



فصلنامه علمی مطالعات حقوق بشر اسلامی



حق بر خودمختاری داده‌های شخصی در پرتو حقوق اسلامی و نظام بین‌المللی حقوق بشر:

چالشی در مرز میان اختیار انسانی و کنترل هوشمند رفتارها

محمدصادق ذوقی^۱، رحمان نجفی سیار^۲

چکیده

این پژوهش با تمرکز بر حق بر خودمختاری داده‌های شخصی می‌پرسد که در چه حدودی می‌توان پیش‌بینی‌گری الگوریتمی را با کرامت انسانی، اختیار واقعی و حاکمیت فرد بر پیرامتن اطلاعاتی او سازگار دانست. مراد از خودمختاری داده‌ای در این مقاله توانایی شخص در کنترل مراحل گردآوری، پردازش، تحلیل و استفاده ثانوی از داده‌های مربوط به خود است و حیثیت داده‌ای به مجموعه برچسب‌ها، امتیازها و پروفایل‌هایی اشاره دارد که سامانه‌های هوشمند بر مبنای آنها درباره فرد قضاوت و تصمیم‌سازی می‌کنند. بر پایه روشی تحلیلی-هنجاری و تطبیقی میان فقه امامیه و نظام بین‌المللی حقوق بشر نشان داده می‌شود که تصمیم‌های متکی بر الگوریتم، هر گاه آثار جدی بر حیثیت، فرصت‌ها و آزادی‌های کنشی اشخاص بر جای گذارند، تنها زمانی از مشروعیت هنجاری برخوردارند که در چهارچوب قواعد سخت صیانت از خلوت، منع تجسس و لاضرر و نیز اصول قانون‌مندی، ضرورت و تناسب مهار شوند. منظومه‌ای از نهی تبعی و تجسس، قاعده لاضرر، حرمانت حریم و سلطنت بر شئون شخصی در فقه امامیه ب|ا حق حمایت از داده‌ها، منع تصمیم صرفاً خودکار، الزام پاسخ‌گویی و امکان بازبینی انسانی در حقوق بشر معاصر هم‌نشین می‌شود و معیارهای عملی همچون حداقل‌گرایی داده، تحدید غرض، شفافیت دلایل موثر، ممیزی تبعیض، اطلاع‌رسانی معنادار، امکان اعتراض موثر و جبران خسارت را پشتیبانی می‌کند. مقاله در پرتو این مبانی نشان می‌دهد که می‌توان پیش‌بینی‌گری را از ابزار کنترل رفتار به ابزار خدمت‌گزار عدالت رویه‌ای بدل کرد و الگویی اسلامی و حقوق بشری برای حکمرانی هوش مصنوعی در سطوح قانون‌گذاری، تنظیم‌گری و طراحی سامانه‌ها پیشنهاد نمود که بار اثبات ضرورت و سودمندی خالص مداخلات را بر دوش متصدیان و نه بر دوش افراد ذی‌نفع می‌گذارد.

کلیدواژه‌ها:

خودمختاری داده‌ها؛ کرامت انسانی؛ فقه امامیه؛ عدالت الگوریتمی؛ حقوق بشر.

۴۱

دوره ۱۵، شماره ۲، پیاپی ۴۱
تابستان ۱۴۰۵

مقاله پژوهشی

تاریخ دریافت:

۱۵-۸-۱۴۰۴

تاریخ پذیرش:

۲۴-۴-۱۴۰۵

صص: ۴۵-۱۹

شابا چاپی: ۵۶۳۷-۲۳۲۲

اسکن کنید



۱. دانش‌آموخته دکتری، فقه و مبانی حقوق، دانشگاه تهران، تهران، ایران. (نویسنده مسئول). zoghims.313@gmail.com

۲. دانشیار، گروه روابط بین‌الملل، دانشکده امنیت ملی، دانشگاه دفاع ملی، تهران، ایران.



مقدمه و بیان مسأله

تحول اقتصاد داده محور و گسترش سامانه‌های هوشمند در حوزه‌هایی مانند اعتبارسنجی بانکی، گزینش شغلی، هدف‌گیری تبلیغاتی و حتی پلیس پیش‌نگر، وضعیت جدیدی برای رابطه فرد و دولت و شرکت‌های داده‌محور ایجاد کرده است؛ در این وضعیت، تصمیم‌هایی که بر پایه پیش‌بینی‌گری الگوریتمی اتخاذ می‌شود نه تنها رفتارهای آتی را حدس می‌زند بلکه به طور فعال فرصت‌ها، برچسب‌ها و نسبت‌های قدرت را بازتوزیع می‌کند. این دگرگونی باعث شده مفهوم سستی حریم خصوصی که بیشتر بر منع افشای اسرار یا ورود فیزیکی به حریم خانه تمرکز داشت برای تبیین وضعیت جدید کافی نباشد؛ در عوض، نیاز به مفهومی پررنگ‌تر با عنوان خودمختاری داده‌ها احساس می‌شود که بر حق فرد در کنترل چرخه کامل داده‌های مربوط به خود تاکید دارد. در این مقاله خودمختاری داده‌ها به صورت توانایی شخص در تعیین حدود گردآوری، پردازش، تحلیل، اشتراک‌گذاری و استفاده ثانوی از داده‌های شناسایی‌کننده او تعریف می‌شود؛ به گونه‌ای که هرگاه این توانایی به طور ساختاری تضعیف شود، اختیار واقعی فرد در شکل‌دهی به سرنوشت خویش نیز مختل می‌گردد. پرسش محوری از همین‌جا سر بر می‌آورد که در چه حدودی می‌توان پیش‌بینی‌گری الگوریتمی را با کرامت انسانی و حق شخص بر خودمختاری داده‌های خود سازگار دانست و چه زمانی این پیش‌بینی به ابزار کنترل هوشمند رفتارها و تضعیف اختیار بدل می‌شود.

مسئله‌هنگامی حادث می‌شود که حیثیت داده‌ای فرد نیز وارد میدان گردد؛ یعنی همان مجموعه امتیازها، رتبه‌ها و پروفایل‌هایی که سامانه‌های هوشمند بر پایه آنها درباره اعتبار، ریسک یا شایستگی اشخاص داوری می‌کنند. این پروفایل‌ها عملاً به چهره حقوقی جدیدی از فرد در فضای دیجیتال تبدیل می‌شوند و می‌توانند در دسترسی او به کار، وام، خدمات عمومی یا حتی آزادی‌های کیفری نقش تعیین‌کننده داشته باشند. در نبود قواعد روشن، پیش‌بینی‌گری از سطح تحلیل آماری خنثی فراتر می‌رود و به نوعی هنجارگذاری نامرئی بدل می‌شود که بدون شفافیت، بدون امکان اعتراض موثر و بدون مداخله انسانی معنادار، اختیار فرد را به حاشیه می‌راند. ادبیات موجود در حقوق ایران و فقه امامیه به شکل پراکنده به حریم خصوصی، منع تجسس، قاعده لاضرر، سلطنت بر شئون شخصی و کرامت انسانی پرداخته است؛ همچنین اسناد بین‌المللی حقوق بشر و مقررات حفاظت از داده‌ها مانند اسناد اروپایی و برخی قوانین داخلی کشورها چارچوب‌هایی برای حفاظت از داده‌ها و محدود کردن تصمیم‌های صرفاً خودکار پیشنهاد کرده‌اند. با این حال هنوز شکافی محسوس میان این مبانی هنجاری و معیارهای عملی برای تنظیم‌گری سامانه‌های پیش‌بین در زمینه‌هایی مانند اعتبارسنجی، پایش امنیتی یا تخصیص خدمات در ایران وجود دارد؛ شکافی که این مقاله در صدد شناسایی و پرکردن آن است.

هدف اصلی مقاله صورت‌بندی مفهومی و عملی حق بر خودمختاری داده‌ها در پیوند با کرامت انسانی در دو سطح است؛ نخست در سطح فقه امامیه و حقوق عمومی ایران که در آن قواعدی مانند نهی از تجسس، تحریم غیبت، قاعده لاضرر، قاعده سلطنت بر شئون شخصی و اصول قانون اساسی مربوط به حریم خصوصی و مصونیت حیثیت به عنوان زیرساخت‌های درون‌زا



برای این حق بازخوانی می شوند؛ دوم در سطح نظام بین المللی حقوق بشر که در آن حق بر زندگی خصوصی، حق حمایت از داده های شخصی و حق عدم تعرض به تصمیم های صرفاً خودکار به عنوان اجزای معماری خودمختاری داده ها تحلیل می شوند. پرسش فرعی مهم این است که چگونه می توان از دل این دو دستگاه هنجاری، معیارهایی سنجش پذیر برای طراحی و بهره برداری از سامانه های پیش بینی گر استخراج کرد؛ معیارهایی مانند حداقل گرای داده، تحدید غرض پردازش، ممنوعیت پروفایلینگ حیثیت زدا، الزامات شفافیت و توضیح پذیری، تضمین مداخله انسانی در تصمیم های پر اثر و پیش بینی مسیرهای روشن اعتراض و جبران. مقاله نشان می دهد که مفاهیم نوینی چون خودمختاری داده ها و حیثیت داده ای را می توان به طور عملیاتی و نه صرفاً نظری تعریف کرد و برای آنها شاخص هایی قابل تطبیق بر روی رویه های موجود در ایران به دست داد.

روش پژوهش در این مقاله تحلیلی هنجاری و تطبیقی است؛ بدین معنا که ابتدا مفاهیم کلیدی مانند خودمختاری داده ها، پیش بینی گری الگوریتمی و حیثیت داده ای بر پایه ادبیات معاصر حقوق داده و نظریه های حریم خصوصی تعریف و عملیاتی می شوند؛ سپس این مفاهیم در پرتو منابع فقه امامیه و متون حقوق عمومی ایران بازخوانی و با قواعد بین المللی حقوق بشر و مقررات پیشرفته حفاظت از داده مقایسه می گردند. در گام بعد، برخی کاربردهای مشخص پیش بینی گری الگوریتمی در زمینه های نزدیک به واقعیت ایران مانند نظام های اعتبارسنجی، پالایش محتوا یا پایش هوشمند برای مدیریت ریسک های امنیتی به صورت نمونه وار بررسی می شوند تا نشان داده شود که فقدان معیارهای روشن خودمختاری داده ها چگونه می تواند به تبعیض ساختاری، هتک حیثیت و تضعیف اختیار بینجامد. نوآوری مقاله در دو سطح است؛ نخست در پیشنهاد خوانشی منسجم از مبانی فقه امامیه و اصول حقوق بشر به مثابه چارچوب مشترک برای صیانت از خودمختاری داده ها در برابر کنترل هوشمند رفتارها؛ دوم در تبدیل این مبانی به مجموعه ای از معیارهای عملی برای قانون گذاری، تنظیم گری و طراحی سامانه های هوشمند در ایران، به گونه ای که بار اثبات ضرورت و سودمندی خالص مداخلات داده محور بر دوش متصدیان گذاشته شود نه بر دوش افراد در معرض تصمیم های الگوریتمی.

مبحث اول: مبانی نظری و انسان شناختی پیش بینی گری الگوریتمی و حق اختیار در پرتو کرامت انسانی

در این مقاله «پیش بینی گری الگوریتمی» به هر سامانه داده بنیانی گفته می شود که با تکیه بر مدل های آماری یا یادگیرنده درباره افراد تصمیم اثرگذار می گیرد و دست کم سه ویژگی هم زمان را دارد: اولاً خودکار بودن بخش مهمی از فرایند تحلیل و پیشنهاد یا اعمال تصمیم، ثانیاً ایجاد اثر حقوقی یا حیثیتی محسوس بر وضعیت فرد مانند اعطای اعتبار، گزینش شغلی، ارزیابی کیفری یا دسترسی به خدمت، ثالثاً اتکا به داده های رفتاری، ارتباطی یا زمینه ای شخص به گونه ای که تغییر در این داده ها بتواند نتیجه را دگرگون کند.

«خودمختاری داده ها» در این چارچوب به توانایی شخص برای کنترل چرخه پردازش تعریف می شود، به این معنا که بتواند اولاً از گردآوری و انواع داده های مورد استفاده آگاه شود، ثانیاً به محتوای اصلی داده های خود و برچسب ها و امتیازهای منتسب



دسترسی پیدا کند، ثالثاً درخواست اصلاح خطاها یا تکمیل توضیحات مربوط را مطرح کند، رابعاً با تصمیم صرفاً خودکار که بر پایه این داده‌ها اتخاذ شده مخالفت کند و ارجاع آن را به بازبینی انسانی بخواهد، خامساً در حدودی معین حذف یا محدود کردن پردازش و استفاده ثانوی از داده‌ها را مطالبه کند.

«حیثیت داده‌ای» نیز به هر برچسب، امتیاز، دسته‌بندی یا ارزیابی ریسکی گفته می‌شود که بر اعتبار اجتماعی، مالی، اداری یا کیفری شخص اثر می‌گذارد، حتی اگر محتوای داده‌های پایه صادق باشد، بر این مبنا هر سامانه‌ای که این ویژگی‌ها و آثار را داشته باشد داخل قلمرو بحث حاضر است و ابزارهای تحلیلی درون سازمانی که نه به تخصیص فرصت یا ریسک برای افراد معین می‌انجامد و نه بر وضعیت حقوقی و اجتماعی آنان اثر قابل‌سنجش دارد از دامنه کاربرد تعاریف این مقاله خارج تلقی می‌شود.

پیش‌بینی‌گری الگوریتمی هنگامی مسئله‌ساز می‌شود که از سطح تحلیل آماری خشی فراتر می‌رود و در قالب سازوکار تصمیم‌گیری برای مدیریت ریسک‌های اجتماعی و توزیع فرصت‌ها به کار گرفته می‌شود. در این سطح هر مدل پیش‌بین در عمل بخشی از نظم هنجاری جامعه را شکل می‌دهد و مستقیماً با حق اختیار و کرامت انسان درگیر می‌شود. در این مبحث پیش‌بینی‌گری نه صرفاً یک فناوری، بلکه سازوکاری برای طبقه‌بندی، برچسب‌زدن و اولویت‌بندی انسان‌ها فرض می‌شود تا نسبت آن با مرزهای شرعی خلوت و حرمت حیثیت سنجیده شود. بنیان اخلاقی و فقهی امامیه، به‌ویژه نهی روشن از تتبع عیوب و عورات اشخاص، معیار اصلی برای ترسیم این مرز تلقی می‌شود و بر پایه آن هرگونه استخراج تهاجمی داده از زیست خصوصی فقط در فرض ضرورت شرعی قابل‌اثبات، همراه با کمینه‌سازی تعرض، امکان نظارت انسانی و حق اعتراض مؤثر قابل‌توجیه است، نه بر اساس صرف کارایی یا منطق پیشگیری؛ در غیر این صورت شیوه‌های شکار داده و برچسب‌زنی آماری جای سنجش‌های مبتنی بر تناسب را می‌گیرند و از افق هنجار شرعی خارج می‌شوند (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵ تا ۳۵۶، قال رسول الله، لا تتبعوا عورات المؤمنین). همین منطق در تعریف غیبت به مثابه ذکر چیزی که فرد در غیبت خود از شنیدن آن کراهت دارد قابل‌توسعه است و به نحو عقلایی هر پردازش برچسب‌زن شهرت‌خراش را در دایره نهی قرار می‌دهد مگر آنکه ضرورت مشروع و ضوابط تناسب و کم‌زیانی به صورت مشخص احراز شود (الحر العاملی، بی تا، ج ۸، ص ۶۰۴، الغیبة ان تذکر اخاک بما یکره). قاعده «لا ضرر و لا ضرار» هنگامی که به‌عنوان قاعده نفی اضرار بر سامانه‌های پیش‌بین تطبیق می‌شود، نتیجه حقوقی روشن‌تری به دست می‌دهد که بر اساس آن هر خروجی قابل‌انتساب به طراحی و بهره‌برداری سامانه که زیان حقوقی یا حیثیتی ایجاد کند باید یا با مداخله انسانی و فرآیندهای اعتراض و بازبینی جبران‌پذیر گردد یا از چرخه تصمیم‌گیری قهری کنار گذاشته شود (الطوسی، بی تا، ج ۷، ص ۱۶۴، لا ضرر و لا ضرار).

تحلیل‌های فقهی درباره معیار هتک مؤمن و صیانت از کرامت عرضی نشان می‌دهد که ملاک حرمت، تنها افشای مستقیم عیب نیست، بلکه هر سازوکاری را دربر می‌گیرد که بدون فراهم کردن حق شنیده‌شدن و امکان دفاع، حیثیت فرد را در معرض تهدید برآوردهای خطاپذیر و تبعیض‌آمیز قرار می‌دهد. بر این اساس، پیش از اعمال هر برچسب یا رتبه‌بندی پرمپامد لازم است امکان



مشارکت و اعتراض فرد به عنوان مقتضای کرامت تضمین شود و تصمیم‌های داده‌بنیاد در ساختاری قرار گیرند که شنیدن روایت فرد را ممکن کند (النجفی، بی تا، ج ۲۲، ص ۶۳). این برداشت با قاعده مضیق جواز نظر به عورات در حد ضرورت نیز هماهنگ است و از مجموع آن‌ها می‌توان قاعده طراحی محدودیت دامنه داده و عمق دسترسی را استخراج کرد؛ بدین معنا که هر نگاه عمقی الگوریتمی به لایه‌های حساس همچون وضعیت سلامت، جنسیت یا باور، جز در فرض ضرورت متناسب و مبتنی بر چارچوب شفاف و مقید به حداقل مداخله، از حد شرعی فراتر می‌رود و ناقض کرامت تلقی می‌شود (الشهید الثانی، بی تا، ج ۷، ص ۴۹). بر پایه این مبانی، صورت‌بندی فقهی بهینه برای حکمرانی الگوریتمی نیاز انتزاعی باقی نمی‌ماند، بلکه می‌تواند به چهار رکن به هم پیوسته و قابل اجرا تبدیل شود؛ نخست آزمون ضرورت و تناسب پیشینی بر مبنای هدف مشروع و کمترین میزان تعرض، دوم الزام به کمینه‌سازی داده و تحدید قلمرو پردازش به قدر حاجت، سوم تضمین مداخله انسانی معنادار در تصمیم‌هایی که آثار حقوقی یا مشابه بر جای می‌گذارند، و چهارم پیش‌بینی مسیرهای روشن اعتراض، بازبینی و جبران که امکان بازگشت اختیار را برای فرد فراهم می‌کند.

در حقوق عمومی ایران همین بنیان‌های هنجاری به قالب‌های حقوقی الزام‌آور ترجمه شده و به این ترتیب زمینه تعریف معیارهای صریح برای کنترل تصمیم‌های الگوریتمی فراهم می‌شود. اصل ۲۲ قانون اساسی با اعلام مصونیت حیثیت، جان، مال و حقوق، فرض را بر ممنوعیت هر تصمیم خودکار حیثیت‌زدا قرار می‌دهد مگر آنکه این تصمیم به حکم قانون و همراه با تشریفات باشد که حق اعتراض و نظارت قضایی را تضمین می‌کند. اصل ۲۵ نیز با منع بازرسی و افشای مکاتبات و هرگونه تجسس جز به حکم قانون، سقفی برای دست‌اندازی به داده‌های ارتباطی ترسیم می‌کند و روشن می‌سازد که هر دسترسی گسترده برای تغذیه سامانه‌های پیش‌بین باید تحت صراحت قانونی و نظارت قضایی قرار گیرد. در سطح قوانین بخشی، ماده ۵۸ قانون تجارت الکترونیکی رضایت صریح را پیش شرط هرگونه ذخیره، پردازش و توزیع داده‌پیام‌های شخصی حساس قرار می‌دهد و در نتیجه هر مدل پیش‌بین متکی بر این داده‌ها محتاج رضایت معتبر یا مجوز خاص قانونی است. ماده ۱۷ قانون جرایم رایانه‌ای انتشار یا در دسترس‌گذاری محتوای خصوصی اشخاص به گونه‌ای که منتهی به ضرر یا هتک حیثیت شود را جرم‌انگاری کرده و نسبت به خروجی‌های افشاگرانه یا امتیازدهی‌هایی که امکان شناسایی فرد را دارند واکنش کیفری نشان می‌دهد. ماده ۱۵۰ قانون آیین دادرسی کیفری نیز کنترل ارتباطات مخابراتی را به قیود سخت ضرورت، مجوز مقام عالی قضایی و تحدید زمانی مقید می‌کند و بدین سان هرگونه تغذیه سامانه‌های پیش‌بین از داده‌های شنود یا کنترل باید در همین چارچوب محدود شود تا تعادل میان کارایی و صیانت از حقوق بنیادین برقرار بماند.

ادبیات حقوقی ایران این چارچوب را در سطح نظری و ساختاری تعمیق کرده و به‌ویژه نشان می‌دهد که چگونه می‌توان از مفاهیم سنتی حریم خصوصی به سوی خودمختاری داده‌ای و کنترل بر پیرامتن اطلاعاتی حرکت کرد. رحمدل با صورت‌بندی حق انسان بر حریم خصوصی، کنترل بر اطلاعات شخصی را شرط خودآیینگی و کرامت تلقی می‌کند و بر این نکته پای می‌فشارد که

تصمیم‌های خودکار باید با اطلاع‌رسانی شفاف، حق مخالفت مؤثر و امکان ارزیابی انسانی همراه باشد تا اختیار واقعی افراد مخدوش نشود (رحمدل، ۱۳۸۴، ص ۱۴۶-۱۱۹). تحلیل موسی‌زاده و مصطفی‌زاده نشان می‌دهد که مبانی عرفی حق بر حریم خصوصی در پیوند علی با کرامت و خودمختاری سامان یافته است و هر پروفایل‌سازی پیش‌بین که بدون رضایت و بدون رعایت تناسب انجام گیرد این پیوند را نقض و زمینه تبعیض ساختاری را فراهم می‌کند (موسی‌زاده و مصطفی‌زاده، ۱۳۹۱، ص ۴۵-۶۸). از منظری مفهومی، اماموردی با تمایز گونه‌های حق در حریم نشان می‌دهد که می‌توان پیرامتن اطلاعاتی شخص را به‌منزله حوزه‌ای با حدود تصرف تعریف کرد؛ خروج از این حدود در پردازش الگوریتمی تعرض به حق محسوب می‌شود و بدین ترتیب اصل کمینه‌سازی داده و تحدید غرض پردازش وجهی حقوقی می‌یابد (اماموردی، ۱۳۹۶، ص ۳۴۷-۳۶۶). پیوند این مبانی با آیین دادرسی در کار کوشکی به معیار ضرورت متناسب در مکان‌های خصوصی می‌رسد که می‌توان آن را به زبان هنجار طراحی برای ابزارهای پیش‌بین در کشف جرم ترجمه کرد تا کارایی به توجیه مطلق برای مداخله تبدیل نشود (کوشکی، ۱۳۹۰، ص ۱۳۵-۱۵۰). در سطح تفسیر قانون اساسی نیز تحلیل حبیب‌زاده و رحیمی‌نژاد با آشکارکردن پارادوکس‌های متن بر لزوم تفسیر کرامت‌محور در رویارویی با فناوری‌های نو، از جمله پروفایل‌سازی الگوریتمی، تأکید می‌کند تا شکاف میان متن و مسئله‌های نوپدید به زیان حقوق بنیادین گسترش نیابد (حبیب‌زاده و رحیمی‌نژاد، ۱۳۸۶، ص ۵۱-۸۲).

مقررات اروپایی و آمریکایی نسبت به مراحل مختلف پیش‌بینی‌گری الگوریتمی ابزارهای صریح‌تری برای تحدید خودکاربودن و تضمین بازگشت اختیار فرد پیش‌بینی کرده‌اند و از این جهت می‌توانند در کنار مبانی فقهی و حقوقی ایران به‌عنوان منبع تطبیقی مورد استفاده قرار گیرند. ماده ۲۲ مقرر عمومی حفاظت از داده‌های اتحادیه اروپا، حق عدم‌تعرض به تصمیم‌های مبتنی بر پردازش صرفاً خودکار با آثار حقوقی یا مشابه را به رسمیت می‌شناسد و سه تضمین مداخله انسانی، امکان بیان نظر و حق اعتراض را الزامی می‌کند (GDPR, art. ۲۰۱۶, ۲۲). ماده ۸ منشور حقوق بنیادین اتحادیه، حق حفاظت از داده‌های شخصی را در سطحی بنیادین تثبیت و بر پردازش منصفانه، اغراض مشخص و نظارت مرجع مستقل تصریح می‌کند، در حالی که ماده ۸ کنوانسیون اروپایی حقوق بشر هر مداخله در زندگی خصوصی و مکاتبات را به سه‌گانه قانونی‌بودن، ضرورت و تناسب مقید می‌سازد و به این وسیله نسبت میان امنیت و آزادی را از منظر دادرسی عادلانه تنظیم می‌کند (EU Charter, ۲۰۱۲/۲۰۰۰, art. ۸, ECHR, ۱۹۵۰, art. ۸). در حقوق داخلی بریتانیا بخش ۱۴ قانون حفاظت از داده‌های ۲۰۱۸ حدود تصمیم‌گیری خودکار را تبیین و راه رجوع انسانی را مقرر می‌دارد (Data Protection Act, ۲۰۱۸, s. ۱۴). در حقوق ایالات متحده نیز الزام به اطلاع‌رسانی اقدام نامساعد و حقوق دسترسی و اعتراض در اعتبارسنجی، تحت رژیم گزارش‌دهی اعتبار منصفانه، مکانیسمی برای پاسخ‌گوکردن مدل‌های پیش‌بین در تخصیص اعتبار ایجاد می‌کند.

پژوهش‌های نظری در حوزه شفافیت و توضیح‌پذیری نشان می‌دهد که مجموعه این مقررات کف حمایت را می‌سازد نه سقف آن و برای صیانت از اختیار و کرامت انسانی، لایه‌های مکمل نهادی و طراحی لازم است. واختر، میتلشتات و فلوریدی بر این نکته



تأکید کرده‌اند که مقرر عمومی حفاظت از داده‌ها حق توضیح عام برای همه تصمیم‌های خودکار برقرار نکرده است و بیشتر به حق آگاهی و حق عدم تعرض اکتفا می‌کند، در نتیجه حفظ خودمختاری اطلاعاتی نیازمند سازوکارهای تکمیلی در سطح حکمرانی و طراحی سامانه‌ها است (Wachter et al., ۲۰۱۷, vol. ۷, p. ۷۶-۹۹). سلبست و پاولز خوانشی کارکردگرایانه از اطلاعات معنادار درباره منطق تصمیم پیشنهاد می‌کنند تا ابزار اعتراض مؤثر و بازیابی اختیار فرد از سطح تشریفات فراتر رود و به امکان نقد واقعی تصمیم نزدیک شود (Selbst & Powles, ۲۰۱۷, vol. ۷, p. ۲۳۳-۲۴۲). برل با تحلیل سه نوع پوشیدگی، یعنی سرت شرکتی، پیچیدگی فنی و ذات آماری مدل‌ها، نشان می‌دهد که توضیح‌پذیری پیش شرط عدالت رویه‌ای است و بدون آن فرآیندهای پیش‌بین به سادگی می‌توانند به هنجارهای تبعیض‌آمیز یا حیثیت‌زدا بدل شوند (Burrell, ۲۰۱۶, vol. ۳, p. ۱-۱۲). همین خطر در صورت‌بندی تبعیض نامستقیم داده‌ای برجسته می‌شود، زیرا حتی در غیاب نیت تبعیض، همبستگی‌های ساختاری در داده قادر است به سلب فرصت و فرسایش کرامت بینجامد و به همین دلیل آزمون‌های تناسب و ضرورت و نیز امکان اعتراض فردی باید در هر چرخه تصمیم‌گیری مبتنی بر پیش‌بینی نهادینه شود (Barocas & Selbst, ۲۰۱۶, vol. ۱۰۴, p. ۶۷۱-۷۳۲). اگر شفافیت، امکان خروج و پاسخ‌گویی در طراحی نهادینه نشود، اختیار واقعی کاربر در زیست‌جهان دیجیتال به شکلی خزنده فرسوده می‌شود؛ نقطه‌ای که پیوند مبانی فقهی منع تبع و حرمت هتک حیثیت با معیارهای حقوقی معاصر برای توضیح‌پذیری، مداخله انسانی و حق اعتراض باید از سطح توصیه‌های اخلاقی فراتر رفته و به قواعد سخت طراحی و نظارت تبدیل شود (Yeung, ۲۰۱۷, vol. ۲۰, p. ۱۱۸-۱۳۶).

۱-۱) مطلب اول: از داده تا پیش‌بینی رفتار؛ تحول مفهوم پیش‌بینی‌گری و تأثیر آن بر آزادی انسان

گذار از گردآوری خام داده‌ها به سمت الگوریتم‌های پیش‌بینی گر رفتار، معنای پیش‌بینی را دگرگون کرده است. در مدل‌های سنتی، پیش‌بینی بیشتر به توصیف احتمالاتی آینده محدود می‌شد، اما امروزه خروجی مدل‌های پیش‌بین در تصمیم‌های حقوقی، اقتصادی و حیثیتی ادغام می‌شود و عملاً آینده را طراحی می‌کند، نه صرفاً توصیف. به محض آنکه این مدل‌ها در تخصیص اعتبار، سنجش ریسک، انتخاب استخدامی یا ارزیابی کیفری به کار می‌روند، قدرت برچسب‌زنی و توزیع فرصت از سطح مشاهده به سطح هنجارسازی ارتقا می‌یابد و به قلب بحث درباره آزادی و اختیار انسان وارد می‌شود. همین جاست که تبیین‌های حقوقی کلاسیک از اختیار، به ویژه در قالب حق آگاهی و حق دسترسی، با محدودیت روبه‌رو می‌شود و روشن می‌گردد که چارچوب اتحادیه اروپا، به روایت خوانش دقیق متن و سیاق مقرر، هرچند حقوقی چون آگاهی، دسترسی و عدم تعرض به تصمیم صرفاً خودکار را مفروض می‌گیرد، اما حق توضیح برای همه تصمیم‌های خودکار را به عنوان حقی عام و صریح نهادینه نکرده است؛ از این رو پاسداشت اختیار و کرامت تنها با تکیه بر متن مقرر ممکن نیست و نیازمند لایه‌های نهادی مکمل در سطح طراحی، نظارت و دادرسی است تا میان منطق بهینه‌سازی مدل و منطق حقوق بنیادین نسبت قاعده‌مند برقرار شود (Wachter, ۲۰۱۷, vol. ۷, p. ۷۶-۹۹).

صورت بندی کارکردگرایانه از «اطلاعات معنادار درباره منطق تصمیم» تلاش می کند این شکاف را کاهش دهد. این رویکرد می پذیرد که دسترسی کامل به کد یا افشای تمامی جزئیات مدل، هم از حیث فنی و هم از حیث اسرار تجاری واقع بینانه نیست، اما تأکید می کند که باید سطحی از شفافیت درباره ورودی های اثرگذار، قواعد کلی استنتاج و حدود اعتبار خروجی فراهم شود تا شخص موضوع تصمیم بتواند اعتراض مؤثر طرح کند و مسیر بازبینی انسانی واقعا بتواند اختیار از دست رفته را بازگرداند. در غیر این صورت حق اعتراض به تشریفات بی ثمر تقلیل می یابد و چرخه تکرار خطاهای ساختاری در پوشش کارایی بازتولید می شود (Selbst, 2017, vol. ۷, pp. ۲۳۳-۲۴۲)؛ این دغدغه با تحلیل کیفی پوشیدگی در سه لایه سربت شرکتی، پیچیدگی فنی و ذات آماری مدل ها پیوند می خورد و توضیح پذیری را از یک امتیاز لوکس به پیش شرط عدالت رویه ای و ابزار صیانت از کرامت در تصمیم های مبتنی بر پیش بینی الگوریتمی تبدیل می کند، زیرا حتی نظام های مبتنی بر حسن نیت نیز در غیاب توضیح پذیری، بر اثر داده های معیوب، قیاس های نادرست یا همبستگی های گمراه کننده، می توانند حیثیت و فرصت افراد را مخدوش سازند (Burrell, 2016, vol. ۳, pp. ۱-۱۲).

تبیین تبعیض نامستقیم داده ای نشان می دهد که مسئله تنها نیت تبعیض گرایانه نیست. الگوهای ساختاری در داده ها، گزینش متغیرهای ظاهرا بی طرف و برآوردهای مدل می تواند بدون قصد صریح تبعیض، به محروم شدن گروه هایی خاص از فرصت های شغلی، اعتباری یا خدماتی بینجامد و تبعیض را به سطحی آماری و پنهان منتقل کند. بر این اساس آزمون های تناسب و ضرورت، همراه با امکان اعتراض فردی کارآمد و مداخله انسانی معنادار، باید در خود طراحی سامانه تعبیه شود تا پیش بینی به پوششی برای تحکیم سوگیری های پیشینی تبدیل نشود و در مدار نظارت پذیری و پاسخ گویی باقی بماند (Barocas, 2016, vol. ۱۰۴, pp. ۶۷۱-۷۳۲)؛ معماری های تنظیم گر که با ترکیب داده های کلان، شخصی سازی پویا و آزمایش های مستمر A/B جریان تصمیم را بی صدا هدایت می کنند، اگر بدون شفافیت، امکان خروج و رژیم پاسخ گویی عمل کنند، به فرسایش خزنه اختیار واقعی می انجامند و نسبت میان کارایی و خودآیینگی را در سطحی زیرپوستی اما مؤثر به نفع کنترل طراحی شده جابه جا می کنند، امری که بدون قواعد پیشینی محدودکننده و الزامات افشای هدف و منطق اثرگذاری، از منظر آزادی های فردی و حریم خصوصی به دشواری قابل دفاع است (Yeung, 2017, vol. ۲, pp. ۱۱۸-۱۳۶).

در سنت حقوقی ایران، بنیان نظری حریم خصوصی به نحو پرمایه ای به اختیار و کرامت پیوند خورده است و کنترل بر اطلاعات شخصی شرط تحقق خودآیینگی و صیانت از شخصیت حقوقی دانسته می شود. نتیجه این پیوند آن است که تصمیم گیری خودکار، چنانچه در فرآیندی با اطلاع رسانی شفاف، امکان مخالفت مؤثر و ارزیابی انسانی ادغام نشود، با هنجارهای بنیادین ناسازگار است و زمینه اضرار حیثیتی و حقوقی را فراهم می کند (رحمدل، ۱۳۸۴، ص ۱۴۶-۱۱۹)؛ این جهت گیری در سطح قانون اساسی نیز بازتاب یافته است، زیرا مصونیت حیثیت، جان، مال و حقوق جز به حکم قانون مفروض گرفته می شود و به تبع آن هر تصمیم خودکار حیثیت زدا باید ذیل مجوز صریح، تشریفات تضمین گر حق اعتراض و نظارت قضایی ارزیابی شود تا قاعده



مصونیت از اعمال خشن اداری خودکار، از حد شعار فراتر رفته و به واقعیت عملی نزدیک شود (قانون اساسی، اصل ۲۲)؛ تحلیل کرامت انسانی در قانون اساسی و تنش های درونی متن، ضرورت تفسیر کرامت محور در مواجهه با فناوری های نو از جمله پروفایل سازی و پیش بینی الگوریتمی را برجسته می سازد تا در وضعیتی که فهم اجتماعی از پیش بینی از ابزار شناخت به ابزار هدایت رفتاری تغییر کرده است، معیار کرامت به عنوان حد نهایی مداخله در تراز تصمیم گیری عمومی و خصوصی حفظ شود و آزادی به حاشیه رانده نشود (حبیب زاده و رحیمی نژاد، ۱۳۸۶، ص ۵۱-۸۲).

۲-۱) مطلب دوم: کرامت و خودآیینی در انسان شناسی اسلامی و نظام حقوق بشر؛ تحلیل تطبیقی مبانی اختیار

کرامت نه صرفاً شأنی انتزاعی بلکه حد نهایی مداخله در نفس و عرض انسان است و از دل همین تلقی است که قاعده های سلبی پاسدار خلوت، نظیر نهی از تتبع عیوب و عورات، صورت بندی ای ایجابی برای حق اختیار می سازند، زیرا هر سازوکار دانشی متکی بر داده اگر بدون احراز ضرورت شرعی و معیار کمزبانی به ژرفای زیست خصوصی فرو رود، از مدار مشروعیت خارج و به مخدوش سازی حیثیت می انجامد و بدین سان مفروضه بنیادین در ترجمان فقهی اختیار این خواهد بود که نگاه الگوریتمی به داده های حساس تنها در قدر حاجت و با امکان بازخواست پذیری و نظارت انسانی موجه است، نه بر مبنای کارایی ابزاری یا توجیهات برآمده از هم بستگی های آماری که به راحتی می توانند به شکار داده و برچسب زنی غیابی بینجامد و درست به همین دلیل است که توسعه عقلایی مفهوم غیبت به مثابه ذکر آنچه شخص در غیبتش کراهت دارد هر پردازش برون خط و پشت صحنه را که شخصیت و شهرت فرد را مخدوش کند در دایره نهی می نشاند مگر در فرض ضرورت متناسب و با قیود شفاف (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵-۳۵۶؛ الحر العاملی، بی تا، ج ۸، ص ۶۰۴).

قاعده اختصاصی عدم تعرض به تصمیم های صرفاً خودکار با آثار حقوقی یا مشابه، مستظهر به تضمین سه گانه مداخله انسانی، امکان اظهار نظر و حق اعتراض، سازوکار بازگرداننده اختیار را در دل طراحی نظام های پیش بین نهادینه می کند و از تبدیل محاسبه به حکم جلوگیری می نماید؛ بدین معنا که انسان شناسی کرامت محور، با پذیرش عقلانیت ابزاری مدل ها، سلطه هنجاری آن ها را به واسطه حق داور انسانی، اطلاع رسانی پیشینی و امکان بازبینی مهار می کند و در نسبت با نظام حقوقی ایران نیز به محض آنکه قلمرو ارتباطات خصوصی در زمره حریم های مصون از تجسس جز به حکم قانون تثبیت شد، هر تغذیه الگوریتمی از داده های ارتباطی ناگزیر در قید تصریح قانونی و نظارت قضایی می افتد تا پیوند کرامت و خودآیینی در سطح تضمین های شکلی و ماهوی یکپارچه گردد و پیش بینی از ساحت هدایت گر نامرئی به ساحت تصمیم بازخواست پذیر ارتقا یابد (GDPR، ۲۰۱۶، art. ۲۲؛ قانون اساسی، اصل ۲۵).

پیوند نظری کرامت و خودمختاری با حریم خصوصی در ادبیات حقوقی ایران به گونه ای است که حق کنترل بر اطلاعات شخصی به شرط لازم خودآیینگی فرد بدل می شود و هر تصمیم خودکار بدون اطلاع رسانی شفاف و امکان مخالفت مؤثر با



مقتضای اختیار ناسازگار است، در حالی که تحلیل ماهیت حریم نشان می‌دهد این حق از سنخ حدود تصرف در پیرامتن اطلاعاتی شخص است و بنابراین هر مداخله الگوریتمی بیرون از این حدود تعرض حقوقی محسوب می‌شود و باید به آزمون ضرورت و تناسب و نیز سازوکار اعتراض و جبران گره بخورد تا نسبت اسلام کرامت‌محور با نظام‌های حقوق بشر معاصر، نه در سطح شعارهای همدلانه بلکه در سطح قواعد سخت طراحی و نظارت نهادینه گردد (موسی‌زاده و مصطفی‌زاده، ۱۳۹۱، ص ۴۵-۶۸؛ امام‌وردی، ۱۳۹۶، ص ۳۴۷-۳۶۶).

۳-۱) مطلب سوم: پیش‌بینی‌پذیری و مسئولیت اخلاقی؛ تعارض میان جبر الگوریتمی و آزادی اراده در نظم حقوقی

در انسان شناسی اسلامی، کرامت تنها یک شأن انتزاعی یا وصف تکریمی نیست، بلکه مرز نهایی برای هر نوع مداخله در نفس و عرض انسان به شمار می‌آید؛ بر این اساس قواعد سلبی پاسدار خلوت، مانند نهی از تتبع عیوب و عورات، به صورت ضمنی بنیانی ایجابی برای حق اختیار و خودآیینی می‌سازند. هر سازوکار دانشی متکی بر داده، اگر بدون احراز ضرورت شرعی و بدون رعایت معیار کم‌زیانی به ژرفای زیست خصوصی نفوذ کند، از مدار مشروعیت هنجاری خارج می‌شود و به تخریب حیثیت می‌انجامد. در ترجمان فقهی اختیار، نتیجه این است که نگاه الگوریتمی به داده‌های حساس فقط در حد حاجت، با دایره دسترسی محدود، همراه با امکان بازخواست‌پذیری و نظارت انسانی قابل قبول است؛ نه براساس صرف کارایی ابزاری یا توجیهات برآمده از هم‌بستگی‌های آماری که به آسانی به شکار داده و برچسب زنی غیابی می‌انجامد. توسعه عقلایی مفهوم غیبت به مثابه ذکر آنچه شخص در غیبت خود از شنیدن آن کراهت دارد، این امکان را فراهم می‌کند که هر پردازش برون خط و پشت صحنه که شخصیت و شهرت فرد را مخدوش کند، در دایره نهی قرار گیرد، مگر در فرض ضرورت متناسب و با قیود شفاف و قابل کنترل (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵-۳۵۶؛ الحر العاملی، بی‌تا، ج ۸، ص ۶۰۴).

در سطح حقوق بشر معاصر، قاعده اختصاصی عدم تعرض به تصمیم‌های صرفاً خودکار با آثار حقوقی یا مشابه، که بر تضمین سه‌گانه مداخله انسانی، امکان اظهار نظر و حق اعتراض استوار است، تلاشی نهادی برای بازگرداندن اختیار در دل طراحی نظام‌های پیش‌بین به شمار می‌آید؛ این قاعده اجازه نمی‌دهد محاسبه خودکار بدون فیلتر داوری انسانی به حکم الزام‌آور تبدیل شود و از این جهت با انسان‌شناسی کرامت‌محور قابل جمع است. این انسان‌شناسی، عقلانیت ابزاری مدل‌ها را به رسمیت می‌شناسد، اما سلطه هنجاری آنها را از طریق حق داوری انسانی، اطلاع‌رسانی پیش‌بینی و امکان بازبینی محدود می‌کند تا پیش‌بینی به نقطه پایان گفت‌وگو بدل نشود. در نسبت با نظام حقوقی ایران، به محض آن‌که قلمرو ارتباطات خصوصی در زمره حریم‌های مصون از تجسس جز به حکم قانون تثبیت شود، هر تغذیه الگوریتمی از داده‌های ارتباطی ناگزیر در قید تصریح قانونی روشن، نظارت قضایی مؤثر و امکان اعتراض فردی قرار می‌گیرد؛ در نتیجه پیوند کرامت و خودآیینی در سطح تضمین‌های شکلی و ماهوی به



صورت یکپارچه سامان می یابد و پیش بینی از ساحت هدایت گر نامرئی به ساحت تصمیم بازخواست پذیر و قابل حسابرسی ارتقا پیدا می کند (GDPR، ۲۰۱۶، art. ۲۲؛ قانون اساسی، اصل ۲۵).

در ادبیات حقوقی ایران، پیوند نظری کرامت و خودمختاری با حریم خصوصی به گونه ای تبیین شده است که حق کنترل بر اطلاعات شخصی، شرط لازم تحقق خودآیینگی فرد تلقی می شود و هر تصمیم خودکار که بدون اطلاع رسانی شفاف و امکان مخالفت مؤثر اتخاذ شود، با مقتضای اختیار ناسازگار است. تحلیل ماهیت حریم نشان می دهد این حق از سنخ حدود تصرف در پیرامتن اطلاعاتی شخص است؛ بنابراین هر مداخله الگوریتمی بیرون از این حدود، تعرض حقوقی محسوب می شود و باید به آزمون ضرورت و تناسب و نیز به سازوکار اعتراض، بازبینی و جبران گره بخورد. بر این مبنا، نسبت اسلام کرامت محور با نظام های حقوق بشر معاصر نه در سطح شعارهای همدلانه، بلکه در سطح قواعد سخت طراحی و نظارت قابل صورت بندی است؛ به این معنا که کرامت، معیار تنظیم دامنه داده های مجاز، شدت مداخله، شکل توضیح پذیری و حدود پاسخ گویی سامانه های پیش بین می شود و گذار از داده به پیش بینی، زیر نظارت اصولی قرار می گیرد که هم از منظر فقهی و هم از منظر حقوق بشر، محور آن انسان خودآیین و برخوردار از حرمت ذاتی است (موسسی زاده و مصطفی زاده، ۱۳۹۱، ص ۴۵-۶۸؛ اماموردی، ۱۳۹۶، ص ۳۴۷-۳۶۶).

یکی از روشن ترین نمونه های تصمیم گیری الگوریتمی در ایران، سازوکار دهک بندی یارانه ها بر پایه پایگاه اطلاعات رفاه ایرانیان است که با تجمع داده های متنوع از حساب های بانکی، املاک، خودرو، سفرهای خارجی و سایر شاخص های اقتصادی، خانوارها را در دهک های درآمدی مختلف طبقه بندی می کند و درباره استمرار یا قطع یارانه نقدی تصمیم می گیرد. مدر عمل، خروجی مدل امتیازدهی این پایگاه، اثر مستقیم بر بهره مندی یا محرومیت خانوار از حمایت معیشتی دارد و مصداق روشن حیثیت داده ای است، زیرا برچسب دهک بالا یا پایین، هم بر تصویر اداری فرد نزد نهادهای دولتی اثر می گذارد هم بر امکان دسترسی او به خدمات عمومی. نقدهای مطرح درباره خطا در شناسایی دهک ها و لزوم ثبت اعتراض در سامانه های رفاهی نشان می دهد تصمیم در اینجا صرفاً فنی نیست، بلکه تصمیمی هنجاری درباره استحقاق است که اگر بدون شفافیت شاخص ها، بدون رضایت معتبر نسبت به جمع و اشتراک داده ها و بدون مسیر اعتراض مؤثر و ارزیابی انسانی اجرا شود، با معیارهای این مقاله درباره خودمختاری داده ها، حق شنیده شدن و قاعده نفی ضرر ناسازگار است. بر مبنای اصول ۲۲ و ۲۵ قانون اساسی، چنین سامانه ای باید در چارچوب تصریح قانونی، نظارت قضایی بر دسترسی به داده های ارتباطی و امکان کنترل فرد بر اطلاعات خود بازطراحی شود تا پیش بینی رفاهی به قهر اداری غیرشفاف تبدیل نگردد و معیار تناسب و ضرورت در سطح داده و تصمیم هم زمان رعایت گردد.

سامانه های اعتبار سنجی بانکی است که توسط شرکت مشاوره رتبه بندی اعتباری ایران و با حمایت وزارت امور اقتصادی و دارایی و بانک مرکزی، برای سنجش ریسک اعتباری اشخاص حقیقی به کار می رود و جایگزین ضامن سستی در تسهیلات خرد شده است. مدر مدل جدید، تعداد شاخص های مورد استفاده از حدود چند شاخص محدود بانکی به صدها شاخص گسترش یافته

است و اطلاعات متنوعی از تسهیلات، تعهدات، چک، مالیات، گمرک، بیمه، سوابق قضایی و محکومیت‌ها، جرایم راهنمایی و رانندگی، قبوض خدماتی و داده‌های اپراتورهای تلفن همراه در محاسبه امتیاز اعتباری به کار می‌رود. نتیجه این فرایند عددی است که مستقیماً بر امکان دریافت وام، سقف تسهیلات و حتی اعتبار اجتماعی شخصی اثر می‌گذارد و دقیقاً در قلب تعریف پیش‌بینی‌گری الگوریتمی و حیثیت داده‌ای قرار می‌گیرد. اگر مسیر دسترسی فرد به داده‌های پایه، امکان اصلاح خطاها، حق اعتراض به تصمیم صرفاً خودکار و رجوع به داوری انسانی در این سامانه به روشنی تضمین نشود، خطر آن وجود دارد که برچسب «ریسک بالا» بدون امکان دفاع مؤثر، به محرومیت ساختاری از فرصت‌های مالی بینجامد و قاعده لا ضرر، اصل مصونیت حیثیت در اصل ۲۲ و ممنوعیت تجسس غیرقانونی در اصل ۲۵ را مخدوش کند. چنین مثالی نشان می‌دهد چارچوب نظری مقاله درباره خودمختاری داده‌ها، کرامت و آزمون ضرورت و تناسب، فقط در سطح انتزاع باقی نمی‌ماند و می‌تواند به صورت معیارهای سنجش‌پذیر برای طراحی و نظارت بر سامانه‌های واقعی تصمیم‌گیری الگوریتمی در ایران به کار گرفته شود.

۲) مبحث دوم: بنیادهای فقهی و اخلاقی حق خودمختاری داده‌ها و صیانت از کرامت انسانی

در چارچوب انسان‌شناسی کرامت محور در فقه امامیه، حق خودمختاری داده‌ها به صورت اضافه‌ای بیرون از متن سستی شکل نمی‌گیرد، بلکه می‌توان آن را به طور درون‌زا از همان بنیان‌های دیرینه‌ای استخراج کرد که در آغاز برای صیانت از ستر و عرض مؤمن وضع شده‌اند و امروز در بستر داده محور قابلیت ترجمه نهادی یافته‌اند. نهی صریح از تجسس و سوء ظن در باب التجسس و سوء الظن از الکافی، قاعده هنجاری عامی را مستقر می‌کند که قلمرو کاوش در عورات و اسرار را پیشینی محدود می‌سازد و بر این اساس حق الناس بر پوشیدگی داده‌های شخصی و منطق رضایت محور در هر گونه دسترسی و پردازش تثبیت می‌شود. توسعه عقلایی تحریم غیبت، از ذکر مخدوش‌کننده در غیاب شخص تا هر پردازش افشاگرانه بدون اذن را دربرمی‌گیرد و نشان می‌دهد که نفی هتک عرض در عصر الگوریتم به معنای نفی افشای داده بی رضایت است، حتی اگر محتوای داده صادق باشد، زیرا معیار اصلی کرامت است نه صرف صدق و کذب (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵؛ النجفی، بی تا، ج ۲۲، ص ۶۳). قاعده لا ضرر در تقریر اصولی شیخ انصاری معیار نفی هر الزام یا معامله مضر را به دست می‌دهد و نسبت به داده‌ها اقتضا می‌کند که هر پردازش و تصمیم‌گیری داده محور مفضی به زیان مؤثر حیثیتی، اقتصادی یا بدنی از اصل در دایره منع قرار گیرد مگر آن که ضرورت نوعی و مجوز شرعی احراز شود. در کنار آن، قاعده سلطنت با دلالت الناس مسلطون علی اموالهم و تأیید لا یحل مال امرئ مسلم الا بطیب نفسه، به طریق تنقیح مناط به حوزه شئون شخصی و اطلاعات منتسب به فرد نیز سرایت می‌کند و تصرف در داده‌ها را جز بر پایه طیب نفس و رضایت معتبر موجه نمی‌شمارد. سنت اخلاقی حفظ سر و لسان، تکلیف عام رازداری را به صورت امانت‌داری اطلاعاتی بر عهده متصدیان پردازش می‌گذارد تا افشای بی‌اذن به منزله خیانت در امانت شناخته شود و بنیان اعتماد اجتماعی را متزلزل نکند (انصاری، بی تا، ج ۵، ص ۱۶۱؛ خمینی، بی تا، ج ۱، ص ۵۳۵؛ الکلینی، ۱۴۰۷ق، ج ۲، ص ۱۱۳).



این صورت بندی نشان می دهد سهم افزوده مقاله صرفا تکرار گزاره های اخلاقی نیست، بلکه تبدیل آنها به اصول عملی برای کنترل چرخه داده است.

این بنیان های فقهی در حقوق عمومی ایران به قواعد الزام آور تبدیل شده و در کنار هم شبکه ای از اصول ماهوی و شکلی را ساخته اند که قدرت مداخله در حریم اطلاعاتی را به نسبت ضرورت، تناسب و نظارت قضایی محدود می سازد. اصل ۲۵ قانون اساسی با منع هرگونه بازرسی، استراق سمع و تجسس مگر به حکم قانون، در مقام سپر مقدم امنیت ارتباطات ظاهر می شود و این حوزه را در ردیف حقوق بنیادین قرار می دهد. اصل ۲۲ با مضمون داشتن حیثیت، جان، مال و حقوق اشخاص از تعرض جز به تجویز قانون، زمینه امتداد مفهوم کرامت به حیثیت داده ای را فراهم می کند و هر پردازش تحقیرآمیز یا حیثیت زدا را در معرض منع قرار می دهد. در سطح قوانین بخشی، ماده ۵۸ قانون تجارت الکترونیکی رضایت صریح و قابل اثبات را مبنای مشروعیت پردازش داده های شخصی حاساس قرار داده و ماده ۷۱ ضمانت اجرای این الزام را تأمین می کند. قانون جرایم رایانه ای با جرم انگاری دسترسی غیرمجاز و اختلال در سامانه های حفاظت شده، سپر کیفری حمایت از خودمختاری داده ها را ایجاد می کند و ماده ۱۵۰ قانون آیین دادرسی کیفری با مشروط کردن هر نوع شنود و دسترسی به داده های اشخاص به ضرورت، مجوز قضایی و تحدید زمانی، سه گانه قانونی بودن، ضرورت و نظارت را در راهبرد مداخله نهادینه می کند. بدین ترتیب تغذیه هر سامانه پیش بینی گرا از داده های ارتباطی و محیطی جز در پرتو این قیود مشروعیت نمی یابد و رابطه قدرت میان متصدی و سوژه داده به قاعده، پاسخ گویی و امکان اعتراض مؤثر مقید می شود؛ نکته ای که این مقاله آن را به طور صریح به حوزه تصمیم گیری الگوریتمی تعمیم می دهد.

در سطح تطبیقی، چارچوب اتحادیه اروپا با تدوین اصول بنیادین در ماده ۵ بند ۱ مقرر عمومی حفاظت از داده ها، از قانونی بودن و شفافیت تا کمینه سازی، دقت، محدودیت نگهداشت، تمامیت و محرمانگی و پاسخ گویی، زیرساخت هنجاری خودمختاری داده ها را مهندسی می کند و در ماده ۷ با سخت گیرانه کردن شرایط اعتبار رضایت، از بار اثبات بر عهده متصدی تا قابلیت آسان پس گرفتن آن، این زیرساخت را در سطح اجرا محکم می سازد. منشور حقوق بنیادین در ماده ۸ حق حفاظت از داده های شخصی را به مثابه حقی مستقل تثبیت می کند و در نظام ایالات متحده، مقرراتی مانند **CCPA** با اعطای حق انصراف از فروش یا اشتراک گذاری و **BIPA** با الزام به رضایت مکتوب برای داده های بیومتریک و تعیین قواعد حذف و نگهداشت، الگویی از اختیار کتتری و مسئولیت پذیری عملیاتی را پیش می کشند. نظریه پردازی های معاصر نشان می دهند که حریم خصوصی زیرساخت شکل گیری سوژه خودگردان است نه حاشیه ای بر آن، نقض های داده ای صرفا به افشا محدود نمی شوند و طیفی از گردآوری بیش از حد، پردازش تبعیض آمیز و تصمیم گیری الگوریتمی را دربرمی گیرند، ناشناس سازی به طور قابل توجهی شکننده است و مشروعیت جریان داده تابع هنجارهای انتقال بافت مند است که باید به دست سوژه در هر زمینه اجتماعی قابل تعیین و تغییر باشد. ترجمان نهادی این مبانی در سطح طراحی و حکمرانی داده اقتضا می کند متولیان داده در حکم امین با تعهد وفاداری و مراقبت

نسبت به منافع سوژه عمل کنند و سامانه‌های نظارتی به شفافیت و پاسخ‌گویی مقید شوند تا حق خودمختاری داده‌ها از سطح شعار به سطح قواعد عملیاتی تبدیل گردد و نسبت قدرت میان متصدی و فرد به سود کرامت انسانی بازتنظیم شود؛ این همان پیوندی است که مقاله میان مبانی فقهی امامیه و استانداردهای بین‌المللی برقرار می‌کند و از آن‌الگوی مشترکی برای تنظیم‌گری هوشمند پیشنهاد می‌دهد.

۱-۲) مطلب اول: مالکیت و سلطنت بر داده‌های شخصی در فقه اسلامی و نظریه‌های معاصر حقوق داده

در بحث مالکیت و سلطنت بر داده‌های شخصی، نقطه عزیمت در فقه امامیه همان قاعده‌ای است که سلطه انسان بر اموال و شئون خویش را به عنوان حقی پیشینی و غیرابزاری شناسایی می‌کند و این سلطه را مبنای تنظیم روابط حقوقی قرار می‌دهد. هنگامی که در تقریرات اصولی کتاب‌البیع به کارکرد گسترده این قاعده نگاه می‌شود، تنقیح مناط اجازه می‌دهد دامنه سلطنت از قلمرو اعیان و منافع مادی به حوزه شئون شخصیت و اطلاعات منتسب به شخص نیز سرایت کند. اگر لایحل مال امری مسلم‌الا بطیب نفسه معیار عام منع تصرف بی‌رضا در دارایی‌های فرد است، داده‌های منتسب به او هرچند ناملموس و در بسترهای دیجیتال پراکنده، در حصار همین طیب نفس قرار می‌گیرند و هرگونه گردآوری، پردازش و انتقال بدون رضایت معتبر، از سنخ تصرف غیرمجاز تلقی می‌شود. تنها در فرض ضرورت مضیق و براساس مجوز معتبر می‌توان این ممنوعیت را کنار زد، به ویژه جایی که حیثیت و کرامت ذاتی انسان به عنوان غایت قواعد فقهی معیار سنجش مشروعیت مداخلات داده‌محور قرار می‌گیرد و به این ترتیب پیوند میان سلطنت، کرامت و کنترل بر داده‌ها به صورت منسجم ظاهر می‌شود (خمینی، بی‌تا، ج ۱، ص ۵۳۵).

همین منطق سلطنت و رضایت با صورت‌بندی‌های هنجاری حریم خصوصی در ادبیات حقوقی معاصر تلاقی پیدا می‌کند و از دل این تلاقی، ایده خوداختیاری داده نه به عنوان برجستگی اعتباری، بلکه به مثابه ترجمان حقوقی کنترل شخص بر پیرامتن اطلاعاتی خود فهم می‌شود. در آثار دانشگاهی درباره حق انسان بر حریم خصوصی، بر این نکته تأکید می‌شود که رضایت باید آگاهانه، صریح و قابل اثبات باشد و نقض آن آثار مدنی و کیفری قابل مطالبه داشته باشد، تحلیلی که امکان صورت‌بندی عملی حق کنترل بر داده‌های شخصی را حتی در فقدان تصریح تقنینی مستقل فراهم می‌کند. ترکیب اصول قانون اساسی، قواعد فقهی و مقررات بخشی اجازه می‌دهد حق کنترل و تصرف بر داده‌های شخصی از دل نظام موجود استنباط شود. در همین راستا، ماده ۵۸ قانون تجارت الکترونیکی با ممنوع کردن ذخیره، پردازش یا توزیع داده‌پیام‌های شخصی حساس بدون رضایت صریح، شالوده حقوقی داخلی رضایت قابل اثبات را مفروض می‌گیرد و نسبت میان سلطنت فقهی و مشروعیت پردازش را به صورت عملیاتی تنظیم می‌کند. ماده ۷۱ همان قانون نیز ضمانت اجرای این الزام را تأمین می‌کند و نتیجه آن است که هر بهره‌برداری بی‌اذن از اطلاعات حساس نه تنها تعرض به شخصیت اخلاقی، بلکه نقض قاعده سلطنت بر شئون شخصی تلقی می‌شود و در مدار پاسخ



گویی حقوقی قرار می گیرد؛ این همان نقطه ای است که سهم افزوده مقاله در نشان دادن ظرفیت ترجمه مستقیم مبانی فقهی به قواعد روشن حکمرانی داده نمایان می شود.

ساختار هنجاری مالکیت و سلطنت بر داده ها در فقه امامیه با مجموعه ای از اصول و قواعد حکمرانی داده در نظام های معاصر تناظر پیدا می کند که به جای تکیه صرف بر استعاره مالکیت، به مهندسی دقیق مسئولیت ها و حدود قدرت در چرخه پردازش می پردازد. اصول بنیادین ماده ۵ بند ۱ مقرر عمومی حفاظت از داده ها، از قانونی بودن، منصفانه بودن و شفافیت تا محدودیت هدف و کمینه سازی و دقت و محدودیت نگهداشت و تمامیت و محرمانگی و پاسخ گویی، در عمل حاشیه های امن سلطنت بر داده را ترسیم می کنند و با الزام به طراحی متناسب با حریم، مسیر اعمال مؤثر اختیار را در سطح فنی و سازمانی هموار می سازند. ماده ۷ همان مقرر شرایط اعتبار رضایت را سخت گیرانه و قابل اثبات می خواهد تا طیب نفس ادعایی به یک صورت شکلی فروکاسته نشود و بار اثبات بر عهده متصدی قرار گیرد، و ماده ۸ منشور حقوق بنیادین اتحادیه اروپا با شناسایی حق حفاظت از داده به عنوان حقی مستقل، مراقبت می کند که سلطنت بر داده به صورت حق مثبت قابل اعمال و تحت نظارت مرجع مستقل متجلی شود، نه صرف ادعای اخلاقی بدون ضمانت اجرا. بدین ترتیب نسبت میان اختیار شخص و قدرت ساختاری متصدیان داده به قواعد سخت گره می خورد و از خطر مالکیت بی پشتوانه فاصله می گیرد، در حالی که مقاله نشان می دهد این منطق در سطح مبانی با قاعده سلطنت فقهی و منطق رضایت معتبر قابل جمع است و می تواند مبنای الگوی مشترک در حکمرانی داده قرار گیرد (GDPR، art. ۵(۱)، GDPR، ۲۰۱۶، art. ۷، EU Charter، ۲۰۰۰، art. ۸).

۲-۲) مطلب دوم: حریم خصوصی و منع تجسس در شریعت اسلامی؛ بازخوانی فقهی حق خلوت در عصر دیجیتال

در بازخوانی فقهی حق خلوت در عصر دیجیتال نقطه آغاز همان نهی پیشینی از تجسس و سوء ظن است که در باب التجسس و سوء الظن از الکافی بر پایه آیه «ولا تجسسوا» قلمرو کاویدن عورات و اسرار را از پیش می بندد و امکان استنباط یک قاعده هنجاری عام برای مصونیت حریم اطلاعاتی اشخاص را فراهم می کند. بر این اساس هر سازوکار گردآوری پنهان کارانه یا کاوش عمیق در لایه های زندگی خصوصی حتی اگر در قالب لاگ برداری مداوم، کوکی های رهگیری یا تحلیل های رفتاری غیر شفاف صورت گیرد فقط در فرض ضرورت مضیق و بر پایه رضایت معتبر و قابل اثبات توجیه پذیر است و در غیر این صورت به نقض حق الناس بر پوشیدگی داده های شخصی می انجامد و از مدار مشروعیت اخلاقی و حقوقی خارج می شود، زیرا معیار محوری در اینجا کارایی صرف فناورانه نیست بلکه صیانت از حیثیتی است که فقه آن را غایت قواعد سلوکی می شناسد و کاهش آن را حتی با ادعای منفعت عمومی مبهم مردود می شمارد (الکلبینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵). تحریم غیبت در تقریر کرامت محور جواهر الکلام دامنه هتک را از گفتار عربیان به هر پردازش افشاگرانه ای تعمیم می دهد که ستر الهی را می درد و شخصیت فرد را حتی با داده های صادق در معرض مخدوش شدن قرار می دهد و در نتیجه برچسب زنی های الگوریتمی حیثیت زدا، امتیازدهی های



مخاطره محور و افشاهای ثانویه بی‌اذن و بدون اطلاع رسانی کافی در دایره ممنوعیت قرار می‌گیرند مگر آنکه ضرورت متناسب و تضمین‌های شفاف ساز احراز شود، ترجمان نهادی این مبانی در محیط‌های دیجیتال به معنای طراحی حداقل گرا در گردآوری داده، تحدید هدف پردازش، و پیش‌بینی مسیر اعتراض و بازبینی انسانی است تا خلوت معنادار از سطح توصیه اخلاقی به جایگاه قاعده سخت حقوقی ارتقا یابد و سهم افزوده مقاله نیز در همین تبدیل مبانی به معیارهای طراحی و حکمرانی آشکار شود (النجفی، بی‌تا، ج ۲۲، ص ۶۲-۶۳).

اگر سنت اخلاقی حفظ السر و حفظ اللسان به عنوان شالوده امانت‌داری فهم شود، متصدی پردازش داده در حکم امین است که نه تنها از افشای بی‌اذن منع می‌شود بلکه مکلف به کاستن از ریسک‌های ثانویه، نگهداشت متناسب و حذف به موقع نیز هست، به این معنا که سکوت امانت‌دارانه در عصر داده به کنترلی فعال بر چرخه دسترسی، انتقال و افشا ترجمه می‌شود و هر دسترسی افزوده باید به ضرورت و هدف مشخص گره بخورد و هر انتقال به بافت و رضایت مقید گردد و هر نقض احتمالی با سازوکارهای پیشینی جبران و پاسخ‌گویی مواجه شود، در غیر این صورت صورت‌بندی فضیلت رازداری در حد پند اخلاقی باقی می‌ماند و در آزمون نهادی ناکام می‌شود (الکلینی، ۱۴۰۷ق، ج ۲، ص ۱۱۳). این منطق در حقوق عمومی ایران با اصل امنیت ارتباطات صورت‌بندی می‌شود، جایی که اصل ۲۵ قانون اساسی هرگونه بازرسی، استراق سمع و تجسس را مگر به حکم قانون منع می‌کند و دسترسی‌های زیرساختی شبکه‌ای، شنودهای فنی و استخراج‌های فراگیر از کانال‌های ارتباطی حتی با دایه پالایش امنیتی تنها در پرتو مجوز خاص و تشریفات مضیق مشروعیت می‌یابند، در سطح کیفری نیز جرم‌انگاری دسترسی غیرمجاز به داده‌ها و سامانه‌های حفاظت‌شده سپر سلبی لازم را فراهم می‌آورد تا خودمختاری داده‌ها از تعرض‌های بی‌اذن مصون بماند و نظم خلوت در ساحت دیجیتال از درون تهی نشود. هنگامی که ماده ۱۵۰ قانون آیین دادرسی کیفری شنود و دسترسی به داده‌های اشخاص را به ضرورت، مجوز مقام قضایی و تحدید زمانی مشروط می‌کند در واقع همان سه‌گانه قانونی بودن، ضرورت و نظارت قضایی را به عنوان معیار مداخله تثبیت می‌کند و به طراحان و بهره‌برداران سامانه‌ها هشدار می‌دهد که تغذیه الگوریتم‌های پیش‌بین از داده‌های ارتباطی و محیطی نقطه کور مقررات نیست بلکه حساس‌ترین میدان پاسخ‌گویی است و بی‌اعتنایی به آن حق خلوت دیجیتال را به امتیازی صوری تنزل می‌دهد. برای داوری عینی در مصادیق، معیارهای انتظار معقول خلوت و نقض کرامت که در ادبیات حقوقی ایران به ویژه در تحلیل تعرض‌های داده‌محور در محیط‌های خصوصی طرح شده‌اند امکان‌تنزیل اصول پیش‌گفته به سطح قاعده قضایی را فراهم می‌کنند، به این صورت که هر فناوری پایشی از دوربین‌های هو شمند و ابزار شنود تا ردیاب‌های مبتنی بر کلان‌داده باید در پرتو پرسش از انتظار معقول خلوت در آن بافت اجتماعی و از منظر میزان هتک کرامت سنجیده شود نه صرفاً به واسطه توان فنی یا منافع ادعایی، در غیر این صورت فاصله میان نهی فقهی تجسس و واقعیت نظارت فراگیر دیجیتال روزبه‌روز افزایش می‌یابد و حق خلوت به نامی شکننده تبدیل می‌شود که کارکرد عملی خود را از دست می‌دهد، ادغام این معیارها در طراحی و حکمرانی داده همراه با التزام به رضایت آگاهانه و قابل اثبات، محدودیت هدف و کمینه



سازی داده راهی است برای تحقق فقه کرامت محور در بطن رژیم های فنی و حقوقی معاصر بی آنکه به نتیجه گیری های شتاب زده یا تقلیل گرایانه فروغلتد و دقیقاً در همین سطح است که این مقاله سهم نوآورانه خود را در تبدیل مبانی فقهی به معیارهای سنجش پذیر برای تنظیم تصمیم های الگوریتمی نشان می دهد (کوشکی، ۱۳۹۰، ص ۱۴۱؛ قانون جرایم رایانه ای، ۱۳۸۸، مواد ۴ و ۸-۱۰).

۲-۳) مطلب سوم: عدالت و مسئولیت الگوریتمی؛ از قاعده لاضرر تا مبانی فقهی منع ظلم دیجیتال

در تحلیل عدالت و مسئولیت الگوریتمی، هرگاه پیش بینی گری داده محور به تصمیم هایی گره بخورد که آثار حقوقی یا حیثیتی دارند، قاعده «لا ضرر و لا ضرار» چارچوبی پیشینی برای تحدید دامنه مشروعیت فراهم می کند و نشان می دهد هر پردازش و تصمیم گیری مفرضی به زیان مؤثر اقتصادی، بدنی یا عرضی از اصل در دایره منع قرار دارد مگر آنکه ضرورت نوعی و مجوز معتبر برای آن احراز شود. در این صورت بار توجیه بر دوش طراح و بهره بردار سامانه قرار می گیرد تا به صورت مستند نشان دهند نسبت سود و زیان اجتماعی چگونه سنجیده شده و چرا مداخله داده محور از مرز ضرورت فراتر نرفته است، علاوه بر این ملزم اند در معماری فرایند، مداخله انسانی معنادار، مسیر اعتراض مؤثر و قابلیت بازبینی و جبران را در دل سیستم تعبیه کنند تا امکان انتساب زیان به فاعل انسانی و نهاد تصمیم گیر برقرار بماند و جبر الگوریتمی به عذر رافع مسئولیت تبدیل نشود (انصاری، بی تا، ج ۵، ص ۱۶۱). در سطح حقوق عمومی، مصونیت حیثیت، جان و حقوق اشخاص که به تصریح قانون اساسی تنها با تجویز قانون قابل تحدید است، بنیانی برای منع هر پردازش تحقیرآمیز یا حیثیت زدا در عرصه داده فراهم می کند و می توان حیثیت داده ای را در امتداد همان کرامت مصون دانست که بی اذن معتبر یا حکم خاص قانون نباید در معرض برچسب گذاری و افشا قرار گیرد؛ بر این اساس عدالت رویه ای ایجاب می کند قبل از اعمال هر نتیجه الگوریتمی با پیامد حقوقی، امکان شنیده شدن، دسترسی به دلایل مؤثر و توقف تصمیم خودکار فراهم شود تا نسبت میان اختیار شخص و قدرت محاسباتی به قاعده پاسخ گویی گره بخورد و سهم مقاله نیز در همین برجسته سازی پیوند قاعده لاضرر با طراحی سازوکارهای اعتراضی سنجش پذیر نمودار شود (قانون اساسی، اصل ۲۲).

در ساحت سنجش هنجاری ابزارها، این نکته که رضایت به تنهایی علت تامه جواز مداخله نیست و در تراحم با حفظ نظام یا منع ضرر باید به صورت مضیق و تحت نظارت قضایی اعمال شود، نسبت عدالت الگوریتمی با حق خلوت و خوداختیاری را از سطح تشریفات فراتر می برد و متصدی داده را مکلف می سازد افزون بر اخذ رضایت آگاهانه و قابل اثبات، از گردآوری بیش از حد، نگهداشت نامحدود و انتقال بی بافت نیز پرهیز کند، زیرا نقض های داده ای صرفاً به افشا محدود نمی شوند و از مرحله جمع آوری تا پردازش تبعیض آمیز و تصمیم سازی ناعادلانه امتداد می یابند و هر یک می تواند مصداقی از «ضرر» باشد که به محض انتساب، ضمان نهادی و جبران می طلبد (اکبری، ۱۴۰۰، ص ۱۰-۱۳؛ Solove, ۲۰۰۶, vol. ۱۵۴, p. ۴۸۸-۵۰۶). در این میان،



تکیه سیاستی بر ناشناس سازی کلاسیک با آشکار شدن شکنندگی شگفت آور امکان بازشناسایی در اقتصاد داده، قدرت اقناعی خود را تا حد زیادی از دست می دهد و ناگزیر هسته عدالت باید به سمت حقوق کنترلی قابل اعمال از جمله حق انصراف، تحدید غرض، کمینه سازی و حق اعتراض منتقل شود تا چرخه های پیوند مجدد داده های پراکنده نتواند زیان های نامرئی بر اشخاص تحمیل کند و ادعای بی ضرر بودن پردازش، به نظارت بیرونی و آزمون های ممیزی پاسخ گو باشد (Ohm, 2010, p. 1708-1727). عدالت الگوریتمی تنها زمانی به صورت نهادی استقرار می یابد که قواعد منع ضرر با امانت داری اطلاعاتی جمع شوند؛ به این معنا که متولیان داده در حکم «امین» موظف به وفاداری و مراقبت از منافع سوژه اند و حق ندارند از عدم تقارن قدرت و اطلاعات برای استخراج ارزش بدون رضایت بهره بگیرند، بلکه باید در طراحی و حکمرانی سامانه ها معیارهای بافت مند انتقال، شفافیت دلایل مؤثر، قابلیت ردپای تصمیم و امکان تصحیح را نهادینه کنند تا موازنه میان شفافیت و صیانت از داده های شخصی که ادبیات داخلی نیز بر ناتمامی معیارهای آن تأکید کرده است به سود کرامت انسانی بازتنظیم شود و هر گونه دسترسی، پردازش یا انتشار پیش از آنکه به عادت سازمانی بدل گردد از غریب ضرورت، تناسب و پاسخ گویی عبور کند و در صورت تراحم، اولویت با رفع ضرر شخص و پیشگیری از بهره کشی از آسیب پذیری های پیش بینی پذیر باشد تا در نهایت شبکه ای از تعهدات سخت از اطلاع رسانی معنادار و مجاری اعتراض کارآمد تا ممیزی تبعیض و سازوکارهای جبران نقش ضامن عملی اجرای قاعده لاضرر در زیست جهان دیجیتال را ایفا کند.

۳) مبحث سوم: تطبیق فقه اسلامی و نظام حقوق بشر در تنظیم گری پیش بینی گری هوشمند

در این مبحث، پیش بینی گری هوشمند به عنوان هر سازوکاری تعریف می شود که با تکیه بر داده های رفتاری، درباره ریسک و فرصت اشخاص تصمیم های اثرگذار اتخاذ می کند و پرسش اصلی آن است که فقه اسلامی و نظام حقوق بشر چه حدودی برای این نوع نظارت پیشینی ترسیم می کنند. نقطه آغاز در فقه امامیه نهی از تجسس و تتبع عورات است؛ حدیث «لا تتبعوا عورات المؤمنین» در الکافی با تکیه بر آیه «ولا تجسسوا» ممنوعیت پایش پنهانی را تثبیت می کند و مرز میان مراقبت مشروع و نظارت نفوذی را نشان می دهد، به گونه ای که هر نظام داده محوری که به نام پیش بینی به حوزه خلوت مؤمن نفوذ کند، جز در فرض ضرورت نوعی و مجوز مضیق در دایره مناهی شرعی قرار می گیرد و مشروعیت خود را از دست می دهد (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵). روایت نبوی «من تتبع عورات المؤمنین تتبع الله عورته» در بحارالانوار این منع را به شکل قاعده بازدارنده ای علیه مراقبت بی ضابطه و افشای خصوصیات صورت بندی می کند و سازوکاری اخلاقی حقوقی به دست می دهد که با اصول کرامت انسانی در اسناد بین المللی هم افق است و در مقام تنظیم گری، به محدود کردن رفتارهای هوش مصنوعی در رصد پیشینی افراد دلالت دارد (المجلسی، ۱۴۰۳ق، ج ۷۵، ص ۲۱۴، من تتبع عورات المؤمنین تتبع الله عورته). در مسالک الافهام ذیل بحث حرمت نظر به عوره، منع مشاهده تنها به عریانی جسمانی منحصر نمی ماند و می توان آن را بر نظارت داده محور و پروفایلینگ کاوشگر لایه های پوشیده حیات خصوصی نیز حمل کرد، خوانشی که وقتی با تأکید تحریر الوسيله بر وجوب ستر و حرمت نظر به عورات غیر جمع



می شود، حصانت حریم را به صورت تکلیف دوطرفه برای ناظر و منظور تثبیت و در زبان امروز به اصل حداقل گرایی در داده و پرهیز از پردازش نامحدود داده های حساس ترجمه می کند (الشهید الثانی، ۱۴۱۳ق، ج ۷، ص ۴۹؛ الخمینی، ۱۴۰۸ق، ج ۱، ص ۱۷).

در نظام حقوقی ایران همین مبانی از سطح فقهی به متن قانون راه یافته و به قواعد الزام آور تبدیل شده است، به گونه ای که اصل ۲۵ قانون اساسی با منع بازرسی، استراق سمع و تجسس مگر به حکم قانون، بنیان حق خلوت ارتباطی را می گذارد و استنهاها را به مجوزهای قضایی مضیق مقید می کند تا پایش الگوریتمی در بستر ارتباطات الکترونیکی نتواند به نظارت فراگیر بدل شود. ماده ۵۸ قانون تجارت الکترونیکی ۱۳۸۲ با الزام به رعایت محرمانگی و ممنوعیت افشای داده های شخصی، سازوکار داخلی تحقق اصول هدف مندی و رضایت معتبر را در سامانه های هوشمند پیش بینی گر فراهم می سازد و ماده ۱۷ قانون جرایم رایانه ای ۱۳۸۸ هرگونه انتشار داده های خصوصی بدون رضایت را جرم می داند و در نتیجه استفاده از داده های صوتی و تصویری برای امتیازدهی الگوریتمی را در معرض مسئولیت کیفری قرار می دهد. ماده ۳ همان قانون که به جاسوسی رایانه ای می پردازد، دسترسی غیرمجاز به داده های سری و شنود محتوای در حال انتقال را مستوجب مجازات می شمارد و برای طراحان سامانه های پیش بینی گر این پیام را دارد که کاوش نفوذی در داده ها بیرون از مجاری قضایی مجاز نیست. ماده ۱۵۰ قانون آیین دادرسی کیفری ۱۳۹۲ نیز اصل منع کنترل ارتباطات مخابراتی را تثبیت و مداخله در داده های شخصی را به فروض محدود امنیتی و مجوز مقام عالی قضایی منحصر می کند و از منظر حقوق تطبیقی، همان سه گانه قانونی بودن، ضرورت و تناسب را که در حقوق بشر معاصر معیار مداخله در حریم خصوصی است در سطح ملی نهاده می سازد.

در سطح بین المللی، نظام های اروپایی و آمریکایی اصولی را که از حیث ماهوی با قواعد فقهی پیش گفته هم خوانی دارند به صورت صریح در قوانین حفاظت از داده و مقررات هوش مصنوعی تدوین کرده اند و همین هم افقی، نقطه اتصال تطبیقی این مقاله است. ماده ۲۲ مقرر عمومی حفاظت از داده ها ۲۰۱۶ حق اشخاص بر عدم ابتلا به تصمیم صرفاً خودکار را تضمین می کند و سامانه های پیش بینی گر را ملزم به فراهم کردن امکان مداخله انسانی، توضیح پذیری و بازبینی می سازد. ماده ۸ منشور حقوق بنیادین اتحادیه اروپا ۲۰۰۰ و اصلاحات ۲۰۱۲ حق بر داده های شخصی را همراه با لزوم پردازش منصفانه، هدف مند و تحت نظارت مرجع مستقل تثبیت می کند و ماده ۸ کنوانسیون اروپایی حقوق بشر ۱۹۵۰ هر مداخله مبتنی بر پیش بینی خطر را تنها در صورت ضرورت قانونی، هدف مشروع و تناسب شدید می پذیرد. ماده ۵ بند ۱ جزء د قانون هوش مصنوعی اروپا ۲۰۲۴ استفاده از سامانه هایی را که صرفاً بر اساس پروفایلینگ خصائص شخصیتی، خطر ارتکاب جرم را پیش بینی می کنند ممنوع می داند و نشان می دهد که مرز مشروعیت پیش بینی کیفری در سطح اتحادیه کجا ترسیم شده است. در حقوق داخلی ایالات متحده نیز مقررات محلی مانند قانون شهر نیویورک شماره ۱۴۴ سال ۲۰۲۱ استفاده از ابزارهای خودکار تصمیم گیری در استخدام را بدون حسابرسی سوگیری و اطلاع رسانی قبلی ممنوع می کند و مشروعیت پیش بینی را به مسئولیت پذیری و شفافیت گره می زند. این مبحث با کنار هم نشاندن این قواعد، سهم افزوده خود را در نشان دادن امکان صورت بندی چارچوبی مشترک ارائه می کند که در آن، نهی

فقهی از تجسس و هتک حرمت با اصول حقوق بشری درباره ضرورت، تناسب، توضیح پذیری و بازیابی انسانی جمع می شود و به نقشه راهی عملی برای تنظیم گری پیش بینی گری هوشمند در ایران بدل می گردد.

در جمع بندی تطبیقی این مبحث می توان سه ستون هنجاری را به صورت کنار هم ترسیم کرد؛ ستون نخست یعنی فقه امامیه با تأکید بر منع تجسس، قاعده لا ضرر و سلطنت بر شئون شخصی، نقطه عزیمت را بر ممنوعیت تقریباً مطلق تتبع عیوب و کاوش در حریم قرار می دهد و فقط در فرض ضرورت مضیق و مجوز شرعی مداخله داده محور را می پذیرد، در حالی که ستون دوم یعنی حقوق اساسی ایران با اصول ۲۲ و ۲۵ و محدودیت های شنود و پردازش، همین مبانی را به زبان قانونی بودن و نظارت قضایی بازنویسی می کند اما در عمل امکان گسترش استثنایها را از طریق قوانین عادی باز می گذارد؛ در ستون سوم، الگوی اروپایی با ماده ۸ منشور حقوق بنیادین، ماده ۸ کنوانسیون اروپایی حقوق بشر، ماده ۲۲ مقرر عمومی حفاظت از داده ها و ممنوعیت های قانون هوش مصنوعی، محور را بر سه گانه قانونی بودن، ضرورت و تناسب و بر منع معدودی از کاربری های پرخطر قرار می دهد و از این جهت نسبت به فقه که اصل را بر حرمت تتبع می گذارد نرم تر و مداخله پذیرتر است. در مقابل، منظومه حقوق بشر اروپایی با وجود شناسایی حق عدم تعرض به تصمیم صرفاً خودکار، هنوز حق توضیح عام و دسترسی صریح به منطق تصمیم را تضمین نکرده است، در حالی که در فقه امامیه تأکید بر امکان دفاع، شنیده شدن و منع هتک ستر مؤمن اقتضا می کند هر تصمیم حیثیت زدا در ساختاری اتخاذ شود که استماع قول طرف و مداخله انسان مسئول را تضمین کند و صرف تکیه بر محاسبه خودکار کافی دانسته نشود. در نهایت می توان گفت فقه امامیه سخت گیرترین قلمرو را برای گردآوری و کاوش داده ترسیم می کند، حقوق اساسی ایران حد میانی و متأثر از همان مبانی را نشان می دهد و منظومه اروپایی در عین استقرار سازوکارهای نیرومند شفافیت و نظارت، میدان و سیع تری برای پیش بینی گری باقی می گذارد؛ همین تفاوت ها و هم پوشانی ها است که نشان می دهد تطبیق در این مقاله صرف نام بردن از متون نیست بلکه تحلیلی هنجاری از نقاط اجتماع و افتراق سه دستگاه در تنظیم پیش بینی گری هوشمند ارائه می کند.

۳-۱) مطلب اول: حق خودمختاری داده‌ها در حقوق بشر بین‌المللی و الزامات صیانت از کرامت انسانی

صورت بندی حق خودمختاری داده ها در حقوق بشر بین المللی زمانی از سطح شعار فراتر می رود که کرامت انسانی به زبان قواعد مشخص برای مهار مداخله در حیطه های خصوصی، خانوادگی و ارتباطی ترجمه شود. در منظومه اروپایی، حق حمایت از داده های شخصی به عنوان حقی مستقل و ایجابی تثبیت شده که لوازم آن پردازش منصفانه، هدف مند و تحت نظارت مرجع مستقل است و در کنار آن، معیارهای کلاسیک احترام به زندگی خصوصی و مکاتبات، سه گانه قانونی بودن، ضرورت و تناسب را بر هر سازوکار پیش بینی گر تحمیل می کند تا جریان تصمیم های داده محور حتی هنگامی که با داعیه منافع عمومی پیش می رود از مدار کرامت خارج نشود و امکان بازخواست پذیری درون زا را حفظ کند (EU Charter, ۲۰۱۲/۲۰۰۰, ECHR art. ۸).



۱۹۵۰، art. ۸). در این چارچوب، حق خودمختاری داده ها صرفاً حق مخالفت با افشا نیست بلکه حق تعیین حدود گردآوری، پردازش و استفاده ثانوی از داده های شخصی است و معیار سنجش پذیر آن در عمل میزان امکان کنترل فرد بر چرخه تصمیم گیری داده بنیان است که این مقاله می کوشد آن را به صورت روشن تر استخراج کند.

در دل همین معماری هنجاری، حق عدم ابتلا به تصمیم صرفاً خودکار با آثار حقوقی یا مشابه جایگاهی محوری می یابد. این حق به نحو پیش فرض بر تصمیم های الگوریتمی اثرگذار قید مداخله انسانی، بیان نظر و امکان اعتراض را تحمیل می کند و نشان می دهد صیانت از اختیار واقعی بدون طراحی مسیر بازگشت انسان به متن تصمیم به سرعت به صوری سازی کرامت می انجامد (GDPR، ۲۰۱۶، art. ۲۲). ادبیات انتقادی حقوق داده یادآور می شود که برخلاف تصور رایج، متن مقرر اروپایی حق توضیح عام برای همه تصمیم های خودکار را برقرار نکرده است و اتکای صرف به اطلاع رسانی کلی کفایت نمی کند. باید در سطح فنی و سازمانی لایه های تکمیلی مسئولیت پذیری و شفاف سازی دلایل موثر تعبیه شود تا اعتراض فردی از تشریفات عبور کرده و به امکان بازبینی واقعی تبدیل شود (Wachter et al., ۲۰۱۷، p. ۷, vol. ۷۶-۹۹). قرائت متنی و نظام مند از همان مقرر بر این نکته تاکید می کند که «اطلاعات معنادار درباره منطق دخیل» هرگاه به صورت عملیاتی و قابل اتکا فراهم شود، اثر تنظیمی مستقیم دارد و سنگ بنای اعتراض موثر و رجوع انسانی را می سازد و به این ترتیب حلقه اتصال میان خودمختاری داده و کرامت قابل اعمال در فرایند شکل گیری تصمیم تقویت می شود (Selbst & Powles، ۲۰۱۷، p. ۷, vol. ۲۳۳-۲۴۲).

با انتقال بحث از سطح حقوق بنیادین به سطح قواعد بخشی حکمرانی فناوری، نسبت میان پیش بینی گری هوشمند و حدود مشروعیت مداخله شفاف تر می شود. ممنوعیت به کارگیری سامانه هایی که صرفاً بر پایه پروفایلینگ و خصائص شخصیتی، ریسک ارتکاب جرم را پیش بینی می کنند مرزی صریح میان تحلیل داده و پیش داوری ماشینی ترسیم می کند و پیامد هنجاری آن این است که تصمیم های پرمخاطره نمی توانند از بار اثبات تناسب و ضرورت مبتنی بر دلایل قابل ممیزی شانه خالی کنند. پیوند طراحی با پاسخ گویی از مسیر تکلیف به حسابرسی سوگیری و اطلاع رسانی پیشینی به ذی نفعان نشان می دهد خودمختاری داده بدون نهادینه سازی ممیزی، افشا و رجوع انسانی به آسانی به وضعیتی نمایشی فروکاسته می شود و تنها با الزام های بیرونی می توان از تبدیل پیش بینی به قهر بی چهره جلوگیری کرد (AI Act، ۲۰۲۴، art. ۵(۱)(د)؛ NYC Local Law ۱۴۴، ۲۰۲۱، P ۸۷۱-۲۰). در این مبحث، سهم افزوده مقاله برجسته کردن همین گذار از اعلام حق به طراحی سازوکارهای نظارتی مشخص در مواجهه با سامانه های پیش بینی گر است.

برای آنکه حق خودمختاری داده ها در مقام عمل به ضامن عدالت رویه ای بدل شود، باید پیامدهای توزیعی تصمیم های پیش بینی گر نیز به طور سنجش پذیر در نظر گرفته شود. پژوهش های کلاسیک در باب تبعیض نامستقیم داده محور نشان داده اند که حتی در غیاب نیت تبعیض، برچسب گذاری و امتیازدهی مبتنی بر همبستگی های ساختاری می تواند به محرومیت های نظام مند و سلب فرصت های برابر بینجامد و به فرسایش کرامت گروه های خاص منجر شود. معماری حقوقی صیانت از کرامت ناگزیر



است در کنار شروط مشروعیت مداخله و الزامات اطلاع رسانی، سازوکارهای حسابرسی تبعیض، اصلاح فرایندی و جبران قابل اعمال را تثبیت کند تا حلقه ادعا تا اجرا کامل شود و حق بر تعیین سرنوشت اطلاعاتی از سطح ادراک نظری به سطح کنش حقوقی ملموس ارتقا یابد (Barocas & Selbst, ۲۰۱۶, vol. ۱۰۴, p. ۶۷۱-۷۳۲).

۳-۲) مطلب دوم: کرامت انسانی در فقه اسلامی و نظام حقوق بشر جهانی؛ بازاندیشی در مبانی انسان‌محوری

در بازاندیشی نسبت کرامت انسانی با انسان‌محوری در عصر پیش‌بینی‌گری ماشینی، نقطه شروع در سنت فقهی امامیه نهی‌های مؤکد از تجسس و هتک ستر است که مرز خلوت را به منزله حیثیتی مصون برای فاعل مختار ترسیم می‌کند. حدیث «لا تتبعوا عورات المؤمنین» در الکافی با منع تتبع عیوب، اصل هنجاری منع نظارت نفوذی را صورت‌بندی می‌کند و به طور مستقیم فهم حق بر پوشیدگی داده و ضرورت پرهیز از کاوش بی ضابطه در لایه‌های زیست خصوصی را پشتیبانی می‌کند؛ نتیجه عملی این مبنا، الزام به تحدید غرض پردازش و امتناع از گردآوری بیش از حد داده‌های شخصی است نه صرفاً توصیه اخلاقی عام (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵). همین منطق در روایت «من تتبع عورات المؤمنین تتبع الله عورته...» در بحار الانوار با شدت بخشیدن حرمت تتبع خصوصیات، مرز میان نصیحت مسئولانه و مراقبت گریبی ضابطه را روشن می‌کند و هر پروفایلینگ فراگیری را که خوشنامی و امنیت حیثیتی افراد را تهدید کند در دایره منع قرار می‌دهد مگر آنکه ضرورت منصوص و ضوابط شفاف احراز شود (المجلسی، ۱۴۰۳ق، ج ۷۵، ص ۲۱۴). هنگامی که جواهر الکلام غیبت را «ذکر اخیک بما یکره» تعریف می‌کند، برجسب زنی‌های پیش‌گویانه‌ای که به بدنام‌سازی نظام‌مند یا تصمیم‌های تبعیض‌آمیز می‌انجامند، از حیث فقهی ذیل هتک ستر مؤمن قرار می‌گیرند و به محض فقدان ضرورت و امکان دفاع، نامشروع می‌شوند و دیگر نمی‌توان آنها را صرفاً خطای فنی یا پیامد ناخواسته دانست، بلکه مصادق ظلم داده‌محور تلقی می‌شوند (النجفی، بی‌تا، ج ۲۲، ص ۶۳). بحث «حرمة النظر إلى العورة» در مسالک الافهام به قیاس اولویت بر نظارت داده‌محور در ساحات پوشیده‌زندی نیز قابل حمل است و مبنایی برای منع کاوش‌های عمیق الگوریتمی در داده‌های حساس فراهم می‌کند مگر در موارد اضطرار منصوص و فقط به قدر حاجت (الشهید الثانی، ۱۴۱۳ق، ج ۷، ص ۴۹). در تحریر الوسیله نیز با وجوب ستر و حرمت نظر به عورات غیر، اصل حصانت حریم به صورت تکلیف دوطرفه تثبیت می‌شود و وقتی این منطق به زبان تنظیم‌گری امروز ترجمه شود، به لزوم حداقل‌گرایی در داده، پرهیز از پردازش مضیق نشده داده‌های حساس و پیش‌بینی حق اعتراض و مداخله انسانی در تصمیم‌های اثرگذار می‌انجامد، در نتیجه کرامت از سطح شعار به سطح سازوکارهای قابل اعمال در چرخه تصمیم‌ارتقا می‌یابد و سهم تحلیلی این مقاله نیز در برجسته کردن همین گذار است (الخمنی، ۱۴۰۸ق، ج ۱، ص ۱۷).

در رویارویی این بنیان فقهی با دستگاه حقوق بشر جهانی، مسئله اصلی تقابل ساده سنت و مدرنیته نیست، بلکه نشان دادن هم‌داستانی هنجاری در صیانت از خودآیینی در برابر معماری‌های پیش‌بینی‌گر است. مفهوم «هایپرنج» به عنوان تنظیم‌گری از رهگذر



طراحی و شخصی سازی پیوسته نشان می دهد سامانه های مبتنی بر کلان داده چگونه با جابه جایی نامحسوس قیود انتخاب، اختیار واقعی را فرسایش می دهند و رفتارها را در مسیرهای از پیش طراحی شده هدایت می کنند؛ بنابراین حتی اگر جمع آوری و استفاده از داده با رضایت شکلی همراه باشد، بدون چارچوب های ضرورت، تناسب و شفافیت و بدون تضمین مسیر خروج و بازبینی انسانی، کرامت به سطحی نمادین فروکاسته می شود و فاعل انسانی به سوژه قابل دستکاری تبدیل می گردد (Yeung, ۲۰۱۷, p. ۱۱۸-۱۳۶). همین دغدغه در نقد «جامعه امتیازدهی» نیز بازتاب دارد؛ آنجا که بر تضمین دادرسی منصفانه در تصمیم های خودکار، تکلیف به اطلاع رسانی اقدام نامطلوب و حق دسترسی به دلایل مؤثر تأکید می شود تا برچسب های پیش گویانه به قهر بی چهره تبدیل نشوند و فرد بتواند با اعتراض مؤثر و رجوع انسانی نسبت میان کرامت و پیش بینی را بازتنظیم کند (Citron & Pasquale, ۲۰۱۴, p. ۱-۳۳). انسان محوری ادعا شده در حکمرانی داده تنها زمانی واجد محتواست که از یک سو قیود فقهی منع تجسس، منع هتک ستر و حصانت حریم به صورت قواعد سخت در طراحی و بهره برداری سامانه ها متبلور شود و از سوی دیگر سازوکارهای حقوق بشری شفافیت و پاسخ گویی با حق شنیده شدن و مداخله انسانی در هر تصمیم اثرگذار گره بخورد؛ این مقاله بر همین نقطه تلاقی دست می گذارد و نشان می دهد چگونه می توان پیش بینی گری را در مدار کرامت قابل سنجش و بازخواست نگاه داشت، نه آنکه آن را به ابزاری برای بی اثر کردن شأن مختار انسان بدل کرد (الکلینی، ۱۴۰۷ق، ج ۲، ص ۳۵۵؛ النجفی، بی تا، ج ۲۲، ص ۶۳).

۳-۳) مطلب سوم: سیاست گذاری هوش مصنوعی بر پایه عدالت و کرامت؛ الگوی اسلامی - حقوق بشری تنظیم گری

سیاست گذاری هوش مصنوعی بر مدار عدالت و کرامت زمانی معنا دار است که نخستین ریل گذاری آن بر حق خلوت ارتباطی و اصل منع مداخلات پنهان استوار شود. هر گونه شنود الگوریتمی ترافیک یا محتوای ارتباطات حتی با داعیه ارتقای کارایی یا پیشگیری از خطر فقط در قالب مجوزهای استثنایی و با تشریفات مضیق قابل توجیه است؛ به این معنا که طراحی سامانه باید از ابتدای امر با سه گانه قانونی بودن، ضرورت و نظارت قضایی سنجیده شود تا نظارت فنی به قهر نامرئی پیش بینی تبدیل نگردد و نسبت میان قدرت محاسباتی و اختیار انسانی در تاریکخانه های داده جابه جا نشود. مقاله بر این نکته تأکید می کند که اصل بر ممنوعیت رصد فراگیر است و بار اثبات ضرورت و تناسب بر دوش طراح و بهره بردار سامانه قرار می گیرد، نه بر دوش افراد در معرض نظارت (قانون اساسی، اصل ۲۵؛ قانون آیین دادرسی کیفری، ۱۳۹۲، ماده ۱۵۰). در سطح حکمرانی خدمات الکترونیکی، الزام به محرمانگی، منع افشای اسرار و تثبیت اصول هدف مندی و حداقل سازی داده، متصدی را مکلف می سازد که افزون بر اخذ رضایت مؤثر و قابل اثبات، از هر کاوش نفوذی و رهگیری سری خارج از مجاری قضایی پرهیز کند؛ استفاده از داده های خام حساس برای امتیازدهی یا طبقه بندی پیش بین در غیر این صورت به سادگی به نقض کرامت و مسئولیت کیفری می انجامد و توجیه



تصمیم را از سطح ادعا به سطح پاسخ‌گویی عملیاتی منتقل می‌کند (قانون تجارت الکترونیک، ۱۳۸۲، ماده ۵۸؛ قانون جرایم رایانه‌ای، ۱۳۸۸، ماده ۱۷؛ قانون جرایم رایانه‌ای، ۱۳۸۸، ماده ۳).

صورت‌بندی نظری این ریل‌گذاری زمانی استحکام می‌یابد که حریم نه صرفاً به قلمرو مکانی، بلکه به مثابه پیرامتن اطلاعاتی شخص و حق تصرف و کنترل بر جریان‌های مرتبط فهم شود. در این تلقی، ضوابطی چون رضایت آگاهانه، تناسب و ضرورت و امکان پس‌گرفتن اراده در مرکز معماری سامانه قرار می‌گیرند و به معیارهای سنجش‌پذیر عدالت رویه‌ای تبدیل می‌شوند؛ رضایت باید صریح، تفکیک شده از شروط نامرتب و همراه با امکان اثبات و بازگشت باشد تا به امتیاز شکلی فروکاسته نشود و کرامت انسانی را از دستبرد تصمیم‌های خودکار مصون نگه دارد (رحمدل، ۱۳۸۴، صص ۱۱۹-۱۴۶). تحلیل ماهیت‌شناسانه حق بر حریم، با تشبیه حریم داده‌ها به نوعی «حریم ارتفاقی منفی»، نشان می‌دهد قانون‌گذار ابزار وضع محدودیت‌های الزام‌آور بر پردازش و پیش‌بینی را در اختیار دارد و می‌تواند تعادل میان آزادی گردش اطلاعات و صیانت از شخصیت حقوقی فرد را از سطح شعار به سطح قاعده قابل اعمال ارتقا دهد (امام‌وردی، ۱۳۹۶، صص ۳۴۷-۳۶۶). در ساحت اجرا، معیار «انتظار معقول خلوت» همراه با شاخص نقض کرامت، ابزار دآوری قضایی مصادیق نوین تعرض داده‌محور از حسگرهای خانگی تا سامانه‌های پیش‌بینی وقوع جرم را فراهم می‌کند و ورود فناورانه بدون مجوز خاص را با الزامات دادرسی منصفانه ناسازگار می‌سازد؛ هر چرخه پیش‌بینی از گردآوری تا نگهداشت و انتشار باید پیشاپیش در ترازوی ضرورت و تناسب سنجیده و ریسک‌های تبعیضی و حیثیتی آن مهار شود (کو شکی، ۱۳۸۶، صص ۱۳۵-۱۵۲). سیاست شفافیت اداری نیز تنها در صورتی به نقطه تعادل می‌رسد که داده‌های عمومی و شخصی به‌دقت تفکیک و استثنائات حریم خصوصی به صورت مضیق اعمال شود؛ در غیر این صورت دسترسی می‌تواند به درز داده و برچسب‌زنی تبعیض‌آمیز بدل شود و سرمایه اعتماد عمومی را فرسوده سازد (یعقوبی، ۱۳۹۹).

نتیجه‌گیری

پیش‌بینی گری هوشمند با وجود توانایی چشمگیر در آشکارسازی الگوهای پنهان و افزایش کارایی، به محض ورود به قلمرو حیثیت، اختیار و فرصت‌های واقعی انسان دیگر نمی‌تواند صرفاً به عنوان محاسبه فنی فهم شود و باید در چارچوب هنجارهایی خوانده شود که کرامت را حد‌نهایی مداخله می‌دانند. این پژوهش نشان داد قواعد فقهی صیانت از خلوت، منع تتبع و حرمان حریم در کنار اصول حقوق بشری قانون‌مندی، ضرورت، تناسب و پاسخ‌گویی می‌توانند به صورت مجموعه‌ای از قیود پیش‌بینی بر طراحی و بهره‌برداری از سامانه‌های پیش‌بین اعمال شوند و فناوری را از ابزار ظاهراً بی‌طرف به نهادی پاسخ‌گو تبدیل کنند. بر این اساس هر چرخه داده از گردآوری و برچسب‌گذاری تا امتیازدهی و اجرا باید با حداقل‌گرایی داده، تحدید غرض پردازش، شفافیت دلایل مؤثر، امکان اعتراض مؤثر و مداخله از سانی معنادار مهار شود و هر جا خطر انگ زنی، تبعیض ساختاری یا انتقال قدرت بی‌قید از فرد به متولیان داده پدید آید، بار اثبات مشروعیت و فایده خالص بر عهده طراح و بهره‌بردار قرار می‌گیرد نه بر



دوش شخص موضوع تصمیم که معمولاً کم اطلاع ترین و کم قدرت ترین بازیگر این میدان است. در نتیجه، معیارهای کرامت محور از سطح توصیه اخلاقی فراتر می روند و به شاخص های سنجش پذیر برای داوری درباره مشروعیت تصمیم های الگوریتمی بدل می شوند.

الگوی اسلامی حقوق بشری تنظیم گری که در این پژوهش صورت بندی شد صرفاً کنار هم نشان دادن دو دستگاه معرفتی نیست بلکه مفصل بندی عملی میان حق تعیین سرنوشت اطلاعاتی و عدالت رویه ای به شمار می آید. این الگو از یک سو با ترجمه قواعد کرامت محور به الزامات مهندسی و حکمرانی از قبیل طراحی متناسب با حریم، ممیزی منظم سوگیری، رد پای پذیری تصمیم و جبران مؤثر، قدرت محاسباتی را در مدار پاسخ گویی نگه می دارد و اجازه نمی دهد جبر الگوریتمی به عذر رافع مسئولیت تبدیل شود. از سوی دیگر با پیوند زدن حق خلوت، اختیار و حیثیت به سازوکارهای قابل اعمال مانند حق دسترسی، اطلاعات معنادار درباره منطق تصمیم، امکان توقف و بازنگری، از فروکاستن انسان به موضوع پیش گویی آماری جلوگیری می کند و نشان می دهد عدالت و کرامت در عصر هوش مصنوعی نه زینت های تکمیلی که اجزای سازنده معماری تصمیم هستند. اگر این قیود به صورت پیشینی در طراحی نهادی و فنی تعبیه شوند، پیش بینی به ابزار خدمت گزار بدل می شود و نسبت میان امنیت، کارایی و آزادی بر محور انسان مختار و با کرامت بازتنظیم می گردد.



فهرست منابع؛

قرآن کریم

قوانین:

۱. قانون اساسی جمهوری اسلامی ایران. ۱۳۵۸.
۲. قانون آیین دادرسی کیفری. ۱۳۹۲.
۳. قانون تجارت الکترونیکی. ۱۳۸۲.
۴. قانون جرایم رایانه‌ای. ۱۳۸۸ (اصلاحی ۱۳۹۹).

کتاب:

۵. اکبری، علیرضا. «حریم خصوصی در نظام حقوقی ایران و اسلام». دوفصلنامه تمدن حقوقی ۴، ش ۹-۱۰ (۱۴۰۰): ۳۶۹-۳۹۲.
۶. اماموردی، محمدحسن. «ماهیت‌شناسی حق بر حریم در نظام حقوقی ایران». مجله حقوق خصوصی ۱۴، ش ۲ (۱۳۹۶): ۳۶۶-۳۶۷.
۷. الأنصاری، مرتضی. کتاب المکاسب. ج ۵. قم: تراث الشیخ الأعظم، بی‌تا.
۸. حبیب‌زاده، محمدجعفر، و اسمعیل رحیمی‌نژاد. «کرامت انسانی در قانون اساسی جمهوری اسلامی ایران». مدرس علوم انسانی ۱۱، ش ۴ (۱۳۸۶): ۵۱-۸۲.
۹. الحر العاملی، محمد بن الحسن. وسائل الشیعة. ج ۸. بیروت: دار إحياء التراث العربی، بی‌تا.
۱۰. الخمينی، روح‌الله. تحریر الوسیلة. ج ۱. قم: دارالعلم، ۱۴۰۸ق.
۱۱. الخمينی، روح‌الله. کتاب البیع. ج ۱. قم: بی‌تا.
۱۲. رحمدل، منصور. «حق انسان بر حریم خصوصی». مجله دانشکده حقوق و علوم سیاسی ۷۰، ش ۱ (۱۳۸۴): ۱۱۹-۱۴۶.
۱۳. الشهيد الثاني، زين‌الدین بن علی. مسالك الأفهام. ج ۷. قم: مؤسسه آل‌البیت، ۱۴۱۳ق.
۱۴. الطوسی، محمد بن حسن. تهذیب الأحکام. ج ۷. قم: مکتبه مدرسه الفقاهه، بی‌تا.
۱۵. الكلینی، محمد بن یعقوب. الکافی. ج ۲. تهران: دارالکتب الإسلامیة، ۱۴۰۷ق.
۱۶. کوشکی، غلامحسین. «حمایت از حریم خصوصی در مکان خصوصی در مقررات دادرسی کیفری ایران». مجله حقوقی دادگستری (۱۳۹۰): ۱۳۵-۱۵۰.
۱۷. موسی‌زاده، ابراهیم، و فهیم مصطفی‌زاده. «نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی». فصلنامه مطالعات حقوقی و سیاستی ۱، ش ۲ (۱۳۹۱): ۴۵-۶۸.
۱۸. النجفی، محمد حسن. جواهر الکلام فی شرح شرائع الإسلام. ج ۲۲. قم: مؤسسه النشر الإسلامی، بی‌تا.
۱۹. یعقوبی، محمدمهدی. «چالش‌های قانون انتشار و دسترسی آزاد به اطلاعات». فصلنامه مدیریت دولتی ۱۲ (۱۳۹۹).
20. Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." *California Law Review* 104, no. 3(2016): 671-732.
21. Burrell, Jenna. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." *Big Data & Society* 3, no. 1(2016): 1-12.
22. California Consumer Privacy Act (CCPA), Cal. Civ. Code 1798.120(2018, as amended 2020).
23. Charter of Fundamental Rights of the European Union, art. (2012/2000) 8.
24. Citron, Danielle Keats, and Frank Pasquale. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89(2014): 1-33.
25. Cohen, Julie E. "What Privacy Is For." *Harvard Law Review* 126(2013): 1904-1933.
26. European Convention on Human Rights, art. (1950) 8.
27. European Union Artificial Intelligence Act (2024), art. 5(1)(d).



28. Fair Credit Reporting Act (FCRA), 15U.S.C. 1681m.
29. Illinois Biometric Information Privacy Act (BIPA), 740ILCS .[2008] 15/14
30. New York City, Local Law No. 144of 2021, .20-871
31. Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press, .2010
32. Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review 57(2010): 1701-1777
33. Regulation (EU) 679/2016(General Data Protection Regulation), arts. 5(1), 7, .22
34. Selbst, Andrew D., and Julia Powles. "Meaningful Information and the Right to Explanation." International Data Privacy Law 7, no. 4(2017): 233-242
35. Solove, Daniel J. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154(2006): 477-560
36. Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR." International Data Privacy Law 7, no. 2(2017): 76-99
37. Yeung, Karen. "'Hypermudge': Big Data as a Mode of Regulation by Design." Information, Communication & Society 20, no. 1(2017): 118-136