مطالعات حقوق تطبیقی
دورهٔ ۸، شمارهٔ ۲
پاییز و زمستان۱۳۹۶
صفحات ۶۳۷ تا ۶۵۳

مطالعهٔ تطبیقی معیارهای جرم‌انگاری در فضای سایبر در نظام کیفری ایران و آلمان

محمد فرجیها*
دانشیار گروه حقوق جزا و جرم‌شناسی دانشکدهٔ حقوق دانشگاه تربیت مدرس
علی علمداری
دانش‌آموختهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه شیراز
(Email: alamdari.al@gmail.com)
(تاریخ دریافت: ۱۳۹۵/۱۱/۰۳ - تاریخ پذیرش: ۱۳۹۶/۰۴/۲۷)

چکیده

معیارهای جرم‌انگاری در فضای سایبر، درواقع نحوهٔ گزینش قواعد اخلاقی و چگونگی تدوین آن در غالب قوانین را تبیین می‌کنند. این رویکرد مبتنی بر معیارهایی مانند اصل فرعی بودن حقوق کیفری و اصل تفکیک در حمایت از داده و سایر اصول یادشده در کنوانسیون جرائم سایبر است. این پژوهش درصدد پاسخگویی به این پرسش است که جرم‌انگاری در فضای سایبر در دو نظام کیفری ایران و آلمان تا چه اندازه تحت تأثیر معیارهای بین‌المللی جرم‌انگاری در این قلمرو بوده و همچنین تجربهٔ نظام کیفری آلمان در این زمینه چه دستاوردهایی برای حقوق کیفری ایران داشته است. برای پاسخگویی به پرسش اصلی این پژوهش از روش‌های کیفی مانند تحلیل گفتمان محتوای قوانین کیفری ایران و آلمان استفاده شده است. یافته‌های پژوهش نشان می‌دهد قانون‌گذار آلمان به‌طور مطلق از داده‌های شخصی حمایت کرده، لیکن قانون‌گذار ایران تنها داده‌های حساس اشخاص را مشمول حمایت دانسته است. همچنین قانون‌گذار آلمان کودک بودن را نوعی آسیب تلقی کرده و در نحوهٔ حمایت از اشخاص تفاوت قائل شده، ولی قانون‌گذار ایران چنین تفکیکی انجام نداده است.

واژگان کلیدی

اصل تفکیک، اصل عدم ارجاع، اصل فرعی بودن، جرائم سایبر، معیارهای جرم‌انگاری.

---

* نویسندهٔ مسئول، فکس: ۰۲۱۸۲۸۸۴۲۵۷ Email: mohammadfarajiha@gmail.com

مقدمه

چنانچه حقوق کیفری را کنترل‌کنندهٔ روابط اجتماعی بدانیم، چگونگی گزینش قواعد اخلاقی از سوی دولت و گنجاندن آن‌ها در قلمرو قوهٔ قهریه به موضوع جرم‌انگاری مرتبط است. معیارهای جرم‌انگاری درواقع نحوهٔ گزینش و تدوین قوانین اخلاقی را معین می‌کند. تعیین این نحوهٔ گزینش بر معیارهایی مبتنی است که پس از بررسی نهادهای بین‌المللی مانند شورای اروپا و در اسناد بین‌المللی همچون کنوانسیون جرائم سایبر و پروتکل الحاقی به‌عنوان تدابیری که باید در سطح ملی اتخاذ گردد به دولت‌های عضو کنوانسیون پیشنهاد شده است. معیارهای اشاره‌شده عبارت‌اند از: اصل تفکیک در حمایت از داده‌ها و اشخاص، اصل شفافیت و عدم ارجاع، اصل فرعی بودن حقوق کیفری.

هدف از نگارش این مقاله تحلیل نظام جرم‌انگاری در فضای سایبر از منظر معیارهای بین‌المللی در دو نظام کیفری ایران و آلمان و نیز طرح امکان بهره‌برداری از دستاوردهای حقوق کیفری آلمان در حقوق کیفری ایران است. دو پرسش اصلی که نگارندگان این پژوهش درصدد پاسخگویی به آن برآمده‌اند، این است: ۱. جرم‌انگاری در فضای سایبر در دو نظام کیفری ایران و آلمان تا چه اندازه تحت تأثیر معیارهای جرم‌انگاری در این قلمرو بوده است؟ ۲. تجربهٔ نظام کیفری آلمان در قلمرو جرم‌انگاری چه دستاوردهایی برای قانون‌گذار کیفری ایران به‌همراه داشته است.

مصادیق قانونی مورد بحث در نظام حقوقی آلمان شامل قانون مجازات با آخرین اصلاحات دسامبر ۲۰۰۸، قانون مقابله با رقابت‌های ناسالم مصوب ۲۰۰۴م و همچنین قانون حمایت از داده با آخرین اصلاحات ۲۰۰۹م است. در نظام حقوقی ایران نیز مصادیق مورد بحث شامل قانون جرائم رایانه‌ای مصوب ۱۳۸۸ش و قانون تجارت الکترونیک مصوب ۱۳۸۲ش است. اگرچه چگونگی رعایت معیارهای جرم‌انگاری رابطه‌ای مستقیم با سیاست کیفری دارد، لیکن نظریه‌های مبنایی حاکم بر نظام حقوقی، سیاست جنایی، رویکردهای کلان کیفری قانون‌گذار، شرایط اجتماعی، سیاسی و اقتصادی، میزان اهمیت و تأثیر ارزش‌های اخلاقی نیز در تعریف اصول محوری جرم‌انگاری در هر نظام حقوقی نقش بسزایی دارند. بر همین اساس، در دو بخش معیارهای چگونگی حمایت از انواع داده‌ها و اشخاص در فضای سایبر و معیارهای حاکم بر نحوهٔ تدوین و نگارش قوانین در حوزهٔ سایبر در قالب پنج اصل شامل اصل تفکیک حمایت از داده، اصل تفکیک حمایت از اشخاص آسیب‌پذیر، اصل وضوح و دقت در تعریف جرائم سایبر، اصل شفافیت در تعریف جرائم سایبر و عدم ارجاع، اصل فرعی بودن حقوق کیفری و توجیه مورد کیفری بررسی خواهد شد تا میزان مطابقت قوانین یادشده در دو نظام کیفری ایران و آلمان با معیارهای بین‌المللی جرم‌انگاری در این قلمرو روشن شود.

اصل تفکیک حمایت از داده

اصل تفکیک بیانگر دو موضوع است. نخست اینکه موارد مختلف نقض حریم خصوصی در فضای سایبر نباید در یک مادهٔ کلی جرم‌انگاری شود و همچنین جرم‌انگاری رفتارهـا در فضـای سـایبر باید مبتنی بر معیارهای مادی و روانی مختلف باشد که موجب تغییر در اوصاف جرائم می‌شوند. اصل تقصیر (قابل مجازات بودن) مستلزم تفکیک میان این موارد بر طبق مصالح مربوط، اعمـال ارتکابی، وضعیت مرتکب و دیگر عناصر روانی است (Sieber, 1994, p.190). فضای سایبر زمینهٔ ایجاد مشابهت در عنصر مادی جرائم ارتکابی در این قلمرو را فراهم نموده و عنصر روانی و سایر اوضاع و احوال است که وصف مجرمانه این رفتارها را از یکدیگر متمایز می‌کند (دزیانی، ۱۳۸۴، ص۱۵). برای نمونه، تغییر داده چنانچه برای کسب منفعت اقتصادی انجـام شـود، کلاهبـرداری رایانه‌ای؛ اگر در یک سند الکترونیکی قابل استناد در مراجع رسمی تحقق یابد، جعل رایانه‌ای؛ و چنانچه روی داده‌های شخصی با هـدف ایجـاد مزاحمـت انجـام شـود، نقـض حـریم خصوصـی اشخاص محسوب می‌شود. لذا این تفکیک و تمایز باید به‌دقت انجام شود.

همچنین عدالت ایجاب می‌کند حمایت قانون‌گـذار از اشـخاص و داده‌هـا در فضـای سـایبر به‌تناسب میزان اهمیت و آسیب‌پذیری انجام شـود. داده‌هـای شخصـی افـراد اهمیـت یکسـانی ندارند؛ برخی از آن‌ها اهمیت ویژه‌ای دارند و جمع‌آوری، پردازش، انتقال یـا افشـای آن‌هـا ذاتـاً حریم خصوصی اطلاعاتی افراد را با چالش روبـرو مـی‌سـازد. ایـن داده‌هـا را داده‌هـای شخصـی حساس (Sensitive personal Data) می‌نامند. انجمن بین‌المللی حقوق جزا و شـورای اروپـا در راستای حمایت از داده‌های یادشده اصول و معیارهایی را پیشنهاد کرده‌اند که بر اساس آن بایـد دولت‌ها مقررات جزایی قابل اجرا در زمینهٔ حقوق فردی را فقـط در مـوارد مهـم اعمـال کننـد؛ به‌ویژه مواردی که داده‌های رایانه‌ای بسیار حساس است و جرم‌انگاری‌ها نیز باید به افعال عمدی محدود شود (Sieber, 1994, p.673)، زیرا اصولاً نقض حریم افراد و داده‌هـای آن‌هـا در فضـای سایبر در صورتی با مجازات همراه می‌شود که شخص به‌طور عمد مرتکب عمل شده باشد و لـذا بر این مبنا جرم‌انگاری اعمال ناشی از بی‌مبالاتی مسـتلزم توجیـه ویـژه اسـت (Report to the convention on Cyber Crime, 2001, p.4).

در این خصوص بند ۱ مادهٔ ۸ دستورالعمل شمارهٔ 45/EC۹۵/ اتحادیهٔ اروپا کشورهای عضـو را ملزم می‌سازد پردازش داده‌های شخصی مربوط به ریشـه‌هـای قـومی و نـژادی، دیـدگاه‌هـای سیاسی، باورهای دینی و فلسفی، عضویت در اتحادیه‌های تجاری و پردازش داده‌های مربوط بـه سلامتی و زندگی جنسی را ممنوع نمایند. داده‌های موضوع این ماده که بـه داده‌هـای شخصـی حساس معروف‌اند از حمایت‌های ویژه برخوردارند و پردازش آن‌ها جز در موارد تعیین‌شده مجاز نیست (اصلانی، ۱۳۸۶، ص۱۶).

بر این اساس، کمیتهٔ حقوق بشر در تفسیر خود از مادهٔ ۱۷ حقوق بشر اعلام می‌کند که هر فرد باید بتواند نهادهای دولتی و خصوصی را که بر اطلاعات شخصی او کنترل دارند، بشناسد (کدخدایی و حاجی ملا، ۱۳۹۳، ص۵۳۹).

کنوانسیون جرائم سایبر با آنکه برابر مفاد مقدمه ازجمله مواد ۷،۵،۴،۳،۲ کنوانسیون یکی از اهداف مهم این سند را حمایت از محرمانگی، حفظ تمامیت، دسترس بودن داده‌ها، به‌ویژه دادهای شخصی دانسته، لیکن هیچ‌گونه تقسیم‌بندی از اقسام داده‌های شخصی ارائه نکرده است. همچنین چگونگی حمایت از داده‌های حساس اشخاص حقیقی و حقوقی و تسری قواعد حمایت از داده‌ها به این دسته از اطلاعات را برعهدهٔ قانون‌گذاران ملی نهاده است. مطابعه تطبیقی نشان می‌دهد که قوانین مربوطه عموماً داده‌های اشخاص حقوقی را شامل نمی‌شود (Personal Data protectionCode, 2003, p.1-10). این مباحث هنگام تنظیم رهنمودهای سازمان توسعه و همکاری اقتصادی هم پیش آمد، ولی درنهایت تمرکز بر حمایت از داده‌های اشخاص حقیقی قرار گرفت و تسری آن به داده‌های اشخاص حقوقی به کشورهای عضو واگذار شد (OECD, 1986, p.22). برخی کشورهای عضو بر این باور بودند که شرکت‌های تجاری و انجمن‌ها باید تحت شمول این رهنمودها قرار گیرند، زیرا ممکن است نحوهٔ اقدام‌های آن‌ها هدف حکومت‌ها را در حفظ بازار آزاد و رقابت موجود در ارائهٔ خدمات دچار اختلال کند (Rustad&Koenhg, 2005, p.368).

قانون‌گذار آلمان بر اساس دستورالعمل شمارهٔ 45/EC۹۵/ اتحادیهٔ اروپا و کنوانسیون جرائم سایبر، در قوانین داخلی قانون فدرال حمایت از داده را تصویب کرد. سپس در مادهٔ ۴ قانون فدرال حمایت از داده، ضمن تبیین چگونگی جمع‌آوری و پردازش داده‌های شخصی، به صورت مطلق داده‌های شخصی را مورد حمایت قرار داده و در بند «الف» مادهٔ ۴ شرط رضایت در قانونی دانستن پردازش داده‌های شخصی را تبیین ساخته است. همچنین در بند «ج» مادهٔ ۴ نیز به موارد استثنایی همچون منافع عمومی، دعاوی حقوقی، حفاظت از منافع حیاتی موضوع داده پرداخته است که به‌موجب آن پردازش داده‌ها حتی در موارد ممنوع فراهم می‌شود. در نظام قانون‌گذاری آلمان میزان سخت‌گیری قوانین دربارهٔ داده‌های حساس به‌مراتب بیش از داده‌های معمولی است و اصول پردازش این داده‌ها به‌خصوص اصل امنیت و شفافیت در مورد این داده‌ها سخت‌گیرانه اعمال می‌شوند و حتی‌الامکان حقوق اطلاعاتی فرد باید دقیقاً در آن رعایت شود (حسنی، ۱۳۸۹، ص۱۸). بر این اساس، قانون‌گذار آلمان به‌طور مطلق از داده‌های شخصی حمایت کرده و شرط پردازش داده‌های اشخاص را منوط به رضایت آن‌ها دانسته است. همچنین در موارد استثنایی جمع‌آوری و پردازش داده را مشروط به رضایت ندانسته است.

قانون‌گذار ایران به‌طور خاص در مادهٔ ۵۸ قانون تجارت الکترونیک مصوب ۱۳۸۲ش به موضوع داده‌پیام‌های شخصی پرداخته و قائل به تفکیک در حمایت از داده‌ها شده است. مادهٔ

۵۸ مقرر می‌دارد: ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی بیانگر ریشه‌های قومی یا نژادی دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است و به‌موجب مادهٔ ۷۱ قانون یادشده نقض آن از سوی مرتکب، جرم و مشمول مجازات است.

مادهٔ ۷۲ قانون تجارت الکترونیک نیز ارتکاب این جرائم را از جانب دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسئول جرم‌انگاری نموده و هرگونه بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی را مشمول مجازات دانسته است.

ماده ۵۸ قانون مذکور مصادیق داده‌های مورد حمایت احصاء نموده، لیکن سخنی از داده‌های صنعتی و تجاری به میان نیاورده است و در مادهٔ ۵۹ قانون تجارت الکترونیک، شرطِ جرم ندانستن رفتار را رضایت شخص دانسته است به اینکه الف) اهداف داده‌پیام‌های شخصی مشخص بوده، به‌طور واضح شرح داده شده باشند. ب) تنها به‌اندازهٔ ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده‌پیام شرح داده شده است، جمع‌آوری و استفاده شود. ج) داده‌پیام صحیح و روزآمد باشد. د) شخص موضوع داده‌پیام بتواند به پرونده‌های رایانه‌ای حاوی داده‌پیام‌های شخصی مربوط به خود دسترسی داشته باشد و داده‌پیام‌های ناقص یا نادرست را محو یا اصلاح کند. قانون‌گذار ایران با اینکه در مقام بیان بوده، از موارد خاص و استثنایی که بنا به دلایل امنیتی و مصالح عمومی بتوان دست به پردازش داده‌ها زد، سخنی به‌میان نیاورده است.

مواد قانونی اشاره‌شده سه عنوان مجرمانهٔ ذخیره، پردازش پیام‌های شخصی حساس و عدم رعایت شرایط قانونی پیام‌های شخصی حساس، و جرائم غیرعمد راجع به داده‌پیام‌های شخصی حساس را بیان نموده است. به این ترتیب، ترک فعل در جرائم پیش‌گفته نمی‌تواند عنصر مادی جرم قرار گیرد؛ زیرا افعالی که عنصر مادی جرائم پیش‌گفته را تشکیل می‌دهند، شامل ذخیره، پردازش داده و توزیع داده‌پیام است. بنابراین، قانون‌گذار ایران فقط داده‌های شخصی حساس را حمایت می‌کند و از مطلق داده‌های شخصی، ازجمله داده‌های تجاری و صنعتی، حمایت نکرده است. بنابراین در نظام حقوقی ایران برخلاف حقوق کیفری آلمان در حمایت از انواع داده‌ها تفکیکی انجام نشده و صرفاً در یک مورد خاص به حمایت از داده‌پیام‌های شخصی پرداخته شده است. همچنین قانون‌گذار ایران موارد استثنایی جمع‌آوری و پردازش داده‌ها بدون رضایت اشخاص را پیش‌بینی نکرده است. به‌نظر می‌رسد نبود منابع اطلاعاتی دقیق و زیرساخت‌های مخابراتی متناسب و همچنین قوانین پایه‌ای و تخصصی ازجمله قانون حمایت از داده، ازجمله مهم‌ترین علت‌های تفاوت در رویکرد قانون‌گذاران دو کشور است (Personal Data protection). Code, 2003, p.1-10

اصل تفکیک حمایت از اشخاص آسیب‌پذیر

یکی از سازوکارهای حمایت کیفری در فضای سایبر، جرم‌انگاری افتراقی رفتارهای آسیب‌زا نسبت به اشخاص آسیب‌پذیر، به‌ویژه کودکان است. این امر در سطح بین‌المللی بیشتر به حمایت از کودکان در برابر سوءاستفادهٔ جنسی محدود می‌شود. کنوانسیون سازمان ملل متحد دربارهٔ حقوق کودک (UN Convention, 1989, P.1577)،کنوانسیون شورای اروپا راجع به حمایت از کودکان در برابر سوءاستفادهٔ جنسی (Council of Europe Treaty Series, 2007, p.201) و یا چارچوب تصمیم‌گیری شورای اتحادیهٔ اروپایی دربارهٔ حمایت از کودکان در برابر سوءاستفادهٔ جنسی (Convention Council of Europe,2001,p.20) همگی بیانگر فرایند جهانی‌شدن حقوق کیفری در قلمرو حمایت از کودکان در برابر هرزه‌نگاری است. کنوانسیون جرائم سایبر نیز در مادهٔ ۹ با عنوان جرائم مرتبط با محتوا، دولت‌های عضو را به جرم‌انگاری هرزه‌انگاری اشخاص زیر ۱۸ سال ملزم ساخته است که بیانگر توافق بین‌المللی در مجرمانه بودن چنین رفتاری است. لیکن چگونگی اجرای این مقررات همواره با اختلاف نظرهایی همراه بوده است؛ نخست اینکه محدودهٔ سنی افراد مورد حمایت در کشورهای مختلف از ۱۴ تا ۱۸ سال متغیر است (Delmas Marty, 2008, p.155).

قانون‌گذار آلمان در مادهٔ ۱۸۴ در خصوص انتشار مطالب مستهجن برای افراد زیر ۱۸ سال اقدام به جرم‌انگاری نموده، مقرر می‌دارد: هر کس مطالب مکتوب شهوت‌انگیز را در اختیار شخص زیر ۱۸ سال قرار دهد یا در دسترس وی بگذارد و یا به وی پیشنهاد دهد و یا در اماکنی که در دسترس اشخاص زیر سن یادشده قرار دارند یا ممکن است اشخاصی در این سنین آن را مشاهده کنند، به نمایش بگذارد، یا خارج از اماکن تجاری، دکه‌ها یا سایر نواحی تجاری که معمولاً مشتری به آنجا وارد نمی‌شود، از طریق دادوستد یا سفارش الکترونیکی یا در کتابخانه‌های عاریه‌ای یا انجمن‌های کتاب‌خوانی، مطالب یادشده را در اختیار آن‌ها قرار دهد یا به آن‌ها پیشنهاد دهد و چنانچه از طریق شیوه‌های تجاری چنین مطالبی را برای استفاده از اشخاص یادشده ارائه یا پیشنهاد دهد، به‌استثنای ارائهٔ مطالب مذکور در فروشگاه‌هایی که افراد زیر ۱۸ سال نمی‌توانند به آن وارد شوند و این مطالب در معرض دید آن‌ها قرار نمی‌گیرد و همچنین واردات چنین مطالبی را از طریق دادوستد سفارشی الکترونیکی انجام دهد و در ملأ عام چنین مطالبی را در اماکنی که اشخاص زیر سن یادشده می‌توانند به آن وارد شوند، یا می‌توانند این‌گونه مطالب را مشاهده کنند، قرار دهد یا از طریق انتشار کتبی این مطالب خارج از چارچوب معاملات تجاری از طریق فروشگاه‌های بازرگانی معمول، پیشنهاد فروش چنین مطالبی را بدهد یا آن را اعلام کند و یا توصیه نماید و بدون اینکه کسی از او درخواست نموده باشد، چنین مطالبی را در اختیار وی قرار دهد و یا در محل نمایش عمومی فیلم در ازای هزینهٔ

ورودی که کلاً یا عموماً برای نمایش فیلم یادشده درنظر گرفته شده است، در معرض دید دیگران قرار دهد یا به‌منظور استفاده از این‌گونه مطالب، آن‌ها را تولید یا ذخیره کند، به‌دست آورد یا تأمین نماید و یا به صادرات و واردات آن بپردازد، یا به‌منظور انتشار چنین مطالبی یا کپی‌برداری از آن‌ها در خارج از قلمرو آلمان، با نقض مقررات کیفری کشور بیگانه اقدام به صادرات مطالب یادشده نماید یا آن‌ها را در دسترس عموم قرار داده یا کاربرد آن را تسهیل نماید، به مجازات مقررشده در قانون محکوم خواهد شد.

این قلمرو حمایت در بیشتر کشورها با عنوان هرزه‌نگاری نرم (Soft pornography) تلقی می‌شود؛ به این معنا که توزیع آن در میان بزرگسالان مجاز و برای کودکان ممنوع است. درمقابل، دیدگاه دیگری با عنوان هرزه‌نگاری مطلق مطرح است؛ به این معنا که توزیع آن حتی میان بزرگسالان نیز ممنوع است (Delmas-Marty, 2008, p.157). قانون‌گذار آلمان در خصوص افراد بزرگسال در بند «الف» مادهٔ ۱۸۴ با عنوان انتشار مطالب مستهجنی که خشونت و رابطهٔ جنسی غیرطبیعی را به‌تصویر می‌کشند، اقدام به جرم‌انگاری نموده است و در بند «ب» مادهٔ ۱۸۴، توزیع، تحصیل، مالکیت، تولید، تأمین، ذخیره، پیشنهاد، اعلام و نشر مطالب مستهجن پیرامون کودکان، چنانچه راجع به سوءاستفادهٔ جنسی از کودکان باشد، جرم دانسته و استفاده یا کپی‌برداری از آن مطالب، اقدام به صادرات یا واردات آن یا تسهیل کاربرد چنین مطالبی را قابل مجازات دانسته است. در مواردی که مجرم به‌صورت حرفه‌ای یا به‌عنوان عضوی از گروه تبهکاری که هدف آن‌ها تداوم ارتکاب چنین جرائمی است اقدام نموده باشد و مطالب مستهجن پیرامون کودکان، اقدامی جنسی واقعی یا عملی را به‌تصویر کشیده باشد، به مجازات بسیار شدید مقرر در قانون محکوم می‌کند. قانون‌گذار آلمان در خصوص چگونگی حمایت قائل به تفکیک شده است، زیرا کودک بودن را یک نوع آسیب تلقی نموده و به این لحاظ حمایت کیفری از کودک را مستلزم تدابیر ویژه دانسته است.

قانون‌گذار ایران در نحوهٔ حمایت، بین بزرگسالان و کودکان قائل به تمایز نشده و به این لحاظ نیز حمایت کیفری لازم را اعمال نکرده است؛ صرفاً در بند «د» مادهٔ ۲۸ که مربوط به صلاحیت دادگاه‌ها است مقرر می‌دارد: چنانچه جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکبْ بزه‌دیده ایرانی یا غیرایرانی باشد، دادگاه‌های ایران صالح به رسیدگی است. در تبصرهٔ ۳ مادهٔ ۳ نیز نحوهٔ مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز دارند، مقرر شده است: استفاده از صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارها و لوح‌های فشردهٔ غیرمجاز موضوع این قانون موجب اعمال حداکثر مجازات مقرر برای عامل خواهد بود.

عدم تفکیک در قانون‌گذاری سایبری به‌نظر می‌رسد بیشتر ناشی از شتاب‌زدگی نظام

کیفری ایران در جرم‌انگاری تحت تأثیر حاکمیت فضای احساسی و اولویت یافتن ملاحظات سیاسی برای پاسخگویی مقطعی و فوری به انتظارات عمومی در پی بازتاب گستردهٔ رسانه‌ایِ این جرائم است. نمونهٔ این فرایند را می‌توان در طرح قانون نحوهٔ مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز دارند مشاهده کرد که به‌دور از دغدغه‌های علمی و کارشناسی به دلیل همسویی با دیدگاه‌های عوام‌گرایانه به‌سرعت در دستور کار قرار گرفت (فرجیها و مقدسی، ۱۳۹۲، ص۱۴۷-۱۴۶)؛ موضوعی که شاید در آغاز کار از اهمیت چندانی برخوردار نباشد. اما واقعیت این است که تمام تلاش‌های قانون‌گذار در راستای تدوین قوانین مناسب برای حمایت از اشخاص و داده‌ها در آنچه به نگارش درمی‌آورد، بروز می‌یابد. شتاب‌زدگی و نگارش نادرست و تفسیر نابجا می‌تواند تمامی تلاش‌های پژوهشی ناشی از طی فرایند دشوار قانون‌گذاری را بی‌حاصل نماید، زیرا چگونگی انشای مواد قانونی به صورت ناخواسته می‌تواند تأثیرات ماهوی بر قوانین داشته باشد. بر این اساس، در ادامه به بررسی معیارهای بین‌المللی چگونگی تدوین و نگارش جرائم سایبر خواهیم پرداخت.

اصل وضوح و دقت در تعریف جرائم سایبر

اصل دقت در تعریف جرائم سایبر بیانگر این موضوع است که قانون‌گذار باید اعمال ممنوع را به‌تفصیل بیان کرده، با ارائهٔ تعاریف دقیق از اعمال غیرقانونی و تعیین اوصاف حقوق ماهوی و محدودهٔ آن، از ابهام و کلی‌گویی خودداری نماید (حسنی، ۱۳۸۹، ص۱۸۱).

مادهٔ ۶ کنوانسیون جرائم سایبر در این خصوص مقرر می‌دارد: قوانین مصوب در این باره باید تا حد امکان با دقت و ظرافت خاصی نوشته شوند تا قابلیت پیش‌بینی مناسب نوع رفتاری را که به محکومیت کیفری منجر می‌شود، فراهم آورند. به‌موجب اصل قانونی بودن جرم و مجازات به‌عنوان یکی از اصول حقوقی که مورد تأکید قانون اساسی است، قانون‌گذار باید عناصر قانونی، مادی و معنوی هر جرم را به‌طور واضح و شفاف و بدون هرگونه ابهام و کلی‌گویی به‌خصوص در امور کیفری اعلام نماید تا شهروندان قانون را بهتر درک کنند و درنتیجه اثر بازدارندگی قانون نیز افزایش یابد.

قانون‌گذار آلمان در بند «الف» مادهٔ ۲۰۲ با عنوان جاسوسی اطلاعات مقرر نموده است: هر کس برخلاف قانون اطلاعاتی را که برای دسترسی وی درنظر گرفته نشده باشد و به‌ویژه در مقابل دستیابی بدون مجوز افراد حفاظت می‌شوند، برای خود یا دیگری تحصیل نماید، درصورتی‌که حفاظت از اطلاعات یادشده را نقض کند، به مجازات حبس یا پرداخت جزای نقدی محکوم خواهد شد. بر طبق مفاد بند ۱، اطلاعات فقط شامل مواردی است که به صورت الکترونیکی یا مغناطیسی یا به شیوه‌ای که به‌آسانی قابل درک نیست، ذخیره یا انتقال یابد.

قانون‌گذار آلمان با بیان عبارت «به‌ویژه محافظت‌شده» (که معیاری است برای تشکیل جرم) این هدف را پیگیری نموده است که بزه‌دیده باید میزان علایق خود را در حفظ امنیت داده‌ها به‌وسیلهٔ ایجاد سطح مشخصی از دسترسی آشکار سازد، ولی این ماده تعریف دقیقی از «حفاظت‌شده» ارائه نکرده است.

این عدم تعریف به‌نظر می‌رسد به این دلیل باشد که به لحاظ فنی، سطح حفاظت و نوع آن با توجه به مقتضیات زمانی به‌طور مستمر در حال تغییر است. قانون‌گذار آلمان به دلیل مشارکت در تدوین و نگارش اسناد بین‌المللی همچون کنوانسیون جرائم سایبر و دستورالعمل‌های شورای اروپا و داشتن تجربهٔ تدوین قوانین مرتبط با این حوزه در تعریف جرائم سایبر با نگرشی کارشناسانه اقدام به جرم‌انگاری کرده است.

قانون‌گذار ایران در مادهٔ ۲۱ قانون جرائم رایانه‌ای، ارائه‌دهندگان خدمات دسترسی را موظف نموده طبق ضوابط فنی و فهرست مقرر از سوی کارگروه تعیین مصادیق، محتوای مجرمانه را که در چارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به‌کار می‌رود، پالایش نمایند و چنانچه عمداً از پالایش محتوای مجرمانه خودداری کنند، مجازات انحلال را پیش‌بینی نموده و مقرر داشته است: چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینهٔ دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبهٔ نخست به جزای نقدی و در صورت تکرار به تعطیلی موقت محکوم خواهند شد. تدوین و نگارش مادهٔ ۲۱ قانون جرائم رایانه‌ای به‌گونه‌ای است که با توجه به معیار شفافیت درعمل ممکن است با مشکلات زیادی روبرو شود:

نخست اینکه بر اساس مادهٔ یادشده گاهی ارائه‌دهندهٔ خدمات، فضای لازم را برای ذخیرهٔ اطلاعات در اختیار گذاشته باشد و طبق قرارداد، مدیریت پردازش به‌عهدهٔ کسی دیگر باشد که در این صورت طبق مادهٔ یادشده ارائه‌کننده مسئول است و پردازش‌کننده مسئولیتی ندارد و این تحمیل مسئولیت به‌نظر درست نمی‌آید. این امر نیز ناشی از آن است که قانون‌گذار ایران میزبان را صرفاً شامل کسانی دانسته است که فضای مورد نظر را در اختیار کاربر قرار می‌دهند، این درحالی است که مادهٔ ۱ کنوانسیون جرائم سایبر، ارائه‌دهندهٔ خدمات میزبانی را هم شامل کسانی که اطلاعات را برای کاربر و برای ارائه‌دهندهٔ خدمات ذخیره می‌کنند و هم شامل اشخاصی که اطلاعات را پردازش می‌نمایند، می‌داند. البته افزون بر ارائه‌دهندهٔ خدمات دسترسی که مشمول مادهٔ ۲۱ قانون جرائم رایانه‌ای و ارائه‌دهندهٔ خدمات میزبانی که مشمول مادهٔ ۲۳ است، گروه سومی نیز وجود دارد که ارائه‌کنندگان خدمات ثبت دامنه نامیده می‌شوند، اما قانون جرائم رایانه‌ای در این خصوص ساکت است. ازجمله مصادیق دیگر، مادهٔ ۲۵ قانون جرائم رایانه‌ای است که به‌موجب آن ارتکاب اعمال زیر جرم و مشمول مجازات قرار می‌گیرد:

الف) تولید یا انتشار یا توزیع و دردسترس قرار دادن یا معاملهٔ داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به‌منظور ارتکاب جرائم رایانه‌ای به‌کار می‌رود. ب) فروش یا انتشار یا دردسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌آورد. ج) انتشار یا در دسترس قرار دادن محتویات آموزشی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی.

به‌نظر می‌رسد قانون‌گذار ایران در تدوین مادهٔ یادشده، مادهٔ ۶ کنوانسیون جرائم سایبر را الگو قرار داده است، ولی تفاوت عمدهٔ آن با مادهٔ ۲۵ قانون جرائم رایانه‌ای شامل دو موضوع است که یکی از آن‌ها موضوع جرم می‌باشد که به‌موجب شق «الف» بند ۱ مادهٔ ۶ کنوانسیون، وسیله‌ای است که برای یکی از چهار جرمِ دستیابی غیرمجاز، شنود غیرمجاز، اخلال در داده و اخلال در سیستم، طراحی و تنظیم شده است. لیکن به‌موجب بند «الف» مادهٔ ۶ موضوع جرم، داده یا نرم‌افزار و هر نوع وسایل الکترونیکی (بدون توجه به نوع جرم) به‌کاررفته که عدم دقت در تدوین مادهٔ ۲۵ موجب شده است توزیع، انتشار و معاملهٔ آن‌ها مشمول مادهٔ ۱۴ و ۱۵ و ۱۶ و هم مشمول مادهٔ ۲۵ قرار گیرد. این درحالی است که اگر قانون‌گذار ایران به تبعیت از کنوانسیون جرائم سایبر، موضوع جرم را به وسایل ارتکاب یکی از چهار جرم دستیابی و شنود غیرمجاز و اخلال در داده و سیستم محدود می‌کرد، اشکال مورد نظر تحقق نمی‌یافت.

با توجه به اینکه بیشتر نرم‌افزارهای موجود ماهیتی دوگانه دارند، کنوانسیون جرائم سایبر در بند ۲ مادهٔ ۶ و بند ۱ (الف)، تولید و فروش، تهیه به‌منظور استفاده، واردکردن، توزیع یا به هر نحو دردسترس قرار دادن دستگاه دارای برنامهٔ رایانه‌ای را چنانچه طراحی یا سازگار شده باشد برای ارتکاب جرائم مندرج در مواد ۲ تا ۵ ممنوع کرده است.کنوانسیون به‌عنوان یک توافق معقول، حوزهٔ عملکرد خود را به مواردی محدود کرده است که دستگاه‌ها در ابتدا به قصد ارتکاب جرم به صورت نوعی طراحی یا سازگار شده باشند. بر اساس این معیار دستگاه‌های دو منظوره از شمول ماده خارج می‌شوند و این درحالی است که قانون‌گذار ایران در موارد اشاره‌شده به این امر دقت لازم را نداشته است و لذا در مادهٔ ۲۵ قانون جرائم رایانه‌ای، فروش یا انتشار یا دردسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم نماید، جرم و قابل مجازات دانسته و این در صورتی است که رمز عبور و کدهای دستیابی و داده‌های مشابه ازجمله وسایلی هستند که دارای کاربردهای دوگانه‌اند. بر همین اساس، مادهٔ ۶ کنوانسیون بیان می‌کند، درصورتی که انتشار و معامله و در اختیار نهادن به‌قصد ارتکاب جرم باشد، بایستی جرم‌انگاری شود؛ درحالی که در بند «ب» مادهٔ ۲۵ صرف انتشار و دراختیار گذاردن را جرم

تلقی نموده است. قانون‌گذار ایران با توجه به مشارکت نداشتن در نهادها و کنوانسیون‌های بین‌المللی همچون کنوانسیون جرائم سایبر و پروتکل الحاقی و همچنین اولین تجربهٔ قانون‌گذاری تخصصی در حوزهٔ سایبر در مقایسه با نظام قانون‌گذاری آلمان، به‌نظر می‌رسد دقت لازم را در نگارش، ازجمله تعریف جرائم سایبر، اعمال نکرده است.

اصل شفافیت در تعریف جرائم سایبر و عدم ارجاع

جرائم فضای سایبر معمولاً با واژگان و اصطلاحاتی تعریف و توصیف می‌شوند که در جرائم فضای واقعی کاربرد دارند، مانند سرقت رایانه‌ای یا کلاهبرداری سایبری و شنود داده‌های الکترونیکی؛ درحالی که به لحاظ عنصر مادی و نحوهٔ ارتکاب، تفاوت اساسی میان این دو وجود دارد. بنابراین، اعمال جرم‌انگاری شده باید تا حد امکان به صورت واضح و روشن از سوی مقررات کیفری مربوط تشریح شوند. استفادهٔ گسترده از روش ارجاع[1] مقررات کیفری را مبهم و غیرشفاف می‌سازد و لذا باید از آن خودداری شود (دزیانی، ۱۳۸۴، ص۲۱) و در مواردی‌که قانون‌گذار ناگزیر به استفاده از ارجاعات صریح یا ضمنی به مقررات کیفری می‌شود لازم است در همان مادهٔ کیفری تعریف مطلوب از اعمال ممنوعه ارائه گردد (Germany Federal Law, p.182-183).

قانون‌گذار ایران در مادهٔ ۳ قانون جرائم رایانه‌ای در خصوص دسترسی غیرمجاز و استفاده از اسناد و داده‌های سری در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مقرر می‌دارد، هر کس مرتکب اعمال زیر گردد، مشمول مجازات خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال؛

ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت؛

ج) افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها.

قانون‌گذار ایران در این ماده به مجازات جاسوسی رایانه‌ای پرداخته و در تبصرهٔ ۱ داده‌های سری را تعریف کرده است، لیکن نحوهٔ تعیین و تشخیص داده‌های سری و نیز چگونگی طبقه‌بندی و حفاظت آن‌ها را به تنظیم آیین‌نامه وابسته کرده که هنوز تصویب نشده است. اما این نکته را باید خاطرنشان کرد که در خصوص اسناد دولتی سری و محرمانه قانون‌گذار در سال ۱۳۵۳ش قانون مجازات انتشار و افشای اسناد محرمانه و سری را به‌تصویب رسانده و در

---

۱. روشی که مطابق آن فعالیت‌هایی که تحت حکومت کدهای غیرکیفری قرار دارند با ارجاع به مقررات کیفری جرم انگاشته شوند.

خصوص اسناد اشاره‌شده تعیین تکلیف کرده است. در تعریف اسناد دولتی و محرمانه در مادهٔ ۱ این قانون آمده است: اسناد دولتی شامل هر نوع نوشته یا اطلاعات ثبت یا ضبط‌شده مربوط به وظایف و فعالیت‌های وزارتخانه‌ها و مؤسسات دولتی و وابسته به دولت و شرکت‌های دولتی از قبیل مراسلاتی است که در مراجع پیش‌گفته تهیه شده یا به آن رسیده باشد. اسناد دولتی سری را نیز شامل اسنادی دانسته است که افشای آن‌ها مغایر با مصالح دولت و یا مملکت باشد. اسناد دولتی محرمانه را شامل اسنادی دانسته است که افشای آن‌ها با مصالح خاص اداری سازمان‌های یادشده در این ماده مغایرت داشته باشد.

قانون‌گذار آلمان در مادهٔ ۹۳ قانون جزایی، نخست اقدام به تعریف اسناد دولتی سری نموده، مقرر می‌دارد: اسرار دولتی، اطلاعات اشیا یا خبری است که فقط در اختیار افراد محدودی قرار دارد و باید به‌منظور پیشگیری از خطر آسیب جدی به امنیت خارجی جمهوری فدرال آلمان از قدرت‌های خارجی مخفی نگه‌داشته شود؛ و اطلاعات مربوط به نقض استقلال، نظم قانونی دموکراتیک یا توافق‌نامه‌های بین‌المللی کنترل تسلیحات که از طرفین توافق‌نامه‌های یادشده مخفی نگه‌داشته شده‌اند، اسرار دولتی نیستند.

در مادهٔ ۹۴ قانون جزایی نیز این‌گونه مقرر می‌کند: هر کس یکی از اسرار دولتی را به یکی از قدرت‌های بیگانه یا رابط آن‌ها انتقال دهد یا به طریقی دیگر زمینه را برای جلب توجه اشخاص غیرمجاز به اسرار دولتی فراهم آورد یا اسرار دولتی را به‌منظور تضعیف جمهوری فدرال آلمان یا به نفع قدرت بیگانه علنی نماید و به این وسیله خطر آسیب جدی به امنیت خارجی جمهوری فدرال آلمان را ایجاد نماید به مجازات محکوم خواهد شد.

در تعریف جرائم خطیر و خاص مقرر می‌نماید: جرائم خطیر و خاص معمولاً در صورتی به‌وقوع خواهند پیوست که مجرم از مسئولیتی که بر اساس آن به حفاظت از اسرار دولتی ملزم شده است سوءاستفاده کند و به‌واسطهٔ عمل مجرمانهٔ او، آسیب جدی به امنیت خارجی جمهوری فدرال آلمان وارد گردد. همان‌طور که مشاهده شد، قانون‌گذار با بیان جرائم خاص و خطیر در همان ماده‌ای که به آن اشاره کرده است و بدون ارجاع به سایر قوانین مصوب، حداکثر در یک مادهٔ دیگر در خود همان قانون اقدام به شفاف‌سازی کرده است.

اصل فرعی بودن حقوق کیفری و توجیه مورد کیفری

فضای سایبر فضای مبتنی بر فناوری‌های نوین است و لذا استفاده از امکانات فناورانه در ایجاد امنیت و حمایت از حقوق اشخاص اهمیت بسیاری دارد؛ بنابراین تا حد امکان، باید از این روش‌ها در جهت حمایت از اشخاص و داده‌های شخصی آن‌ها استفاده کرد. این روش‌ها به‌اصطلاح روش‌های حمایتی نامیده می‌شوند؛ روش‌هایی همچون رمزنگاری داده‌ها و اتخاذ

تدابیر امنیتی متناسب برای پیشگیری جرائم هزینه‌های کمتری را به دولت تحمیل می‌کند. حکومت باید صنعت را به نوآوری تشویق کند؛ به‌ویژه در ایجاد محصولات امنیتی جدید، کدهای رفتاری، ابزارهای گزینش محتوا که می‌تواند مکملی برای حمایت کیفری به‌شمار آیند (Sieber, 2000, p.319-399).

در مقابل این نوع رویکرد، روش‌های واکنشی یا روش‌های حقوقی قرار دارند که این نوع حمایت باید اساساً مبتنی بر مقررات اداری و مدنی باشد. مقررات حقوق مدنی و قراردادهای میان موضوع داده‌ها و سازمان‌ها دخیل در پردازش داده‌ها می‌توانند در بیشتر موارد راهگشا باشند. در این موارد نیز سودمندی قوانین کیفری و ارعاب فردی و جمعی باید مد نظر قرار گیرد. درنهایت لازم است تفاوت میان آنچه غیراخلاقی است و آنچه مجرمانه تلقی می‌شود درنظر گرفته شود.

در نظام قانون‌گذاری آلمان بر اساس همین اصل فرعی بودن حقوق کیفری تا حد امکان از جزای نقدی مبتنی بر ضمانت اجراهای اداری استفاده شده است. حتی در خصوص جرائمی که عواملی مانند نوع داده‌ها، دامنهٔ جرم، شیوهٔ ارتکاب باعث می‌شود که نتیجهٔ مجرمانه خفیف باشد، استثناهایی را پیش‌بینی و اعمال می‌نماید؛ به این صورت که برخی تخلفات جزئی یا قابل اغماض از شمول جرائم تعریف‌شده خارج می‌شوند. ضمانت اجراهای اداری و جزای نقدی مقرر در مادهٔ ۴۳ و ۴۴ قانون فدرال حمایت از داده را می‌توان در راستای اصل یادشده توجیه کرد. در آلمان قواعد هماهنگی میان کارکردهای گوناگون ارائه‌دهندگان خدمات اعمال شده است. بر مبنای این نظریه ارائه‌کنندگان خدمات دسترسی تا زمانی که بر اطلاعاتی که انتقال می‌دهند تأثیر نگذارند یا اطلاعات یا دریافت‌کننده اطلاعات را گزینش نکنند، مسئول نخواهند بود و در صورت مسئولیت نیز به‌موجب قرارهای مدنی و اداری مجازات می‌شوند. این راه‌حل، موازنه مناسبی را میان پیشگیری از جرم و جریان آزاد داده‌ها در شبکه‌های رایانه‌ای بین‌المللی برقرار می‌سازد (Sieber, 2001, p.231-239).

قانون‌گذار ایران نیز مطابق این رویکرد در مادهٔ ۲۱ قانون جرائم رایانه‌ای دربارهٔ ارائه‌دهندگان خدمات دسترسی و در مادهٔ ۲۳ در خصوص ارائه‌کنندگان خدمات میزبانی، مجازات انحلال و جزای نقدی مقرر نموده است، زیرا رعایت نکردن این امر موجب بروز پدیده‌ای با عنوان تورم کیفری می‌شود. مطابق این رویکرد در تدوین قوانین سایبری باید مجازات کیفری صرفاً در جرائم خطرناکی که مقررات اداری یا مدنی توان مقابله با آن را ندارند، اعمال گردد. همچنین باید سودمندی قوانین کیفری، ارعاب فردی و جمعی، میزان مجازات و افزایش خطر جرم در جرم‌انگاری مد نظر قرار گیرد (حسنی، ۱۳۸۹، ص۱۸۹).

نتیجه

هرچه جرم‌انگاری بر مطالعات و تفکرات عمیق استوار باشد، نظام کیفری را کارآمدتر خواهد ساخت. بر این اساس، تدوین و اعلام معیارهای جرم‌انگاری می‌تواند با ایجاد شفافیت در رویکرد قانون‌گذار و ایجاد چارچوبی علمی، مانع اشتباهات حاکم در تدوین سیاست کیفری شود و حقوق شهروندان را تضمین کند. اینکه چه داده‌هایی باید حمایت شوند و نیز مشخص کردن حدود اختیارات حکومت و حمایت‌های ویژه از شهروندان در برابر این اختیارات و تعیین اقشار آسیب‌پذیر و حمایت‌های مخصوص از این اقشار، هریک مؤلفه‌هایی هستند که به‌عنوان یک معیار بین‌المللی جرم‌انگاری در فضای سایبر مطرح می‌شوند.

تمرکز این مقاله بر تحلیل نظام جرم‌انگاری در فضای سایبر از منظر معیارهای بین‌المللی در دو نظام کیفری ایران و آلمان و نیز معرفی تجربه‌های قانون‌گذاری کیفری در آلمان به‌نظام داخلی ایران بوده است. با بررسی میزان تأثیرپذیری نظام کیفری ایران و آلمان از معیارهای بین‌المللی جرم‌انگاری و مقایسه این دو نظام کیفری با یکدیگر می‌توان بر نتایج زیر تأکید کرد:

- دقت در تفکیک جرائم و همچنین تمایز نهادن در نحوهٔ حمایت از داده‌ها برحسب اهمیت آن ازجمله معیارهای اساسی جرم‌انگاری در جرائم سایبر است. برخی از داده‌های شخصی به دلیل حساسیت موضوع داده، باید از حمایت‌های ویژه‌ای برخوردار شوند و پردازش آن‌ها جز در موارد خاص و مصرح مجاز نیست. قانون‌گذار آلمان به‌طور مطلق از داده‌های شخصی حمایت کرده، لیکن موارد استثنایی را نیز پیش‌بینی نموده است که جمع‌آوری، پردازش، افشای داده‌ها نیازمند رضایت شخص نیست. قانون‌گذار ایران نیز تنها داده‌های حساس اشخاص را در قبال پردازش، مشمول حمایت قرار داده است؛ با اینکه در مقام بیان موارد استثنا بوده، در خصوص موارد خاص و استثنایی که بنابه دلایل امنیتی و مصالح عمومی باید جمع‌آوری و پردازش شوند، سخنی به‌میان نیاورده است.
- یکی از معیارهای جرم‌انگاری در فضای سایبر، حمایت از اشخاص آسیب‌پذیر است که قانون‌گذار آلمان با توجه به این رویکرد، کودک بودن را یک نوع آسیب تلقی کرده و به این لحاظ در نحوهٔ حمایت از اشخاص قائل به تفکیک شده و در نتیجهٔ جرم‌انگاری جرائم سایبر تدابیر حمایتی ویژه را برای حمایت از کودکان تدوین کرده است. لیکن قانون‌گذار ایران در نحوهٔ حمایت، بین بزرگسالان و کودکان تمایز قائل نشده و حمایت کیفری ویژه از اقشار آسیب‌پذیر به‌ویژه کودکان را مد نظر قرار نداده است.
- قانون‌گذار آلمان در تدوین و نگارش جرائم سایبر، برخلاف ایران نخست تلاش کرده است اعمال ممنوع در مقررات کیفری را به‌تفصیل بیان کرده، از کلی‌گویی خودداری

کند و اعمال جرم‌انگاری‌شده را تا حد امکان به صورت واضح و روشن از طریق مقررات کیفری مربوطه تشریح کند و در مواردی که از ارجاعات صریح یا ضمنی به مقررات کیفری استفاده کرده، در همان مادهٔ کیفری، تعاریف لازم از اعمال ممنوع را ارائه نموده و درنهایت هنگام جرم‌انگاری رفتار در فضای سایبر، مجازات را بر مبنای مقررات اداری و مدنی قرار داده و تا حد امکان از جزای نقدی مبتنی بر ضمانت اجراهای اداری استفاده کرده است.

- جامعیت نظام قانون‌گذاری آلمان در تدوین مقررات کیفری متناسب با معیارهای بین‌المللی در مقایسه با حقوق کیفری ایران، به‌نظر می‌رسد ناشی از صنعتی بودن کشور آلمان و لزوم حمایت کیفری متناسب با ماهیت فضای مجازی به‌منظور ایجاد انگیزه برای سرمایه‌گذاری‌های صنعتی و تجاری، همچنین انتقال و مبادلهٔ دانش و فناوری‌های بین‌المللی و وابستگی متقابل این امر به حمایت کافی از داده‌ها است. زیرا عدم حمایت کیفری متناسب در فضای سایبر می‌تواند از جنبه‌های مختلف به کشور آسیب وارد کند و مانع انتقال دانش و فناوری به کشور شود؛ چراکه شرکت‌های سرمایه‌گذاری بین‌المللی در صورت عدم حمایت کافی از داده‌های تجاری و صنعتی، رغبتی برای انتقال فناوری خود به کشورهای دیگر نخواهند داشت.

منابع و مآخذ

الف) فارسی

۱. اصلانی، حمیدرضا (۱۳۸۶)، «درآمدی بر حقوق حاکم بر حمایت از داده‌های شخصی در حوزهٔ بهداشت و سلامت»، فصلنامهٔ علمی و پژوهشی رفاه اجتماعی، ش ۲۵، ص ۳۴۲-۳۲۱.

۲. آیین‌نامهٔ طرز نگهداری اسناد سری و محرمانه دولتی و نحوهٔ مشخص نمودن انواع اسناد و اطلاعات مصوب ۱دی ۱۳۵۴؛ روزنامهٔ رسمی ش ۹۰۵۶، ۱۳ بهمن ۱۳۵۴.

۳. جلالی، امیرحسین (۱۳۸۴)، کنوانسیون جرائم سایبر، تهران: مرکز مطبوعات و انتشارات قوهٔ قضائیه.

۴. دزیانی، محمدحسن (۱۳۸۳)، جرایم کامپیوتری، ج۱و۲، سازمان برنامه و بودجه، دبیرخانهٔ شورای عالی انفورماتیک، چاپ محدود.

۵. حسنی، جعفر (۱۳۸۹)،«معیارهای جرم‌انگاری موارد نقض حریم داده‌های شخصی در فضای سایبر»، مجموعه مقالات حقوق فناوری اطلاعات، معاونت حقوقی و قضایی قوهٔ قضائیه، ص

۱۷۱,-۱۹۴

۶. عالی‌پور، حسن (۱۳۸۴)،«جرم‌های مرتبط با محتوا: سیاه فناوری اطلاعات»، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، چ۱، تهران: نشر سلسبیل، ص ۲۲۱,-۲۲۶

۷. کدخدایی، عباسعلی و حاجی ملا، هیوا (۱۳۹۳)، «افشای اطلاعات طبقه‌بندی‌شده از سوی پایگاه ویکی‌لیکس؛ تقابلی نوین میان حق دسترسی به اطلاعات و امنیت ملی»، نشریهٔ مطالعات حقوق تطبیقی دانشگاه تهران، دورهٔ پنجم، ش۲، ص ۵۵۷-۵۳۵.

۸. مقدسی، محمدباقر و فرجیها، محمد (۱۳۹۲)، «ویژگی‌های سیاست‌های کیفری عوام‌گرا؛ مطالعهٔ تطبیقی»، نشریهٔ مطالعات حقوق تطبیقی دانشگاه تهران، دورهٔ چهارم، ش۲، ص ۱۳۷-۱۵۵.

ب) خارجی

9. Bundesdaten schutzgesetz (BGBl.I 1990 S.2954),as amended by the law of 14 September1994,available at:<http://www.iuscomp.org/gla/statutes/BDSG.html>2013/08/16 >. 10.

10. Campbell Quinn & m.kennedy,david, (2002), The psychology of computer criminals in computer security handbook forth edition kohn wiley & sons Ins, United States of American, New York11.

11. Convention on Cybercrime, (2001), Budapest.23.XI.2001, available at : html://www.covention.coe.int/Treaty/en/Treaties/Html/185.html>.2006/06/19>.

12. Concil of Europe, (1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.3.1981(ETS NO.108).

13. Concil of Europe,(2001), Explanatory report to the Convention on Cybercrime, 14. Concil of Europe, (2007), Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of the Concil of Europe.

15. Demetriou, Christina & silke, Andrew, (2003), A Criminological Internet sting, Oxford Univerity press Inc, British journal of Criminology Vol.43.

16. Directive 95/46/EC of the European parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of the personal data and on the free movement of such data available,at:<http:www.cdt.org/privacy/eudirective/Eu-Directive-html>.2006/04/16>

17. Delmas-Marty,Mirelle/Siber,Ulrich, (2008) «Les chemins de 1harmonissation penale,Collection de L UMR de Droit Compare de Pris»,volum 15,paris.p.127-202.

18. Gesetz gegen den unlauteren Wettbewerb vom 3. Juli 2004(BGBl. I 2004 32/1414) available at: < http://www.iuscomp.org /gla/literature/ heidenreich.htm. sd footnote 2 sym>.2012/05/12>

19. Michael Alistair Kelman, (2002) Electronic Commerce:law and practice,sweet &Maxwell,London.

20. Michael L.Rusted &Thomas H.Koeng, (2005) Rebooting Cybertort Law,Washington Law Rewie,Vol.80
21. Personal Data protection Code, (2003) sction 4, (1)(b).
22. Recommendation of the Coucil of the OECD Concering, (1997) «Guidelines for The Cryptography policy,Strafgesetzbuches»,des Gesetzes durch Artikel 3 des Gesetzes vom 2.10.2009 (BGBl. I S. 3214)
23. Sieber,Ulrich, (1986) «The international hand book on computer crime» ,Computer-related economic crime and the infringerments of privacy
24. Sieber.Ulrich, (1994) Information Technology Crime:Heymann,vol.6
25. Sieber.Ulrich, (2001) «Responsibility of Internet-providers,In Law,Information and Information Technologhy» ,E.Lederman,R.Shapira(eds.)The Hague,Kluwer International. p.231-292.
26. United Nation, manual on the prevention and control of computer – related crime,para.114.
27. United Nations, (1989) Convention on the Right of the Child,P.1577 unts.
28. William R.cheswick und steeven M.Belovin,Teil v, von:prof.Dr.ulrich sieber (1996) «Fire walls and scherheit im internet» von: Addision –wesley publishing company.