وزارت علوم، تحقیقات و فناوری
مرکز تحقیقات سیاست علمی کشور

گزارش سیاستی

بررسی مقایسه‌ای قواعد حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا در نظام‌های حقوقی منتخب، و تدوین مدل مفهومی در نظام حقوقی جمهوری اسلامی ایران

مرکز تحقیقات سیاست علمی کشور

آبان ماه ۱۴۰۱


بسم الله الرحمن الرحيم

گزارش سیاستی

بررسی مقایسه‌ای قواعد حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا در نظام‌های حقوقی منتخب، و تدوین مدل مفهومی در نظام حقوقی جمهوری اسلامی ایران

تهیه‌کننده:

بهنار احمدوند (عضو هیأت‌علمی مرکز تحقیقات سیاست علمی کشور)

نشانی: میدان ونک، خیابان ملاصدرا، خیابان شیراز جنوبی، خیابان دکتر قانعی‌راد، شماره ۹

وبگاه: www.nrisp.ac.ir

تلفن: ۸۸۰۳۶۱۴۴

فهرست مطالب

خلاصه مدیریتی..... ۱
۱-مقدمه..... ٤
۲- الگوهای حاکم بر حمایت از حریم خصوصی و حفاظت از داده شخصی در اینترنت اشیا در پرتو مطالعات تطبیقی..... ۹
۲-۱- اتحادیه اروپا..... ۱۰
۲-۲- ایالات متحده امریکا..... ۱۲
۲-۳- جمهوری خلق چین..... ۱٤
۳- الگوی مطلوب حمایت از حریم خصوصی و حفاظت از داده شخصی در نظام حقوقی ایران..... ۱٦
٤- نتیجه‌گیری و پیشنهاد..... ۲۵
منابع..... ۲۷

فهرست جداول

جدول ۱. چالش‌های اینترنت اشیا و راهکارهای برون‌رفت از آن.....۷

جدول ۲. قواعد حاکم بر حمایت از حریم خصوصی و حفاظت از داده شخصی در مقررات اتحادیه و شورای اروپا.....۱۱

جدول ۳. قواعد حمایت از حریم خصوصی و حفاظت از داده شخصی در نظام حقوقی ایالات متحده امریکا...۱۳

جدول ٤. قواعد حمایت از حریم خصوصی و حفاظت از داده شخصی در نظام حقوقی چین.....۱٦

خلاصه مدیریتی

اینترنت اشیا به عنوان نسل جدید اتصال و ارتباط اشیای هوشمند از طریق اینترنت مفهومی است که به تازگی وارد ادبیات حکمرانی کشور شده است. لازمه دستیابی به کاربرد کامل این نسل از فناوری جمع‌آوری جزئی‌ترین اطلاعات با سرعت و وسعت گسترده و تجزیه و تحلیل آن‌ها می‌باشد. با توجه به امکان شناسایی هویت و دسترسی به اطلاعات مربوط به زندگی خصوصی افراد از طریق تحلیل و ترکیب داده‌های جمع‌آوری شده، حفاظت مؤثر از حریم خصوصی و داده‌های شخصی به عنوان یک امر بایسته مطرح شده است. نظام حقوقی ایران به علت نوپا بودن کشور در این حوزه فاقد قانونی می‌باشد که به حمایت از حریم خصوصی و حفاظت از داده‌های شخصی شهروندان در این مقوله اختصاص داشته باشد. با توجه به اهمیت موضوع، تدوین قانون یا قوانینی برای موضوع اشاره شده از نیازهای ضروری این حوزه قلمداد می‌گردد. بر اساس آموزه‌های حقوق تطبیقی برای برون‌رفت از چالش‌های مشابه می‌توان از تجارب دیگر نظام‌ها سود برد.

پژوهش حاضر بر اساس روش تحلیلی- توصیفی به دنبال یافتن الگوهای موجود برای حمایت از حریم خصوصی و حفاظت از داده شخصی در اینترنت اشیا در نظام‌های حقوقی منتخب می‌باشد و از این طریق سعی دارد به این سؤال پاسخ دهد که کدام نوع الگوی قانون‌گذاری، برای کشور مطلوب می‌باشد.

در نظام‌های حقوقی بررسی شده سه رویکرد وجود دارد: رویکرد اول، رویکرد حق محوردر سطح اتحادیه اروپاست که به قانونگذاری جامع در این خصوص پرداخته است. هم قواعدی عام در مورد حمایت از داده‌های شخصی وجود دارد و هم قواعد خاص برای حمایت از حوزه‌های خاص اطلاعات شخصی یا حمایت در برابر فناوری‌های اطلاعاتی خاص. کنوانسیون حمایت از افراد در برابر پردازش خودکار داده‌های شخصی مصوب شورای اروپا در سال ۱۹۸۱ که در سال ۲۰۱۸ نیز تکمیل و روزآمد شده است، مقررات عمومی حمایت از اشخاص حقیقی در برابر پردازش داده‌های شخصی و جریان آزاد این داده‌ها مصوب اتحادیه اروپا در سال ۲۰۱۶ دو سند مادر هستند. افزون بر آن‌ها مصوبات متعددی درباره حمایت از حریم خصوصی و داده‌های شخصی نیز وجود دارد که می‌توان به دستورالعمل حریم خصوصی و ارتباطات الکترونیک مصوب۲۰۰۲، دستورالعمل حمایت از داده برای پلیس و مقامات دادرسی کیفری مصوب ۲۰۱۶ و مقررات حمایت از اشخاص حقیقی در برابر پردازش داده‌های شخصی توسط نهادها، مؤسسات، دفاتر و آژانس‌های اتحادیه و جریان آزاد این داده‌ها مصوب ۲۰۱۸ اشاره نمود.

رویکرد دوم، رویکرد امریکایی (رویکرد تجارت محور)است که به رویکرد حقوق و اقتصاد موسوم است و از بازار داده‌های شخصی دفاع می‌کند؛ در این کشور، از داده‌های شخصی به عنوان کالاهای قابل عرضه در بازار توسط شرکت‌ها و کارگزاری‌های داده دفاع می‌شود و به افراد اجازه داده می‌شود درباره انتقال و واگذاری داده‌های شخصی خود در قبال دریافت پول یا عوض دیگر تصمیم بگیرند. بنابراین به خلاف نظام اروپایی، از اطلاعات اشخاص تنها در حوزه‌های خاصی که احتمال سوء استفاده علیه آنها وجود دارد حمایت می‌کند. در نظام حقوقی امریکا به خلاف کشورهای اروپایی، حمایت عام و جامعی از داده‌های شخصی وجود ندارد. تنها مقررات سختگیرانه ای در خصوص حفاظت از داده های آنلاین کودکان و داده‌های مربوط به سلامت و بهداشت عمومی وجود دارد. افزون بر این، تنظیم-گری خصوصی یعنی استفاده از فنون و روش‌ها و رویه‌هایی از سوی بخش خصوصی، در حمایت از حریم خصوصی اشخاص نقش مهمی دارند و دخالت دولت برای تنظیم‌گری در این زمینه را غیرضروری ساخته‌اند. استفاده از فنون «حریم خصوصی تفارقی» از روش‌های مهمی است که توسط گوگل و اپل استفاده می‌شود.

رویکرد سوم، رویکرد چین(امنیت محور) استکه به جهت تاخر زمانی در زمینه وضع قواعد و سیاست‌ها درباره داده‌های شخصی، ترکیبی از قواعد اروپایی و امریکایی در زمینه حمایت از داده‌های شخصی را با توجه به ملاحظات امنیتی خود به کار برده‌اند. مبنای این رویکرد آن است که دولت در حمایت از داده‌های شخصی باید حاکمیت داشته باشد و وابستگی به نظام فناوری اطلاعات امریکا، آن‌ها را در معرض آسیب‌پذیری قرار می‌دهد. از این رو، در وهله نخست، بین جمع‌آوری و پردازش داده‌های شخصی در داخل و خارج از کشور تفکیک قایل شده‌اند. در داخل کشور نیز بین دو دسته ملاحظات تمایز قایل شده‌اند: ملاحظات تجاری موجود میان کنترل‌گرها و پردازشگرها و اشخاص موضوع داده و ملاحظات امنیتی و حاکمیتی موجود میان دولت، کنترل‌گرها و پردازشگرها. بر اساس این ملاحظات، رعایت برخی از اصول ناظربر پردازش داده‌های شخصی (در اروپا) را از سوی کنترل‌گرها در مورد اشخاص و موضوع داده الزامی کرده‌اند و در عین حال، ملزم به رعایت الزامات حکومتی دانسته و ارائه کلیه داده‌های مورد نیاز را در سریع‌ترین شکل ممکن به مراجع دولتی، الزامی شناخته است. این الزام به‌ویژه برای سرمایه‌گذاران خارجی و شرکت‌های فعال در چین همواره منشأ نگرانی و تنش با دولت چین بوده است.

در تدوین مدل مفهومی ایران، تلفیقی از رویکردهای سه‌گانه با ابتنای اصلی بر نظام اتحادیه اروپایی پیشنهاد می‌شود. استفاده از رویکرد خود تنظیم‌گری امریکایی در شرکت‌ها، استفاده از ماده واحدهای جهت شمولیت احکام مواد قوانین مرتبط به داده در حوزه اینترنت اشیا نظیر مدل اروپایی، اقتباس از مدل امریکایی نسبت به حساسیت در مورد حفاظت از داده‌های مربوط به حوزه سلامت و بهداشت عمومی و کودکان و اقتباس از مدل چین در طبقه بندی اطلاعات و عدم تجربه سیستم قانون‌گذاری تفرقی پیشنهاد شده است.

۱- مقدمه

از مؤلفه‌های مُعرِّف دهه‌های اخیر که از آن تحت عنوان انقلاب صنعتی چهارم[1] یاد می‌شود می‌توان به رشد و گسترش تحولات و پیشرفت‌ها در حوزه فناوری اطلاعات و ارتباطات، اینترنت و اتوماسیون هوشمند اشاره کرد. اینترنت اشیا[2] معماری نوظهور جهانی مبتنی بر اینترنت است که هدف آن اتصال و تسهیل ارتباط و تعامل بین اشیای متصل به اینترنت و ارائه خدمات آنی به مصرف‌کنندگان به شیوه‌ای کاربردی و قابل اعتماد است. به عبارت دیگر اینترنت اشیا به ارتباط سنسورها و دستگاه‌ها و تجهیزات به شبکه‌ای که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند و خدماتی ارائه دهند اطلاق می‌گردد؛ این مفهوم می‌تواند به سادگی ارتباط یک گوشی هوشمند با تلویزیون، یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد (Haller et.al, 2008, p. 5). رشد سریع فناوری‌های نوین و مبتنی بر اینترنت که مؤلفه‌های اصلی آن استفاده از سخت افزارهای در مقیاس کوچک و رایانش است تأثیرات گسترده‌ای برای زندگی انسان‌ها به همراه داشته است. به عنوان مثال پیشرفت‌های موجود در فن‌آوری ارتباطات (از جمله دیجیتالی شدن ارتباط از راه دور، بهبود فناوری فیبر نوری، فناوری‌های بی‌سیم و غیره) منجر شده است حجم عظیمی از داده‌ها با سرعت بیشتری منتقل شوند. همچنین تولید تجهیزات و حسگرهای پیشرفته با توانایی جمع‌آوری جزئی‌ترین اطلاعات از محیط پیرامون افراد از جمله اطلاعات جغرافیایی، تصاویر زنده، اصوات و حتی تشخیص رفتار عاطفی و پدیده‌های فیزیولوژیکی مانند استرس و هیجان، امکان گردآوری اطلاعات با کیفیت بالا را فراهم کرده است. گذشته از موارد اشاره شده توسعه راهکارهای ذخیره‌سازی اطلاعات از جمله ظرفیت‌های حافظه تقویت شده دستگاه‌ها و تجهیزات هوشمند و رایانش ابری این امکان را فراهم ساخته که داده‌های افراد را در مقیاس عظیمی ذخیره‌سازی کرد. داده‌های جمع‌آوری شده هنگامی که با الگوریتم‌هایی که به دنبال یافتن «معنا و ارتباط» بین داده‌ها هستند ترکیب می‌شوند یک محیطی دیجیتالی برای فرد فراهم می‌کنند که قادر به احساس دنیای بیرون و تصمیم‌گیری برای اهداف از پیش تعیین شده بدون مداخله انسان است. به عبارت دیگر هنگامی‌که حسگرهای هوشمند متصل به اشیای مورد استفاده روزمره افراد همچون ساعت‌های هوشمند، خودروهای هوشمند، تجهیزات پزشکی هوشمند، خانه هوشمند و... اطلاعات جمع‌آوری شده از محیط پیرامون را از طریق اینترنت با دیگر «اشیای هوشمند» به اشتراک می‌گذارند،

[1] Industry 4.0
[2] Internet of Things

می‌توانند بدون مداخله انسان با یکدیگر به تعامل پرداخته و خدماتی برای کاربران آن ارائه دهند. امروزه فناوری اینترنت اشیا در حوزه‌های متعددی همچون سلامت افراد، حمل و نقل و کنترل ترافیک، مدیریت عرضه و تقاضا در بازار، بازاریابی شخصی‌سازی شده و نیز خانه‌های هوشمند خدمات متنوعی برای کاربران آن ارائه می‌دهد. ارائه خدمت شخصی‌سازی شده به طور آنی در اینترنت اشیا مشروط به جمع‌آوری سیل عظیمی از داده مربوط به فرد و تبادل آن بین سایر اشیا است. همراه با افزایش اتصال اشیای هوشمند به اینترنت تعداد فزاینده‌ای از بازیگران از جمله صاحبان وب‌سایت‌ها و شرکت‌های بازاریابی در حال جمع‌آوری، نگهداری و استفاده از اطلاعات مصرف‌کنندگان برای نیل به اهداف خود می‌باشند. در حالی که جمع‌آوری داده‌ها می‌تواند به نفع مصرف‌کنندگان باشد – به عنوان مثال، با اجازه دادن به شرکت‌ها برای ارائه محصولات متناسب‌تر به مصرف‌کنندگان– با این وجود باعث نگرانی‌هایی مربوط به حریم خصوصی افراد می‌گردد زیرا مصرف‌کنندگان در اغلب موارد نمی‌توانند نحوه استفاده از اطلاعات خود توسط این نهادها را کنترل کنند یا اطلاعی از اینکه چه نوع اطلاعاتی از ایشان جمع‌آوری شده است ندارند. اطلاعات شخصی جمع‌آوری شده از دستگاه‌های هوشمند مبتنی بر اینترنت اشیا ممکن است به طور بالقوه ارزش تجاری و مالی داشته باشد. تولیدکنندگان محصولات و شرکت‌های ارائه دهنده خدمات می‌توانند با خرید این اطلاعات مزایای متعددی از جمله خدمات شخصی‌سازی شده برای مصرف‌کننده به ارمغان بیاورند. در اغلب موارد ارائه دهندگان خدمات اینترنت اشیا بدون اطلاع فرد داده‌ها را به اشخاص ثالث می‌فروشند و فرد اختیاری در تصمیم‌گیری در این باره ندارد. گذشته از بحث عدم اطلاع و رضایت فرد در دسترسی به اطلاعات، هرچه داده‌های بیشتری از افراد جمع‌آوری شود و در دسترس اشخاص ثالث قرار گیرد به همان اندازه منجر به عدم توازن بین روابط مصرف‌کننده و شرکت‌ها می‌شود چرا که اشخاص اخیر می‌توانند مصرف‌کنندگان را به طور مستقیم تحت تأثیر قرار دهند. امروزه تلفن‌های همراه و سایر اشیای هوشمند حاوی اطلاعات حساس و خصوصی افراد می‌باشند و افرادی که به مجموعه این داده‌ها دسترسی دارند می‌توانند با تحلیل آن‌ها به جزئی‌ترین الگوی رفتاری فرد از عادات خواب و سیگار کشیدن و نوع شخصیت و وضعیت تأهل گرفته تا نوع جنسیت و سن فرد دست پیدا کنند. شرکت‌ها و مؤسسات می‌توانند با پی بردن به الگوی رفتاری افراد درباره آنها در حوزه‌هایی مثل بیمه یا استخدام تصمیم‌گیری کنند(Smith, 2019, p. 864). این تصمیم‌گیری با توجه به اینکه به طور خودکار و بدون دخالت و اطلاع فرد صورت می‌گیرد ممکن است منتهی به رفتار تبعیض آمیز و نقض حریم خصوصی فرد گردد.

یکی دیگر از چالش‌های عضر فناوری اطلاعات و ارتباطات تأمین امنیت داده‌های افراد به ویژه داده‌های شخصی آنان می‌باشد. (European Commission, 2014). اینترنت اشیا، هم مصرف‌کنندگان و هم مشاغل را با تعدادی از تهدیدات امنیتی مواجه می‌کند. مجرمان سایبری می‌توانند از طریق هک اشیای هوشمند به تعداد زیادی از اطلاعات شخصی و حساس افراد به طور غیرمجاز دسترسی یابند. آنها همچنین ممکن است به سرورها یا سرورهای مبتنی بر فضای ابری حمله کنند که در آن مقادیر زیادی داده ذخیره شده است. استفاده از رمزهای عبور ضعیف یا پیش‌فرض در دستگاه‌ها و نیز ضعف‌های برنامه نویسی برای تامین امنیت اینگونه اشیا، داده‌های افراد را با تهدیدات امنیتی زیادی مواجه می‌کند. محدودیت‌های فنی و ساختاری دستگاه‌های حسگر و سنجشگر اینترنت اشیاو نیز با توجه به اینکه این دستگاه‌ها توسط تولیدکنندگان مختلفی عرضه می‌گردد به همین جهت ممکن است تمام تولیدکنندگان الزامات امنیتی را در محصولات خود رعایت نکنند و در نتیجه ورود غیر مجاز هکرها را تسهیل کنند. گذشته از این با نظر به اینکه فناوری‌های حسگر اینترنت اشیابه طور لحظه‌ای با یکدیگر در ارتباط می‌باشند و داده‌ها را بین خود تبادل می‌کنند و بینشان اتصال لحظه‌ای وجود دارد از این رو نقض امنیتی در یکی از آنان می‌تواند زمینه هک شدن سایر تجهیزات گردد، این امر نشان می‌دهد در فناوری اینترنت اشیا تهدیدات امنیتی تنها محدود به فردی نیست که از خدمات آن استفاده می‌کند بلکه سایر افراد نیز صرف نظر از موقعیت جغرافیایی خود می‌تواند متأثر گردد. با توجه به اینکه نقض امنیت داده ممکن است خطرات مالی و جانی به همراه داشته باشد اتحادیه اروپایی به دلیل حساسیت فناوری‌های اینترنت اشیای پزشکی، مقررات ۲۰۱۷/۷٤٥ مربوط به تجهیزات پزشکی را تصویب کرده است.[۳] بر اساس این مقررات تجهیزات پزشکی هوشمند باید به گونه‌ای طراحی شوند که خطرات مرتبط با تعامل منفی احتمالی بین نرم افزار و محیط فناوری اطلاعات را به حداقل برسانند. این مقررات در رابطه با طراحی نرم افزارهایی که در این حوزه مورد استفاده قرار می‌گیرد اعلام می‌دارد این نرم افزارها باید مطابق با آخرین پیشرفت‌های موجود در حوزه فناوری اطلاعات طراحی شوند و امنیتی حداقلی (در برابر دسترسی غیرمجاز) برای کاربران آن فراهم کنند (Chiara, 2020, p.8).

با توجه به اینکه روز به روز تعداد اشیای هوشمند متصل به اینترنت افزایش می‌یابد و داده‌های بیشتری جمع‌آوری می‌گردد و از سوی دیگر از داده‌های افراد در بخش عمومی و خصوصی برای اهداف گوناگون مورد استفاده قرار می‌گیرد تدوین یک چارچوب حقوقی برای حفاظت از داده‌های اشخاص

[۳] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

که متناسب با تحول‌های فعلی و پیش رو باشد یک بایسته تلقی می‌گردد (اقدسی و محقق داماد، ۱۴۰۰: ۵۰). در حوزه قانون‌گذاری درباره حفاظت از داده شخصی نظام‌های حقوقی اتحادیه اروپایی، ایالات متحده آمریکا به علت داشتن سابقه طولانی در این حوزه و گذر از آزمون و خطاها، و نظام حقوقی چین به عنوان یکی از نظام‌های نوپا اما مستحکم اهمیت ویژه‌ای دارند. برخلاف نظام‌های اشاره شده در ایران قانونی که به طور ویژه به حفاظت از داده‌های شخصی شهروندان اختصاص داشته باشد وجود ندارد و تنها در برخی حوزه‌ها از جمله تجارت الکترونیک به اصول حفاظت از داده اشاره شده است. درجدول زیر به اهم چالش‌ها و راهکارهای مطروحه در موضوع اینترنت اشیا پرداخته شده است:

جدول ۱- چالش‌های اینترنت اشیا و راهکارهای برون‌رفت از آن

عنوان چالش	شرح چالش	راهکارهای برون‌رفت از چالش‌ها
نقض حریم خصوصی از طریق پردازش اطلاعات حساس	داده‌هایی که از طریق اشیا هوشمند جمع‌آوری و پردازش می‌شود ممکن است حاوی اطلاعاتی از جزئی‌ترین لایه‌های خصوصی زندگی افراد باشد. دسترسی و انتشار این اطلاعات ممکن است آثار زیانبار جبران‌ناپذیری برای افراد به همراه داشته باشد.	نظام‌های حقوقی اتحادیه اروپایی و جمهوری خلق چین برای محافظت از حریم خصوصی افراد و جلوگیری از شناسایی هویت افراد موضوع داده در قوانین خود الزاماتی و شرایطی برای پردازش داده‌ها توسط کنترلگر و پردازشگر مقرر کرده‌اند و روش‌هایی همچون ناشناس‌سازی داده پیش‌بینی نموده‌اند.
حفاظت از داده‌های شخصی	قابلیت شناسایی افراد؛ نقش انفعالی افراد موضوع داده و نامتقارن بودن وضعیت اطلاعاتی؛ کیفیت نامطلوب روش‌های اخذ رضایت از فرد موضوع داده، تصمیم‌گیری خودکار و نمایه‌سازی، عدم تکافوی راهکارها و حقوق سنتی برای حفاظت از داده‌های افراد	افراد موضوع داده برای اینکه بتوانند در اطلاعات و داده‌های خود دخل و تصرف کنند و نسبت به پردازش آنان به پردازشگر یا کنترلگر رضایت دهند نمی‌توانند به روش‌های سنتی اتکا کنند. در این راستا حقوق متنوع و مشخصی برای افراد موضوع داده پیش‌بینی شده است.
تامین امنیت داده‌های شخصی	محدودیت‌های فنی و ساختاری دستگاه‌های حسگر و سنجشگر	در برخی از نظام‌های حقوقی که قوانین جامع و مدون برای حفاظت از داده‌ها تصویب کرده‌اند اصول و

	اشیای هوشمند؛ دسترسی غیرمجاز؛ حملات سایبری	الزاماتی برای پردازشگر و کنترلگر در راستای تامین امنیت داده‌ها مطابق با روش‌ها و فناوری‌های روز پیش‌بینی کرده‌اند. بررسی دوره‌ای کارایی روش‌های اتخاذ شده و نیز اطلاع‌رسانی به افراد موضوع داده و مقامات ذی‌صلاح از دیگر مواردی است که برای برون‌رفت از چالش‌های اشاره شده مطرح شده است.
فقدان استانداردهای حاکم بر اشیا هوشمند	**فقدان استانداردهای واحد برای اشیای هوشمند جهت تعامل با یکدیگر؛ تضعیف تعامل‌پذیری بین اشیا و محدود شدن قابلیت انتقال داده‌ها**	تولیدکنندگان اشیا هوشمند و نیز تجهیزاتی که برای ارائه خدمات اینترنت اشیا استفاده می‌شود از استانداردها و اصول مشخصی استفاده نمی‌کنند و این امر باعث می‌شود تعامل‌پذیری بین اشیا تضعیف گردد. برای حل این چالش کشورها شروع به ایجاد سازمان‌های جدید برای تدوین استانداردها کرده‌اند. به عنوان مثال طبق گزارش پارلمان اتحادیه اروپایی موسسه استانداردهای ارتباطات اروپا در تلاش است استانداردهایی برای این حوزه تعریف کند.

تناسب و عدم تناسب این سه رویکرد در مطالعه تطبیقی با وضعیت حقوقی ایران و مزایا و معایب هرکدام و چگونگی تبلور آن در نظام حقوقی کشورمان، جهت تدوین مدل مفهومی موضوع در نظام حقوقی جمهوری اسلامی ایران، نتیجه این طرح پژوهشی است.هدف اصلی پژوهش حاضر پاسخ به این پرسش اصلی می‌باشد که الگوی مطلوب حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا برای کشور، با توجه به مطالعه تطبیقی، چگونه خواهد بود و در صورت عدم مطلوبیت چه راهکاری می‌توان پیشنهاد داد. پاسخ به پرسش اشاره شده مستلزم پاسخ به برخی سؤالات فرعی به

شرح زیر می‌باشد: چالش‌ها و موانع موجود در حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا در نظام حقوقی کشورهای منتخب چیست؟ راهکارهای موجود در حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیادر نظام حقوقی کشورهای منتخب چیست؟ اهمیت پاسخ به پرسش‌های مذکور در این نکته نهفته است که اینترنت اشیا در کشور ایران در مراحل ابتدایی خود قرار دارد و در این مسیر با تغییرات گسترده در فناوری مواجهه می‌باشد؛ انتخاب رویکرد نامناسب برای حفاظت از داده‌ها از یک‌سو و توسعه اینترنت اشیا از سوی دیگر می‌تواند هدررفت سرمایه‌های ملی را به دنبال داشته باشد و موجب کاهش رشد کسب و کارهای مبتنی بر داده گردد. در معدود مطالعات صورت گرفته به خلاء قانونی موجود و لزوم تدوین چارچوب حقوقی اشاره شده است (زارعیان، واحد، ۱۳۹۹: ٦٨)

سیاست‌گذاری کلان ملی در خصوص چالش‌های موجود در حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا، ارائه چهارچوب مناسب جهت نگارش قوانین و مقررات با رویکرد جامع و مطابق با نیاز فعلی، رفع فقر ادبیات حقوقی و جاماندگی قوانین از روند شتابان در این حوزه از مهم‌ترین دغدغه‌های نگارش این پژوهش می‌باشد.

۲- الگوهای حاکم بر حمایت از حریم خصوصی و حفاظت از داده شخصی در اینترنت اشیا در پرتو مطالعات تطبیقی

حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در اینترنت اشیا در سیستم های صنعتی هوشمند (انقلاب صنعتی چهارم) از موضوعات مهمی است که مورد توجه حقوق‌دانان قرار گرفته است. آنچه این الزام را به وجود می آورد این واقعیت است که دسترسی غیرمجاز به داده ها در اینترنت اشیا می تواند به عواقب زیانباری چون حملات و جرایم سایبری، از میان رفتن حریم خصوصی و دستکاری داده‌ها منتج شود. در صورتی که اگر اقدامات حفاظتی مقتضی در این خصوص صورت نگیرد، چنین رویدادهای نامطلوبی می توانند موجودیت و کارکرد برنامه‌های کاربردی مبتنی بر اینترنت اشیا را به خطر بیاندازند.(آقابزرگ لواسانی،۱۳۹۸) کشورها و مناطق مختلف در سراسر جهان به دنبال تشویق نوآوری و اینترنت اشیا قواعد و مقرراتی دارند که در ادامه به بررسی سه الگوی حاکم در این زمینه می‌پردازیم:

۲-۱- اتحادیه اروپا

در خصوص حمایت از حریم خصوصی و حفاظت از داده‌های شخصی، اتحادیه اروپایی یک از پیشگامان توسعه نظام قاعده‌مند و جامع حمایت از حریم خصوصی و حفاظت از داده شخصی می‌باشد. حمایت از حریم خصوصی با توجه به بستر تاریخی آن در اروپا و حفاظت از داده‌های شخصی با توجه به حساسیت آن، به عنوان یک حق بشری شناخته شده است. آخرین تلاش قانون‌گذار اتحادیه اروپایی برای ایجاد یک نظام جامع برای حفاظت از داده‌ها در مقرات عمومی حفاظت از داده انعکاس یافته است. تأثیر این مقررات تا به اکنون به اندازه‌ای بوده است که سایر نظام‌های حقوقی برای تدوین قوانین ملی خود آن را الگوی خود قرار داده‌اند، نمونه بارز آن قانون حمایت از اطلاعات شخصی جمهوری خلق چین مصوب ۲۰۲۱ است. از سال ۱۹۹۵ با توسعه فناوری اطلاعات و ارتباطات از یک‌سو و موضوع حریم خصوصی از سوی دیگر کشورهای اروپایی سعی داشته‌اند با شناسایی برخی اصول برای پردازش داده و نیز حقوق ویژه برای افراد از اطلاعات و داده‌های اشخاص به عمل آورند. با توجه به ارزش اقتصادی تجارت داده‌های اشخاص اتحادیه اروپایی به عنوان نهادتنظیم‌گر برای تسهیل جریان اطلاعات و نیز حمایت از حریم خصوصی و حفاظت از داده‌های اشخاص مقررات عمومی حفاظت از داده را به تصویب رساند. به طور کلی درباره چارچوب این مقررات می‌توان گفت قانون‌گذار سعی داشته است با پیش‌بینی ۳ مورد از داده‌های اشخاص حفاظت کند: ۱. پیش‌بینی اصول حاکم بر چرخه پردازش داده (اصل قانونی بودن، عدالت و شفافیت پردازش داده‌های شخصی، اصل هدف مشخص و اصل دقیق بودن داده‌های شخصی، اصل کمینه‌سازی و محدودیت ذخیره‌سازی، اصل امنیت و اصل مسئولیت پردازندگان) ۲. تجهیز افراد موضوع داده به حقوق ویژه (حق اطلاع و دسترسی به داده‌های شخصی، حق اصلاح و حذف، حق محدودسازی پردازش، حق انتقال داده‌های شخصی، حق اعتراض) ۳. ساز و کارها ضمانت اجراهای غیر کیفری و مجازات نقدی در صورت عدم رعایت قانون. داشتن چنین ساختاری باعث شده است از این مقررات تحت عنوان مدل حق‌محور حفاظت از داده یاد شود.

جدول ۲- قواعد حاکم بر حمایت از حریم خصوصی و حفاظت از داده شخصی در مقررات اتحادیه و شورای اروپا

موضوع قواعد		مقررات عمومی حفاظت از داده (G.D.P.R)	کنوانسیون مدرن شورای اروپا برای حفاظت از افراد در برابر پردازش داده‌های شخصی
قلمروی اجرایی		قلمروی موضوعی: نسبت به تمامی داده‌های شخصی چه اینکه به طور کامل با ابزارهای خودکار پردازش شود یا نیمه خودکار اعمال می‌شود قلمروی جغرافیایی: در مورد پردازش داده شخصی در زمینه فعالیت‌های کنترل‌کننده یا پردازشگری کـه محل استقرارشان (مقر) در اتحادیه اروپاست، صرف نظر از اینکه آیا پردازش در اتحادیه رخ می‌دهد یا خیر، اعمال می‌شود	ماده (۳): نسبت به تمامی پردازش‌هایی که توسط بخش عمومی و خصوصی انجام می‌شود اعمال کنند.
اصول بنیادین	**اصل قانونی بودن، عدالت و شفافیت پردازش داده‌های شخصی**	**ماده (۵ (۱) (الف))**	**ماده (۵ (۳))؛ ماده (۵ (٤) (الف))**
	اصل هدف مشخص و اصل دقیق بودن داده شخصی	**ماده (۵ (۱) (ب))؛ ماده (۵ (۱) (د))**	**ماده (۵ (٤) (ب))؛ ماده (۵ (٤) (د))**
	اصل کمینه‌سازی و محدودیت ذخیره‌سازی	**ماده (۵ (۱) (ج))؛ ماده (۵ (۱) (ه))**	**ماده (۵ (٤) (ج))؛ ماده (۵ (٤) (د))؛**
	اصل امنیت داده	**ماده (۵ (۱) (ج))؛ ماده (۵ (۱) (و))**	**ماده ۷**
	اصل مسئولیت‌پذیری	**ماده(۵ (۲))**	**ماده (۱۰ (۱))**
حقوق افراد موضوع داده	حق اطلاع و دسترسی	**ماده (۱۲) الی (١٦)**	**ماده (۸)**
	حق اصلاح و حذف داده‌های شخصی	**ماده (١٦) و (۱۷)**	**ماده (۹ بند ۱ (ه))**
	حق محدودسازی پردازش داده‌های شخصی	**ماده (۱۸)**	**ماده (۹ (۱) (د))**
	حق انتقال داده‌های شخصی	**ماده (۲۰)**	-
	حق اعتراض	**ماده (۲۱)**	**ماده (۹ (۱) (د))**
نهاد نظارتی		**نظارت بر اجرای مقررات با هدف حفظ حقوق و آزادی اشخاص حقیقی در ارتباط با پردازش و تسهیل جریان آزاد داده‌های فردی فصل ششم مواد (۵۱) الی (۵۹)**	**با هدف نظارت بر اجرای مقررات کنوانسیون توسط کشورهای عضو ماده (۱۵)**

۲-۲- ایالات متحده امریکا

حمایت از حق حریم خصوصی چنانکه در اتحادیه اروپایی به عنوان یک حق بشری پذیرفته شده در قوانین فدرال ایالات متحده آمریکا شناخته نشده است. حفاظت از اطلاعات شخصی به عنوان جنبه‌ای از حریم خصوصی افراد به طور پراکنده نیز تنها به رعایت یک‌سری الزامات مربوط به پردازش داده محدود شده است. قانون‌گذار فدرال بی‌آنکه حق مشخصی تحت عنوان حمایت ازحریم خصوصی داده یا حفاظت از داده‌های شخصی پیش‌بینی کرده باشد، در قوانین متعدد برخی از انواع داده‌ها که اهمیت بیشتری دارند به ویژه اطلاعات مربوط به حوزه سلامت، بهداشت، بیمه، حریم خصوصی آنلاین کودکان، گزارش‌های مالی و اعتباری را تحت حمایت قانونی قرار داده و الزاماتی برای اشخاص مشمول قوانین مقرر کرده است. از میان قوانین فدرال اشاره شده می‌توان به قانون مسئولیت‌پذیری و انتقال‌پذیری بیمه سلامت مصوب ۱۹۹٦، قانون حفاظت از حریم خصوصی آنلاین کودکان مصوب ۱۹۹۸ اشاره کرد. در نظام حقوقی ایالات متحده با توجه به اینکه تنها داده‌هایی خاصی (مالی، بهداشت، سلامت، حریم خصوصی آنلاین کودکان) در سطح فدرال مورد حمایت قانون‌گذار قرار گرفته است بسیاری از افراد برای اجرای حق حریم خصوصی خود با مشکلاتی مواجه می‌باشند و تنها متکی به سیاست‌های حفظ حریم خصوصی شرکت‌ها و کسب و کارهای مبتنی بر داده و الزامات محدود پیش‌بینی شده در آن می‌باشند. علاوه بر این مورد در سطح فدرال نهادهایی به موجب قانون ایجاد شده است که اگرچه به طور مستقیم مربوط به حفاظت از داده افراد نمی‌باشند اما انجام برخی از رفتارها توسط شرکت‌ها و تولیدکنندگان و ارائه دهندگان خدمات را که با داده‌های افراد سر و کار دارند ممنوع اعلام می‌دارند و بر آن نظارت دارند. برای مثال کمیسیون تجارت فدرال اعمال یا اقدامات ناعادلانه یا فریبنده در تجارت را ممنوع اعلام کرده است. این کمیسیون با اقدامات و توصیه‌های خود سعی کرده است خلاءهای موجود در حمایت قانونی از حریم خصوصی افراد را مرتفع نماید. از آنجا که کسب و کارها خارج از شمول قوانین خاص حفظ حریم خصوصی موجود هستند در بسیاری موارد منبع اصلی تنظیم‌گری در ایالات متحده کمیسیون تجارت فدرال است. کمیسیون اشاره شده بر خلاف قوانین فدرال محدود به حوزه خاصی از کسب و کار و تجارت نمی‌باشد و صلاحیت آن بر تمام شرکت‌هایی که در حوزه تجارت فعالیت می‌کنند تسری دارد. در رابطه با خط‌مشی‌های حمایت از حریم خصوصی اطلاعاتی افراد کمیسیون تجارت فدرال اعلام داشته است شرکت‌ها و ارائه دهندگان خدمات هنگامی که برخلاف تعهدات خود در خط مشی‌های حریم خصوصی عمل می کنند یا هنگامی که علی رغم اعلام تعهدشان مبنی بر حفاظت و تأمین امنیت داده‌های شخصی نتوانند در برابر دسترسی‌های غیرمجاز از اطلاعات

افراد محافظت کنند اقداماتشان گمراه کننده و فریبنده تلقی می‌شود و کمیسیون صلاحیت دارد تحقیقات و اقدامات لازم از جمله طرح دعوی را انجام دهد. به عبارت دیگر در صورتی که اشخاص اشاره شده اطلاعات افراد را برخلاف موارد مندرج در خط‌مشی حمایت از حریم خصوصی جمع‌آوری، ذخیره، استفاده و افشا کنند یا این اطلاعات را با اشخاص ثالث برای اهداف دیگر به اشتراک بگذارند اقداماتشان تحت شمول مفهوم اعمال گمراه کننده قرار می‌گیرد. الگوی ایالات متحده آمریکا که از آن تحت عنوان مدل مینیمالیستی حفاظت از داده نیز یاد می‌شود، برای مدتی سرمشق برخی از نظام‌های حقوقی به ویژه چین بوده است.

جدول ۳. قواعد حمایت از حریم خصوصی و حفاظت از داده شخصی در نظام حقوقی ایالات متحده امریکا

قوانین حفاظت از حریم خصوصی اطلاعاتی (فدرال/ایالتی)	اطلاعات تحت حمایت قانون	دامنه اجرایی قانون	ماهیت مقررات	نهاد مجری قانون	امکان طرح دعوی فردی برای جبران خسارت
قانون مسئولیت‌پذیری و انتقال‌پذیری بیمه سلامت	اطلاعات مربوط به سلامت و بهداشت افراد	ارائه دهندگان خدمات بهداشتی برنامه‌های مربوط به امور درمانی برنامه‌های دولتی که هزینه‌های مراقبت های بهداشتی را پرداخت می‌کنند	الزام اخذ رضایت از فرد به منظور به اشتراک گذاری و افشای داده‌ها / امنیت داده‌ها	وزارت بهداشت و خدمات انسانی ایالات متحده آمریکا	
قانون حفاظت از حریم خصوصی آنلاین کودکان	اطلاعات قابل شناسایی جمع‌آوری شده به صورت آنلاین از کودک زیر سیزده سال	اپراتورهای وب‌سایت‌ها یا خدمات آنلاین که (۱) وب-سایت یا خدمات خود را به کودکان معرفی می کنند یا (۲) دانش واقعی دارند که در حال جمع‌آوری اطلاعات شخصی از کودک هستند	الزام اخذ رضایت مصرف‌کننده برای جمع‌آوری داده‌ها و به اشتراک گذاری آن/ لزوم تامین امنیت اطلاعات	کمیسیون تجارت فدرال	
قانون کمیسیون تجارت فدرال	ممنوعیت طیف گسترده‌ای از شیوه‌های ناعادلانه و گمراه کننده در تجارت و رقابت که باعث تضرر مصرف‌کننده می‌شود	کلیه اشخاص یا نهادهای تجاری غیر از برخی از مؤسسات مالی خاص و مؤسسات غیرانتفاعی	الزامات مربوط به حفاظت از حریم خصوصی اطلاعاتی و ممنوعیت خط‌مشی‌ها حریم خصوصی و شیوه های امنیتی ناعادلانه یا فریبنده	کمیسیون تجارت فدرال	

قانون حریم خصوصی مصرف‌کننده کالیفرنیا	هرگونه اطلاعاتی که مربوط به مصرف‌کننده می‌باشد و به طور مستقیم یا غیر مستقیم باعث شناسایی یا توصیف وی می‌گردد	صاحبان مشاغل و کسب‌و-کارها و ارائه دهندگان خدمات به جز مؤسسات غیرانتفاعی	الزامات مربوط به رعایت حقوق مقرر برای مصرف‌کننده و خط‌مشی-های حفظ حریم خصوصی و امنیت اطلاعات	دادستان کل ایالت کالیفرنیا	

۲-۳- جمهوری خلق چین

در حالی که کشورهای عضو اتحادیه اروپا و نیز نظام حقوقی ایالات متحده از سال‌ها پیش در حال گسترش قواعد حاکم بر حفظ حریم خصوصی خود بر داده‌های شخصی بودند جمهوری خلق چین تنها در چند سال اخیر توجه خود را معطوف کرده است. قانون اساسی این کشور به عنوان عالی‌ترین قانون تنها به جنبه‌های سنتی حریم خصوصی توجه داشته است و اشاره‌ای به حق حفاظت از داده‌ها نداشته است. با این‌حال حقوقدانان با استناد به اینکه قانون اساسی چین به کرامت و منزلت فرد توجه داشته است و حریم خصوصی نیز جنبه‌ای از احترام به کرامت انسان محسوب می‌شود اعلام داشته‌اند حریم خصوصی به طور کلی تحت لوای این قانون می‌باشد. بر اساس آموزه‌های حقوق تطبیقی هر کشور در مواجهه با چالش‌های جامعه خود ابتدا سعی می‌کند به راهکارهای قانونی که در دیگر کشورها برای همان چالش استفاده شده است نظری بیندازند و سپس بر اساس مبانی خود آن راهکار را وارد نظام حقوقی خود کنند. نظام حقوقی چین به علت فقدان تجربه در این حوزه ابتدا با شیوه آزمون و خطا مسیر نظام حقوقی ایالات متحده را پیمود و همانند آن در برخی حوزه‌ها اقدام به قانون‌گذاری کرد. با توسعه و رسوخ اصول بین‌المللی حاکم بر حفاظت از داده از یکسو و تصویب مقررات عمومی حفاظت از داده اتحادیه اروپایی به عنوان قانونی جامع و همه شمول در حوزه حفاظت از داده‌های شخصی از سوی دیگر، قانون‌گذار چین برای اجتناب از ایزوله شدن کشور در سطح بین‌المللی با تاسی از مقررات عمومی حفاظت از داده اقدام به طرح مدل جدید خود کرد. قانون‌گذار جمهوری خلق چین پس از به رسمیت شناختن حق حریم خصوصی و حق حفاظت از اطلاعات شخصی در قانون مدنی خود در قالب حقوق مربوط به شخصیت افراد، قانون حمایت از اطلاعات شخصی جمهوری خلق چین و قانون امنیت داده جمهوری خلق چین به تصویب رساند. قانون حمایت از اطلاعات شخصی که در تقنین آن از مقررات عمومی حفاظت از داده الگوبرداری شده است، موسسات عمومی و خصوصی و کسب و کارها را به طور یکسان ملزم کرده از اصول و الزامات حاکم بر پردازش داده‌های شخصی که

مشابه آن در نظام حقوقی اتحادیه اروپایی مشاهده می‌شود پیروی کنند. قانون‌گذار جمهوری خلق چین برای تطابق قوانین با ارزش‌ها و اهداف جامعه و توجه به لزوم اعمال حاکمیت دولت در عرصه اطلاعات شهروندان در قانون امنیت داده جمهوری خلق چین برای کنترل‌گران و پردازش‌گران تعهدات مضاعفی در نظر گرفت. بر اساس این قانون اشخاص مذکور موظف شده‌اند در سریع‌ترین زمان ممکن اطلاعات و داده‌هایی که توسط دولت معین می‌شوند در اختیار حکومت قرار دهند. این الزام اگرچه به ویژه برای سرمایه‌گذاران خارجی و شرکت‌های فعال و کسب و کارهای مبتنی بر داده در چین همواره منشأ نگرانی و تنش با دولت چین بوده است با این وجود به علت گستردگی موضوع و تاثیر آن بر زندگی خصوصی افراد از یکسو و نیز بحث رعایت منافع عمومی، اقتصادی، فرهنگی و ملی کشور باعث شده است لزوم نقش گسترده دولت در حوزه حفاظت از داده به طور فزآینده‌ای مورد توجه قرار گیرد. کشور چین از جمله نظام‌های حقوقی است که در آن برای حاکمیت نقش فعال و پویایی در راستای حفاظت از داده‌های شهروندان و امنیت ملی پیش‌بینی شده است. قانون تعهدات و الزاماتی برای دولت مقرر کرده است. طبق ماده (۱۳) قانون امنیت داده مصوب ۲۰۲۱ دولت موظف شده است یک برنامه کلی برای هماهنگی و توسعه امنیت داده‌ها تدوین کند و به موجب ماده (۱۷) نیز استانداردهایی را برای استفاده از داده‌های شخصی ایجاد کند. یکی از نوآوری‌های این قانون در مقایسه با نظام‌های حقوقی منتخب الزام دولت به ارائه طبقه‌بندی داده‌های شخصی بر اساس اهمیت داده‌ها در توسعه اقتصادی و اجتماعی و همچنین میزان آسیب به امنیت ملی، منافع عمومی و حقوق و منافع قانونی افراد موضوع داده است. ماده (۲۱) قانون امنیت داده در این باره بیان می‌دارد داده‌های مربوط به امنیت ملی، اقتصاد ملی، جنبه‌های مهم زندگی مردم، منافع عمومی و غیره از جمله داده‌هایی می‌باشند که دولت برای محافظت از آنها باید سیستم مدیریت سختگیرانه‌ای را ایجاد کند. در قانون امنیت داده توضیح بیشتری درباره طبقه‌بندی داده‌ها ارائه نشده است و طراحی آن بر عهده دولت گذاشته شده است. از دیگر مسئولیت‌های دولت ایجاد نظامی برای پاسخگویی به خطرات امنیتی است. به موجب ماده (۲۲) دولت باید یک مکانیسم متمرکز، منسجم، مؤثر و معتبر برای ارزیابی، گزارش‌دهی، اشتراک اطلاعات، نظارت و هشدار اولیه در برابر خطرات امنیتی داده‌ها ایجاد کند. در این راستا ماده (۲۳) قانون امنیت اطلاعات اعلام داشته است در صورت وقوع یک حادثه امنیتی، ادارات ذی‌صلاح مربوطه باید مطابق با قانون واکنش اضطراری را آغاز کنند، از جمله اقدامات مربوطه را برای جلوگیری از آسیب بیشتر و از بین بردن خطرات امنیتی انجام دهند و در صورت لزوم عموم مردم را از خطرات موجود مطلع کنند.

جدول ٤. قواعد حمایت از حریم خصوصی و حفاظت از داده شخصی در نظام حقوقی چین

نظام حقوقی چین	قوانین و مقررات حفاظت از اطلاعات شخصی	اطلاعات تحت حمایت قانون	دامنه اجرایی	حقوق اشخاص موضوع داده	رویکرد قانون‌گذاری
	قانون حمایت از اطلاعات شخصی جمهوری خلق چین	انواع گوناگون اطلاعات ثبت شده به صورت الکترونیکی یا به طرق دیگر و مرتبط با شخص حقیقی شناسایی شده یا قابل شناسایی.	تمامی اشخاص بخش عمومی و خصوصی که اطلاعات افراد را پردازش می‌کنند	تمام حقوق پیش‌بینی شده در مقررات عمومی حفاظت از داده در این قانون نیز منعکس شده است.	قانون‌گذار چین در ابتدا با تصویب قوانینی پراکنده در حوزه‌های گوناگون از رویکرد ایالات متحده برای حفاظت از داده استفاده کرده است. با توجه به اهمیت یکنواخت‌سازی داده‌ها قانون‌گذار چین برای اولین بار قانون حمایت از اطلاعات شخصی را تصویب نمود. ارائه حمایت جامع و مشابه رویکرد اتحادیه اروپایی و نیز توجه به منافع عمومی و امنیت ملی و نیز وضع مقررات سختگیرانه برای انتقال فرامرزی داده‌ها از ویژگی‌های رویکرد چین می‌باشد.

۳- الگوی مطلوب حمایت از حریم خصوصی و حفاظت از داده شخصی در نظام حقوقی ایران

با تشکیل شورای عالی فضای مجازی سیاست‌گذاری در فضای اینترنت شتاب بیشتری به خود گرفته است و این نهاد مصوباتی نیز در مورد الزامات حاکم بر اینترنت اشیا به تصویب رسانده است؛ لیکن مصوبات شورای عالی فضای مجازی در کشور نقش سیاست‌گذاری دارد و بدون پیش‌بینی ساز و کار اجرایی، در عمل برای چالش‌های این حوزه راهکاری وجود ندارد.

توسعه فناوری‌های نوین و کسب و کارهای مبتنی بر آنان در گرو جلب اعتماد کاربران می‌باشند. جلب رضایت افراد زمانی محقق می‌گردد که اطمینان داشته باشند قانون‌گذار به شیوه‌ای موثر از حقوق و منافع ایشان حمایت می‌کند. قانون‌گذاری و مقررات‌گذاری در حوزه حفاظت از داده‌های اشخاص در

بخش‌های مختلف باید با در نظر گرفتن این نکته همراه باشد که قانون قطعاً نمی‌تواند همسو با رشد فناوری اطلاعات و ارتباطات باشد و برای جلوگیری از جمود قانونی و اجرایی و پویایی نظام حقوقی در برابر تغییرات، لازم است مقررات مربوط به حفاظت از داده‌های اشخاص به گونه‌ای خنثی نگاشته شوند. فارغ از این نکته باید به این موضوع توجه شود که استفاده از فناوری‌های نوین و داده‌های اشخاص می‌تواند منبعی برای رشد و گسترش تجارت و بازاریابی باشد، از این رو مقررات‌گذاری باید به گونه‌ای باشد که مانع شکل‌گیری بستر تجارت نگردد.

پیش از تدوین مدل مفهومی کشور بر اساس نتایج حاصله از مقایسه تطبیقی و با توجه به اینکه نظام حقوقی ایران، رومی–ژرمن و مبتنی بر حقوق نوشته است، در پی پاسخ دادن به این پرسش هستیم که چه مرجعی صلاحیت تصمیم‌گیری و قاعده‌مند نمودن این حوزه را داراست. وجود خلاءهای قانونی به دلیل پیشرفت سریع تکنولوژی در حوزه فناوری اطلاعات، از یک‌سو و عدم تکافوی سیاست‌گذاری (شورای عالی فضای مجازی) که فقط سیاست‌گذاری کلان را مشخص می‌کند و فاقد حکم اجرایی و عملی است، از سوی دیگر و روند کند قانون‌گذاری در کشور باعث شد که شورای اجرایی فناوری اطلاعات زیر مجموعه وزارت ارتباطات و فناوری اطلاعات به تصویب پراکنده و غیرمتمرکز احکام مورد نیاز در حوزه فناوری اطلاعات و ارتباطات بپردازد و از آنجا که این مقررات‌گذاری صرف، فقط برای دستگاه‌های درون قوه مجریه لازم الاجراست، بقیه نهادهای کشور در این حوزه بلاتکلیف می‌باشند. پیدایش مقررات پراکنده و غیرمتمرکز و ایجاد صلاحیت‌های موازی در تصمیم‌گیری سبب می‌شود قضات که عموماً با مسائل حقوقی فناوری اطلاعات و ارتباطات آشنایی کافی ندارند، به قواعد جامع و متحدی برای اصدار رأی دسترسی نداشته باشند و ساختارهای متعدد، برای تصمیم‌گیری در این حوزه با صلاحیت‌های موازی پدیدار شوند.

در نظام حقوقی ایران در قوانین متعددی به حریم خصوصی و داده‌های شخصی افراد اشاره شده است و برای نقض آن مجازات کیفری مقرر شده است. نامتناسب بودن مجازات و صرف اتکا به اقدامات کیفری برای حفاظت از حریم خصوصی افراد ممکن است مانع رشد کسب و کارهای مبتنی بر داده و عقب ماندگی کشور گردد. گذشته از این برای شکل‌گیری گفتمان حفاظت از داده در نظام حقوقی ایران لازم است تمامی شهروندان و مسئولان از مفهوم قانونی آن آگاه باشند و بتوانند از حقوق شناسایی شده خود مطلع شوند. برای نیل به این هدف لازم است حقوق حریم خصوصی افراد به ویژه حریم خصوصی اطلاعاتی آنان در یک سند قانونی گرد آوری شوند و برای حفاظت از اطلاعات اشخاص الزاماتی مقرر

گردد. با عنایت به اصل (۷۱) قانون اساسی و صلاحیت تام و منحصر به فرد مجلس شورای اسلامی به‌عنوان نهاد تقنین، در نظام حقوقی ایران که رومی-ژرمن و مبتنی بر حقوق نوشته است؛ قانونگذاری در حوزه حریم خصوصی و حفاظت از داده‌های شخصی به طور کلی و در حوزه اینترنت اشیا به-طورخاص می‌تواند بسیار مطلوب و کارآمد باشد. لیکن فرآیند طولانی که برای پیش‌نویس لوایح پنج‌گانه وزارت ارتباطات و فناوری اطلاعات د ر این حوزه مورد اعمال قرارگرفت، سبب شد که از سال ۱۳۹۵ تا کنون، متون مذکور به عنوان پیش‌نویس در کمیسیون‌های دولت معطل بماند و بعضاً احکامشان به علت رشد شتابان فناوری، بیات و مستمعل شوند و بی‌تردید در صورت طرح مجدد، نیاز به بازنگری و به روز رسانی دارند. بروکراسی‌های اداری طولانی، تغییر مکرر مدیران بخش‌های دولتی مرتبط و تأثیر سلایق شخصی آنان بر سرنوشت لوایح تاثیرگذار است و گاه به دلایل صرفاً سیاسی و نه فنی و حقوقی یک لایحه مورد نیاز کشور درعرصه ارتباطات و فناوری اطلاعات از دستور کار خارج می‌شود. در نهایت لوایح پنج‌گانه از کانال کمیسیون‌های دولت خارج نشد و هیچ‌گاه به مجلس برای طی تشریفات مقرر، اعلام وصول نشد. اخیراً نمایندگان مجلس نیز در خصوص موضوع مورد بحث این پژوهش، طرحی را در دستور کار قرار داده‌اند که به علت عدم تخصص کافی نمایندگان مجلس در امورات اجرایی این حوزه، از غنای کافی برخوردار نیست و احتیاج به اصلاح و بازبینی‌های متعددی دارد که قطعاً زمانبر خواهد بود. برفرض تصویب قانون لازم الاجرا در این حوزه پس از طی همه مراحل و تشریفات مقرر، گاه تصویب آیین‌نامه‌های اجرایی مرتبط در قوه مجریه به علت سلیقه متفاوت با قوه مقننه بسیار به تعویق می‌افتد. در نهایت قانونی که بعد از سالها و طی تشریفات بالاخره تصویب و به مرحله اجرا می‌رسد، آنقدر دیر به نظام حقوقی تزریق می‌شود که کماکان از شتاب فناوری جا مانده و برای مسائل نوپیدا حکمی ندارد. از سوی دیگر روند اصلاح قانون نیز انقدر با کندی و بروکراسی سنگین اداری انجام می‌شود که این مساله نیز مشکل را مضاعف می‌نماید.

و اما پرسش دوم و مهم این مبحث آن است که در تدوین مدل ایران از کدام الگو بهره‌برداری نماییم. در پاسخ باید خاطرنشان نمود که به دلایلی که در ادامه به آنها پرداخته می‌شود بهتر است از رویکرد تلفیقی برای تدوین مدل کشور بهره‌برداری نماییم.

نظام حقوقی اتحادیه اروپایی و ایالات متحده‌آمریکا هر دو به طور همزمان در طول دهه ۱۹۷۰ توجه خود را به حفاظت از داده‌ها معطوف کردند. در آغاز سال ۱۹۸۰ سازمان همکاری و توسعه اقتصادی رهنمودهای خود در رابطه با حفاظت از حریم خصوصی داده را منتشر کرد و به دنبال آن این دو نظام

حقوقی به نحوی سعی کردند اصول مندرج در این سند را وارد قوانین خود کنند. رهنمودهای سازمان همکاری و توسعه اقتصادی جز اسناد حقوقی نرم[۴] محسوب می‌شوند و اصول اساسی آن به عنوان حداقل استانداردهای بین المللی محسوب می‌شوند. به دنبال انتشار این سند شورای اروپا در راستای ارائه حمایت یکدست از داده ها کنوانسیون حفاظت از افراد در برابر پردازش خودکار داده‌های شخصی را به تصویب رساند. مقررات این کنوانسیون در مقایسه با رهنمودهای سازمان همکاری و توسعه اقتصادی، کنوانسیون شورای اروپا دربردارنده مقررات سختگیرانه‌ای بود. تا این زمان رویکرد هر دو نظام حقوقی دربردارنده اصول کم و بیش مشابهی بود با اینحال گسیختگی بین رویکرد دو نظام زمانی آغاز شد که شورای اروپا از دولت‌های عضو خود خواست به کنوانسیون ملحق شوند و قوانین داخلی خود را مطابق با آن تنظیم کنند. از این زمان هر یک از دو نظام حقوقی راه خود را پیش گرفتند. اروپا با تجربه تلخی که از جنگ جهانی دوم و نقض حریم خصوصی داشت حریم خصوصی و به تبع آن به مرور حق حفاظت از داده را به عنوان یک حق بشری مورد حمایت قانون قرار داد. در مقابل، حریم خصوصی و داده‌های شخصی در ایالات متحده آمریکا با حق آزادی بیان، آزادی تجارت مواجه شد و در پرتو آنان تعدیل گردید. این تفاوت در نگرش باعث شده است این دو نظام حقوقی در دو سطح با یکدیگر تفاوت‌های عمیقی داشته باشند: ۱) شیوه قانون‌گذاری برای حمایت از حریم خصوصی و ۲) تفاوت در سطح حمایت قانونی. اتحادیه اروپایی نظام حفاظت از داده‌های شخصی اشخاص حقیقی را بر مبنای یک قانون واحد و جامع بنیان نهاده است؛ آغازگر این مدل از حفاظت از داده دستورالعمل حفاظت از داده‌های شخصی مصوب ۱۹۹۵ بود که در نهایت مقررات عمومی حفاظت اتحادیه اروپا جایگزین آن شد. برخلاف مدل حق محور و جامع در اتحادیه اروپایی، حریم خصوصی داده‌ها در نظام حقوقی ایالات متحده آمریکا از طریق مجموعه‌ای از قواعد کامن لا، قوانین فدرال، قوانین ایالتی و قانون اساسی برخی ایالات مورد حفاظت قرار گرفته است. به طورکلی عدم وجود تعریف واحد از داده‌های شخصی باعث شده است در نظام حقوقی ایالات متحده حمایت ضعیف تری نسبت به اطلاعات افراد در قانون و مقررات نوشته فراهم شود، در مقابل مدل اتحادیه اروپایی با تعریف گسترده از اطلاعات و داده‌های شخصی بستر حمایت گسترده و جامعی را فراهم کرده است. موفقیت مقررات عمومی حفاظت از داده اتحادیه اروپایی را از تعداد زیاد کشورهایی که قوانین داخلی خود را مبتنی بر آن تنظیم کرده اند می‌توان سنجید (Greenleaf, 2019).

[۴] Soft law instrument

تجربه برخی از نظام‌های حقوقی از جمله ایالات متحده نشان داده است که این نظام حقوقی با اتکا به شیوه خودتنظیم‌گری توانسته حمایت موثر و کاملی که با مقتضای خواسته‌های افراد همسو باشد ارائه دهد. توضیح بیشتر آنکه رویکرد غالب در ایالات متحده امریکا این است که قانونگذاری می‌تواند مانعی برای رشد و توسعه نوآوری در فناوری‌های نوظهور باشد و احتمال دارد از نوآوری جلوگیری کند. صنایع مختلف رویکرد خود تنظیم‌گری برای حمایت از حریم خصوصی و حفاظت از داده را انتخاب کردند. بنابراین امریکا با قانونگذاری مجزا و مستقل مخالف است به عنوان مثال در سطح فدرال قانون جامعی برای حفاظت از اطلاعات افراد وجود ندارد به همین منظور برای مسئول تلقی کردن ارائه‌دهندگان خدمات اینترنت اشیا در برابر نقض حریم خصوصی افراد به قوانین معدود و پراکنده فدرال از جمله قانون مسئولیت‌پذیری و انتقال‌پذیری بیمه سلامت مصوب ۱۹۹۶ و قانون حفاظت از حریم خصوصی آنلاین کودکان اتکا خواهد کرد. همان‌گونه که مشخص است این قوانین حوزه محدودی را در برمی‌گیرد. از این‌رو تمامی دستگاه‌های مبتنی بر اینترنت اشیا تحت شمول قانون قرار نمی‌گیرند. بنابراین شرکت‌ها رویکرد خودتنظیم‌گری را در پیش‌گرفته‌اند و رویه‌های قانونی قضات در این کشور، به صورت خودکار این حوزه را قاعده‌مند می‌نماید. اما در برخی موارد کاربران بدون توجه به خط‌مشی‌های حریم خصوصی سازمان‌های عمومی و خصوصی اطلاعات خود را در اختیار آنان قرار می‌دهند، بی‌آنکه در آتیه بتوانند تغییراتی در آن ایجاد کنند. فارغ از این همراه با گسترش فناوری اطلاعات، تهدیدات امنیتی از جمله دسترسی غیرمجاز به داده‌های اشخاص با روش‌های نوین تسهیل یافته است. صرف اتکا و اعتماد به سازمان ها و کسب‌وکارها بر اینکه الزامات امنیتی لازم برای حفاظت از داده‌های افراد را رعایت خواهند کرد نمی‌تواند گزینه مناسبی برای حفاظت از حریم خصوصی افراد باشد. به‌همین علت و به دلیل فقدان قانون جامع در حوزه حفاظت از داده شخصی در سطح فدرال و وجود نهادهای پراکنده برای نظارت بر حریم خصوصی از یکسو و اتکای اصلی به رویکرد خودتنظیم‌گری، جهت پیشگیری از تضییع حقوق شهروندان، کمیسیون تجارت فدرال ایالات متحده امریکا به‌عنوان یک آژانس مستقل با مأموریت اصلی حمایت از حقوق و منافع مصرف‌کننده سعی در پرکردن خلاءهای موجود درنظر گرفته شده است. رویکرد ایالات متحده امریکا بی‌بدیل و منحصر به فرد است و از کارآیی لازم برای این کشور برخوردار است؛ لیکن اقتباس از این الگو برای ایران با معایب و مضرات ذیل‌الذکر همراه است:

نخست آنکه نظام حقوقی ایران مبتنی بر قانون نوشته و واحد است. نداشتن قانون متمرکز، با نظام حقوقی کشور همخوانی ندارد. بنابراین عدم تصویب قانون واحد و تکیه بر مقررات پراکنده و معدود

هزینه‌های بسیاری به همراه دارد. دوم آنکه ضعف عملی قضات در ایران و بی‌اعتمادی تاریخی به قوه قضاییه در کشور باعث می‌شود که نتوان برای قاعده‌مند کردن حوزه فناوری‌های نوظهور به رویه‌های قضایی صادره از قضات اتکاء نمود. سوم آنکه نظام خود تنظیم‌گری برای نظام حقوقی کشور ما، شهروندان و شرکت‌های موجود به گونه مطلوب جا نیفتاده و قطعاً با شکست و هزینه‌های هنگفتی همراه خواهد بود. چرا که نظام حقوقی ایران در این حوزه تازه گام نهاده است و صرف اتکا به رویکرد خودتنظیم‌گری نمی‌تواند تضمین‌های حقوقی کافی برای حفاظت از داده‌های شخصی ارائه دهد و ممکن است موجب هدر رفت سرمایه‌های ملی گردد.

به‌نظر می‌رسد اقتباس از مقررات سخت‌گیرانه ایالات متحده امریکا در مورد مسائل مربوط به حمایت از حریم خصوصی و حفاظت از داده‌های شخصی در حوزه بهداشت و کودکان برای تدوین مدل ایران مطلوب و مورد استفاده باشد. وارد نمودن کدهای دستوری خودتنظیم‌گری در برخی موارد درکسب-وکارهای آنلاین در ایران آغاز شده؛ هرچند از غنای مطلوبی برخوردار نیست لیکن می‌تواند به‌عنوان مقدمه، زمینه‌هایی برای آشنایی نظام حقوقی کشور، شهروندان و قضات با خودتنظیم‌گری را فراهم نماید.

با عنایت به تأسی بسیاری از نظام‌های حقوقی دنیا از مدل اتحادیه اروپایی و باتوجه به این نکته که نظام حقوقی ایران بر مبنای نظام حقوقی رومی-ژرمن و مبتنی بر حقوق نوشته است؛ لذا مدل اتحادیه اروپا با توجه به آنچه پیشتر به طور مبسوط مورد بررسی قرار گرفت، به عنوان یکی از موفق‌ترین رویکردهای موجود در حوزه حمایت از حریم خصوصی و حفاظت از داده می‌تواند الگوی مناسبی برای نظام حقوقی ایران باشد. آشنایی ذهنی شهروندان، شرکت‌ها، بخش‌های مختلف دولتی و خصوصی و قضات با این مدل نیز در پذیرش آن به عنوان الگوی مناسب برای ایران، بی‌تأثیر نیست. در این مدل، مفهوم حق حریم خصوصی، حق بر حفاظت داده به وضوح تبیین و به رسمیت شناخته شده است. این حقوق به درستی از یکدیگر تفکیک شده، سپس چارچوب حفاظت از داده و قواعد آن به رشته تحریر درآمده؛ قواعد به طور متمرکز در یک متن واحد قرار گرفته و از تصویب مقررات پراکنده و جزئی پرهیز شده است. در این رویکرد حق‌محور، اصول پردازش داده‌های شخصی، حقوق و تکالیف کنترل-گران و پردازش‌گران داده به تدقیق مورد بررسی و قاعده‌گذاری قرار گرفته؛ حقوق افراد موضوع داده برای حفاظت از اقراد در برابر پردازش داده‌های شخصی مشخص شده است. هدف از وضع قواعد حفاظت از داده‌های شخصی این است که فرد را در موقعیتی قرار دهد که بتواند تصمیم بگیرد چه

اطلاعاتی و به چه میزانی از او در اختیار دیگران قرار می‌گیرد و این اطلاعات به چه نحوی از حیث کمیت و کیفیت پردازش شود. نهاد نظارتی مستقل با اختیارات ویژه در مقام حل و فصل اختلافات و در صورت لزوم جبران خسارت ناشی از پردازش داده و رسیدگی به نقض مقررات مربوط به حفاظت از داده می‌باشد. انتخاب ماهیت روش‌های جبران خسارت (مدنی/کیفری/اداری) به‌صلاحدید نهاد نظارتی کشورهای عضو صورت می‌گیرد. علاوه بر این، نهاد نظارتی می‌تواند مقام‌های قضایی را از نقض مقررات کمیسیون مطلع و در صورت لزوم اقامه دعوی نماید. در این مجال قصد بازگویی مقررات اتحادیه اروپا را که در مبحث‌های پیشین به تدقیق مورد بررسی قرار گرفته را نداریم؛ لیکن به علت مأنوس بودن مدل اتحادیه اروپایی با نظام حقوقی کشور، به نظر می‌رسد شرکت‌ها، شهروندان، بخش-های دولتی و حاکمیتی، قضات، کنترل‌گران و پردازش‌گران با داشتن قوانین مدون و واحد قرابت ذهنی بیشتری دارند.

در میان اسناد و منابع موجود در اتحادیه اروپایی اشاره مستقیم به قوانین و مقررات قابل اعمال در حوزه اینترنت اشیا نشده است. اما نظریه شماره ۸/۲۰۱٤ تحت عنوان «تحولات اخیر در اینترنت اشیا» با این استدلال که داده‌های جمع‌آوری شده در شمول تعریف داده شخصی مقرر در دستورالعمل حفاظت از داده مصوب ۱۹۹۵ قرار می‌گیرند و افراد درگیر در صنعت اشیا که داده‌های افراد را پردازش می‌کنند ذیل عنوان پردازش‌گر و کنترل‌گر قرار می‌گیرند، دستورالعمل اشاره شده را در این حوزه قابل اعمال بیان می‌دارد. بهره‌گیری از این راهکار در نظام حقوقی ایران نیز، می‌تواند مورد استفاده قرارگیرد؛ چرا که اکثر تلاش‌های فعلی در حوزه تقنین در سال‌های اخیر (که اکثراً هم بی‌نتیجه مانده‌اند.) در جهت قانونگذاری پیرامون قواعد مربوط به داده‌های شخصی بوده و در متون، حکمی پیرامون وضعیت داده در اینترنت اشیا موجود نمی‌باشد. دلیل مغفول ماندن از این مقوله، می‌تواند همه‌گیر نشدن این فناوری در کشور نیز باشد. با استفاده از راهکار اتحادیه اروپایی می‌توان طی تصویب یک ماده واحده، احکام موجود را به داده‌های مورد استفاده در اینترنت اشیا، تسری داد.

از معایب بهره‌گیری از مدل نظام حقوقی اتحادیه اروپایی این است که قانونگذار اتحادیه اروپایی قواعد متراکم، جزئی و متمرکز را وضع می‌نماید لیکن با گذشت زمان، بر اساس روند شتابان و رو به توسعه فناوری‌های نوپدید و با توجه به اشکالات و نواقصی که در قانون وجود دارد، سریعاً قواعد را به روزرسانی و اصلاح می‌کند. لیکن متأسفانه در نظام حقوقی ایران تصویب، تصحیح و تغییر قانون با روند و تشریفات طولانی همراه است که قاعدتاً باعث می‌شود نظام حقوقی از روند پیشرفت تکنولوژی

عقب بماند. مطول و جزئی نگاشتن احکام و ضمانت اجراهای قانونی و عادت نظام حقوقی به یافتن تمام راهکارها در قانون نوشته، سبب می‌شود در اجرا ابتکار عمل و خلاقیت را از مقام ناظر و قوه قضاییه ستانده شود و سکوت، ابهام واجمال قانون در موارد نوظهور، عملاً تصمیم‌گیری دراین حوزه را دشوار می‌نماید و بلاتکلیفی شهروندان، دستگاه‌های مرتبط و شرکت‌ها را به دنبال دارد. از سوی دیگر تنظیم موسع و پیش‌بینی جزئی و دقیق قواعد در حوزه فناوری‌های نوظهور می‌تواند مانعی برای رشد و توسعه این صنعت قلمداد گردد. شناخت وضع موجود از یک‌سو و بهره‌گیری ازفواید مقایسه تطبیقی از سوی دیگر، ما را در رسیدن به خاستگاه پژوهش حاضر؛ که همانا دستیابی و تدوین الگوی مطلوب و مدل بومی مبتنی بر نظام حقوقی کشور در این موضوع است یاری می‌نماید...

در حالی که کشورهای عضو اتحادیه اروپا و نیز نظام حقوقی ایالات متحده از سال‌ها پیش در حال گسترش قواعد حاکم بر حفظ حریم خصوصی خود بر داده‌های شخصی بودند جمهوری خلق چین تنها در چند سال اخیر توجه خود را معطوف کرده است. قانون اساسی این کشور به عنوان عالی‌ترین قانون همانند قانون اساسی ایران تنها به جنبه‌های سنتی حریم خصوصی توجه داشته است و اشاره‌ای به حق حفاظت از داده‌ها نداشته است (Pernot-Leplay, 2020, P. 66) با اینحال چنان که اشاره شد حقوقدانان با استناد به اینکه قانون اساسی چین به کرامت و منزلت فرد توجه داشته است[۵] و حریم خصوصی نیز جنبه‌ای از احترام به کرامت انسان محسوب می‌شود اعلام داشته‌اند حریم خصوصی به طور کلی تحت لوای این قانون می‌باشد. بر اساس آموزه‌های حقوق تطبیقی هر کشور در مواجهه با چالش‌های جامعه خود ابتدا سعی می‌کند به راهکارهای قانونی که در دیگر کشورها برای همان چالش استفاده شده است نظری بیندازند و سپس بر اساس مبانی خود آن راهکار را وارد نظام حقوقی خود کنند. نظام حقوقی چین به علت فقدان تجربه در این حوزه ابتدا با شیوه آزمون و خطا مسیر نظام حقوقی ایالات متحده را پیمود و همانند آن در برخی حوزه‌ها اقدام به قانون‌گذاری کرد. با توسعه و رسوخ اصول بین‌المللی حاکم بر حفاظت از داده از یکسو و تصویب مقررات عمومی حفاظت از داده اتحادیه اروپایی به عنوان قانونی جامع و همه شمول در حوزه حفاظت از داده‌های شخصی از سوی دیگر، قانون‌گذار چین برای اجتناب از ایزوله شدن کشور در سطح بین‌المللی با تأسی از مقررات عمومی حفاظت از داده اقدام به طرح مدل جدید خود کرد. قانون‌گذار جمهوری خلق چین پس از به رسمیت شناختن حق حریم خصوصی و حق حفاظت از اطلاعات شخصی در قانون مدنی خود در قالب حقوق مربوط به شخصیت افراد، قانون حمایت از اطلاعات شخصی جمهوری خلق چین و قانون امنیت داده

[۵] اصل ۳۸ قانون اساسی جمهوری اسلامی ایران

جمهوری خلق چین به تصویب رساند. قانون حمایت از اطلاعات شخصی که در تقنین آن از مقررات عمومی حفاظت از داده الگوبرداری شده است، مؤسسات عمومی و خصوصی و کسب و کارها را به طور یکسان ملزم کرده از اصول و الزامات حاکم بر پردازش داده‌های شخصی که مشابه آن در نظام حقوقی اتحادیه اروپایی مشاهده می‌شود پیروی کنند. قانون‌گذار جمهوری خلق چین برای تطابق قوانین با ارزش‌ها و اهداف جامعه و توجه به لزوم اعمال حاکمیت دولت در عرصه اطلاعات شهروندان در قانون امنیت داده جمهوری خلق چین برای کنترلگران و پردازشگران تعهدات مضاعفی در نظر گرفت. بر اساس این قانون اشخاص مذکور موظف شده‌اند در سریع‌ترین زمان ممکن اطلاعات و داده‌هایی که توسط دولت معین می‌شوند در اختیار حکومت قرار دهند. این الزام به ویژه برای سرمایه‌گذاران خارجی و شرکت‌های فعال و کسب و کارهای مبتنی بر داده در چین همواره منشأ نگرانی و تنش با دولت چین بوده است(Pernot-Leplay, 2020, P. 116)

در ماده (٦٠) قانون حمایت ازاطلاعات شخصی چین، اداره امنیت سایبری و یکپارچه‌سازی سیستم‌های اطلاعاتی را به‌عنوان نهاد نظارتی مسئول برنامه‌ریزی جامع و هماهنگی، نظارت و مدیریت حمایت از اطلاعات شخصی در سطح جمهوری خلق چین درنظر گرفته است. استفاده و الگوبرداری از رویکرد چین، می‌تواند برای کشور ما در بخش الگوبرداری از اتحادیه اروپا به دلایل پیش‌تر گفته شده مطلوب باشد ولی در حوزه رویکرد سخت‌گیرانه امنیتی که چین در پیش‌گرفته باید به قانونگذار ایران هشدار داد که پررنگ کردن نقش دولت و سخت‌گیری شدید امنیتی در این حوزه منجر به شکست شرکت‌های فعال و کسب و کارهای مبتنی بر داده در بازار و تهدیدی برای سرمایه‌گذاری خارجی در کشور باشد. مزیتی که رویکرد امنیت‌محور چین دارد و برای ایران نیز قابل بهره‌برداری می‌باشد این نکته است که در ماده (۱۷) قانون امنیت داده جمهوری خلق چین مصوب ۲۰۲۱، دولت را به ارائه طبقه‌بندی داده‌های شخصی بر اساس اهمیت داده‌ها در توسعه اقتصادی و اجتماعی و همچنین میزان آسیب به امنیت ملی، منافع عمومی و حقوق و منافع قانونی افراد موضوع داده، الزام نموده است. بنابراین استفاده از این روش و طبقه‌بندی داده‌ها در نظام حقوقی کشور می‌تواند مرز مداخله دولت را تعیین نماید و از حساسیت‌ها و نگرانی‌های بخش خصوصی و شهروندان در خصوص دسترسی و سوء استفاده‌های احتمالی دولت در این حوزه را کاهش دهد.

٤- نتیجه‌گیری و پیشنهاد

رشد و گسترش روزافزون اینترنت از یک‌سو و انقلاب فناوری اطلاعات‌وارتباطات از سوی دیگر، تمام نظام‌های اجتماعی و حقوقی را تحت‌الشعاع خود قرار داده است و قانون‌گذاران را با وضعیت نوپدیدی مواجه کرده است. کشور ایران نیز از این تأثیر مستثنی نبوده و بررسی نظام سیاسی و حقوقی کشور نشان می‌دهد تنظیم مقررات در حوزه فضای مجازی در سال‌های اخیر به ویژه پس از تشکیل شورای عالی فضای مجازی شتاب بیشتری به خود گرفته است. نظام حقوقی ایران در مقایسه با سایر نظام‌های منتخب سابقه چندانی در حوزه مقررات‌گذاری اینترنت ندارد و از این نظر یک نظام نوپا می‌باشد. برنامه‌ریزی و سرمایه‌گذاری در پروژه‌های مبتنی بر فناوری‌های نوظهور به ویژه فناوری اینترنت اشیا در کشورمان به طور جدی از سال ۱۳۹۵ آغاز شده است که از جمله می‌توان به طرح‌ها و استارت آپ‌های بخش حمل‌ونقل، محیط زیست، خودرو هوشمند، موقعیت‌یابی هوشمند، کشاورزی، مدیریت انرژی اشاره کرد. با توجه به اهمیت موضوع و نظر به اینکه شناخت اعضای جامعه از حقوق خود می‌تواند نقش بسیار سازنده‌ای برای نیل به هدف قانون‌گذار باشد؛ لازم است در یک قانون جامع اصول و الزامات و ضمانت اجراهای غیرکیفری برای بازیگران این حوزه مقرر گردد و نهادی غیر از مراجع دادگستری عهده‌دار رسیدگی به درخواست‌ها و تقاضای افراد در رابطه با نقض داده‌هایشان تعیین شود. در قوانین فعلی نظام حقوقی ایران از جمله قانون انتشار و دسترسی آزاد به اطلاعات، قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای مصادیقی یافت می‌شود که شباهت‌هایی با قوانین موجود در سطح بین‌الملل به ویژه مقررات عمومی حفاظت از داده و قانون حمایت از اطلاعات شخصی چین دارند. با استخراج اصول و قواعد از قوانین موجود در نظام داخلی و عاریه برخی از موارد دیگر از دو قانون اشاره شده می‌توان نظام اثربخشی برای حمایت از حریم خصوصی و حفاظت از داده در نظام حقوقی تدوین کرد؛ این استدلال با بررسی کلیات طرح حمایت از حریم خصوصی و حفاظت از داده و اطلاعات شخصی که در تدوین آن از مقررات عمومی حفاظت از داده الگوبرداری شده است تائید می‌شود. با توجه به اینکه این لایحه اولین تلاش برای قانون‌گذاری برای حفاظت از داده‌های شخصی می‌باشد بی‌شک خالی از خلاء نمی‌باشد. با توجه به گستردگی و پیچیدگی موضوع نمی‌توان تنها به قانون‌گذاری اکتفا کرد. بخشی از تلاش قانون‌گذاری باید به گونه‌ای باشد که اشخاص درگیر در این حوزه به شفافیت عمل تشویق شوند؛ یکی از طرق نیل به این هدف تشویق خودتنظیمی و شفافیت عمل برای پردازندگان داده به ویژه کسب و کارهای مبتنی بر داده می‌باشد که می‌تواند از طریق ارائه تشویق‌ها و معافیت‌های قانونی حاصل شود. یکی دیگر از خلاءهای موجود، عدم پیش‌بینی نقش فعال و پویا برای دولت جهت

مداخله و تنظیم‌گری می‌باشد. تجربه نظام‌های دیگر نشان می‌دهد با توجه به نوپدید بودن موضوع و آثار گسترده آن بر جامعه مداخله دولت‌ها برای حفاظت و حمایت از حقوق اشخاص و منافع عمومی و امنیت ملی یک بایسته است. در نظام حقوقی ایران با توجه به جدید بودن موضوع هنوز اجماعی درباره نقش دولت در این حوزه شکل نگرفته است؛ لیکن تلفیقی از رویکردهای سه‌گانه با ابتنای اصلی بر نظام اتحادیه اروپایی پیشنهاد می‌شود. استفاده از رویکرد خود تنظیم‌گری امریکایی در شرکت‌ها، استفاده از ماده واحدهای جهت شمولیت احکام مواد قوانین مرتبط به داده در حوزه اینترنت اشیا نظیر مدل اروپایی، اقتباس از مدل امریکایی نسبت به حساسیت در مورد حفاظت از داده‌های مربوط به حوزه سلامت و بهداشت عمومی و کودکان و اقتباس از مدل چین در طبقه بندی اطلاعات و عدم تجربه سیستم قانون‌گذاری تفرقی پیشنهاد شده است.

منابع

- آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات مصوب هیئت وزیران در تاریخ ۱۳۹۳/۰۸/۲۱
- آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ریاست قوه قضاییه در تاریخ۱۳۹۳/۰۵/۱۲
- آئین‌نامه تائید نمونه تجهیزات ارتباطی و فناوری اطلاعات مصوب کمیسیون تنظیم مقررات ارتباطات ۱۳۸۷/۰۹/۱۰
- آیین‌نامه داخلی شورای عالی فضای مجازی مصوب شورای عالی فضای مجازی در تاریخ ۱۳۹۱/۰٤/۱۰
- اساسنامه سازمان تنظیم مقررات و ارتباطات رادیوئی مصوب هیئت وزیران در تاریخ ۱۳۸۸/۱۱/۲۱
- اقدسی، فاطمه و محقق داماد، مریم سادات (۱٤۰۰). ابعاد حقوقی حریم خصوصی در اینترنت اشیا. **فصلنامه پژوهش‌های حقوقی میان‌رشته‌ای،۲،۲، صص. ۵۰-٦۷.**
- امیریان، امین و مالمیر، محمود و حیدری، مسعود (۱٤۰۰). تحلیل قانون جرایم رایانه ای در بستر جرم شناسی نظری. علوم خبری، ۱۰(۳۷)، ۲۲٤-۱۱۹.
- انصاری, باقر و عطار, شیما (۲۰۲۲). حمایت از داده‌ها در چین؛ مطالعهٔ تطبیقی با رویکرد حمایت از داده‌ها در امریکا و اتحادیهٔ اروپا. مطالعات حقوق تطبیقی، ۱۳(۱)، ۹۱-۱۱۳.
- انصاری، باقر (۱۳۸٦). حقوق حریم خصوصی. تهران: انتشارات سمت.
- تقوی فرد، محمدتقی محمدرضا و فقیهی، تقوا مهدی و جمشیدی، محمدجواد (۱۳۸۹). مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب. ۸۹، ۳۳۳-۳۰۱.
- حکم حکومتی تشکیل و انتصاب اعضای شورای عالی فضای مجازی در تاریخ ۱۳۹۰/۱۲/۱۷
- **حیدری، علی مراد و جعفری، علی** (۱۳۹۸). جرایم علیه داده‌پیام‌های شخصی در تجارت الکترونیکی. پژوهشنامه حقوق کیفری ۱ (۲۲)، ۵۱-۷٤.
- رییسی دزکی، لیلا و قاسمزاده لیاسی، فلور (۱۳۹۹). چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر. مجله حقوقی دادگستری، ۸٤(۱۱۰)، ۱۱۹-۱٤۲.
- رئوفی، علی اصغر و جمشیدی راد، محمد صادق (۱۳۹۹). اصول حاکم بر لایحه حریم خصوصی ۱۳۹۹. مبانی فقهی حقوق اسلامی، ۱۳(۲۵)، ۱۳۵-۱٦۰.
- زارعیان، داود و واحد، فائزه (۱۳۹۹). **بررسی حقوقی رگولاتوری‌های حمایت از داده. رسانه، ۳۱ (۱) صص٤۷-۷۲.**
- الزامات حاکم بر اینترنت اشیا در شبکه ملی اطلاعات مصوبه شورای عالی فضای مجازی در تاریخ ۱۳۹۷/۰۷/۳۰

- سند راهبردی جمهوری اسلامی ایران در فضای مجازی مصوبه شورای عالی فضای مجازی در تاریخ ۱٤۰۱/۰۵/۱۱
- شیوه‌نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی مصوب کمیسیون انتشار و دسترسی آزاد به اطلاعات در تاریخ ۱۳۹۸/۰۹/۱۰
- فروغی، فضل‌الله و برجی، محمدناصر و مصلحی، جواد (۱۳۹۳). مبانی ممنوعیت نقض حریم خصوصی در حقوق ایران و آمریکا. مطالعات حقوقی ٦(۳) ۱۳۷-۱۷۲.
- قانون اساسی جمهوری اسلامی ایران مصوب ۱۳۵۸ و اصلاحات بعدی
- قانون انتشار و دسترسی آزاد به اطلاعات مصوب مجلس شورای اسلامی در تاریخ ۱۳۸۷/۱۱/۰٦
- قانون آیین دادرسی کیفری مصوب مجلس شورای اسلامی در تاریخ ۱۳۹۲/۱۲/۰٤ با اصلاحات ۱۳۹٤/۰۳/۲٤
- قانون تجارت الکترونیکی مصوب مجلس شورای اسلامی در تاریخ ۱۳۸۲/۱۰/۱۷
- قانون جرایم رایانه‌ای مصوب مجلس شورای اسلامی در تاریخ ۱۳۸۸/۰۳/۰۵
- قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات مصوب مجلس شورای اسلامی در تاریخ ۱۳۸۲/۰۹/۱۹
- قبولی درافشان، محمدهادی و بختیاروند، مصطفی و آقا محمدی، اکرم (۱۳۹۷). حق فراموش شدن در ترازو: نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان؟!. پژوهش حقوق عمومی،۵۸، ۱۳۵-۱۱۳.
- قناد، فاطمه و علیقلی، امیره (۱۳۹۹). مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی. حقوق فناوری های نوین (حقوق قراردادها و فناوری های نوین)، ۱(۱)، ۳۲۲-۲۹۷.
- لطیف زاده، مهدیه و قبولی درافشان، سید محمدمهدی و محسنی، سعید و عابدی، محمد (۱٤۰۰). تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا. پژوهشنامه پردازش و مدیریت اطلاعات، ۳۷(۲)، ٤۷۲-٤۳۹.
- محسنی، فرید (۱۳۹۵). **حریم خصوصی اطلاعات (مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه). تهران: انتشارات دانشگاه امام صادق.**
- مرادخانی، فردین و تکلو، سمیه (۱٤۰۰). تعدد نهادهای قانون گذاری با تأکید بر جایگاه مصوبات شورای عالی فضای مجازی در نظام حقوقی ایران؛مطالعات حقوقی معاصر، ۱۲(۲۲)، ۲۵-٦۷
- مرکز پژوهش های مجلس. (۱۳۹۹). اینترنت اشیا (۱): فناوری ها، استانداردها و چالش ها.
- مرکز پژوهش های مجلس. (۱۳۹۹). اینترنت اشیا (۲): مقررات اینترنت اشیا و مقایسه قوانین آن در اتحادیه اروپا، آمریکا و چین
- منشور حقوق شهروندی مصوب ریاست جمهوری اسلامی ایران در تاریخ ۱۳۹۵/۰۹/۲۹

– موسموتی، ماریا (۱٤۰۱). تقنین قانون اثربخش، ترجمه آرین پتفت و آرتین جهانشاهی، تهران: انتشارات سمت.

– نوری، محمد علی و نخجوانی، رضا (۱۳۸۲). امضای سند در عصر کامپیوتر: حقوق تجارت الکترونیکی. وکالت، ۱٦، ۱–۸۰.

– هوشیدری فراهانی، فاطمه و حسن‌زاده، محمد و زندیان، فاطمه (۱۳۹۷). تبیین بسترهای پیاده‌سازی قانون انتشار و دسترسی آزاد به اطلاعات در ایران. راهبرد اجتماعی فرهنگی، ۷(۱)، ۳۹–٦۵.

– یاوری، اسدالله (۱۳۹۵). گزارش نشست علمی مفهوم و قلمرو حریم خصوصی در نظام حقوقی ایران مرکز مطبوعات و انتشارات قوه قضاییه.

– Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows, Strasbourg, 8.11.2001.

– Ali, Z., Ali, H., & Badawy, M. (2015). *Internet of Things (IoT): Definitions, Challenges and Recent Research Directions*. International Journal of Computer Applications, 128(1), 37-47. https://www.ijcaonline.org/research/volume128/number1/ali-2015-ijca-906430.pdf

– Banisar, D. (2006). The Right to Information in the Age of Information. In Human rights in the global information society. Massachusetts: MIT Press.

– Bennett, C. J. (2020). *The Modernized Convention 108+*. Centre for International Governance Innovation, 1-5.https://www.jstor.org/stable/resrep27512.8

– Bygrave, L. (2014). *Data Privacy Law—An International Perspective*. Oxford: University Press.

– California Consumer Privacy Act (CCPA) adopted by California State Legislature in 2018.

– Catuogno, L., & Turchi, S. (2015). *The Dark Side of the Interconnection: Security and Privacy in the Web of Things*. 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 205-212 https://doi.org/10.1109/IMIS.2015.86

– Charter of Fundamental Rights of the European Union [2000]

– Chiara, P. G. (2022). *The IoT and the new EU cybersecurity regulatory landscape*. International Review of Law, Computers & Technology, 1–20. https://doi.org/10.1080/13600869.2022.2060468

– Children's Online Privacy Protection Act of 1998.

– Civil Code of the People"s Republic of China (CCPRC), enacted on 2020.

– Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.

– Commission of The European Communities, Communication (90) 314 final, 13.9.1990.

– Commission of The European Communities, Communication (92) 422 final, 28.10.1992.

– Commission recommendation of 12 may 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification.

– Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data.

– Committee of ministers of the Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of ministers on 26 September 1973 at the 224th meeting of the ministers' Deputies.

– Committee of ministers of the Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted by the Committee of ministers on 20 September 1974 at the 236th meeting of the ministers' Deputies.

– Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609.

– Congressional Research Service. (2019). *Data Protection Law: An Overview* https://crsreports.congress.gov/product/pdf/R/R45631

– Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data adopted by Council of Europe in 1981.

– Cybersecurity Law of the People's Republic of China, enacted on 2016.

– Data Security Law of the People's Republic of China enacted on 2021.

– De Hert, P., & Papakonstantinou, V. (2014). *The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition.* Computer Law & Security Review, 30(6), 633–642. https://doi.org/10.1016/j.clsr.2014.09.002

– De Terwangne, C. (2021). *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*. Computer Law & Security Review, 1-18. https://doi.org/10.1016/j.clsr.2020.105497

– Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

– Directive 95/46/EC of the European Parliament and 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.

– EC Communication 2015: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, 6 May 2015.

– Esayas, S. (2015, October 15). *The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the "All or Nothing" Approach*. European Journal of Law and Technology, 6(2), 1-23. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746831

– European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. 2020. "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade".

– European Commission, Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things 2014.

– European Union Agency for Fundamental Rights and Council of Europe. (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

– Federal Trade Commission Act of 1914.

– Federal Trade Commission, (1998). *privacy online: a report to congress.*

– Federal Trade Commission, (2021). *Report to congress on privacy and security.*

– Federal Trade Commission. (2015). *Internet of Things: Privacy & Security in a Connected World*.

– https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

– Forgó, N., Hänold, S., & Schütze, B. (2017). *The Principle of Purpose Limitation and Big Data*. RePEc – Econpapers, 17-42. https://econpapers.repec.org/bookchap/sprperchp/978-981-10-5038-1_5f2.htm

– Ghorbani, H. R., & Ahmadzadegan, M. H. (2017). *Security challenges in internet of things: survey*. 2017 IEEE Conference on Wireless Sensors (ICWiSe), 6-12. https://doi.org/10.1109/icwise.2017.8267153

– Godkin, E. L., & Reputation, I. T. H. O. (1890). *The Rights of the Citizen*. Scribners. https://www.unz.com/print/Scribners-1890jul-00058/

– Gokhale, P., Bhat, O., & Bhat, S. (2007). *Introduction to IOT*. International Advanced Research Journal in Science, Engineering and Technology ISO, 3297(1), 41-44. https://doi.org/10.17148/IARJSET.2018.517

– González Fuster, G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. In Law, Governance and Technology Series. Springer International Publishing. https://doi.org/10.1007/978-3-319-05023-2

– Gubbi, H. & Buyya, R. & Marusic, S. & Palaniswami, M. (2013). *Internet of Things (IoT): A vision, architectural elements, and future directions*. Future Generation Computer Systems, 29, 7, pp. 1645–1660.

– Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.

– Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD).

– Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD) 1980.

– Haller, S. & Karnouskos, S. & Schroth, C. (2008). *The Internet of Things in an Enterprise Context.* Future Internet - FIS 2008, First Future Internet Symposium, pp. 1-15.

– Health Insurance Portability and Accountability Act of 1996 (HIPAA).

– Hert, P. J. A. de, & Gutwirth, S. (2006). *Privacy, data protection and law enforcement: Opacity of the individual and transparency of power*. Privacy and the Criminal Law, 61–104. https://research.tilburguniversity.edu/en/publications/privacy-data-protection-and-law-enforcement-opacity-of-the-indivi

– Hoofnagle, C. J. (2016). Federal Trade Commission Privacy Law and Policy. Cambridge University Press.

– IEEE (2015). *Internet of Things/M2M from Research to Standards: The Next Steps.* Available at: http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standardsnext-steps

– International Telecommunication Union (ITU) (2012). *Overview of the Internet of things*.https://www.itu.int/rec/T-REC-Y.2060-201206-I

– Kelly, C. (2022). *Data Privacy Regulations in the United States, China, and the European Union*. Honors College Theses, 1-24. https://digitalcommons.georgiasouthern.edu/honors-theses/756/

– Kochman, B. (2018). *Tech Giants Want Uniform Privacy Law, But No GDPR* https://www.law360.com/articles/1086064/tech-giants-want-uniform-privacy-law-but-no-gdpr

– Kounoudes, A. D., & Kapitsaki, G. M. (2020). *A mapping of IoT user-centric privacy preserving approaches to the GDPR*. Internet of Things, 11, 1-41. https://doi.org/10.1016/j.iot.2020.100179

– Kounoudes, A. D., & Kapitsaki, G. M. (2020). *A mapping of IoT user-centric privacy preserving approaches to the GDPR*. Internet of Things, 11, 1-42. https://doi.org/10.1016/j.iot.2020.100179

– Kubben, P., Dumontier, M., & Dekker, A. (2019). *Fundamentals of Clinical Data Science*, Springer Nature. https://library.oapen.org/handle/20.500.12657/22918

– Kuner, C., Bygrave, L., Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR)_ A Commentary*. Oxford University Press.

– Legal Committee of Parliamentary Assembly, Doc. 2326, report of the Legal Committee, 1967 - 19th Session - Third part.

– Lombardi, M. & Pascale, F. & Santaniello, D. (2021). *Internet of Things: A General Overview between Architectures, Protocols and Applications*. ***Information***, 12, 2, pp. 1-20.

– Milaj, J. (2020). *Safeguarding Privacy by Regulating the Processing of Personal Data – An EU Illusion?* European Journal of Law and Technology, 11(2). https://ejlt.org/index.php/ejlt/article/view/787

– Modernised Convention For The Protection Of Individuals With Regard To The Processing Of Personal Data adopted by Council of Europe in 2018.

– Nordic conference of jurists the right of privacy international commission of jurists geneva. (1967). https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-1967-eng.pdf

– Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). *Security Requirements for the Internet of Things: A Systematic Approach.* Sensors, 20(20), 1-35. https://doi.org/10.3390/s20205897

– Parliamentary Assembly, Recommendation 509 (1968) on Human rights and modern scientific and technological developments.

– Parliamentary Assembly, Recommendation 890 (1980) on protection of personal data.

– Prosser, W. L. (1960). *Privacy*. Cal. L. Rev., 48(3).

– Purtova, N. (2018). *The law of everything. Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology, 10(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

– Qi, A., Shao, G., & Zheng, W. (2018). *Assessing China's Cybersecurity Law*. Computer Law & Security Review, 34(6), 1342–1354. https://doi.org/10.1016/j.clsr.2018.08.007

– Radio Equipment Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014.

– Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies. of the Community and on the free movement of such data.

– Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

– Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

– Regulation 2016/679 - 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).

– Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing [1975].

– Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing [1979].

– Richards, D. (1977). *Unnatural Acts and the Constitutional Right to Privacy: A Moral Theory*. Fordham Law Review, 45(7), 1281-1348. https://ir.lawnet.fordham.edu/flr/vol45/iss7/2/

– Richards, N. M. (2011). *The Limits of Tort Privacy*. J. Telecommun. High Technol. Law, 357-384.

– Rou, T. (1990). ***Chinese Civil Law***. Beijing: The Press of Laws.

– Sharma, S., Menon, Pranav. (2020). *Data privacy and GDPR handbook*. Wiley Press. http://www.worldcat.org/title/data-privacy-and-gdpr-handbook/oclc/1129177348

– Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). *Security, privacy and trust in Internet of Things: The road ahead*. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

– Singh, A. (2013). *Protecting Personal Data As A Property Right*. ILI Law Review, 123-139. https://ili.ac.in/pdf/p9_atul.pdf

– Smith, N. (2019). *Protecting Consumers in the Age of the Internet of Things Protecting Consumers in the Age of the Internet of Things*. st. john's law review 93, 12, 852-881.

– Smith, N. (2019). *Protecting Consumers in the Age of the Internet of Things*. St. JOHN's L. REV, 93, pp. 851-881.

– Solove, D. J. (2008). *Understanding Privacy*. Cambridge: Hardward university press.

– Solove, D. J., & Hartzog, W. (2013). *The FTC and the New Common Law of Privacy*. SSRN Electronic Journal, 583-676.

– Stam, A., & Kleiner, B. (2020). *Data anonymisation: legal, ethical, and strategic considerations*, Swiss Centre of Expertise in the Social Sciences, 1-15 https://doi.org/10.24449/FG-2020-00011

– Standards for Privacy of Individually Identifiable Health Information adopted by The U.S. Department of Health and Human Services in 1998.

– Tamò-Larrieux, A. (2018). Designing for Privacy and its Legal Framework. In Law, Governance and Technology Series. Springer International Publishing. https://doi.org/10.1007/978-3-319-98624-1

– The amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108), allowing the European Communities to accede, adopted by the Committee of Ministers on 15 June 1999, in Strasbourg.

– The China Personal Information Protection Law (PIPL) enacted on 2021.

– The Security Standards for the Protection of Electronic Protected Health Information adopted by The U.S. Department of Health and Human Services in 2003.

– The Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005

– The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data, Opinion 4/2007 on the concept of personal data.

– Thinakaran, K., Dhillon, J. S., Gunasekaran, S. S., & Chen, L. F. (2018). *Developing a Privacy Compliance Scale for IoT Health Applications*. Computer Science and Information Technology, 6(4), 54–62.

– Turner, S., Galindo Quintero, J., Turner, S., Lis, J., & Tanczer, L. M. (2020). *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment*. New Media & Society, 23(10), 2862-2881.

– Tzanou, M. (2017). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publication.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3076400#:~:text=Maria%20Tzanou

– United Nations Guidelines for the Regulation of Computerized Personal Data Files 1990.

– van der Sloot, B. (2017). *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?*. Law, Governance and Technology Series, 3–30. https://doi.org/10.1007/978-3-319-50796-5_1

– Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

– Wachter, S. (2017, December 6). *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR*. ssrn, 1-22. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083554

– Wang, H. (2011). *Protecting Privacy in China*. Springer Berlin Heidelberg.

– Warren, S. D., & Brandeis, L. D. (1890). *The Right to Privacy*. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160

– Yang, LX. (2006). *The law of personality rights*. Beijing: Court Press.

– Yu, C., Zhang, L., Zhao, W., & Zhang, S. (2019). *A blockchain-based service composition architecture in cloud manufacturing*. International Journal of Computer Integrated Manufacturing, 33(7), 701–715. https://doi.org/10.1080/0951192x.2019.1571234

– Zhang, XB. (2004). *The legal protection of the right to privacy*. Beijing: The Masses Press.

– Zhengxin, H. (2020). *China Enters an Era with a Civil Code. Www.chinajusticeobserver.com. Retrieved August 16, 2022, from https://www.chinajusticeobserver.com/a/china-enters-an-era-with-a-civil-code*

آراء قضایی

– Case C-615/13 P Client Earth (CJEU , 16 July 2015)
– CJEU, Case C-25/17, *Jehovan todistajat*, 10 July 2018
– ECJ, Google Spain v AEPD and Mario Costeja González,C-131/12 ,2014
– Estate of Elvis Presley v Russen (513 F Supp 1339 (1981).
– Judgment of the European Court of Justice C-101/2001of 06.11.2003 (Lindqvist), §27
– Katz v. United States, 389 U.S. 347 (1967)
– Katz v. United States, 389 U.S. 347 (1967)
– Mario Costeja González vs. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos 2014
– Whalen v. Roe, 429 U.S. 589 (1977)

– http://english.mofcom.gov.cn/article/lawsdata/chineselaw/200211/20021100049916.shtml
– https://dr.shiravi.com/archives/4723
– https://ito.gov.ir/fa/afta/
– https://www.cra.ir/commission
– https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act
– https://www.usatoday.com/story/tech/news/2018/09/26/amazon-attgoogle-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002
– https://filter.internet.ir/index.html#
– https://www.law360.com/articles/1086064/tech-giants-want-uniform-privacy-law-but-no-gdpr
– https://eur-lex.europa.eu/eli/dir/2002/58
– https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001R0045
– https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679R(02)&from=EN
– https://gdpr-info.eu/recitals/no-26
– https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF
– https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680R(01)&rid=3

– https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf