Comparative Law Review, Vol. 13, No. 1, Spring & Summer 2022 (Research Article)

Data Protection in China; A Comparative Study of the Data Protection Approach in the United States and the European Union

Bagher Ansari
Associate Professor, Faculty of Law & Political Science, University of Shahid Beheshti, Tehran, Iran
(Email: b_ansari@sbu.ac.ir)

Shima Attar[*]
Ph.D. in Private Law, Faculty of Law & Political Science, University of Allameh Tabataba`i, Tehran, Iran

(Received: 2021/11/09, Accepted: 2022/03/05)

Abstract
While the European Union and the United States have each designed their own model for personal data protection, China is swiftly developing a particular data protection system in order to have power and competitive advantage over European countries, the United States and Japan. To explain the model, this article seeks to answer the question: what are the main features of the Chinese personal data protection model? Has China been impressed by the American or European model? For this purpose, the specific model designed by this country based on American and European patterns has been explained and analyzed. The results show that by imposing fragmented and sectoral regulations, China had first taken a similar approach to the United States' in the field of data protection. It has then gradually moved towards the European approach and considered adoption of a comprehensive data protection law. Eventually, however, it has taken different approaches regarding the private and public sectors, data localization and restrictions on cross-border data transfer. Given that Iran has also just started the design of a data protection system, being informed about these approaches, especially the Chinese one, can put their strengths and weaknesses before Iranian policymakers and legislators.

Keywords
Cybersecurity, China, Privacy, Personal data, Artificial intelligence.

[*] Corresponding Author; Email: shimaattar@gmail.com Fax:0982122368015

مطالعات حقوق تطبیقی
دورهٔ ۱۳، شمارهٔ ۱
بهار و تابستان ۱۴۰۱
صفحات ۹۱ تا ۱۱۳ (علمی - پژوهشی)

حمایت از داده‌ها در چین؛ مطالعهٔ تطبیقی با رویکرد حمایت از داده‌ها در امریکا و اتحادیهٔ اروپا[1]

باقر انصاری
دانشیار دانشکدهٔ حقوق و علوم سیاسی دانشگاه شهید بهشتی
(Email: b_ansari@sbu.ac.ir)
شیما عطّار*
دانش‌آموختهٔ دکتری حقوق خصوصی دانشکدهٔ حقوق و علوم سیاسی دانشگاه علامه طباطبائی
(تاریخ دریافت: ۱۴۰۰/۰۸/۱۸، تاریخ پذیرش: ۱۴۰۰/۱۲/۱۴)

چکیده

درحالی که اتحادیهٔ اروپا و امریکا هرکدام مدل خاصی را برای حمایت از داده‌های شخصی طراحی کرده‌اند، چین به‌سرعت در حال توسعهٔ نظام خاصی در زمینهٔ حمایت از داده‌ها است تا قدرت و مزیت رقابتی را برای این کشور در برابر کشورهای اروپایی، امریکا و ژاپن به‌دنبال داشته باشد. برای تبیین این مدل، نگارندگان این مقاله درصدد پاسخ به این پرسش‌اند که مشخصه‌های اصلی مدل حمایت از داده‌های شخصی در چین چیست؟ آیا چین در طراحی این مدل، از الگوی امریکا تأثیر پذیرفته است یا از الگوی اروپا؟ به این منظور، مدل خاصی که این کشور با اقتباس از الگوهای امریکایی و اروپایی طراحی کرده، تبیین و تحلیل شده است. نتیجهٔ این مطالعه نشان می‌دهد که چین در حوزهٔ حمایت از داده‌ها ابتدا با وضع مقررات پراکنده و بخشی، رویکردی مشابه امریکا اتخاذ کرده، سپس به‌تدریج به سمت رویکرد اروپایی و تصویب قانون جامع حمایت از داده متمایل شده، ولی سرانجام، رویکرد خاص و ترکیبی را اتخاذ کرده است؛ به این ترتیب که در مورد بخش خصوصی و بخش عمومی، محلی‌سازی داده‌ها و محدودیت انتقال فرامرزی داده‌ها احکام متفاوتی دارد. با توجه به اینکه ایران نیز در ابتدای مسیر طراحی نظام حمایت از داده‌هاست، آشنایی با این رویکردها و به‌ویژه رویکرد چین، می‌تواند نقاط قوت و ضعف آنها را پیش روی سیاست‌گذاران و قانون‌گذاران ایران قرار دهد.

واژگان کلیدی

امنیت سایبری، چین، حریم خصوصی، داده‌های شخصی، هوش مصنوعی

---

۱. این مقاله برگرفته از مطالعه‌ای است که با عنوان «ابعاد حقوقی جمع‌آوری، پردازش و تجاری‌سازی داده‌ها در هوش مصنوعی» در *مرکز پژوهش و نوآوری فانوس* انجام شده است.

* نویسندهٔ مسئول؛ فکس: ۰۲۱۲۲۳۶۸۰۱۵ Email: shimaattar@gmail.com

مقدمه

اروپا و امریکا در دههٔ ۱۹۷۰ و تقریباً به‌طور هم‌زمان، ساختاربندی نظام حمایت از داده‌ها را با تکیه بر اصول عام حمایت از داده آغاز کردند. درحالی که در اروپا سوءاستفاده از حریم خصوصی و داده‌های شخصی در طول جنگ جهانی دوم و پس از آن، سبب شناسایی داده‌های شخصی به‌عنوان مصداقی از حق حریم خصوصی گردید، در امریکا حمایت از داده‌ها در تعادل با منافع تجاری مرتبط و آزادی بیان یادشده در متمم نخست قانون اساسی مورد توجه قرار گرفت. نتیجهٔ تفاوت این دو رویکرد در طی سال‌ها در سطح تصویب اسناد قانونیِ حمایت از داده‌های شخصی آشکار شد؛ اتحادیهٔ اروپا ساختار حمایتی خود را بر مبنای حاکمیت یک قانون جامع حمایت از داده‌ها در قالب «دستورالعمل حمایت از افراد در برابر پردازش خودکار داده‌های شخصی و جریان آزاد این داده‌ها» در سال ۱۹۹۵ (the Directive 95/46/EC on protection of individuals with regard to the processing of personal data and on the free movement of such data) و نسخهٔ اصلاحی جایگزین آن در سال ۲۰۱۶ با عنوان مقررات عمومی حمایت از داده‌های شخصی (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) با دو هدف حمایت از حقوق بنیادی افراد در زمینهٔ پردازش داده‌های شخصی و جلوگیری از ایجاد مانع در برابر جریان آزاد داده‌ها در اتحادیهٔ اروپا پایه‌ریزی کرده است؛ درحالی که امریکا حمایت از داده‌ها را به‌طور پراکنده در بخش‌های خاص مانند سلامت، ارتباطات، امور مالی و اعتباری مورد توجه قرار داده است.

با توجه به اینکه به‌طور سنتی داده‌های شخصی در ذیل حریم خصوصی تعریف می‌شوند، نخستین نشانه برای احراز وجود یا نبود حمایت از داده‌های شخصی در هر نظام حقوقی، شناسایی یا عدم شناسایی حق حریم خصوصی است. این حق در اروپا، نخست در مادهٔ ۸ کنوانسیون اروپایی حقوق بشر و آزادی‌های اساسی و سپس در منشور حقوق بنیادی شناسایی شد. درحالی که چین با تکیه بر ارزش‌های جمعی و کمونیستی و اتخاذ رویکرد مخالفت با ارزش‌های غربی مسیر خاصی را درپیش گرفت که مانع حمایت از حریم خصوصی می‌شد[1]. به همین دلیل، وضع قوانین و مقررات مربوط به حمایت از داده‌ها در چین قدمت چندانی ندارد و این کشور عمدتاً در سال‌های اخیر (به‌ویژه سال ۲۰۲۰) برای ایجاد نظام حمایت از داده‌ها تلاش می‌کند که ازجمله می‌توان به اختصاص فصلی از «قانون مدنی» (Civil Code of the

۱. در عصر حاضر نیز مفهوم حریم خصوصی برای شهروند جمهوری خلق چین با درک شهروند غربی از این مفهوم بسیار متفاوت است. ترکیب واژگانی «حریم خصوصی» برای شهروند چینی مفهومی ناآشنا و غریب است به گونه‌ای که نمی‌تواند میان واژهٔ حریم خصوصی با اصطلاح راز شرم‌آور (shameful secret) تمایزی قائل شود.

People's Republic of China) به «حریم خصوصی و حمایت از اطلاعات شخصی» (Rights to Privacy and Protection of Personal Information) و تصویب «قانون حمایت از اطلاعات شخصی» (Personal Information Protection Law of the People's Republic of China) به‌عنوان یک قانون جامع با هدف حمایت از اطلاعات شخصی اشاره کرد.

با اینکه شناسایی حق حریم خصوصی از پیش‌فرض‌های حمایت از داده‌های شخصی است، «قانون اساسی چین» (Constitution of the People's Republic of China)[1] هیچ اصلی در مورد حریم خصوصی و حمایت از داده‌ها ندارد و تنها در اصل ۴۰ به آزادی و حریم خصوصی مکاتبات اشاره کرده است. با وجود این، اختصاص یکی از بخش‌های قانون اساسی به حقوق بنیادی شهروندان و همچنین صراحت اصلاحیهٔ ۲۰۰۴ قانون اساسی بر تعهد دولت به احترام و حمایت از حقوق بشر، نشانگر پذیرش ضمنی حق حریم خصوصی در این کشور قلمداد شده است (De Hert & Papakonstantinou, 2015: 15).

ابتکارهای قانونی برای حمایت از داده‌های شخصی در چین، نخستین بار با مصوبه «کمیتهٔ دائمی کنگرهٔ ملی خلق چین» (The Standing Committee of the National People's Congress) تحت عنوان «تصمیم راجع به ارتقای حمایت از اطلاعات آنلاین» (The Decision on Strengthening Online Information Protection) در دسامبر ۲۰۱۲ رقم خورد. این مصوبه مشتمل بر ۱۲ بند، بر جمع‌آوری و پردازش اطلاعات شخصی در بخش عمومی و خصوصی اعمال می‌شد و از اطلاعات الکترونیکی که می‌تواند موجب شناسایی هویت افراد گردد و حریم خصوصی آن‌ها را نقض کند، حمایت می‌کرد.

گام بعدی تصویب «قانون مدنی جمهوری خلق چین» در ۲۸ می ۲۰۲۰ بود که از اول ژانویه ۲۰۲۱ لازم‌الاجرا شد و نقطهٔ عطف ایجاد نظام حمایت از داده‌های شخصی در این کشور است. در کنار این قانون عام، «قانون امنیت سایبری جمهوری خلق چین» (Cybersecurity Law of the People's Republic of China) لازم‌الاجرا از ژوئن ۲۰۱۷، «قانون امنیت دادهٔ جمهوری خلق چین» (Data Security Law of the People's Republic of China) لازم‌الاجرا از سپتامبر ۲۰۲۱، و «قانون حمایت از اطلاعات شخصی جمهوری خلق چین» (Personal Information Protection Law of the People's Republic of China) لازم‌الاجرا از نوامبر ۲۰۲۱، مهم‌ترین ابتکارهای قانونی این کشور در حوزهٔ حمایت از داده‌ها را تشکیل می‌دهد که

---

۱. این قانون در سال ۱۹۸۲ تصویب و در سال‌های ۱۹۸۸، ۱۹۹۳، ۱۹۹۹، ۲۰۰۴ و ۲۰۱۸ اصلاح گردیده است. قانون اساسی یک مقدمه و چهار فصل دارد (اصول کلی، حقوق و وظایف اساسی شهروندان، ساختار حاکمیت، پرچم و نشان ملی و پایتخت). برای مطالعهٔ بیشتر، ر.ک. طباطبائی، حسین (۱۴۰۰)، مطالعات حقوقی چین «از کجا آغاز کنیم؟»، چ ۱، تهران: نگاه بینه.

به همراه «استانداردهای ملی فناوری امنیت اطلاعات- مشخصات امنیت اطلاعات شخصی» (National Standard of Information security technology— Personal information security specification) مصوب سال ۲۰۱۸ و نسخهٔ جدید آن در سال ۲۰۲۰، ساختار اصلی حمایت از داده‌ها را در چین تشکیل داده‌اند.

به دلیل شهرت چین در داشتن رویکرد امنیتی و نظارت بر حریم خصوصی و اعمال سانسور و محدودیت در دسترسی آزاد به اطلاعات، اغلب فرض می‌شود که حمایت از داده‌ها در چین جنبهٔ نمایشی دارد و تلقی ابتدایی از موضع این کشور در حمایت از داده‌های شخصی همواره توأم با هراس، بدبینی و تردید بوده است. هرچند غلبهٔ این تفکر تردیدآمیز به جهت بروز برخی رفتارهای محدودکننده از سوی چین چندان نابه‌جا نبوده است، اما واقعیت آن است که چین به‌سرعت در حال شکل‌دهی و ساختاربندی چارچوب حمایت از داده و سرمایه‌گذاری در حوزهٔ فناوری‌های نوین مانند هوش مصنوعی است و قوانینی در این زمینه تصویب کرده که در نوع خود مترقی است.

در بُعد بین‌المللی، چین هنوز خود را در قالب توافق خاصی به حمایت از داده‌های شخصی متعهد نکرده است. با وجود همکاری‌های نزدیک با سازمان همکاری اقتصادی و توسعه (Organization for Economic Co-operation and Development (OECD))، هنوز «رهنمودهای حمایت از حریم خصوصی و جریان فرامرزی داده‌های شخصی» (Guidelines on the Protection of Privacy and Trans border Flows of Personal Data) این سازمان را امضا نکرده است، یا با اینکه نام چین در فهرست اسامی کشورهایی که شورای اروپا کنوانسیون حمایت از افراد در برابر پردازش خودکار داده‌های شخصی (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of Council of Europe) را برای امضا و تصویب ارسال نموده، دیده می‌شود، اما این کنوانسیون را نیز امضا نکرده است (De Hert & Papakonstantinou, 2015 :16).

به‌نظر می‌رسد که چین در فرایند تدوین اصول و قواعد ناظر بر داده‌های شخصی، ابتدا همسو با مدل امریکایی گام برداشته (وضع مقررات بخشی) و سپس با تصویب قانون امنیت سایبر و تدوین قانون حمایت از اطلاعات شخصی، به پیروی از مدل اروپایی به سمت تصویب قانون جامع حمایت از داده‌ها حرکت کرده است. اما ازآنجا که در راستای تقویت حمایت از داده‌های شخصی رویکردی سخت‌گیرانه درپیش گرفته و اولویت را بر نظارت اجتماعی- سیاسی و تمرکز بر منفعت عمومی و امنیت ملی داده است، می‌توان نظام حمایت از داده‌ها در چین را مدل ویژهٔ این کشور در حمایت از داده‌های شخصی دانست و در خصوص أخذ رویکردی مشابه در ایران تأمل کرد.

در این مقاله، تلاش‌های چین برای پذیرش الگوی مناسب در حمایت از داده‌های شخصی و الگوی نهایی این کشور در حمایت از داده‌ها تبیین و تحلیل می‌شود. ازآنجا که ایران نیز در ابتدای مسیر انتخاب الگوی حمایت از داده‌های شخصی است، آشنایی با نظام حمایت از داده‌ها

در چین، در مقایسه با الگوی امریکا و اروپا، می‌تواند برای سیاست‌گذاران و قانون‌گـذاران کشـور ما نکات قابل استفاده‌ای داشته باشد. به این منظور، نخست، الگوبرداری چین از مدل حمایت از داده‌ها در امریکا، سپس الگوبرداری چین از مدل حمایت از داده‌ها در اتحادیهٔ اروپـا و سـرانجام، مدل خاصی که چین در مورد حمایت از داده‌ها اختیار کرده است مطالعه مـی‌شـود و دسـتاورد آن برای نظام حقوقی ایران بیان می‌گردد.

۱. الگوبرداری از مدل حمایت از داده‌ها در امریکا

چین در ابتدای فرایند حمایت از داده‌ها، با الگـوبرداری از امریکـا، چـارچوب قـانونی حمایـت از داده‌ها را در بخش‌های خاص در قالب مقررات پراکنده و همراه با نظام نظارتی متکثر پـی‌ریـزی کرد که اهم ویژگی‌های این دوره در ادامه توضیح داده می‌شود.

۱. ۱. تصویب قوانین و مقررات بخشی

تمایل اولیهٔ چین به وضع مقررات گوناگون در بخش‌های مختلف مانند حوزه‌های مالی، سلامت، خدمات پستی و حمایت از مصرف‌کنندگان از مدل امریکایی متأثر است. باتوجه به نوع صنعت و نوع اطلاعات، در بخش‌های مختلف بانکی، بیمه، پزشکی، اطلاعات کارت‌های اعتباری و ارتباطات از راه دور، مقرراتی به‌طور پراکنده در چین وضع گردیده که بر حمایت از داده‌ها تأثیرگذار بـوده است. اهم این مقررات عبارت‌اند از: مقررات برای تنظیم بازار خدمات اطلاعات اینترنتـی ۲۰۱۲ (Provisions on Regulating the Market Order of Internet Information Services)، مقررات اداری صـنعت بررسـی اعتبـار ۲۰۱۳ (Regulation on the Administration of Credit Investigation Industry)، مقررات حمایت از اطلاعات شخصی کاربران اینترنت و ارتباطات از راه دور ۲۰۱۳ (Provisions on Protecting the Personal Information of Telecommunications and Internet User)، تدابیر اداری برای اطلاعات سلامت ۲۰۱۴ (Administrative Measures for Population Health Information)، مقررات مربوط به مدیریت سوابق پزشکی در مؤسسات پزشـکی ۲۰۱۴ (Regulation on medical records management in medical institutions)، مقررات مربوط به خدمات اطلاعاتی برنامه‌های اینترنتـی موبایـل ۲۰۱۶ (The administrative applications information services provisions on mobile Internet)، مقـررات مربـوط بـه خدمات جست‌وجوی اطلاعات اینترنت ۲۰۱۶ (The administrative provisions on Internet information search services)، تصمیم راجع به حذف دسته‌ای از الزامات تأییدی اداری ۲۰۱۷ (Decision on removing a batch of administrative approval requirements) و درنهایـت تدابیر اجرایی بانک خلق چین به‌منظور حمایت از حقوق و منافع مالی مصرف‌کنندگان در سـال

Implementing Measures of the People's Bank of China for the Protection of) ۲۰۲۰ .(Financial Consumers' Rights and Interests

۱. ۲. نظام نظارتی متکثر

در چین، وفق قانون امنیت سایبر، «ادارهٔ فضای سایبر چین» (Cyberspace Administration) وظیفهٔ برنامه‌ریزی و هماهنگی فعالیت‌های نظارتی و اداری در حوزهٔ فضای سایبر را برعهده دارد. در حوزه‌های مختلف نیز مراجع نظارتی متعددی پیش‌بینی شده‌اند. برای مثال، «وزارت صنعت و فناوری اطلاعات» (Ministry of Industry and Information Technology) وظیفهٔ نظارت و ادارهٔ اطلاعات شخصی در بخش مخابرات و اینترنت را برعهده دارد و «وزارت امنیت عمومی» (Ministry of Public Security) می‌تواند ضمانت اجرای اداری را مقرر کند و تحقیقات کیفری علیه تحصیل، فروش یا افشای غیرقانونی اطلاعات شخصی را انجام دهد. همچنین، مطابق قانون حمایت از حقوق و منافع مصرف‌کنندگان (Law on Protection of the Rights and Interests of Consumers) وظیفهٔ نظارت و ادارهٔ اطلاعات شخصی مصرف‌کنندگان برعهدهٔ «ادارهٔ دولتی تنظیم بازار» (State Administration for Market Regulation) قرار گرفته است[1].

در وضعی مشابه، در نظام حقوقی امریکا، «کمیسیون تجارت فدرال» (Federal Trade Commission) مهم‌ترین مرجع نظارتی در سطح فدرال است. در کنار کمیسیون تجارت فدرال، در حوزه‌های مختلف مراجع نظارتی متعددی وجود دارد؛ برای مثال، «کمیسیون سلامت و خدمات انسانی» (Health and Human Services commission) برای قوانین مربوط به بهداشت و سلامت، و «کمیسیون ارتباطات فدرال» (Federal Communications Commission) برای قوانین مربوط به ارتباطات. بنابراین، در نظام حقوقی امریکا در سطح فدرال مرجع نظارتی واحدی پیش‌بینی نشده است و نظارت از سوی یک مقام مستقل حمایت از داده‌ها صورت نمی‌گیرد. چین نیز یک مقام ناظر مستقل پیش‌بینی نکرده و همانند مدل امریکایی از نظام نظارتی متکثر برخوردار است و مقام‌های متعددی عهده‌دار اجرای مقررات حمایت از داده‌ها در بخش‌های مختص به خود شده‌اند.

۲. الگوبرداری از مدل حمایت از داده‌ها در اتحادیهٔ اروپا

چین همسو با کشورهای زیادی که مدل اروپایی حمایت از داده‌ها را برگزیده‌اند، با تصویب قانون امنیت سایبر در سال ۲۰۱۶ و به‌دنبال آن، اصلاح استاندارد ملی فناوری امنیت اطلاعات،

1. Ning, susan & hen wu, "data protection 2020- A practical cross-border insight into data protection law", 2020, available at: < https://iclg.com/practice-areas/data-protection-laws-and-regulations/china>.

گنجاندن مقررات حمایت از اطلاعات شخصی در قانون مدنی، تصویب قانون امنیت داده و قانون حمایت از اطلاعات شخصی در سال ۲۰۲۱، جهت‌گیری خود را به سمت وضع قواعد سخت‌گیرانه، دقیق و جامع همانند مقررات عمومی اتحادیهٔ اروپا راجع به حمایت از داده‌های شخصی تغییر داده است.

۲. ۱. به سمت تصویب قانون جامع حمایت از داده‌های شخصی

گنجاندن مقرراتی در مورد حمایت از اطلاعات شخصی در قانون مدنی و سپس تصویب قانون حمایت از اطلاعات شخصی، نشانگر تمایل چین به ایجاد یک نظام جامع حمایت از داده‌هاست. قانون مدنی جمهوری خلق چین در فصل ششم از کتاب چهارم راجع به «حقوق شخصیت» (Personality Rights)، با شناسایی «حق حریم خصوصی و حمایت از اطلاعات شخصی» پایهٔ حمایت از داده‌های شخصی در نظام حقوقی چین را بنیان نهاده است. به لحاظ تاریخی، حق حریم خصوصی در ذیل حقوق شخصیت تعریف نمی‌شد. قانون مدنی برای نخستین بار در مادهٔ ۱۰۳۲ حریم خصوصی را تعریف کرد[۱]. مادهٔ ۱۰۳۳ نیز اصل ممنوعیت پردازش اطلاعات شخصی مگر با رضایت صریح یا در موارد مصرح قانونی را بیان کرد. همچنین، اطلاعات شخصی اشخاص حقیقی، در مادهٔ ۱۰۳۴ تعریف و مشمول حمایت این قانون قلمداد شد، مادهٔ ۱۰۳۵ به تعریف پردازش و اصول آن، مادهٔ ۱۰۳۶ به مبانی قانونی پردازش، مادهٔ ۱۰۳۷ به حقوق اشخاص، و مادهٔ ۱۰۳۸ به وظایف و تعهدات پردازشگر پرداختند. در پایان این مواد نیز مادهٔ ۱۰۳۹ سازمان‌های دولتی و کارکنان آنها را به حفظ محرمانگی اطلاعات شخصی در زمان انجام وظایف ملزم کرد[۲].

---

۱. مادهٔ ۱۰۳۲ قانون مدنی: «حریم خصوصی، زندگی شخصی شخص حقیقی است که نباید مورد مزاحمت قرار گیرد (مختل شود) یا فضای خصوصی، فعالیت‌های خصوصی و اطلاعات خصوصی که فردی تمایلی ندارد دیگران از آن اطلاع پیدا کنند».

۲. جدا از فصل حمایت از اطلاعات شخصی، در برخی مواد قانون مدنی به‌طور پراکنده مقررات مرتبط با حمایت از داده به‌چشم می‌خورد: مادهٔ ۱۱۱ ذیل فصل پنجم (حقوق مدنی) از کتاب اول (مقررات عمومی) اطلاعات شخصی اشخاص حقیقی را تحت حمایت این قانون می‌داند (عبارتی که عیناً در مادهٔ ۱۰۳۴ تکرار و تأکید شده است)، در ادامه مقرر می‌دارد که «هر سازمان یا فردی که نیاز به دسترسی به اطلاعات شخصی دیگران دارد، باید در تطابق با قانون عمل کرده، امنیت این اطلاعات را تضمین کند، نباید به‌طور غیرقانونی اطلاعات شخصی را جمع‌آوری، استفاده یا پردازش کند، انتقال دهد، فراهم آورد، به اطلاع عموم رساند یا با آن تجارت کند».
قانون مدنی مقرراتی برای حمایت از اطلاعات شخصی در بخش‌های خاص مانند آژانس‌های گزارش اعتباری (مادهٔ ۱۰۳۰) و مؤسسات پزشکی (مادهٔ ۱۲۲۶) نیز وضع کرده است: مادهٔ ۱۰۳۰ در کتاب چهارم (حقوق شخصیت)، پیش از ورود به فصل حمایت از اطلاعات شخصی، تأکید می‌کند که «مقررات این کتاب در مورد حمایت از اطلاعات شخصی و مقررات مرتبط با آن در سایر قوانین، و مقررات اداری، در ارتباط میان اشخاص

بنابراین، در رویکرد جدید قانون مدنی، حق فردی حمایت از اطلاعات شخصی به‌عنوان یک حق مدنی مستقل و اساسی در چین پذیرفته شده است (Yang Gao, 2020: 185).

پیش از قانون مدنی، قانون امنیت سایبر نیز به‌عنوان یک قانون خاص، ملاحظات امنیتی مربوط به پردازش داده‌های شخصی را مورد توجه قرار داده بود و از این لحاظ، نقطهٔ عطفی در چشم‌انداز حمایت از داده‌ها در چین به‌حساب می‌آید. ویژگی مهم این قانون، تنظیم الزاماتی برای محلی‌سازی داده‌هاست. مطابق این قانون، اطلاعات شخصی و «داده‌های مهمِ» جمع‌آوری یا تولیدشده از سوی اپراتورها در چین باید در این کشور ذخیره شود. درصورتی که اپراتور شبکه بخواهد این داده‌ها را به خارج از چین منتقل کند باید ضرورت انتقال داده را اثبات نماید و ارزیابی‌های امنیتی را اعمال کند. به‌منظور تکمیل الزامات و مفاهیم معرفی‌شده در این قانون نیز «ادارهٔ استانداردسازی چین» (Standardization Administration)، استاندارد ملی فناوری اطلاعات- مشخصات امنیت اطلاعات شخصی را در ۲۹ دسامبر ۲۰۱۷ و نسخهٔ نهایی بازبینی‌شده آن را در مارس ۲۰۲۰ منتشر کرده است. این استانداردها به‌طور داوطلبانه اجرا می‌شوند و نشانگر چگونگی تفسیر مقامات از قوانین هستند و کارکردی قابل مقایسه با رهنمودهای «هیئت اروپایی حمایت از داده‌های اتحادیهٔ اروپا» (European data protection board) دارند و به تبیین و توضیح جزئیات اسناد می‌پردازند؛ هرچند قالب آنها با قالب اسناد مشابه اروپا متفاوت است؛ رهنمودهای اتحادیهٔ اروپا قالب متون توضیحی با ساختاری مشابه کتابچهٔ راهنما دارند و رهنمودهای چینی در قالب مشابه با ساختار قوانین الزام‌آور و با ویژگی شبه‌الزام‌آور (Pernot-Leplay, 2020:78). از سوی دیگر، قالب و یا ساختار رهنمودها به‌ویژه استاندارد ۲۰۲۰ به‌نوعی قابل مقایسه با مقررات اتحادیهٔ اروپا در مورد داده‌های شخصی است. هر دو سند به ۱۱ قسمت تقسیم شده‌اند و مقرراتی را حول محورهای اصلی یعنی مقررات عمومی، اصول پردازش و حقوق اشخاص موضوع داده مقرر کرده‌اند.

هم‌زمان با تصویب قانون مدنی، کمیتهٔ دائمی کنگرهٔ ملی خلق چین پیش‌نویس قانون امنیت داده را در ماه جولای ۲۰۲۰ منتشر و در ژوئن ۲۰۲۱ تصویب نمود. قانون امنیت داده نسبت به قانون امنیت سایبر دامنهٔ وسیع‌تری را- خواه به لحاظ صلاحیت سرزمینی و خواه از نظر مقررات‌گذاری در مورد انواع داده‌ها و «فعالیت‌های داده‌ای» (Data activities)- پوشش داده، در تعریف داده نیز از مفهوم داده‌های شخصی فراتر رفته و داده‌ها را براساس میزان اهمیت آن در توسعهٔ اقتصادی، امنیت ملی و منافع عمومی طبقه‌بندی کرده است. همچنین،

حقوق مدنی و پردازشگران اطلاعات اعتباری مانند آژانس گزارش اعتباری اعمال می‌شود». مادهٔ ۱۲۲۶ نیز مؤسسات پزشکی و کارکنان آنها را ملزم به حفظ محرمانگی اطلاعات شخصی بیماران کرده و هرگونه افشای این اطلاعات را مستوجب مسئولیت مدنی دانسته است.

اقدام متقابل در برابر هرگونه مقررات‌گذاری تبعیض‌آمیز علیه چین در حوزهٔ داده‌ها را مجاز شناخته، مقرر می‌دارد که اگر دولت خارجی در سرمایه‌گذاری‌ها و تجارت‌های مرتبط با داده یا فناوری‌های داده‌محور اقدام تبعیض‌آمیزی علیه این کشور به‌کار برد، چین می‌تواند در این خصوص اقدام متقابل صورت دهد (Pernot-Leplay, 2020: 78).

در نهایت، چین با تصویب قانون حمایت از اطلاعات شخصی درصدد برآمده است تا الزامات موجود در قوانین و مقررات پراکنده راجع به حمایت از داده‌ها را ادغام و ذیل یک قانون یکپارچه تدوین کند. در تصویب این قانون، ضمن توجه به موضوعات مطرح‌شده در نتیجهٔ فناوری‌های نو و الگوبرداری از مقررات اتحادیهٔ اروپا در مورد داده‌های شخصی، سیاست‌ها و ارزش‌های چین مورد توجه قرار گرفته است. این قانون که با هدف حمایت از حقوق و منافع افراد، تنظیم فعالیت‌های پردازش اطلاعات شخصی، حمایت از جریان قانونی داده‌ها و تسهیل استفادهٔ معقول از اطلاعات شخصی تدوین شده است، مشتمل بر ۸ فصل و ۷۴ ماده و دربردارندهٔ عناوینی چون «اصول عمومی، قواعد پردازش اطلاعات شخصی، قواعد انتقال فرامرزی اطلاعات شخصی، حقوق شخص موضوع داده، تعهدات نهادهای پردازشگر، مقام مسئول حمایت از داده، مسئولیت قانونی و مقررات تکمیلی» است. دامنهٔ شمول وسیع‌تر، وضوح بیشتر در طبقه‌بندی نقش‌ها، مبانی قانونی بیشتر برای پردازش در کنار اصل رضایت، الزامات بیشتر در مورد داده‌های مکانی، قواعد روشن‌تر برای انتقال فرامرزی، حقوق قوی‌تر برای اشخاص موضوع داده، پیش‌بینی مقامی برای تضمین رعایت الزامات قانونی حمایت از داده‌های شخصی در شرکت‌ها (مقامی مشابه با مأمور حمایت از داده‌ها (Data protection officer) در مقررات حمایت از داده‌های شخصی در اتحادیهٔ اروپا) و شناسایی حق بر حریم خصوصی پس از مرگ، تعهدات حمایتی و مسئولیت قانونی سنگین‌تر، ازجمله ابتکارات این سند نسبت به قوانین و مقررات پیش از آن است.

بنابراین، می‌توان گفت که قانون مدنی به‌عنوان قانونی عام، پایهٔ اصلی و کلیات حمایت از داده‌های شخصی را پی‌ریزی کرده و قانون حمایت از اطلاعات شخصی به‌عنوان قانون خاص، آنچه را که در قانون مدنی آمده، بسط و گسترش داده است. این دو قانون با یکدیگر هم‌پوشانی داشته، تعارضی در تعاریف، اصول و حقوق مرتبط با داده‌های شخصی در آنها دیده نمی‌شود.

۲. ۲. نکات برجستهٔ قوانین و مقررات چین و مقایسهٔ آنها با مقررات اتحادیهٔ اروپا

قوانین و مقررات چین در مورد داده‌های شخصی را می‌توان بر اساس معیارهای زیر تحلیل و با مقررات مشابه اتحادیهٔ اروپا مقایسه کرد:

۲. ۲. ۱. دامنهٔ شمول

چین در قانون امنیت داده‌ها، قواعدی با آثار فراسرزمینی وضع کرده است که به‌موجب آن، سازمان‌ها و افراد خارج از چین که فعالیت‌های داده‌محور آنها به امنیت ملی، منافع عمومی یا حقوقی شهروندان چین آسیب می‌رساند، مشمول این قانون خواهند بود. قانون حمایت از اطلاعات شخصی هم مقرر داشته است که بر فعل پردازش داده‌های شخصیِ افراد (فارغ از ملیت فرد) که در چین صورت گیرد، اعمال می‌شود. همچنین بر مواردی که هدف از فعالیت‌های پردازشی (ولو فعل پردازش در چین صورت نگیرد)، فراهم آوردن محصولات و خدمات برای افراد در چین باشد یا این فعالیت‌ها با هدف تجزیه و تحلیل و ارزیابی رفتار فرد در چین صورت گیرد اعمال می‌گردد. پردازشگرانِ مستقر در خارج از کشور اما تحت حاکمیت این قانون، موظف‌اند که یک نهاد یا نمایندهٔ مسئول حمایت از اطلاعات شخصی در چین تعیین کرده، اطلاعات مرتبط را در ادارهٔ دولتی مربوط ثبت کنند. این معیار به طرز قابل‌توجهی مشابه قلمرو سرزمینی مادهٔ ۳ مقررات اتحادیهٔ اروپا در مورد داده‌های شخصی است. این احکام، نشانگر تمایل چین به اعمال قانون خود بر کلیهٔ اشخاصی است که به ارائهٔ خدمت یا کالا در بازار چین اشتغال دارند و یا رفتار افراد در چین را تجزیه و تحلیل و ارزیابی می‌کنند.

برابر مادهٔ ۱۱۱ قانون مدنی و مادهٔ ۲ قانون حمایت از اطلاعات شخصی، اطلاعات شخصی اشخاص «حقیقی» مورد حمایت است و هیچ سازمان یا فردی مجاز به نقض حقوق اطلاعات شخصی اشخاص حقیقی نیست. مادهٔ ۱۰۳۲ قانون مدنی نیز اشخاص «حقیقی» را مشمول حمایت حریم خصوصی و اطلاعات شخصی دانسته است.

۲. ۲. ۲. تعریف مفاهیم و اصطلاحات کلیدی

در این قوانین، مفاهیم و اصطلاحات کلیدی ازجمله اطلاعات شخصی، کنترلگر و پردازشگر، پردازش و نیز رضایت به شرح زیر تعریف شده‌اند:

قانون مدنی در مادهٔ ۱۰۳۴ «اطلاعات شخصی» را به این صورت تعریف کرده است: «اطلاعات ثبت‌شده به صورت الکترونیکی یا به‌طرق دیگر که می‌تواند به تنهایی یا همراه با سایر اطلاعات برای شناسایی شخص حقیقی به‌کار رود. مانند نام، تاریخ تولد، شمارهٔ شناسایی، اطلاعات بیومتریک، محل اقامت، شمارهٔ تلفن، ایمیل، اطلاعات سلامت و مانند آن». قانون حمایت از اطلاعات شخصی در مادهٔ ۴ تعریفی نزدیک به تعریف بند ۱ مادهٔ ۴ مقررات اتحادیهٔ اروپا در مورد داده‌های شخصی ارائه کرده است: «انواع گوناگون اطلاعات ثبت‌شده به صورت الکترونیکی یا به طرق دیگر و مرتبط با شخص حقیقی شناسایی شده یا قابل شناسایی است». در واقع، میان تعریف اطلاعات شخصی در چین با تعریف داده‌های شخصی در مقررات اتحادیه

هم‌پوشانی زیادی وجود دارد و «قابلیت شناسایی» شخص موضوع داده، محوریت مرکزی را در هر دو تعریف به خود اختصاص داده است. توضیح دیگر آنکه مادهٔ ۳۰۱ و ضمیمهٔ A استاندارد ۲۰۲۰، در جزئیات از مقررات اتحادیه فراتر رفته و مثال‌های بسیاری را برشمرده است.

قانون مدنی نامی از اطلاعات شخصی حساس نبرده است، اما این اصطلاح در مادهٔ ۲۹ قانون حمایت از اطلاعات شخصی به «اطلاعات شخصی که افشاء یا استفاده غیرقانونی از آن می‌تواند منجر به برخورد تبعیض‌آمیز یا آسیب جدی به امنیت شخصی یا مالی شود، ازجمله نژاد، قومیت، عقاید مذهبی، بیومتریک شخصی، اطلاعات سلامت پزشکی، حساب‌های مالی و محل زندگی شخصی» تعریف شده است. این تعریف به لحاظ مفهومی همسو با تعریف مقررات اتحادیهٔ اروپا از داده‌های شخصی حساس قرار نمی‌گیرد، چراکه تمرکز مقررات اتحادیهٔ اروپا بر طبقه‌بندی داده‌هاست[1] و نه میزان آسیبی که وارد می‌شود. در واقع، چین «رویکرد مبتنی بر ریسک» را برگزیده و فارغ از طبقه‌بندی انواع داده، هرگونه اطلاعاتی را که آسیب به آن، آسیب به شخص یا مال تلقی شود در زمرهٔ اطلاعات شخصی حساس می‌داند[2].

قانون مدنی در پردازش اطلاعات شخصی از اصطلاح «پردازشگر» استفاده کرده، اما تعریفی از پردازشگر ارائه نداده، اصطلاح کنترلگر را به‌کار نبرده و خلاف مقررات اتحادیهٔ اروپا تمایزی میان کنترلگر و پردازشگر داده قائل نشده است. قانون حمایت از اطلاعات شخصی نیز اصطلاح کنترلگر داده را به‌کار نبرده و از اصطلاح پردازشگر استفاده کرده است. به‌عبارتی، مسئولیت‌ها و الزامات متابعتی (compliance) را به پردازشگرِ داده- که معادل کنترلگر در مقررات اتحادیه است- محول کرده است. تعهدات حمایت از اطلاعات شخصی در این سند به‌عهدهٔ فرد یا سازمانی گذاشته شده است که به‌طور مستقل، اهداف و ابزار پردازش اطلاعات شخصی را تعیین می‌کند.

شایان توجه است که استاندارد ۲۰۲۰، برخلاف این دو سند، واژهٔ پردازشگر را به‌کار نبرده است و برای شخصی که اهداف و ابزار پردازش اطلاعات شخصی را مشخص می‌کند، همچون مقررات اتحادیه، از اصطلاح کنترلگر استفاده کرده است.

مادهٔ ۱۰۳۵ قانون مدنی مفهوم گسترده‌ای از «پردازش» ارائه کرده و آن را با به‌کارگیری واژگان «جمع‌آوری، ذخیره، استفاده، پالایش، انتقال و تهیه» تعریف کرده است. درج عبارت «مانند آن» در انتهای تعریف، به معنای تمثیلی بودن موارد یادشده است. تعریف قانون حمایت از اطلاعات شخصی از «پردازش» همانند تعریف مقررات اتحادیه، اعمالی مانند جمع‌آوری، ذخیره، استفاده، پالایش، انتقال، تهیه یا افشای اطلاعات شخصی را دربر گرفته است. استاندارد ۲۰۲۰ نیز تمامی مراحل چرخهٔ پردازش را به روشی دقیق و با ذکر جزئیات بیان کرده و به این ترتیب از مقررات اتحادیه پیشی گرفته است.

---

۱. اتحادیهٔ اروپا از داده‌های حساس تحت عنوان «طبقه‌بندی خاص داده» حمایت ویژه‌ای می‌کند.

۲. شایان ذکر است که قانون امنیت سایبر از داده‌های حساس تعریف و طبقه‌بندی ارائه نکرده است.

مفهوم رضایت در مادهٔ ۱۴ قانون حمایت از اطلاعات شخصی، تقریباً مشابه مفهوم رضایت در بند ۱۱ مادهٔ ۴ مقررات اتحادیهٔ اروپا در مورد داده‌های شخصی است. البته رضایت مندرج در این بند باید توأم با فعل مثبت باشد، اما در استاندارد ۲۰۲۰، رضایت به صورت فعل مثبت و منفی نیز معتبر است. درحالی که تا پیش از قانون مدنی و قانون حمایت از اطلاعات شخصی، رضایت ضمنی معتبر قلمداد می‌شد، قانون مدنی به‌صراحت در مادهٔ ۱۰۳۳ پردازش اطلاعات شخصی را جز در موارد مصرح در قانون یا وجود رضایت صریح از سوی شخص موضوع داده، ممنوع دانسته است. قانون جدید نیز رضایت صریح را برای اطلاعات شخصی حساس الزامی دانسته و ضمیمهٔ C استاندارد ۲۰۲۰ هم به‌طور روشن و با ذکر جزئیات کامل، نحوهٔ کسب رضایت صریح را پیش‌بینی کرده است.

در خصوص پروفایلینگ (Profiling) و مستعارسازی (Pseudonymisation)، مادهٔ ۳,۸ و ۳,۱۵ استاندارد ۲۰۲۰ از عبارتی مشابه مقررات اتحادیهٔ اروپا استفاده کرده است. مادهٔ ۳,۱۴ این استاندارد نیز بی‌نام‌سازی (Anonymisation) را مانند یادآوری (Recital) شمارهٔ ۲۶ مقررات اتحادیهٔ اروپا تعریف کرده است.

۲. ۲. ۳. مبانی قانونی و اصول پردازش

قانون مدنی در مادهٔ ۱۰۳۵ به اصول پردازش پرداخته و مقرر کرده است که پردازش اطلاعات شخصی باید با اصول قانونی بودن و موجه بودن مطابق باشد و در صورت ضرورت و با أخذ رضایت از شخص حقیقی یا سرپرست او صورت گیرد.

در مورد مبانی قانونی پردازش، برخلاف قانون امنیت سایبری، قانون مدنی و قانون حمایت از اطلاعات شخصی، مبانی قانونی پردازش را محدود به رضایت ندانسته‌اند. قانون مدنی در مادهٔ ۱۰۳۶ سه مبنای قانونی را برشمرده است که به‌موجب آن مسئولیتی متوجهٔ پردازشگر نخواهد بود: ۱) پردازش معقول بوده، تا میزانی صورت گیرد که شخص حقیقی یا سرپرست او رضایت داده است؛ ۲) پردازش معقول راجع به اطلاعاتی باشد که شخص حقیقی، خود منتشر کرده یا راجع به اطلاعاتی که قبلاً به‌طور قانونی افشا شده، مگر آنکه شخص یادشده به‌صراحت مخالفت کند یا پردازش موجب ورود لطمه به نفع مهمی از او گردد؛ ۳) در پردازش معقول، تدابیر لازم برای حمایت از نفع عمومی یا حقوق و منافع قانونی شخص اتخاذ شود. اگرچه، دو مبنا یا استثنای ذکرشده در مادهٔ ۱۰۳۶ (به‌جز رضایت) پیش از این در سند استاندارد ۲۰۲۰ هم مورد اشاره قرار گرفته بود، درج آن در قانون مدنی اهمیت زیادی دارد؛ زیرا سند استاندارد برخلاف قانون مدنی از الزام قانونی برخوردار نیست. از این رو، شناسایی مبانی جدید در قانون مدنی به معنای دقت و اطمینان قانونی بیشتر برای ارزیابی فعالیت‌های پردازش است.

قانون حمایت از اطلاعات شخصی مبانی را گسترش داده، رویکردی مشابهِ مقررات اتحادیهٔ

اروپا را دنبال کرده، مقرر می‌دارد که در مواردی همچون ضروری بودن برای انعقاد یا اجرای یک قرارداد، لزوم اجرای وظایف و الزامات قانونی، پاسخ به یک رویداد اضطراری در بهداشت عمومی یا ضرورت حمایت از سلامتی و جان یا مال فرد و لزوم انتشار اخبار و نظارت افکار عمومی برای اهداف منفعت عمومی، پردازشگر می‌تواند اطلاعات شخصی را پردازش کند.

قانون حمایت از اطلاعات شخصی الزامات خاصی را برای پردازش اطلاعات شخصی جمع‌آوری‌شده در اماکن عمومی (مانند فرودگاه و ایستگاه قطار) مقرر کرده است. تصاویر یا اطلاعات شخصی قابل شناسایی جمع‌آوری‌شده به‌واسطهٔ تجهیزات گیرندهٔ تصویر و دستگاه‌های شناسایی هویت که در مکان‌های عمومی مستقر شده‌اند تنها برای اهداف حفظ امنیت عمومی می‌توانند مورد استفاده قرار گیرند و افشای داده‌های حاصل از آنها برای دیگران جز با رضایت افراد و یا الزام قانونی امکان‌پذیر نیست. بر همین اساس، چین متهم به نقض حریم خصوصی افراد با استفاده از فناوری تشخیص چهره شده است[1]. اگرچه دولت چین مدعی است جمع‌آوری تصاویر شخصی افراد در راستای حمایت از آنها و جلوگیری از کلاهبرداری است یا به‌واسطهٔ نظارت گسترده و به کمک تجهیزات تصویربرداری و پردازش توانسته است پاندمی کرونا را کنترل کند[2].

۲. ۲. ۴. حمایت از کودکان

در مورد حمایت از کودکان، قانون مدنی در مادهٔ ۱۷ خود اشخاص زیر ۱۸ سال را کودک شمرده و در مواد ۱۰۳۵ و ۱۰۳۶ رضایت سرپرست را برای پردازش داده الزامی دانسته است. مادهٔ ۱۲ پیش‌نویس تدابیر اداری و مادهٔ (۴) ۵,۴ سند استاندارد ۲۰۲۰ محدودیت سنی را به ۱۴ سال کاهش داده و مقرر داشته است که در پردازش اطلاعات شخصی اشخاص زیر ۱۴ سال باید رضایت سرپرست آنها از پیش أخذ گردد.

۲. ۲. ۵. حقوقِ شخص موضوع داده

در قوانین و مقررات چین همهٔ حقوق شناخته‌شده برای اشخاص موضوع داده شناسایی شده است؛ ازجمله: حق آگاهی، تصمیم‌گیری، اعمال محدودیت یا اعتراض به پردازش داده‌های

1. The New York Times, "Inside China's dystopian dreams: A.I., shame and lots of cameras", 2018, available at: <https://www.nytimes.com/2018/07/08/business/china-surveillancetechnology.html>.
2. DW, "Using facial recognition against COVID-19", 2020, available at: <https://www.dw.com/en/using-facial-recognition-against-covid-19/av-53868752>; Aljazeera, "Coronavirus: China uses facial recognition and infrared scanners", 2020, available at: <https://www.aljazeera.com/program/newsfeed/2020/2/24/coronavirus-china-uses-facial-recognition-and-infrared-scanners>; France 24, "Facial recognition tech fights coronavirus in Chinese city", 2021, available at: <https://www.france24.com/en/live-news/20210713-facial-recognition-tech-fights-coronavirus-in-chinese-city>.

شخصی، حق دسترسی، دریافت رونوشت، اصلاح و تکمیل اطلاعات شخصی و در شرایط خاص حق درخواست حذف، انصراف از رضایت و درخواست توضیح از پردازشگر در خصوص قواعد پردازش و حق انتقال داده‌ها.

به‌طور خاص، قانون مدنی در مادهٔ ۱۰۳۷ مقرر می‌دارد که شخص حقیقی می‌تواند اطلاعات شخصی خود را در تطابق با قانون پس بگیرد یا رونوشتی از آن دریافت کند. در صورت اطلاع از نادرست بودن اطلاعات، از حق اعتراض و درخواست اصلاح یا سایر تدابیر لازم برای اقدام به‌موقع (بدون تأخیر یا فوت وقت) برخوردار است. درصورتی که شخص حقیقی متوجه شود که پردازشگر، مقررات قانون یا مقررات اداری یا قرارداد فی‌مابین را نقض کرده است، می‌تواند از پردازشگر بخواهد که اطلاعات شخصی را بدون تأخیر حذف کند.

مادهٔ ۴۹ قانون حمایت از اطلاعات شخصی نیز به مدیریت اطلاعات شخصی متوفی و اعمال حقوق وی از سوی وراث پرداخته است. میان قوانین حمایت از داده‌های شخصی کشورها، تنها کشور فرانسه در «قانون جمهوری دیجیتال» (Loi pour une République numérique) حق حریم خصوصی پس از مرگ را به‌رسمیت شناخته است که به‌موجب آن، هر فردی پیش از مرگ می‌تواند دستورالعملی در مورد ذخیره، حذف یا افشای داده‌های شخصی تهیه کرده، آن را نزد شخص ثالث یا کمیسیون حمایت از داده‌ها (به‌عنوان نهاد رگولاتور یا مرجع نظارتی) تودیع نماید. قانون حمایت از اطلاعات شخصی با کمی تفاوت حقی مشابه را به‌رسمیت شناخته و این حق را برای وراث قائل شده است که در مورد اطلاعات شخصی متوفی (برای مثال، اعمال حق حذف یا فراموشی) تصمیم‌گیری کنند.

همچنین، مادهٔ ۲۴ این قانون، در راستای حمایت از حقوق اشخاص موضوع داده مقرر داشته است که استفاده از الگوریتم‌های رایانه‌ای برای تصمیم‌گیری خودکار مبتنی بر داده‌های افراد باید شفاف و منصفانه باشد.

۲. ۲. ۶. وظایف و تعهدات پردازشگر

قانون مدنی در مادهٔ ۱۰۳۸ وظایف پردازشگر را به این صورت برشمرده است: «پردازشگر نباید اطلاعات شخصی جمع‌آوری و ذخیره‌شده را افشاء یا دستکاری کند یا اطلاعات شخصی را بدون رضایت شخص در دسترس دیگری قرار دهد مگر این‌که اطلاعات پس از پردازش نتواند برای شناسایی فرد خاص مورد استفاده قرار گیرد یا قابل بازگشت به وضعیت اصلی نباشد. پردازشگر باید تدابیر فنی و اقدامات ضروری برای امنیت اطلاعات شخصی جمع‌آوری و ذخیره‌شده را بکار برده و از درز، دستکاری یا ازبین رفتن آن جلوگیری به عمل آورد و در صورت وقوع این موارد یا احتمال وقوع آنها باید بدون تأخیر تدابیر جبرانی را انجام دهد، شخص مرتبط را مطلع سازد و به مقامات ذیصلاح گزارش دهد». این وظایف که در تشابه با مقررات اتحادیهٔ اروپا وضع

گردیده در قانون حمایت از اطلاعات شخصی نیز پیش‌بینی شده است. وفق مواد ۸ و ۹ قانون اخیر، پردازشگر باید امنیت اطلاعات شخصی را تضمین کند. همچنین در مواد ۵۱ تا ۵۹ تعهداتی برعهدهٔ پردازشگر گذاشته شده است که ازجمله می‌توان به ایجاد رویه‌ها و فرایندهایی برای حمایت از اطلاعات شخصی، اجرایی کردن راه‌حل‌های فنی برای تضمین امنیت داده و انجام ارزیابی خطرها در برخی فعالیت‌های پردازشی اشاره کرد.

قانون حمایت از اطلاعات شخصی، برخی از شرکت‌ها (در مقام پردازشگر) را به تعیین مقام نظارتی مستقل برای تضمین تطابق پردازش اطلاعات شخصی کاربران با این قانون ملزم کرده است. این الزام برای پلتفرم‌های اینترنتی دارای کاربران زیاد و حجم وسیع اطلاعات شخصی و یا با مدل‌های فعالیت پردازشی پیچیده، پیش‌بینی شده است. همچنین این شرکت‌ها ملزم به انتشار گزارش‌ها در مورد فعالیت‌های خود در حمایت از حریم خصوصی کاربران هستند. در واقع، نهادی مشابهِ مأمور حمایت از داده‌ها در مقررات اتحادیهٔ اروپا که تعیین آن از سوی کنترلگر یا پردازشگر در شرایط خاصی مانند پردازش از سوی سازمان‌های عمومی، سازمان‌هایی با فعالیت پردازش اساسیِ مستلزم نظارت مستمر و قانونمند بر طیف وسیعی از اشخاص موضوع داده و سازمان‌هایی با فعالیت پردازش اساسی مستلزم پردازش طیف وسیعی از داده‌های شخصی حساس یا داده‌های مرتبط با محکومیت‌های کیفری الزامی است، پیش‌بینی شده است.

۲. ۲. ۷. ضمانت اجراهای قانونی

همان‌طور که پیش‌تر اشاره شد، قانون حمایت از اطلاعات شخصی در فصل ششم خود با عنوان «واحدهایی که وظیفهٔ حمایت از اطلاعات شخصی را برعهده دارند» به مقام مسئول یا یا نهاد رگولاتور یا مرجع حمایت از داده‌ها اختصاص یافته است. وظیفهٔ نظارت و مدیریت در حوزهٔ حمایت از داده‌ها برعهدهٔ ادارهٔ فضای سایبر گذاشته شده است. واحدهای مربوط در شورای دولتی نیز در حیطهٔ وظایف خود مسئولیت حمایت از اطلاعات شخصی، نظارت و مدیریت این حوزه را برعهده دارند. هر سازمان یا فردی می‌تواند هرگونه فعالیت پردازشی غیرقانونی را به این مراجع گزارش دهد. این مراجع، ملزم به رسیدگی به شکایات و گزارش‌های مرتبط بوده و باید شاکی را در مدت زمان معقول از نتیجهٔ شکایت مطلع سازند.

قانون حمایت از اطلاعات شخصی، ضمانت‌اجراهای قانونی را نسبت به ضمانت اجراهای مندرج در قانون امنیت سایبر وسعت بخشیده و علاوه بر لزوم اصلاح در موارد نقض، حسب مورد ضمانت اجرای مصادره منافع کسب‌شدهٔ غیرقانونی، تعلیق کسب و کار و لغو مجوزهای مرتبط را پیش‌بینی کرده است. طبق این قانون، عدم متابعت با الزامات حمایتی مشمول جریمه خواهد شد. برابر مادهٔ ۶۶ همین قانون، سازمانی که اطلاعات شخصی را به‌طور غیرقانونی پردازش کند یا تدابیر امنیتی ضروری برای حمایت از اطلاعات شخصی را به‌کار نگیرد، ممکن

است از سوی مراجع یادشده، به جریمهٔ نقدی تا یک میلیون یوآن محکوم شود. درصورتی که نقض جدی باشد، جریمه ممکن است تا پنجاه میلیون یوآن یا ۵ درصد از درآمد سالانهٔ سال مالی قبلی افزایش یابد.

طبق این قانون، در موارد نقض اصول و حقوق داده، پردازشگر باید تدابیر جبرانی سریع را اتخاذ کرده، مقام ذی‌صلاح و فرد متأثر از نقض را مطلع سازد. در این مورد، برخلاف مقررات اتحادیهٔ اروپا مهلت زمانی ۷۲ساعته درنظر گرفته نشده است.

۲. ۲. ۸. انتقال فرامرزی داده‌ها

رویکرد چین در انتقال فرامرزی داده‌ها کاملاً متفاوت با اتحادیهٔ اروپاست. قانون حمایت از اطلاعات شخصی مقرر می‌دارد که پردازشگر در صورت أخذ رضایت صریح از شخص موضوع داده و انجام ارزیابی خطرها، مجاز به انتقال داده‌های شخصی خواهد بود. همچنین، انتقال باید برای تحقق یکی از این الزامات باشد: ۱- اجرای تعهدات قراردادی با پردازشگر خارج از مرزها به‌گونه‌ای که الزامات مندرج در قانون را محقق کند؛ ۲- ارزیابی تأثیرات امنیتی که به تأیید ادارهٔ فضای سایبر چین رسیده باشد؛ ۳- أخذ گواهینامه حمایت از اطلاعات شخصی از نهاد صادرکننده مورد تأیید ادارهٔ فضای سایبر.

۳. مدل خاص چین در حمایت از داده

اگرچه تصویب قانون امنیت سایبری و قانون مدنی و قانون حمایت از اطلاعات شخصی نشانگر هم‌گرایی بیشتر نظام حمایت از داده‌ها در چین با قواعد اتحادیهٔ اروپاست، مدل چین نسبت به مدل اروپایی سخت‌گیری کمتری دارد. حقوق داده‌ها در چین واجد خصوصیاتی است که در اتحادیهٔ اروپا و امریکا به‌چشم نمی‌خورد. تفاوت در حمایت از داده‌های شخصی افراد در بخش خصوصی و عمومی، الزامات محلی‌سازی داده و محدودیت در انتقال داده‌ها ازجمله مواردی است که مدل خاص این کشور در حمایت از داده‌ها را برجسته می‌کند و بی‌شک بر تحولات و سیاست‌های این حوزه در اتحادیهٔ اروپا و امریکا تأثیر قابل‌توجهی خواهد گذاشت.

در این میان، توجه به ویژگی‌های خاص سیاست دولت چین در امر حاکمیت بر فضای سایبر حائز اهمیت است. این سیاست بر ترکیبی از محدودیت اینترنت، سانسور و نظارت حکومت که تا حد زیادی بر جلوگیری از گسترش مخالفت با حکومت تک‌حزبی چین و ممانعت از دسترسی شهروندان این کشور به گزارش‌های مستقل دربارهٔ کشورشان یا سایر نقاط جهان متمرکز شده است. محدودیت در اینترنت در این کشور از همان سال‌های اولیهٔ ظهور اینترنت آغاز شده است. تا پیش از آن حکومت چین سیاستِ باز و بهره‌مندی از دانش غربی برای اصلاح

نظام اقتصادی را سرلوحه کار قرار داده بود. از سال ۲۰۰۰ با معرفی «دیوار آتش بزرگ» (Great Firewall) معروف به «پروژهٔ سپر طلایی» (Golden Shield Project)، نظام سانسور و نظارت بر اینترنت از سوی دولت چین شکل گرفت. از آن زمان، چین توانسته است از طریق یکی از بزرگ‌ترین سیستم‌های فیلترینگ اینترنت در جهان، بر اقیانوس داده‌ها و اطلاعات نظارت کند. چین به‌واسطهٔ فیلترینگ و فناوری‌های نظارتی، مدل کنترل اطلاعاتی خود را از سایر مدل‌ها متمایز کرده است (Wright, 2019: 76). از نظر منتقدان، چنین رویکردی می‌تواند چشم‌انداز جریان آزاد اطلاعات در جهان را به‌خطر اندازد، ولی چین همواره اظهار داشته که اعمال محدودیت‌ها تنها برای حفظ نظم اجتماعی و حمایت از امنیت ملی این کشور است.

۳. ۱. رویکرد متفاوت در قبال بخش خصوصی و عمومی

ویژگی برجستهٔ نظام حقوق داده‌ها در چین، تقویت حمایت از داده‌ها در برابر اقدامات بخش خصوصی است. در مقابل، دسترسی دولت به داده‌های شخصی تشدید شده و حمایت مقبولی از داده‌ها در مقابل تعرض‌های حاکمیت وجود ندارد. اساساً این باور وجود دارد که حمایت از داده‌ها در چین در درجهٔ نخست برای محافظت از قدرت حاکمیت صورت می‌گیرد (Palmieri, 2019: 316). حمایت از داده‌ها نه به‌عنوان ابزاری برای تضمین حریم خصوصی افراد بلکه ابزاری برای حفاظت از امنیت ملی محسوب می‌شود (Determann, 2020: 245). از این رو، حمایت از داده‌ها در مورد بخش خصوصی تا حد بسیاری تکامل یافته، ولی انتقادات زیادی نسبت به محدودیت‌های مقرر به بهانهٔ امنیت ملی و منافع عمومی و نظارت گسترده بر افراد با استفاده از فناوری‌هایی چون شناسایی چهره مطرح است[1].

بنابراین، رویکرد چین هم با رویکرد اتحادیهٔ اروپا که حمایت از داده‌ها را به‌عنوان حقی بنیادی به‌رسمیت شناخته و در قبال بخش خصوصی و عمومی حمایت‌های مشابهی را اتخاذ نموده، متفاوت است، و هم با رویکرد امریکا که پیش از حمایت از داده‌های شخصی در برابر بخش خصوصی، حمایت از داده‌های شخصی را در مقابل دولت رقم زده است.

نکتهٔ شایان توجه دیگر این است که چین در حوزهٔ حمایت از داده‌های شخصی تمرکز خود را بر حمایت از «مصرف‌کننده» قرار داده است، نه «شخص موضوع داده»؛ به این معنا که ضمن حمایت از داده‌های شخصی افراد به‌عنوان مصرف‌کننده، منافع ملی و عمومی را مرجح بر منافع فردی می‌داند (De Hert & Papakonstantinou, 2015: 21).

1. The New York Times, "Inside China's dystopian dreams: A.I., shame and lots of cameras", 2018, available at: <https://www.nytimes.com/2018/07/08/business/china-surveillancetechnology.html>.

۳. ۲. الزامات محلی‌سازی داده و محدودیت در انتقال فرامرزی داده

باتوجه به اینکه انتقال داده‌های شخصی در حجم بالا بـه خـارج از کشـور مـی‌توانـد بـرای امنیـت اجتماعی یا ملی مخاطره‌آمیز باشد، در کشورهای اروپایی، چین و روسیه و اخیراً در امریکـا، خـارج شدن انواعی از داده‌ها از کشور ممنوع شده است؛ به این معنا کـه ایـن داده‌هـا بایـد در سـرورهای محلی یا ملی ذخیره شوند (انصاری و دیگران، ۱۴۰۰: ۲۳۸). مقررات مربوط به محلی‌سازی داده‌ها که ایجاب می‌کند حداقل کپی داده‌های شخصی داخل کشور باقی بمانـد و سـایر محـدودیت‌هـای اعمال‌شده بر انتقال فرامرزی داده‌های شخصی، ابهامات زیادی دارد. چین بـه دلیـل نبـود معاهـدهٔ بین‌المللی خاص، تبادل داده‌ها را همسو با ایدئولوژی خـود تنظـیم کـرده اسـت. در برابـر، امریکـا محدودیتی برای انتقال داده‌ها به کشور ثالث درنظر نگرفته و مخالف محلی‌سازی داده‌هاسـت و آن را مانعی برای تجارت می‌شناسد. در اتحادیهٔ اروپا نیز انتقال فرامرزی داده‌ها هرچند باید بـا رعایـت شرایطی ازجمله سطح حمایت مناسب از داده‌ها در کشور ثالث یـا اسـتفاده از شـروط قـراردادی و قواعد الزام‌آور صورت گیرد، این محدودیت تأثیر جدی بر جریان آزاد داده‌ها ندارد.

در چین به‌موجب مادهٔ ۱ قانون امنیت سایبر و بر اساس اصـل حاکمیـت سـایبری (cyber-sovereignty) فضای سایبر تابع منافع و ارزش‌های کشور در درون مرزهاست؛ این امر به معنای اعمال حاکمیت دولت است بر فضای سایبری (معماری اینترنت، محتـوا و جریـان داده‌هـا) کـه اغلب با اهـداف امنیتـی صـورت مـی‌گیـرد. برابـر مـادهٔ ۳۷ قـانون امنیـت سـایبر، اپراتورهـای زیرساخت‌های اطلاعاتی مهم که داده‌های شخصـی یـا داده‌هـای مهـم را جمـع‌آوری یـا تولیـد می‌کنند، باید داده‌ها را در چین ذخیره نمایند. انتقال داده‌ها نیز تنهـا در صـورت ضـرورت و بـا انجام ارزیابی‌های امنیتی قابل انجام است (Pernot-Leplay, 2020: 103).

توجیه دولت چین از الزام به محلی‌سـازی داده‌هـا، حمایـت از حـریم خصوصـی افـراد و همچنـین توسعهٔ اقتصادی چین و جلوگیری از دردسترس قرارگـرفتن اطلاعـات بـرای سـرویس‌هـای امنیتـی در جهان است (Pernot-Leplay, 2020:106). در این مورد، چین تا حدودی موفق عمل کرده اسـت؛ بـرای مثال توانسته است شرکت امریکایی «اپل» (Apple) را به ایجاد مرکز دادهٔ محلـی در تطـابق بـا الزامـات دولت چین مجبور کند. به بیان دیگر، با تصویب قانون امنیت سایبر در سال ۲۰۱۶، چین شرکت اپـل را به ذخیرهٔ داده‌های مشتریان در سرورهای محلی داده ملـزم کـرده اسـت. در سـال ۲۰۱۷، اپـل قـرارداد تأسیس نخستین مرکز داده با این کشور را امضا و ساخت این مرکز را در سال ۲۰۱۹ آغاز نمود.

۴. دستاورد مطالعهٔ رویکرد حمایت از داده‌ها در چین برای نظام حقوقی ایران

در حقوق ایران تاکنون قانون جامعی در مورد حمایت از داده‌های شخصـی بـه‌تصـویب نرسـیده است. قانون تجارت الکترونیکی مصوب ۱۳۸۲ مهم‌ترین قانونی اسـت کـه بـر مبادلـهٔ داده‌هـای

الکترونیکی حاکم است. این قانون از یک سو، داده‌پیام شخصی را تعریف کرده و از سوی دیگر، اصول پردازش داده‌های شخصی و حقوق اشخاص موضوع داده را تعریف و ارزش اثباتی داده‌ها را پیش‌بینی کرده است. با وجود این، قانون یادشده صرفاً بر معاملات افراد در فضای مجازی حاکم است و روابط گسترده‌ای را که خارج از معاملات ازجمله در خصوص سکوهای مجازی وجود دارد، دربر نمی‌گیرد.

قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ دومین قانون مهم است که احکامی دربارهٔ جمع‌آوری و پردازش داده‌های شخصی دارد. این قانون حق دسترسی شهروندان ایرانی به اطلاعات موجود در مؤسسات عمومی و آن دسته از مؤسسات خصوصی را که خدمات عمومی ارائه می‌دهند شناسایی کرده است و در مواد ۱۴ و ۱۵ خود، اطلاعات راجع به حریم خصوصی یا اطلاعات شخصی را از شمول حق دسترسی عمومی خارج دانسته، تنها اشخاص موضوع داده اجازهٔ دسترسی به این اطلاعات را یافته‌اند. دسترسی سایر اشخاص به اطلاعات خصوصی به رضایت صریح و مکتوب از سوی شخصِ موضوع داده، منوط شده است. کمیسیون انتشار و دسترسی آزاد به اطلاعات در سال ۱۳۹۷ با تصویب «شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی» تلاش کرده است تا مفهوم و مصادیق داده‌های شخصی را به‌تفصیل روشن کند. این سند، مهم‌ترین مصادیق داده‌های شخصی مکانی، اقتصادی، آموزشی، سلامت، ارتباطی و سایر داده‌ها را برشمرده است. با وجود این، قانون یادشده نسبت به جمع‌آوری و پردازش داده‌های شخصی- چه در بخش عمومی و چه در بخش خصوصی- ساکت است و صرفاً احکام دسترسی به داده‌ها یا انتشار داده‌ها را روشن کرده است.

قانون جرایم رایانه‌ای مصوب ۱۳۸۸، ضمن شناسایی دسترسی غیرمجاز به داده‌های متعلق به دیگران، سرقت یا تخریب آن داده‌ها، از ارائه‌دهندگان خدمات ارتباطی و میزبانی اینترنت خواسته است تا داده‌های کاربران و داده‌های ترافیک آنها را تا مدت معینی ذخیره و نگهداری کنند تا در صورت نیاز، امکان مراجعه به آنها وجود داشته باشد؛ با این همه، حمایت از داده‌های شخصی، موضوع مستقیم این قانون نبوده است.

غیر از قوانین یادشده، شورای عالی فضای مجازی نیز در برخی از مصوبات خود به موضوع پردازش داده‌ها به‌طور کلی و پردازش داده‌های شخصی به‌طور خاص ورود کرده است. مصوبهٔ «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی» مصوب ۱۳۹۶، لزوم ذخیره‌سازی داده‌های کاربران ایرانی در سرورهای داخل کشور و نیز ضرورت رعایت قوانین و مقررات ایران از سوی سکوهای مجازی خارجی را پیش‌بینی کرده که به معنای الزامات محلی‌سازی داده‌ها است (همانند دولت چین). به‌موجب تبصرهٔ ۲ نخستین جزء بند ۱ این مصوبه، برای اینکه پیام‌رسان‌های اجتماعی خارجی بتوانند مجوز فعالیت دریافت کنند باید علاوه بر داشتن سایر شرایط لازم، اولاً ذخیره‌سازی و پردازش داده‌ها را در داخل کشور انجام دهند و ثانیاً در فرایند

أخذ مجوز فعالیت، همراه با ثبت اطلاعات، نمایندهٔ حقوقی تام‌الاختیار خود را نیز که باید شخصی در داخل کشور باشد به وزارت ارتباطات و فناوری اطلاعات معرفی نمایند.

مصوبهٔ «الزامات حاکم بر اینترنت اشیاء در شبکهٔ ملی اطلاعات» مصوب ۱۳۹۷ که با هدف حفظ و تقویت حاکمیت‌پذیری فضای مجازی تصویب شده است نیز به‌طور ضمنی در مقام بیان «الزامات عمومی اینترنت اشیاء» و «الزامات اختصاصی اینترنت اشیاء» از لزوم حمایت از داده‌های شخصی سخن گفته است.

سرانجام آنکه می‌توان از «سند راهبردی جمهوری اسلامی ایران در فضای مجازی» نام برد که به مدیریت کلان و تعیین سیاست‌های کلی در فضای مجازی اختصاص دارد. این سند، «صیانت از حریم خصوصی» را از ارزش‌های حاکم بر مدیریت فضای مجازی کشور دانسته است.

این مصوبات به دلیل آنکه به‌عنوان سیاست کلی یا راهبردهای جمهوری اسلامی ایران در زمینهٔ فضای مجازی تصویب شده‌اند، به‌طور مستقیم قابلیت اعمال و اجرا ندارند و هنوز در قوانین و مقررات اجرایی راهی پیدا نکرده‌اند؛ بنابراین، بخش قابل‌توجهی از آنها هنوز رعایت و محقق نشده است.

استفاده از تجربیات و نقاط قوت دستاوردهای کشورهای اروپایی و دولت چین می‌تواند در حمایت بهینه از داده‌های شخصی در کشور ما به‌کار آید و ما را در تدوین و تصویب قانون خاص و جامعی دربارهٔ داده‌های شخصی راهنمایی کند.

نتیجه

تا پیش از تصویب قانون حمایت از اطلاعات شخصی، قانون جامعی برای حمایت از داده‌ها در جمهوری خلق چین وجود نداشت. این کشور نخست با الهام از الگوی مقررات‌گذاری امریکا به وضع قوانین و مقررات‌بخشی پرداخت و مراجع نظارتی متعددی با مسئولیت‌های نسبتاً هم‌پوشان دایر کرد. تصویب قانون مدنی، قانون حمایت از اطلاعات شخصی و دیگر قوانین و مقررات مربوط به امنیت داده و استانداردها، به تغییر الگوی حمایت از داده‌های شخصی به سمت الگوی اروپایی انجامید.

با وجود مشابهت‌هایی که میان مدل حمایت از داده‌ها در چین و الگوی اروپایی وجود دارد نظام حمایت از داده‌ها در چین را می‌توان ویژه و خاص این کشور دانست که پس از طی مراحل بلوغ می‌تواند مورد استقبال کشورهای دیگر که دارای دغدغه‌ها و ارزش‌های مشابه هستند، مانند کشورهای درحال توسعه و شرکای تجاری چین، قرار گیرد. تمرکز بر امنیت و ثبات ملی، حاکمیت سایبری و تفاوت برخورد با حمایت از داده‌ها در بخش خصوصی و بخش عمومی مهم‌ترین عناصر شکل‌دهندهٔ مدل چینی هستند. مدل چینی با ویژگی‌های گاه متناقض و یا

حتی موازی، ازجمله تدوین اصول حاکمیت سایبر، هم نظارت حکومت بر پردازش داده‌های شخصی را افزایش داده است هم از داده‌های مصرف‌کنندگان در برابر تعرض‌های بخش خصوصی به نحو مناسب حمایت می‌کند. با توجه به سیاست‌های اقتصادی و سیاسی و نیز استراتژی سایبری این کشور، در آینده نه‌چندان دور تأثیرگذاری آن بر جهان اجتناب‌ناپذیر است. چنان‌که به‌رغم عملکرد با تأخیر این کشور در حمایت از داده‌های شخصی، در خصوص مقرره‌گذاری هوش مصنوعی به‌سرعت وارد عمل شده و دیدگاه‌های خود را در خصوص قواعد هوش مصنوعی در جهان مطرح، و همپای امریکا و اروپا در رقابت جهانی تنظیم‌گری هوش مصنوعی شرکت کرده است. مطمئناً رویکرد جدید این کشور بر سیاست‌گذاری‌ها و مقررات درحال تدوین برای فناوری‌های نوین اطلاعاتی مانند هوش مصنوعی در اتحادیهٔ اروپا و امریکا تأثیرات زیادی به دنبال خواهد داشت. سیاست‌گذاران و قانون‌گذاران کشور ما نیز می‌توانند از تجربیات و آورده‌های مفید چین در این حوزه استفاده کرده، نظامی مناسب برای حمایت از داده‌های شخصی در کشور فراهم آورند.

منابع و مآخذ

الف) فارسی

۱. انصاری، باقر؛ عطّار، شیما؛ صالحی، امیرحسین (۱۴۰۰)، **حقوق داده‌ها و هوش مصنوعی (مفاهیم و چالش‌ها)**، چ ۱، تهران: شرکت سهامی انتشار.

۲. طباطبائی، سید حسین (۱۴۰۰)، **مطالعات حقوقی چین «از کجا آغاز کنیم؟**، چ ۱، تهران: نگاه بینه.

ب) انگلیسی

1. Aljazeera, "Coronavirus: China uses facial recognition and infrared scanners", 2020, available at: <https://www.aljazeera.com/program/newsfeed/2020/2/24/coronavirus-china-uses-facial-recognition-and-infrared-scanners>.
2. Annoni, A. & Benczur, P.& Bertoldi, P.& Delipetrev, B.& De Prato, G.& Feijoo, C.& Fernandez Macias, E.& Gomez Gutierrez, E.& Iglesias Portela, M.& Junklewitz, H.& Lopez Cobo, M.& Martens, B.& Figueiredo Do Nascimento, S.& Nativi, S.& Polvora, A.& Sanchez Martin, J.I.& Tolan, S.& Tuomi, I. & Vesnic Alujevic, L. (2018), **Artificial Intelligence: A European Perspective**, Craglia, M. editor(s), Luxembourg: Publications Office of the European Union.
3. "China Issues Draft Data Security Law for Public Comment", 2020, available at: <https://www.lw.com/thoughtLeadership/lw-china-issues-draft-data-security-

law-for-public-comment>.
4. Civil Code of the People's Republic of China, 2020.
5. Constitution of the People's Republic of China, 2018.
6. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of Council of Europe, Strasbourg, 1981.
7. Cybersecurity Law of the People's Republic of China, 2017.
8. Daly, Angela & Hagendorff, Thilo & Hui, Li & Mann, Monique & Marda, Vidushi & Wagner, Ben & Wang, Wei & Witteborn, Saskia (2019), "Artificial Intelligence, Governance and Ethics: Global Perspectives", the Chinese University of Hong Kong Faculty of Law, Research Paper No. 2019- 15.
9. Data Security Law of the People's Republic of China, 2021.
10. De Hert, Paul ; Papakonstantinou, Vagelis (2015). The data protection regime in China, Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs Civil Liberties, Justice and Home Affairs, European parliament.
11. Deloitte, "Global artificial intelligence industry whitepaper", 2019, available at: < https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/global-ai-development-white-paper.html>.
12. Determann, Lothar (2020), "Healthy Data Protection", Michigan Technology Law Review, Vol. 26.
13. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
14. DW, "Using facial recognition against COVID-19", 2020, available at: <https://www.dw.com/en/using-facial-recognition-against-covid-19/av-53868752>.
15. European Commission, "USA- China- EU plans for AI: where do we stand?", 2018, available at: <https://ati.ec.europa.eu/reports/technology-watch/usa-china-eu-plans-ai-where-do-we-stand-0>.
16. France 24, "Facial recognition tech fights coronavirus in Chinese city", 2021, available at: <https://www.france24.com/en/live-news/20210713-facial-recognition-tech-fights-coronavirus-in-chinese-city>.
17. Geller, Anja (2020), "How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", Journal of European and International IP Law, 69(12).
18. Kewalramani, Manoj (2018), "China's Quest for AI Leadership: Prospects and Challenges", Takshashila Working Paper.
19. National Standard of Information security technology— Personal information security specification, 2020.
20. Ning, susan & hen wu, "data protection 2020- A practical cross-border insight into data protection law", 2020, available at: < https://iclg.com/practice-areas/data-protection-laws-and-regulations/china>.
21. "Number of internet users in China from December 2008 to December 2020",

2021, available at: <https://www.statista.com/statistics/265140/number-of-internet-users-in-china/>
22. Palmieri, Nicholas F. (2019), "Data Protection in an Increasingly Globalized World", Indiana law journal, vol. 94.
23. Pernot-Leplay, Emmanuel (2020), "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?", Penn State Journal of Law & International Affairs, Vol. 8, No. 1.
24. Personal Information Protection Law of the People's Republic of China, 2021.
25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
26. The New York Times, "Inside China's dystopian dreams: A.I., shame and lots of cameras", 2018, available at: <https://www.nytimes.com/2018/07/08/business/china-surveillancetechnology.html>.
27. Wright, Nicholas d. (2019), **Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global and Creative Perspectives**, independently published.
28. Yang Gao, Reymond (2020), "Personal Information Protection Under Chinese Civil Code: A Newly Established Private Right in The Digital Era", Tsinghua China Law Review, Vol. 13.
29. Zhao, Bo & Chen, Weiquan (2019), "Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Exterritorial Application in China", US-China Law Review, Vol. 16, No. 3.