیثیت، جان یا مال شخص موضوع داده ضروری باشد؛ ب)برای صیانت از حیثیت یا جان دیگری یا پیشگیری از زیان مالی شدید به او ضروری باشد؛ پ) برای پیشگیری یا پاسخ به تهدیدهای نظم، ایمنی و امنیت عمومی ضروری باشد؛ ت) برای کشف جرائم یا تخلفات یا شناسایی متهمان یا اجرای احکام قضایی و انتظامی ضروری باشد. (تبصره ـ استناد به هریک از معاذیر بالا تنها در صورتی موجه است که گزینه دیگری امکان‌پذیرنباشد). همچنین طبق ماده ۱۳ لایحه نیز بهره‌برداری مالکانه از داده‌های شخصی، بدون رضایت شخص موضوع آن‌ها در صورتی بلامانع است که: الف) گمنامی وی حفظ شود؛ ب) عرفا زیان مادی یا معنوی برای وی نداشته باشد؛ پ) جلب رضایت وی عملاً امکان‌پذیر نباشد. نیز آنکه طبق بند ۵ ماده ۲ طرح حمایت از حریم خصوصی و بند ب، ماده ۲، بخش دوم، باب یکم لایحه صیانت و حفاظت از داده‌های شخصی، داده‌های مذکور در ماده ۵۸ ذیل داده‌های حساس قابل تعریف هستند.

هرچند داده‌های شخصی مفهومی نسبی است و درباره مصادیق و اشخاص مورد حمایت بین کشورهای مختلف اتفاق نظر وجود ندارد، اما ماده ۵۸ یادشده از حیث

مصادیق داده‌های شخصی با گرایش عمومی کشورها به‌ویژه اتحادیه اروپا دارای ایراد است. درواقع، ماده ۵۸ داده‌های شخصی مورد حمایت را به داده‌هایی محدود کرده که اصطلاحاً «حساس» یا «غیرقابل جمع‌آوری» نامیده می‌شوند. در حالی که بند ۱ ماده ۴ مقررات حمایت از داده‌های عمومی اتحادیه اروپا محدوده داده‌های شخصی را گسترده کرده و چنین بیان می‌کند: «... هرگونه اطلاعات مربوط به شخص حقیقی قابل شناسایی کسی است که مستقیم یا غیرمستقیم، به‌ویژه با اشاره به یک شناسه خاص مانند نام، شماره شناسایی، اطلاعات مکان، شناسه آنلاین یا شناسایی یک یا چند عامل و ویژگی فیزیکی، فیزیولوژیکی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی قابل‌شناسایی باشد.» این تعریف تمامی جنبه‌های شخصیتی یک فرد را که عامل شناسایی اوست بیان می‌کند.

همان‌طورکه ملاحظه می‌شود از دید اتحادیه اروپا هرگونه اطلاعاتی که براساس آن بتوان یک شخص حقیقی را شناسایی کرد از مصادیق داده‌های شخصی محسوب و قابل حمایت خواهد بود. بدین ترتیب داده‌های مرتبط یا آدرس جغرافیایی یا پستی، شماره ملی، شماره گواهی‌نامه رانندگی، شماره حساب بانکی، شماره کارت بانکی، شماره اشتراک آب و برق و گاز و تلفن و همچنین عکس یا تصویری که شناسایی شخص را ممکن سازد، داده شخصی محسوب می‌شود. این در حالی است که برابر ماده ۲۹ پیش‌نویس لایحه، داده‌های شخصی اعم از حساس و غیرحساس موضوع جرم قرار گرفته و حساس بودن داده‌های مورد تعرض تنها موجب تشدید مجازات است و به نظر می‌رسد از آنجا که پیش‌نویس لایحه نسبت به قانون تجارت الکترونیکی عام است و درخصوص داده‌های شخصی غیرحساس تعارضی بین دو مقرره نیست، در صورت قانون شدن پیش‌نویس لایحه باید به آن استناد کرد (حیدری و جعفری، ۱۳۹۹: ۵۹)

دیگر آنکه، برخی از نویسندگان چنین نقد کرده‌اند که این ماده به ظاهر بر رعایت اصل تحصیل قانونی و مبتنی بر رضایت شخص موضوع گردآوری و پردازش، تأکید کرده است، اما باید توجه داشت که واژه «ذخیره» را، که در این ماده از مصادیق اعمال ممنوع تلقی شده است، نمی‌توان مرادف با اصطلاح «گردآوری» تلقی کرد، زیرا گردآوری ناظر بر مرحله تحصیل داده‌ها و ذخیره ناظر بر مرحله نگهداری داده هاست. با این وصف، نمی‌توان به ممنوعیت گردآوری غیرمجاز داده‌ها براساس این ماده قائل بود (قناد و علیقلی، ۱۳۹۹: ۳۱۷) درنتیجه در جرم گردآوری غیرمجاز داده‌ها و به تبع آن سایر تکالیف

پردازشگر در این خصوص ممنوع نبوده و مشمول حمایت کیفری نمی‌گردد (جیشانکار، ۱۳۹۴: ۱۰۵). اما با توجه صدر ماده ۵۸ که لفظ پردازش را بیان نموده است و نظر به تعریف پردازش ـ که ذیل عنوان «مفهوم پردازش» در رساله حاضر گذشت ـ نقد این نویسندگان وارد نیست چرا که مفهوم پردازش هرگونه اقدام بر روی داده‌ها ازجمله گردآوری را شامل می‌شود.

٤. نقد لایحه صیانت و حفاظت از داده‌ها شخصی

مؤخرترین فعالیت تقنینی لایحه صیانت و حفاظت از داده‌های شخصی است که پیش‌نویس آن به پیشنهاد وزارت ارتباطات و فناوری اطلاعات توسط سازمان فناوری اطلاعات تدوین و در مرداد ۱۳۹۷ منتشر و سپس به کمیسیون فرعی حوزه دولت الکترونیک ریاست جمهوری ارجاع شد تا نهادهای مربوطه پیش‌نویس این لایحه را بررسی کنند و اوایل سال ۱۳۹۸ نسخه نهایی این لایحه آماده و اکنون این نسخه به کمیسیون اصلی حوزه دولت الکترونیک ارسال شده تا در هیئت وزیران تصویب شود. از سوی دیگر این لایحه به‌صورت طرح نیز به مجلس ارائه شده است. بررسی‌های انجام‌شده، همچنین حاکی از آن است، شکایاتی که در زمینه پردازش و استفاده غیرمجاز از داده‌های شخصی نزد مراجع قضایی مطرح می‌شود، به‌واسطه توسیع عناوین اتهامی ذیل جرایم ذکر شده در قانون جرایم رایانه‌ای قرار می‌گیرد (حیدری و جعفری، ۱۳۹۹: ۵۴)

در مورد خلأهای قانونی حقوق ایران در زمینه حمایت کیفری از داده‌های شخصی ابتدا مقدمتاً باید گفت در حقوق موضوعه ایران، تا دهه ۱۳۸۰، قوانین و مقررات روشنی در حمایت از حریم خصوصی اطلاعات وجود نداشت. پس از ورود فناوری‌های ارتباطی نو به ایران و سوء استفاده برخی اشخاص از این فناوری‌ها برای افشای امور خصوصی افراد و هتک حیثیت آنان، دولت نیز حمایت از حریم خصوصی را مورد توجه بیشتر قرار داد و قوانین و مقرراتی روشن در این باره تصویب کرد (انصاری و همکاران، ۱۴-۱: ۹۲). در حال حاضر، تعابیر مختلفی در حمایت از حریم خصوصی اطلاعات در قوانین و مقررات ایران مشاهده می‌شود؛ برای مثال در قانون مطبوعات از عبارت «اسرار شخصی»، قانون مجازات اسلامی از عبارت «اسرار مردم»، قانون آزادی اطلاعات از عبارت‌های «داده‌های شخصی» و «حریم خصوصی»، قانون جرایم رایانه‌ای از عبارت «صوت یا تصویر یا فیلم

خصوصی یا خانوادگی یا اسرار دیگری» و در مصوبات شورای عالی انقلاب فرهنگی و مجمع تشخیص مصلحت نظام از عبارت «حریم خصوصی» استفاده شده است (انصاری، ۱۴۰۲: ۱۵۳-۱۳۶) اما در نهایت در سیاست جنایی ایران، یعنی در قوانین و آیین‌نامه‌ها، تعریف حریم شخصی به‌طور صریح عنوان نشده است همین موضوع می‌تواند ابهاماتی را در این خصوص فراهم آورد چرا که عدم تعیین حدود مفهوم حریم شخصی توسط قانون می‌تواند زمینه تفاسیر متعدد را در جایگاه‌های مختلف فراهم آورد و همین مطلب نیز مسیر تخلف از قوانین را به صورت عمد یا غیرعمد فراهم می‌آورد. همچنین با توجه به گذشت زمان از تصویب قوانین، در حال حاضر ضمانت اجراهای موجود در برخی قوانین از بازدارندگی کافی برخوردار نیستند، لذا به روزرسانی این مواد ضروری به نظر می‌رسد.

پراکندگی مراجع قانونگذاری و همچنین تعدد قوانین و عدم انسجام در آن‌ها به‌طور واضحی مشهود است که این موضوع عدم کفایت یا نارسایی قوانین را بیش از آنچه وجود دارد، اظهار می‌دارد. این امر علاوه بر تنقیح قوانین، ایجاد وحدت در مراجع قانونگذاری یا ایجاد مرجعی برای همراستا نمودن مراجع قانونگذاری یا نظارت بر آن‌ها را ضروری می‌نماید تا هم مخاطب سریعتر و راحتتر و همچنین با ابهام کمتر، به تمام شرایط قانونی اشراف پیدا نماید و هم مراجع قانونگذاری احاطه کامل و دقیقی نسبت به همه جوانب قانون در این زمینه داشته باشند که هم نسبت به اشکالات و هم نسبت به خلأها و همچنین به روزرسانی مواد اقدام به موقع صورت گیرد.

یکی دیگر از اشکالات موجود در رابطه با قانونگذاری در زمینه حمایت از داده‌های شخصی، ارجاع قانون در موارد مهم و اساسی به آیین‌نامه است به عبارت دیگر واضح است که قوت آیین‌نامه چه به جهت ماهوی و چه به جهت اجرایی نسبت به قانون ضعیف‌تر بوده و همچنین در برخی موارد شاهد عدم تصویب آیین‌نامه در زمان مقرر و یا عدم تصویب و یا حتی عدم امکان دسترسی به آیین‌نامه وجود دارد که این موضوع می‌تواند اشکالات متعددی را برای اجرای قانون فراهم آورد.

نکته دیگر اینکه در برخی موارد قانونگذار به حمایت از داده‌های حساس پرداخته و داده‌های غیرحساس مورد غفلت واقع شده است. این بدان معنا است که نه‌تنها در حمایت از داده‌های حساس خلأ قانونی وجود دارد بلکه این خلأ در حمایت از داده‌های غیرحساس بیشتر احساس می‌شود.

در زمینه اصول حاکم بر داده‌های شخصی نیز باید گفت که این اصول در قانون تجارت الکترونیک بیان شده است اما اصول مذکور کامل نبوده و همه مقتضیات این اصول در قانون فوق پیش‌بینی‌نشده است (اصلانی۱۳۸۶، ۳۶۳). باید در نظر داشت که همه اصول مرتبط با حوزه حمایت از داده‌های شخصی و همچنین مقتضیات آن ذیل قانون تجارت الکترونیک قابل تعریف نیست لذا عدم وجود برخی از اصول در این قانون ممکن است به جهت عدم شمول قانون بوده باشد. همچنین است آنچه که در رابطه با مقتضیات اصول مطرح شد چرا که اصول عام بوده و مقتضیات آن نیز گستره وسیع‌تری نسبت به قانون تجارت الکترونیک را دارا می‌باشند بنابراین در بعضی موارد برخی از مقتضیات اصول مطرح در قانون تجارت الکترونیک با توجه به شمول سایر قوانین در قوانین و مقررات دیگری مورد تصویب قرار گرفته است. به این ترتیب اشکال اصلی در این حوزه این است که این اصول باید در یک قانون جامع مطرح شود و مقتضیات آن نیز در همان قانون مورد پیش‌بینی قرار گیرد اینکه اصول در یک قانون خاص مطرح شود و مقتضیات آن در برخی قوانین و مقررات دیگر به صورت پراکنده مورد نظر قرار گیرد واضح است که مورد تأیید نیست. به‌عنوان مثال اصول ممنوعیت افشا، امنیت، انتخاب و ... در قانون تجارت الکترونیک مورد طرح قرار نگرفته است. برای بحث مقتضیات نیز می توان به قانون انتشار و دسترسی آزاد اشاره نمود به این صورت که اصل رضایت در قانون تجارت الکترونیک آمده اما برخی از مقتضیات این اصل بنا به شمول قانون انتشار و دسترسی آزاد به اطلاعات، ذیل این قانون مورد اشاره قرار گرفته است.

در قوانین موجود نقایص مختلفی نیز در ارتباط با اشخاص و مؤسسه‌های گردآوری و پردازش‌کننده داده‌ها و ارائه‌دهندگان خدمات اینترنتی وجود دارد که لایحه «حریم خصوصی» این ایراد را از حیث تکالیف و مسئولیت‌های کیفری ارائه‌دهندگان خدمات اینترنتی تا حدودی حل کرده است. ولی این لایحه نیز درخصوص نحوه تشکیل، فعالیت، وظایف و اختیارات و نیز مسئولیت‌های اشخاصی که به گردآوری و پردازش داده‌های شخصی می‌پردازند ساکت است (زرکلام، ۱۳۸۶: ۱۹۵) که افزودن این موارد به لایحه مذکور ضروری به نظر می‌رسد.

در باب وضعیت بحث از داده‌های شخصی تجاری و اقتصادی در حقوق ایران نیز باید گفت که گذشته از فقدان قوانین حمایت از داده‌ها در حوزه حقوق رقابت، در باب حمایت

از داده‌های شخصی مربوط به فعالیت تجاری و اقتصادی اشخاص، نص قانونی که مفید حمایت قانونی از این قبیل داده‌ها و منع پردازش آن‌ها باشد به چشم نمی‌خورد. به نظر می‌رسد فقدان حمایت از داده‌های شخصی تجاری و اقتصادی داده‌ها در درازمدت تأثیر منفی بر روابط اقتصادی و جریان اطلاعات کشورمان گذارده و ایران را در لیست سیاه کشورهای حمایت‌کننده از داده قرار دهد و جریان اطلاعات از این کشورها به ایران را با مشکل مواجه نماید، ازاین‌رو اصلاح قانون برای مقابله با این وضعیت ضروری است.

بنابه آنچه که بیان شد تصویب قانون جامع و کامل درخصوص حمایت از داده‌های شخصی یا بازبینی، تکمیل و ایجاد یکپارچگی در قوانین موجود در کشور ضروری به نظر می‌رسد و درنهایت می‌توان گفت، رویکرد قوانین ایران برای جلوگیری از نقض حریم خصوصی بیشتر جنبه کیفری دارد و در برخی موارد به جبران خسارت و مسئولیت مدنی نیز اشاره شده است. در مقررات اتحادیه اروپا رویکرد اصلی غیرکیفری است و فقط به جریمه نقدی در صورت نقض قوانین اشاره کرده است و برخلاف قوانین ایران مجازات حبس را برای مجازات نقض حریم خصوصی در نظر نگرفته است. جدا از مجازات‌های مقرر در قوانین مذکور، این نکته نیز حائز اهمیت است که فرهنگ‌سازی و آماده کردن اشخاص برای اجرای قانون جدید تأثیر بسزایی در حاکمیت قانون دارد. این مهم زمانی رخ می‌دهد که تمامی اقشار جامعه آگاه شوند. با آگاه‌سازی افراد درباره حقوق و وظایفشان می‌توان از خسارت‌های احتمالی بعدی جلوگیری کرد (قناد، ۱۳۹۹: ۳۱۹-۳۱۸) و در پیشگیری از جرم و به‌طور خاص جرائم نقض داده‌های شخصی موفق بود. این در حالی است که در ایران در این زمینه فرهنگسازی مورد نیاز، صورت نگرفته است.

نتیجه‌گیری

در تحقق الگوی مطلوب در سیاست جنایی ایران اشکالات متعددی قابل ملاحظه است، یکی از این اشکالات مقدماتی اما مهم، این است که در قوانین و آیین‌نامه‌ها، تعریف حریم شخصی به‌طور صریح عنوان نشده است همین موضوع می‌تواند ابهاماتی را در این خصوص فراهم آورد چرا که عدم تعیین حدود مفهوم حریم شخصی توسط قانون می‌تواند زمینه تفاسیر متعدد را در جایگاه‌های مختلف فراهم آورد و همین مطلب نیز مسیر تخلف از قوانین را به صورت عمد یا غیرعمد ایجاد می‌کند. نکته دیگر اینکه در برخی موارد

قانونگذار به حمایت از داده‌های حساس پرداخته و داده‌های غیرحساس مورد غفلت واقع شده است. این بدان معنا است که نه‌تنها در حمایت از داده‌های حساس خلأ قانونی وجود دارد بلکه این خلأ در حمایت از داده‌های غیرحساس بیشتر احساس می‌شود.

اصول پردازش داده‌های شخصی در نظام حقوقی ایران در ماده ۵۹ قانون تجارت الکترونیک مقرر شده است. باید در نظر داشت که همه اصول مرتبط با حوزه حمایت از داده‌های شخصی و همچنین مقتضیات آن ذیل قانون تجارت الکترونیک قابل تعریف نیست لذا عدم وجود برخی از اصول در این قانون ممکن است به جهت عدم شمول قانون بوده باشد. همچنین است آنچه که در رابطه با مقتضیات اصول مطرح شد چرا که اصول عام بوده و مقتضیات آن نیز گستره وسیع‌تری نسبت به قانون تجارت الکترونیک را دارا می‌باشند بنابراین در بعضی موارد برخی از مقتضیات اصول مطرح در قانون تجارت الکترونیک با توجه به شمول سایر قوانین در قوانین و مقررات دیگری مورد تصویب قرار گرفته است. به این ترتیب اشکال اصلی در این حوزه این است که این اصول باید در یک قانون جامع مطرح شود و مقتضیات آن نیز در همان قانون مورد پیش‌بینی قرار گیرد، این که اصول در یک قانون خاص مطرح شود و مقتضیات آن در برخی قوانین و مقررات دیگر به صورت پراکنده مورد نظر قرار گیرد مورد تأیید نیست. به‌عنوان مثال اصول ممنوعیت افشا، امنیت، انتخاب و ... در قانون تجارت الکترونیک مورد طرح قرار نگرفته است. برای بحث مقتضیات نیز می توان به قانون انتشار و دسترسی آزاد اشاره نمود به این صورت که اصل رضایت در قانون تجارت الکترونیک آمده اما برخی از مقتضیات این اصل بنا به شمول قانون انتشار و دسترسی آزاد به اطلاعات، ذیل این قانون مورد اشاره قرار گرفته است.

در حقوق موضوعه ایران، اگرچه ضعف‌های در این حوزه وجود دارد اما حمایت‌هایی از داده‌های شخصی به‌طور صریح یا ضمنی مورد نظر قرارگرفته و قانون‌گذار در قوانین مختلف، اَعمال مختلفی همچون دسترسی، ذخیره‌سازی، پردازش، انتشار، توزیع و انتقال را در ارتباط با داده‌های شخصی مورد حمایت کیفری قرار داده است؛ در حالی که گردآوریِ غیرمجاز داده‌های شخصی و وظایف پردازشگر را جرم‌انگاری نکرده است. در جرائم رایانه‌ای نیز اگرچه در ماده ۸ (ماده ۷۳۶ قانون مجازات اسلامی) به اَعمال مرتبط با پردازش غیرمجاز داده‌های شخصی مانند حذف، تخریب و یا مختل کردن پرداخته شده است

اما دسترسی غیرمجاز به داده‌های شخصی دیگری به‌طور عام مورد قانون‌گذاری واقع نشده است بلکه تنها دسترسی غیرمجاز به داده‌های محافظت‌شده توسط تدابیر امنیتی (ماده ۱) و دسترسی غیرمجاز به داده‌های سریِ در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی (ماده ۳) مورد جرم‌انگاری قرار گرفته است. علاوه بر موارد گفته‌شده، عدم جرم‌انگاری اَعمالی همچون فراهم نمودن موجبات دسترسی غیرمجاز به داده‌های شخصی و پردازش غیرمجاز آن‌ها و همچنین فروش داده‌های شخصیِ متعلّق به دیگری (علاوه بر فروش یا انتشار یا در دسترس قرار دادن گذرواژه متعلق به دیگری در ماده ۲۵ جرائم رایانه‌ای) از جانب قانون‌گذار، به‌شدت قابل تأمّل و انتقاد به نظر می‌رسد. با تصویب قانون جدید آیین دادرسی کیفری، حمایت از داده‌ها نقشی پررنگ‌تر به خود گرفت. تشکیل «مرکز ملّی داده‌های قوه قضائیه» (ماده ۶۵۰)، وظیفه قوه قضائیه مبنی بر فراهم آوردن تمهیدات فنی و قانونی لازم برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان (ماده ۶۵۸) و همچنین تعیین ضمانت اجرا به‌منظور مقابله با نقض عمدی و غیرعمدی حریم داده‌های شخصی (مادتین ۶۶۰ و ۶۶۱) از مهم‌ترین مصادیق حمایت از داده‌ها در قانون مزبور است. آخرین گام برداشته‌شده در سطح قانون‌گذاری به‌منظور حمایت از داده‌های شخصی را می‌توان در تصویب قانون مدیریت داده‌ها و اطلاعات ملّی در سال ۱۴۰۱ ملاحظه نمود. اگرچه این اقدام گام مثبتی در حمایت از داده‌های شخصی محسوب می‌شود اما لازم به ذکر است که آنچه در این قانون مورد نظر قرار گرفته، حمایت از داده‌های شخصی با محوریت انتقال و تبادل داده‌ها بین دستگاه‌ها و نهادها است و نمی‌توان این قانون را قانون حمایت از داده‌های شخصی صرف؛ به این معنی که به تمام حوزه‌های مربوط به حمایت از داده ورود کرده باشد، دانست.

با وجود تفصیل مقررات عمومی اتحادیه اروپا در ارتباط با تعیین ضمانت اجرای اداری در قبال نقض حریم داده‌های شخصی، این موضوع در حقوق ایران و قانون مدیریت داده‌ها و اطلاعات ملی، مسکوت مانده و تنها در ماده ۹ قانون مزبور، ضمانت اجرای کیفریِ انفصال از خدمت به مدت شش ماه تا پنج سال یا حبس تعزیری به مدت نود و یک روز تا شش ماه برای متخلف یا اخلال‌کننده در پردازش و تبادل یا مستنکف از اجرای این قانون، پیش‌بینی شده است. به بیان دیگر، قانون‌گذار ایران علاوه بر عدم تفصیل در تعیین مجازات اداری، در قبال تخلف اداریِ منجر به نقض حریم داده‌های شخصی نیز مبادرت به تعیین

ضمانت اجرای کیفری نموده است. در ارتباط با نهاد یا نهادهای متولی راهبرد سرکوب اداری در حقوق ایران نیز، اتحادیه کشوری کسب‌وکارهای مجازی از مهم‌ترین آن‌هاست که با اِعمال ضمانت اجرای تعلیق فعالیت و نماد، می‌تواند مبادرت به اِعمال سرکوب اداری در قبال پردازش غیرمجاز داده‌ها در کسب‌وکارهای مجازی نماید.

یکی دیگر از اشکالات موجود در رابطه با قانونگذاری در زمینه حمایت از داده‌های شخصی، ارجاع قانون در موارد مهم و اساسی به آیین‌نامه است به عبارت دیگر واضح است که قوت آیین‌نامه چه به جهت ماهوی و چه به جهت اجرایی نسبت به قانون ضعیف‌تر بوده و همچنین در برخی موارد شاهد عدم تصویب آیین‌نامه در زمان مقرر و یا عدم تصویب و یا حتی عدم امکان دسترسی به آیین‌نامه وجود دارد که این موضوع می‌تواند اشکالات متعددی را برای اجرای قانون فراهم آورد.

به نظر می‌رسد درخصوص متولّیان راهبردهای مختلف پیشگیری، کنترل و سرکوب در ارتباط با داده‌های شخصی، مهم‌ترین مشخصه حقوق موضوعه فعلیِ ایران، تشتّت و عدم انسجام نهادهاست؛ به‌عنوان نمونه در حوزه راهبرد پیشگیری، می‌توان به انجام آگاه‌سازی از جانب سه نهاد (مرکز ملی فضای مجازی، مرکز ماهر و آپا) و انجام خودتنظیم‌گری از جانب سه نهاد (کارگروه تعامل‌پذیری دولت الکترونیک، سازمان فناوری اطلاعات و اتحادیه کشوری کسب‌وکارهای مجازی) اشاره نمود. در حوزه راهبرد کنترل نیز انجام نظارت بر اجرای مقررات از جانب دو نهاد (مرکز ملی فضای مجازی، سازمان تنظیم مقررات و ارتباطات رادیویی) و انجام بازرسی از جانب پنج نهاد (کارگروه تعامل‌پذیری دولت الکترونیک، مرکز ماهر، اتحادیه کشوری کسب‌وکارهای مجازی، بخش ستادی پلیس فتا و دادسرای جرائم رایانه‌ای) محل تأمّل بوده و ضمن ایجاد تداخل در وظایف و موازی کاری در انجام راهبردهای مربوطه، دستیابی به الگوی مطلوب را نیز با چالش مواجه نموده است. علاوه بر اینها، اعطای اختیارات سرکوبگرانه به کارگروه تعیین مصادیق مجرمانه (با اکثریت اعضای غیرحقوقی) نیز مورد انتقاد است. با توجه به ضرورت دقت حقوقی و تخصصی در حوزه اختیارات سرکوبگرانه، به نظر می‌رسد بهتر است این حوزه ذیل قانونگذاری‌های مجلس باقی بماند.

در حوزه استقلال نهادهای نظارتی ایران نیز می‌توان گفت که در حقوق ایران، نهادهای نظارتی از استقلال به معنای استقلال در عملکرد، برخوردار هستند اما در برخی موارد،

تداخل در وظایف و موازی کاری دیده می‌شود و همچنین در بعضی نهادها، جایگاه نظارتی در برخی موضوعات با ابهام همراه است. نکته دیگر اینکه چنانچه بحث استقلال را به استقلال در نظارت بر حمایت از داده‌های شخصی تعریف کنیم این استقلال در هیچ‌یک از نهادها دیده نمی‌شود بلکه هریک از این نهادهای نظارتی به مجموعه‌ای از امور نظارت دارند که بخشی از آن به بحث حمایت از داده باز می‌گردد.

منابع

- ابراهیمی، شهرام. (۱۳۹۱). جرم‌شناسی پیشگیری، چاپ دوم، تهران: نشر میزان.
- آنسل، مارک. (۱۳۹۱). دفاع اجتماعی، ترجمه محمد آشوری و علی‌حسین نجفی ابرندآبادی، چاپ چهارم، تهران: انتشارات گنج دانش.
- انصاری، باقر. (۱۴۰۲). حقوق داده (اصول پردازش داده‌های شخصی)، تهران: شرکت سهامی انتشار.
- انصاری، باقر؛ عطار، شیما؛ زند، حسین زند؛ صالحی، امیرحسین صالحی. (۱۴۰۱). مطالعه تطبیقی حمایت از داده‌های شخصی در اروپا، چین و ایران. تهران: شرکت سهامی انتشار.
- جیشانکار، کی. (۱۳۹۴). جرم‌شناسی فضای مجازی: کشف جرایم اینترنتی و رفتار مجرمانه، ترجمه حمیدرضا ملک‌محمدی، چاپ اول، تهران: نشر میزان.
- حیدری، علی‌مراد؛ جعفری، علی. (۱۳۹۹). جرایم علیه داده پیام‌های شخصی در تجارت الکترونیک، *پژوهشنامه حقوق کیفری*، دوره ۲۱، شماره ۱.
- دلماس‌مارتی، می‌ری. (۱۳۸۱). نظام‌های بزرگ سیاست جنایی، ترجمه علی‌حسین نجفی ابرندآبادی، تهران: نشر میزان.
- رجبی، ابوالقاسم. (۱۴۰۲). شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا ـ قانون اساسی، قوانین و مقررات فدرال و ایالتی. تهران: گزارش مرکز پژوهش‌های مجلس.
- رئیسی، لیلا؛ قاسم‌زاده لیاسی، فلور. (۱۳۹۹). چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر، *نشریه حقوقی*، دوره ۸۴، شماره ۱۱۰.
- زرکلام، ستار. (۱۳۸۶). حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)» *پژوهشنامه حقوق اسلامی*، دوره ۸، شماره ۱.
- زیبر، اولریش. (۱۳۹۰). جرایم رایانه‌ای، ترجمه احمد رحیمی مقدم و مصطفی بختیاروند، تهران: انتشارات گنج دانش.

- عباسی کلیمانی، عاطفه؛ اکبری، عاطفه. (۱۳۹۸). جرایم سایبری، تهران: انتشارات مجد.
- عزیزی، امیرمهدی. (۱۳۹۸). حقوق کیفری جرایم رایانه‌ای، چاپ سوم، تهران: انتشارات مجد.
- فرهادی آلاشتی، زهرا؛ جوان‌جعفری بجنوردی، عبدالرضا. (۱۳۹۶). چالش‌های رویارویی پیشگیری موقعیت‌مدار از جرایم سایبری فرامرزی، فصلنامه پژوهش‌های اطلاعاتی و جنایی، دوره ۱۲، شماره ۱.
- قناد، فاطمه؛ علیقلی، امیره. (۱۳۹۹). مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی، *دو فصلنامه حقوق قراردادها و فناوری‌های نوین*، دوره ۱، شماره ۱.
- گروهی از نویسندگان. (۱۴۰۱). دانشنامه رفتار سایبری [به کوشش باقر شاملو]، چاپ اول، تهران: نشر میزان.
- لازرژ، کریستین. (۱۴۰۰). درآمدی بر سیاست جنایی، ترجمه علی‌حسین نجفی ابرندآبادی، چاپ دهم، تهران: نشر میزان.
- وطنی، امیر؛ اسدی، حمید. (۱۳۹۵). سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم، *پژوهشنامه حقوق اسلامی*، دوره ۱۷، شماره ۴۳.

References

- European Union Agency for Fundamental Rights. 2018. *Handbook on European data protection law: 2018 Edition*. Council of Europe.