فصلنامهٔ علمی دیدگاه‌های حقوق قضایی
مقالهٔ پژوهشی، دورهٔ ۲۵، شمارهٔ ۹۱، پاییز ۱۳۹۹، صفحات ۲۳۳ تا ۲۵۵
تاریخ دریافت: ۱۳۹۷/۰۶/۱۸ - تاریخ پذیرش: ۱۳۹۹/۱۰/۰۱

# اصول حمایت کیفری از داده در فضای سایبر؛ در پرتو اسناد بین‌المللی و نظام کیفری ایران و آلمان

| **محمد فرجیها*** | دانشیار گروه حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه تربیت مدرس، تهران، ایران
| **علی علمداری** | کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه شیراز، شیراز، ایران

## چکیده

جرم‌انگاری یک رفتار در فضای سایبر، تعیین‌کنندهٔ قلمرو آزادی افراد و محدودهٔ سایر ابزارهای کنترل اجتماعی رسمی و غیررسمی تلقی می‌گردد. لذا می‌بایست دارای اصول راهبردی مشخص باشد. این اصول جرم‌انگاری عبارت‌اند از: اصل تعامل مداخله‌های کیفری با مداخله‌های حمایتی، اصل تمایز در تعیین قلمرو و محدودهٔ عناوین مجرمانه و سایر شرایط نامبرده شده در کنوانسیون جرائم سایبر و پروتکل الحاقی مصوب ۲۰۰۱ میلادی که به‌عنوان الگو و راهنما، نحوهٔ گزینش و کاربست قواعد اخلاقی و چهارچوب معیارها و محدودیت‌ها را با تکیه بر مبانی نظری معین و ملاحظات هنجاری و ارزشی تعیین می‌نماید. این پژوهش با استفاده از روش توصیفی‌تحلیلی در مقام پاسخ به این پرسش است که اصول بین‌المللی جرم‌انگاری تا چه اندازه در جرم‌انگاری در فضای سایبر در دو نظام عدالت کیفری ایران و آلمان مدنظر قرار گرفته است و تجربهٔ نظام کیفری آلمان در این قلمرو چه دستاوردهایی برای نظام کیفری ایران داشته است؟ یافته‌های پژوهش نشان می‌دهد قانون‌گذار آلمان مطابق کنوانسیون جرائم سایبر و اسناد بین‌المللی میان قلمرو و محدودهٔ عناوین مجرمانه تفکیک قائل شده است و تا حد امکان، از جزای نقدی مبتنی بر ضمانت‌اجراهای اداری و مدنی

---

* نویسندهٔ مسئول؛ *Email:* mohammadfarajiha@gmail.com

استفاده نموده است. لیکن قانون‌گذار ایران چنین تفکیکی را قائل نشده است. به نظر می‌رسد تجربهٔ نظام کیفری آلمان در ایجاد تعامل میان ضمانت‌اجراهای کیفری و حمایتی قابلیت انتقال به نظام کیفری ایران را دارد.

**واژگان کلیدی:** جرائم سایبر، حمایت از داده، جرم‌انگاری، اصل تمایز، اصل عمدی بودن

**مقدمه**

توسعهٔ فضای سایبر جوامع را به‌طور بنیادین دچار تغییر و تحول نموده است. فضای سایبر که نخست به‌منظور ایجاد رفاه و آسایش هر چه بیشتر افراد مورد بهره‌برداری قرار می‌گرفت به‌موازات وابستگی روزافزون جوامع بشری به این فناوری به‌تدریج به‌عنوان ابزاری جهت نیل به آمال مجرمان تبدیل شد که بزهکاران بخشی از فعالیت مجرمانهٔ خود را به فضای سایبر منتقل نمایند یا از رهگذر چنین بستری مرتکب اعمال مجرمانه شوند (پیکا، ۱۳۹۳: ۱۱). عضویت در جامعهٔ جهانی، منافع مشترک بین‌المللی و ضرورت همکاری‌های بین‌المللی در حوزهٔ سایبر برای برخورد با برهم‌زننده‌های نظم بین‌المللی دولت‌ها را ناگزیر می‌نماید که برخی رفتارها را به‌طور مستقیم یا غیرمستقیم با الهام گرفتن از کنوانسیون‌های بین‌المللی مجرمانه تلقی نمایند؛ ازجمله کنوانسیون جرائم سایبر (بوداپست) که آلمان به آن پیوسته است و ایران بدون پیوستن به آن صرفاً از آن در نحوهٔ جرم‌انگاری در قلمرو فضای سایبر الگوبرداری نموده است؛ زیرا اگر حقوق کیفری را کنترل‌کنندهٔ روابط اجتماعی بدانیم، چگونگی گزینش قواعد اخلاقی از سوی دولت و وارد نمودن آن‌ها به قلمرو قوهٔ قهریه به موضوع جرم‌انگاری مرتبط است. جرم‌انگاری یک رفتار فرایندی است که بر اساس آن قانون‌گذار از طریق تصویب قوانین اعمالی را به‌منظور حفظ ارزش‌های اجتماعی و نظم عمومی یا جهات دیگر جرم قلمداد می‌نماید. (عبدالفتاح، ۱۳۸۱: ۱۳۵)

گرانیگاه این پژوهش تحلیل ظرفیت‌ها و اصول جرم‌انگاری در فضای سایبر بر مبنای اسناد بین‌المللی ازجمله کنوانسیون جرائم سایبر (بوداپست) ۲۰۰۱ میلادی، پروتکل الحاقی به کنوانسیون جرائم سایبر ۲۰۰۱ میلادی، دستورالعمل سازمان ملل متحد دربارهٔ پیشگیری و کنترل جرائم مرتبط با رایانه ۱۹۹۴، توصیه‌نامه‌های شورای اروپا در مورد جرائم مرتبط با رایانه و نیز چهارچوب چگونگی کاربست این اصول در دو نظام عدالت کیفری ایران و آلمان و طرح امکان کاربست دستاوردهای حقوق کیفری آلمان به‌نظام کیفری ایران است. پرسش اصلی این پژوهه که نگارندگان درصدد پاسخ‌گویی به آن برآمده‌اند، این است: ۱. اصول مورداشاره در کنوانسیون‌های بین‌المللی تا چه اندازه در جرم‌انگاری یک رفتار در فضای سایبر در نظام عدالت کیفری ایران و آلمان مدنظر قرارگرفته است؟ چهارچوب مصادیق قانونی موردبحث در نظام حقوقی آلمان شامل قانون مجازات با آخرین

اصلاحات ۲۰۰۹، قانون حمایت از داده با آخرین اصلاحات سال ۲۰۰۹ است. مصادیق قانونی موردبحث در نظام حقوق ایران نیز شامل قانون تشدید مجازات مرتکبین اختلاس، ارتشاء و کلاهبرداری مصوب ۱۳۶۷، قانون تجارت الکترونیک مصوب ۱۳۸۲، قانون مجازات نیروهای مسلح مصوب ۱۳۸۲، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ است.

اصول جرم‌انگاری با هدف تدوین راهبردی سریع و مؤثر در همکاری بین‌المللی و به‌منظور هماهنگی ارکان تشکیل‌دهندهٔ جرم در حقوق جزای ماهوی داخلی کشورها در غالب اسناد بین‌المللی به‌عنوان الگو و راهنمایی بین‌المللی تعیین می‌نماید که با احتساب ماهیت عمومی و جهانی شبکه‌های اطلاعاتی، چه اعمالی باید از حیطهٔ اقتدار نظام عدالت کیفری خارج شوند. تعیین چگونگی این گزینش و کاربست در نظام‌های عدالت کیفری مبتنی بر رعایت اصولی است همچون اصل تعامل مداخله‌های کیفری با مداخله‌های حمایتی، اصل عمدی بودن، اصل تمایز در تعیین قلمرو و محدودهٔ عناوین مجرمانه، اصل تمایز در حمایت از اشخاص حقیقی و حقوقی که در اسناد بین‌المللی همچون کنوانسیون جرائم سایبر ۲۰۰۱ میلادی، پروتکل الحاقی به کنوانسیون جرائم سایبر ۲۰۰۱ میلادی، به‌عنوان تدابیری که باید در سطح ملی اتخاذ شوند به دُوَل عضو کنوانسیون پیشنهاد شده است. در این پژوهه تلاش شده است ذیل چهار مبحث ضمن تحلیل اصول جرم‌انگاری در فضای سایبر در چهارچوب مصادیق مطروحه، در تحلیل محتوای کنوانسیون و محتوای قوانین نظام عدالت کیفری ایران و آلمان مبنا به‌تناسب صرفاً آن بخش از مواد قانونی است که با اصول جرم‌انگاری در ارتباط است و از مصادیق رعایت یا عدم رعایت شرایط مورد اشاره است.

### ۱. اصل تعامل مداخله‌های کیفری با مداخله‌های حمایتی

به‌موجب کنوانسیون جرائم سایبر، یک رفتار در فضای سایبر برای اینکه جرم‌انگاری شود باید به‌اندازهٔ کافی سرزنش‌پذیر باشد؛ زیرا اگر رفتاری را که قانون‌گذار جرم شناخته است به‌قدر کافی صدمه و سرزنش در پی نداشته باشد حقوق و آزادی افراد مخدوش خواهد شد و مردم عملاً از دستور قانون‌گذار مبنی بر عدم ارتکاب چنین رفتاری سرپیچی خواهند نمود. بر مبنای اصل تعامل مداخله‌های کیفری با مداخله‌های حمایتی و بند ۴۰ گزارش توجیهی کنوانسیون جرائم سایبر، در مواجهه با رفتارهای نابهنجار در فضای سایبر، جرم‌انگاری آخرین راه چاره است. زیرا در حقوق کیفری کرامت‌محور که دغدغهٔ سیاست‌گذاران کیفری است، در هر جرم‌انگاری باید چنان مصلحتی در حمایت از حقوق و آزادی‌های افراد وجود داشته باشد که بر مفسدهٔ ناشی از محدودکردن این حقوق و آزادی‌ها چیرگی داشته باشد. (ناتری، الحسینی و طباطبایی، ۱۳۹۰: ۲۷۲) براین اساس، در رویارویی با نابهنجاری‌ها نمی‌توان از منافع، مصالح و ارزش‌ها به‌طور یکپارچه

حمایت کیفری کرد و همهٔ مصادیق نقض آزادی را جرم‌انگاری نمود. (نوبهار، ۱۳۹۰: ۱۱۹) این به آن معنا است که جرم‌انگاری امری موردی و استثنایی و نیازمند دلایلی منطقی است.

فضای سایبر یک فضای مبتنی بر فناوری‌های نوین است و لذا استفاده از امکانات فناورانه در ایجاد امنیت و حمایت از حقوق اشخاص از اهمیت بالایی برخوردار است. با توجه به اینکه جرائم ارتکابی در فضای سایبری عمدتاً توسط نیروهای سازمان‌یافته و با طراحی و نقشهٔ قبلی و نیز توسط اشخاص رقیب یا اخراج‌شده از سازمان‌های مزبور صورت می‌گیرد. (رضوی، ۱۳۸۶: ۱۲۴) لذا کاربست روش‌های حمایتی در چهارچوب پیشگیری اجتماعی در غالب آموزش‌های تخصصی و عمومی در رسانه‌های گروهی همانند آنچه در سند «رهنمود عملی پیشگیری از جرم سازمان ملل متحد» بر آن تأکید شده است و پیشگیری وضعی در غالب نصب دیوار آتشین[1] و پالایهٔ استفاده از پروکسی[2]، محصولات امنیتی، کدهای رفتاری، ابزارهای گزینش محتوا را می‌توان روش مناسبی دانست به‌منظور پرهیز از جرم‌انگاری یک رفتار در فضای سایبر؛ زیرا کمترین لطمه را به منافع و آزادی‌های خصوصی وارد می‌آورد. به تعبیر کلارکسون برای کنترل رفتاری که می‌تواند به‌خوبی توسط دیگر رشته‌های حقوقی تحت نظم درآید نباید از حقوق کیفری استفاده کرد. (Clarkson, 1995: 161) روش‌های مورداشاره که در کنوانسیون جرائم سایبر و پاراگراف ۴۵ گزارش توجیهی کنوانسیون جرائم سایبر ۲۰۰۱ میلادی به آن تأکید شده است و هزینه‌های کمتری به دولت و دستگاه قضایی تحمیل می‌نماید، به‌اصطلاح روش‌های حمایتی نامیده می‌شوند.حکومت باید صنعت را به نوآوری تشویق نماید به‌ویژه به ایجاد محصولات امنیتی جدید، کدهای رفتاری، ابزارهای گزینش محتوا که می‌تواند مکملی برای حمایت کیفری به شمار آیند (Sieber, 2000: 319).

در مقابل این نوع گرایش، روش‌های واکنشی یا حقوقی قرار دارند، که این نوع حمایت باید مبتنی بر مقررات اداری و مدنی باشد؛ زیرا مقررات اداری و حقوق مدنی و قراردادهای میان موضوع داده‌ها و سازمان‌های دخیل در پردازش داده‌ها می‌توانند در اکثر مواقع راه گشا باشند. به اعتقاد دکتر روکسین، حقوق کیفری تنها وسیلهٔ مناسب برای حمایت از ارزش‌ها و منافع موجه نیست، بر این اساس حقوق کیفری تنها زمانی کاربرد می‌یابد که دیگر راه‌ها مانند اقامهٔ دعوای مدنی و راه‌حل‌های اداری و ضمانت‌اجرای غیرکیفری بازدارندگی لازمه را نداشته باشند (Jareborg, 1995: 524). یکی از

---

1. Fire Wall

۲. Proxy: سروری است که به‌عنوان یک واسطه بین کاربر و سرور عمل می‌کند. هنگامی‌که رایانه‌ای از طریق پروکسی به اینترنت وصل است و می‌خواهد به یک فایل دسترسی پیدا کند، ابتدا درخواستش را به یک سرور پروکسی می‌فرستد و سپس پروکسی به رایانه مقصد متصل شده، فایل درخواستی را دریافت می‌کند.

فیلسوفان حقوق کیفری به نام «جاناتان شنشک» پیشنهاد می‌نماید در زمانی که درصدد جرم‌انگاری رفتاری هستیم، باید آن رفتار به‌طور متوالی و به‌گونه‌ای موفقیت‌آمیز از میان سه پالایه عبور نماید. در صورت شکست درگذر این پالایه‌ها نمی‌توان آن را جرم شناخت و در صورت گذر از هر سه پالایه جرم دانستن رفتار موجه است. درون‌مایهٔ این اصل بیشتر ناظر بر این واقعیت است که انتخاب مجازات همواره نیازمند توجیه کافی است. (Duff & Garland, 1994: 2) مطابق این تئوری، نخست باید اثبات شود که بر اساس اصول و مبانی نظری، دولت به مداخله در حوزهٔ حقوق و آزادی‌های فردی شهروندان از طریق ممنوعیت یا ایجاد محدودیت کیفری مجاز است. بعد از عبور رفتار از پالایهٔ نخست باید روش‌هایی که کمترین مزاحمت ممکنه را برای فرد ایجاد می‌نمایند و کمتر جنبهٔ آمرِه دارند، در قیاس با روش‌هایی که مزاحمت بیش‌تری را برای فرد ایجاد می‌نمایند در ارجحیت قرار گیرند و درنهایت باید عواقب عملی جرم‌انگاری یک رفتار و سود و زیان اجتماعی اجرا و عدم‌اجرای قانون کیفری پیشنهادی مورد ارزیابی دقیق قرار گیرد. در سطح بین‌المللی اختلاف‌نظرهای چشمگیری در مورد روش‌ها و سطح حمایت در قانون اداری، مدنی، جزایی یا اجرایی، وجود دارد و نیز ناهماهنگی‌های جدی نیز در مورد مقدار حمایتی که حقوق کیفری باید در زمینهٔ حقوق خصوصی و فردی تضمین کند، وجود دارد. لیکن مطابق پاراگراف ۳۵ گزارش توجیهی کنوانسیون جرائم سایبر تقدم باید به ضمانت‌اجراهای غیرکیفری داده شود، به‌ویژه هنگامی که روابط طرفین به‌وسیلهٔ یک قرارداد تنظیم می‌شود؛ و مقررات جزایی فقط در مواردی باید به کار گرفته شود که قانون مدنی و قانون حمایت از دادهای رایانه‌ای، تدابیر قانونی مناسب را فراهم نکند.

قانون‌گذار ایران به‌رغم توصیه‌های بین‌المللی ازجمله کنوانسیون جرائم سایبر و دستورالعمل سازمان ملل متحد دربارهٔ پیشگیری و کنترل جرائم مرتبط با رایانه مصوب ۱۹۹۴ به‌منظور ایجاد تعامل میان مداخله‌های کیفری با مداخله‌های حمایتی در مادهٔ ۲۴ قانون جرائم رایانه‌ای ایران درخصوص استفاده بدون مجوز از پهنای باند بین‌المللی مقرر می‌دارد: «هر کس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یک‌صد میلیون‌تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد». این در شرایطی است که مطابق اصول ناظر بر حمایت کیفری، کارکرد حقوق کیفری نباید مداخله در زندگی خصوصی افراد یا تلاش برای اعمال الگوهای خاص رفتاری باشد. (Faure & Visser, 1995: 247) در نظام کیفری آلمان استفاده از پهنای باند بین‌المللی توسط مردم در عرصهٔ داده‌پردازی، استفاده از فضای سایبر با پهنای باند پرسرعت بین‌المللی و بهره‌گیری ازاین‌گونه ارتباطات تحت ضوابط خاصی به‌عنوان یک حق

شهروندی پذیرفته شده است (الهی‌منش و سدره‌نشین، ۱۳۹۵: ۱۳۹) و مجازات کیفری صرفاً در جرائم خطرناکی که مقررات اداری یا مدنی توان مقابله با آن را ندارند اعمال می‌شود؛ زیرا اگر رفتار ارتکابی به‌قدر کافی صدمه و سرزنش در پی نداشته باشد، جرم‌انگاری آن رفتار، حقوق و آزادی افراد را مخدوش خواهد نمود و مردم عملاً از دستور قانون‌گذار مبنی بر عدم ارتکاب چنین رفتاری سرپیچی خواهند نمود. همانند آنچه درخصوص استفاده از فیلترشکن‌ها و استفاده از تجهیزات دریافت اینترنت ماهواره‌ای در ایران قابل‌مشاهده است.

در نظام کیفری آلمان منطبق با پاراگراف ۳۷ کنوانسیون جرائم سایبر به‌منظور ایجاد تعامل میان مداخله‌های کیفری و حمایتی تا حد امکان از جزای نقدی مبتنی بر ضمانت‌اجراهای مدنی و اداری استفاده می‌شود. حتی در مورد جرائمی که عواملی مانند نوع داده‌ها، دامنهٔ جرم، شیوهٔ ارتکاب باعث می‌گردد نتیجهٔ مجرمانه خفیف باشد، موارد استثنائاتی را پیش‌بینی و اعمال می‌نماید که به‌موجب آن برخی تخلفات جزئی و قابل‌اغماض را از شمول جرائم تعریف‌شده مستثنا گردد. در صورت مسئولیت نیز، به‌موجب قراردادهای مدنی و اداری مجازات می‌نماید. جلوه‌ای از رعایت این اصل را می‌توان در مادهٔ ۴۳ و ۴۴ قانون فدرال حمایت از دادهٔ آلمان مشاهده نمود که به‌موجب این مصوبه ارائه‌دهندگان خدمات دسترسی تا زمانی که بر اطلاعاتی که انتقال می‌دهند، تأثیر نگذارند یا اطلاعات یا دریافت‌کنندهٔ اطلاعات را گزینش نکنند، مسئول نمی‌باشند و در صورت مسئولیت نیز، به‌موجب قراردادهای مدنی و اداری مجازات می‌شوند و این راه‌حل، موازنهٔ مناسبی را میان پیشگیری از جرم و جریان آزاد داده‌ها در شبکه‌های رایانه‌ای بین‌المللی برقرار می‌سازد (Sieber, 2001: 231-239). قانون‌گذار ایران مطابق اصل تعامل مداخله‌های کیفری و حمایتی در مادهٔ ۲۱ قانون جرائم رایانه‌ای دربارهٔ ارائه‌دهندگان خدمات دسترسی و در مادهٔ ۲۳ درخصوص ارائه‌دهندگان خدمات میزبانی، مجازات انحلال و جزای نقدی مقرر نموده است. مطابق موارد پیش‌گفته، نظام عدالت کیفری آلمان مطابق اصل تعامل مداخله‌های کیفری و حمایتی تلاش نموده تا حد امکان مجازات کیفری را صرفاً در جرائم خطرناکی که مقررات اداری یا مدنی توان مقابله با آن را ندارند، اعمال نماید. لیکن قانون‌گذار ایران به‌رغم توصیهٔ اسناد بین‌المللی بدون توجه به‌پیش شرط‌های جرم‌انگاری که شامل اصل صدمه و سرزنش است، رفتارهایی را جرم‌انگاری نموده است که انجام چنین رفتاری در کشورهای توسعه‌یافته به‌عنوان یک حق شهروندی مورد حمایت قانون‌گذار قرار گرفته است و این رویکرد با اصول مطرح‌شده در اسناد بین‌المللی مبنی بر اصل مداخلهٔ حداقلی دولت‌ها در فضای سایبر در تعارض است.

## ۲. اصل عمدی بودن در جرائم سایبر

اصولاً نقض حریم خصوصی افراد در فضای سایبر باید در صورتی مجازات گردد که مرتکب به‌طور عمد عمل نماید، جرم‌انگاری اعمال ناشی از بی‌مبالاتی مستلزم توجیه ویژه است. پاراگراف ۳۹ کنوانسیون جرائم سایبر به‌خصوص در مقدمه و پاراگراف ۱۲۱ گزارش توجیهی کنوانسیون به‌صورت پیش‌شرط مقرر می‌دارد: به‌عنوان یک اصل، همهٔ جرائم گنجانده‌شده در کنوانسیون جرائم سایبر، می‌باید از روی عمد انجام‌شده باشند تا مسئولیت جزایی نسبت به مرتکب قابل‌اعمال باشد و در موارد خاص نیز وجود یک عنصر عمدی خاص مکمل برای تحقق جرم ضروری است. پاراگراف ۳۷ گزارش توجیهی کنوانسیون جرائم سایبر به اعضا پیشنهاد می‌نماید تا در جرم‌انگاری در فضای سایبر تخلفات جزئی را از شمول جرائم تعریف‌شده در کنوانسیون استثنا نمایند. انجمن بین‌المللی حقوق جزا نیز، پیشنهاد می‌نماید که مقررات جزایی قابل‌اجرا در زمینهٔ حقوق فردی باید فقط در موارد مهم به‌ویژه مواردی که داده‌های رایانه‌ای بسیار حساس یا اطلاعاتی را که قانون به‌طور سنتی موردحمایت قرار داده است، استفاده شود و جرم‌انگاری نیز نسبت به افعال عمدی محدودشده باشد (Sieber, 1994: 673-691).

قانون‌گذار آلمان مطابق اصول مطرح‌شده در اسناد بین‌المللی در مادهٔ ۱۵ قانون مجازات مقرر می‌دارد: «اگر قانون در مورد جرائم غیرعمد به‌صراحت مجازاتی تعیین نکرده باشد فقط جرائم عمد قابل مجازات هستند». مطابق این رویکرد قانون‌گذار آلمان در بند ۲ مادهٔ ۱۱ قانون مجازات مقرر می‌دارد: «در صورتی می‌توان فعل را عمدی محسوب نمود که کلیه عناصر قانونی فعل مجرمانه را که مستلزم قصد مجرم به انجام فعل مجرمانه است موجود باشد مگر اینکه قصور، موجب نتیجه خاصی شود که از فعل مذکور حاصل‌شده است». با توجه به‌صراحت مادهٔ ۱۵ قانون مجازات آلمان تنها شمار اندک و خاصی از جرائم غیرعمدی وجود دارد که حتی در صورت سهل‌انگاری صرف (بدون قصد) در شبکه داده‌ها به وجود آمده و قابل مجازات است.

حقوق‌دانان آلمانی مانند یشک و وایگند معتقدند که حقوق کیفری هرگز نمی‌تواند هر جا که اختلالی در نظم اجتماعی حاصل شد، مداخله کند، بلکه باید در حمایت از ارزش‌های مبنایی نظام اجتماعی که به‌صورت عمدی مورد نقض واقع‌شده است، ظاهر شود (Jescheck, 1996: 8). این شیوهٔ جرم‌انگاری در فضای سایبر تحت تأثیر اسناد بین‌المللی در نظام عدالت کیفری ایران موردتوجه قرار نگرفته است و قانون‌گذار در قانون جرائم رایانه‌ای واژهٔ عمد برای احراز مسئولیت کیفری و احراز سوءنیت را لحاظ ننموده است. برای نمونه مادهٔ ۱۳ قانون جرائم رایانه‌ای در مبحث کلاهبرداری مرتبط با رایانه مقرر می‌دارد: «هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی

با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مـال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون تا یک‌صد میلیون ریال یا هر دو مجازات محکوم خواهد شد». این در شرایطی است که در موارد خاص (کلاهبرداری)، وجود یک عنصر عمدی خاص مکمل (قصد کسب بهرهٔ اقتصادی) برای تحقق جرم لازم است. کنوانسیون جرائم سایبر (بوداپست) در پاراگراف ۹۰ گزارش توجیهی ضرورت جرم‌انگاری کلاهبرداری رایانه‌ای را مشروط به ارتکاب از روی عمد نموده است. لذا احراز این جرم نیازمند وجود قصد متقلبانهٔ خاص یا قصد سوء دیگر برای خود یا دیگری است. بر این اساس فعالیت‌های تجاری برای مثال استفاده از کوکی[1] یا نرم‌افزارها و برنامه‌های کاربردی جمع‌آوری اطلاعات برای مقایسهٔ میزان بازدید و فروش در فضای سایبر و تعیین سطح مبادلات که بدون مجوز از سایت بازدید و گزارش تهیه می‌نماید و بیشتر با هدف توسعه و بازاریابی محصولات تجاری در سطح بین‌المللی مورداستفاده قرار می‌گیرد و بر اساس رقابت بازار با قصد متقلبانه صورت نمی‌گیرد نباید جرم‌انگاری شوند. این درصورتی‌که به‌موجب مادهٔ ۱۳ قانون جرائم رایانه‌ای ایران انجام این فرایند جرم محسوب و مرتکب مشمول مجازات خواهد شد.

امروزه با گسترش فناوری ارتباطات و اطلاعات؛ انجام بخش عمدهٔ امور اداری و تجاری و صنعتی با رایانه با چالش‌هایی مواجه گردیده است به‌طوری‌که تعداد وقایع ناشی از هرگونه بی‌مبالاتی در فضای سایبر افزایش‌یافته و بر این اساس اصل سوءنیت، دیگر پاسخ‌گوی وضعیت موجود نیست. لذا جرائم ناشی از بی‌مبالاتی و قصور نیز، در نظام‌های کیفری پیش‌بینی و جرم‌انگاری شده‌اند. مطابق این رویکرد قانون‌گذار آلمان برای نمونه دربند ۳ مادهٔ ۳۱۷ قانون مجازات مقرر می‌دارد: «هر کس از روی بی‌احتیاطی با ایجاد اختلال در یک سیستم ارتباط دور عمومی، از کار آن جلوگیری نماید و یا آن را به خطر بیندازد، به‌طوری‌که عملکرد یکی از اجزای آن را مختل کند، آسیب برساند، از بین ببرد یا غیرقابل استفاده نماید و یا جریان برقی را که برای دستگاه در نظر گرفته‌شده است قطع نماید به مجازات حبس تا یک سال یا پرداخت جریمه نقدی محکوم خواهد شد». در مصوبهٔ مورداشاره ایجاد اختلال و صدمه‌زدن به سرورهای داده می‌تواند جزو یا مرحلهٔ مقدماتی جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی باشد. دستیابی غیرمجاز به سامانه‌های رایانه‌ای معمولاً به‌وسیلهٔ خدشه‌زننده‌های جوانی که انگیزه‌های مختلفی ازجمله سلب حمایت از داده، یا نفوذ در بانک‌های داده‌ها و یا مطرح‌شدن در بین دوستانشان یا مطبوعات دارند صورت می‌پذیرد.

---

1. Cookie

انجام این‌گونه رفتارها در فضای سایبر اغلب چون بخشی از قضایای جاسوسی نسبت به داده‌ها را تشکیل می‌دهد و تلاش‌های مجرم برای شناخت نقاط ضعف یک سامانه ممکن است فشاری بر آن سامانه تحمیل کند و موجب بروز نقص داده، بلوکه شدن سامانه‌های ارائهٔ خدمات عمومی شود، قانون‌گذار انجام این‌گونه رفتارها در فضای سایبر را جرم‌انگاری می‌نماید.

جلوه‌ای از تخطی از اصل عمدی بودن در فضای سایبر را می‌توان در بند ۲ مادهٔ ۹۷ قانون مجازات آلمان مشاهده نمود که قانون‌گذار مقرر می‌دارد: «هرکس که به‌واسطه بی‌مبالاتی فاحش، اسرار دولتی را که توسط یکی از مراجع رسمی یا به دستور وی محرمانه نگهداری می‌شود و به دلیل منصب دولتی، موقعیت خود در دولت یا به‌واسطه وظیفه‌ای که از طرف مقامی رسمی بر عهده وی گذاشته‌شده است، به اسرار مذکور دسترسی دارد، در اختیار اشخاص غیرمجاز قرار دهد و بدین‌وسیله، باعث خطر و ایجاد آسیب جدی به امنیت خارجی به جمهوری فدرال آلمان گردد، به مجازات حبس تا پنج سال یا پرداخت جریمه نقدی محکوم خواهد شد». این رویکرد قانون‌گذار در جرم‌انگاری اعمال غیرعمد زمانی مؤثر است که مطابق با کنوانسیون جرائم سایبر و پروتکل الحاقی صرفاً نسبت به موضوعات مهم و امنیتی و به‌صورت استثنایی در جرم‌انگاری موردتوجه قرار گیرد. زیرا هرگونه عدم توجه به این موضوع و جرم‌انگاری بی‌ضابطه با توجه به ماهیت فضای سایبر ممکن است موجب افزایش سیاههٔ جرائم و تورم کیفری شود. قانون‌گذار ایران مطابق با کنوانسیون جرائم سایبر اعمال غیرعمد را نسبت به موضوعات مهم و امنیتی و به‌صورت استثنایی جرم‌انگاری نموده است. برای نمونه در مادهٔ ۷۳ قانون تجارت الکترونیک ایران مصوب ۱۳۷۰ قانون‌گذار اقدامات ناشی از بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرم‌انگاری نموده است و مقرر می‌دارد: «اگر به‌واسطه بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرائم راجع به داده‌پیام‌های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون ریال محکوم می‌شود». مصداقی دیگر از این رویکرد را می‌توان در مادهٔ ۵ قانون جرائم رایانه‌ای ایران مشاهده نمود که قانون‌گذار مقرر می‌دارد: «چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه‌های مربوط هستند و به آن‌ها آموزش لازم داده‌شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آن‌ها قرارگرفته است براثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات و انفصال‌ازخدمت از شش ماه تا دو سال محکوم خواهند شد». جرم موضوع این ماده خاص است به دلیل اینکه فقط مأمور دولتی مسئول

حفظ یا امنیت یا حفاظت فنی داده‌ها است و غیرعمدی است. زیرا شخص از روی بی‌احتیاطی یا عدم رعایت تدابیر امنیتی باعث می‌شود اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مخابراتی و رایانه‌ای دست یابند. جرم‌انگاری افعال غیرعمد در فضای سایبر در مصادیق مورداشاره در نظام کیفری ایران و آلمان بیشتر به دلیل حساسیت داده‌های سری و جنبهٔ امنیتی آن‌ها صورت پذیرفته است که قانون‌گذار هرگونه بی‌احتیاطی یا بی‌مبالاتی و اهمال اشخاص را برنمی‌تابد و جرم‌انگاری این اعمال را ضروری می‌پندارد.

### ۳. اصل تمایز در تعیین قلمرو و محدودهٔ عناوین مجرمانه

با توجه به اینکه بستر فضای سایبر مبتنی بر داده‌های الکترونیکی است؛ لذا بسیاری از جرائم ارتکابی در فضای سایبر به‌لحاظ عنصر مادی شبیه هم هستند و این عناصر روانی و سایر اوضاع‌واحوال است که عناوین جرائم ارتکابی در فضای سایبر از هم متمایز می‌نمایند. مادهٔ ۶ کنوانسیون جرائم سایبر (بوداپست) و کمیتهٔ منتخب جرائم رایانه‌ای شورای اروپا در مصوبهٔ R (89)9 مقرر می‌دارد: قوانینی که این جرائم را تصویب می‌کنند باید رفتارهای ممنوع را به‌دقت شرح دهند و معیارهای مادی و روانی مختلف که باعث تغییر در اوصاف جرائم می‌شوند باید مدنظر قرار گیرند و جرائم مهم از غیرمهم، جرائم عمدی از جرائم مبتنی بر قصور تفکیک شوند و در میزان مجازات آن‌ها نیز تفاوت ایجاد گردد؛ و از به‌کارگیری بیش از حد روش ارجاع به مواد قانونی دیگر حتی‌الامکان اجتناب شود. (European Committee on Crime Problems, 1990: 89) زیرا اصل قانونی بودن جرم و مجازات که مورد تأکید قانون اساسی است برای قانون‌گذار تکالیفی ایجاد نموده که به‌موجب آن باید قانون‌گذار عناصر قانونی، مادی و معنوی هر جرم را به‌طور واضح و شفاف و بدون هرگونه ابهام و کلی‌گویی علی‌الخصوص در امور کیفری اعلام نماید تا شهروندان قانون را بهتر درک و در نتیجه اثر بازدارندگی قانون نیز افزایش یابد.

قانون‌گذار ایران به‌رغم توصیه‌هایی که در اسناد بین‌المللی ازجمله کنوانسیون جرائم سایبر و پروتکل الحاقی مصوب ۲۰۰۱ میلادی درخصوص ایجاد تمایز در تعیین قلمرو و عناوین مجرمانه شده است، در مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲ مقرر می‌دارد: «هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن‌که به‌طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوط صورت می‌گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی‌شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارد افشاء غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی است مانند دیسک‌های حاوی اطلاعات یا معدوم کردن آن‌ها یا سوءاستفاده‌های مالی که نظامیان به‌وسیله رایانه

مرتکب می‌شوند جرم محسوب و حسب مورد مشمول مجازات مندرج در مواد مربوط به این قانون می‌باشند». مادهٔ ۱۳۱ قانون مجازات جرائم نیروهای مسلح ایران شامل چندین جرم رایانه‌ای به شرح ذیل است: ۱. جعل رایانه‌ای توسط نظامیان ۲. جرم تخریب اسناد یا سامانه‌های رایانه‌ای توسط نظامیان ۳. جاسوسی و افشاء اطلاعات رایانه‌ای توسط نظامیان ۴. سرقت یا معدوم کردن اشیاء دارای ارزش اطلاعاتی توسط نظامیان ۵. سوءاستفاده مالی از طریق رایانه توسط نظامیان. این رویکرد قانون‌گذار که در یک ماده و با یک تعریف کلی از جرم، تکلیف همهٔ جرائم رایانه‌ای که توسط کارکنان نیروهای مسلح ارتکاب می‌یابند مشخص و مسئولیت تغییر مادهٔ مذکور را به مراجع عالی قضایی و قضات سپرده است، به نظر می‌رسد بیشتر ناشی از شتاب‌زدگی نظام کیفری در جرم‌انگاری تحت تأثیر اولویت یافتن ملاحظات سیاسی و امنیتی برای پاسخ‌گویی مقطعی و فوری به انتظارات عمومی در پی بازتاب گستردهٔ این جرائم بوده است که به دور از دغدغه‌های علمی و کارشناسی تحت حاکمیت فضای احساسی به‌سرعت در دستور کار قرار گرفته است. (فرجیها و علمداری، ۱۳۹۶: ۶۴۴-۶۴۳) جلوه‌ای دیگر از این رویکرد را می‌توان در مبحث کلاهبرداری در دو نظام کیفری ایران و آلمان مشاهده نمود. مادهٔ ۸ کنوانسیون جرائم سایبر در مبحث کلاهبرداری مرتبط با رایانه مقرر می‌دارد: «هر یک از اعضاء باید به‌گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم بر اساس حقوقِ داخلی خود، هرگونه اقدامات عمدی و غیر حق را که به‌قصد فریب یا دیگر مقاصد ناروا و در راستای جلب منفعت اقتصادی غیر حق برای خود یا دیگری صورت می‌پذیرد، جرم‌انگاری نماید که این اقدامات غیر حق شامل هرگونه واردکردن، تغییر، حذف یا قطع داده‌های رایانه‌ای و هرگونه ایجاد اختلال در عملکرد یک سیستم رایانه‌ای می‌شود».

قانون‌گذار آلمان مطابق مادهٔ ۸ کنوانسیون جرائم سایبر در مادهٔ ۲۶۳ ب قانون مجازات در مبحث کلاهبرداری به‌منظور تحصیل وجه، مال، منفعت مقرر می‌دارد: «هر کس با قصد تحصیل منفعت مالی غیرقانونی برای خود یا دیگری، با تحت تأثیر قرار دادن نتیجه عملیات پردازش داده‌ها از طریق ساماندهی غلط یک برنامه رایانه‌ای، استفاده از داده‌های غلط یا ناقص، استفاده غیرمجاز از داده‌ها یا سایر دخالت‌های غیرمجاز درروند پردازش داده‌ها، به مال دیگری خسارت وارد نماید، به مجازات حبس تا پنج سال یا پرداخت جریمه نقدی محکوم خواهد شد.» عنصر ورود خسارت به مال دیگری به‌عنوان نتیجهٔ مجرمانه‌ای که در این ماده موردتوجه واقع شده است منطبق با پاراگراف شمارهٔ ۸ گزارش توجیهی کنوانسیون جرائم سایبر و دستورالعمل‌های حمایت از داده‌های شخصی شورای اروپا است که مقرر می‌دارد دست‌کاری متقلبانه جهت کلاهبرداری در صورتی باید

جرم‌انگاری شود که به‌طور مستقیم منجر به وارد آمدن ضرر اقتصادی و یا موجب از بین رفتن تصاحب مالکانهٔ دیگری بر اموالش شوند.

قانون‌گذار آلمان در باب کلاهبرداری و تقلب جهت دریافت اعتبار در مادهٔ ۲۶۵ ب قانون مجازات مقرر می‌دارد: «هر کس، در ارتباط با تقاضای دریافت اعتبار، تمدید آن یا تغییر شرایط اعتبار برای یک شرکت یا مؤسسه بازرگانی یا برای یک شرکت یا مؤسسه بازرگانی واهی اسناد ناقص یا غلطی را، به‌ویژه اسناد مربوط به محاسبه موجودی، سود یا ضرر، خلاصه صورتحساب دارایی‌ها و بدهی‌ها و گزارش ارزشیابی اموال ارائه دهد، یا اظهارات مکتوب غلط یا ناقصی را درخصوص وضعیت مالی شرکت یا مؤسسه موردنظر ارائه دهد که به نفع متقاضی اعتبار و مؤثر در تصمیم‌گیری مؤسسه اعتباری درخصوص تقاضانامه آن باشد، یا شرکت یا مؤسسه موردنظر در مورد رکود وضعیت مالی در اسناد یا اظهارات مکتوب خود که مرتبط با تصمیم‌گیری مؤسسه اعتباری درخصوص تقاضای دریافت اعتبارات، مؤسسه مذکور را مطلع نگرداند، به مجازات حبس تا سه سال یا پرداخت جریمه نقدی محکوم خواهد شد». قانون‌گذار در این ماده مطابق مادهٔ ۸ کنوانسیون جرائم سایبر شرط توسل به وسایل متقلبانه را عنصر سازندهٔ این جرم دانسته است.

قانون‌گذار آلمان درخصوص کلاهبرداری و تقلب جهت دریافت خدمات در مادهٔ ۲۶۵ الف قانون مجازات مقرر می‌دارد: «هر کس با تقلب و با این هدف که هزینه‌ای پرداخت ننماید، از خدمات دستگاه‌های خودکار یا شبکه مخابراتی که جهت تأمین خدمات عمومی در نظر گرفته‌شده است و یا از وسایل حمل‌ونقل استفاده کند و یا ورود به نمایشگاه یا مؤسسه‌ای را به دست آورد، به مجازات حبس تا یک سال یا پرداخت جریمه نقدی محکوم خواهد شد». مگر آنکه فعل مذکور بر طبق قوانین دیگر، مجازات شدیدتری داشته باشد». به شرحی که گذشت قانون‌گذار آلمان در سه مادهٔ قانونی مجزا کلاهبرداری جهت تحصیل وجه، مال، منفعت (۲۶۳ ب)، کلاهبرداری و تقلب جهت دریافت اعتبار (۲۶۵ ب) کلاهبرداری و تقلب جهت دریافت خدمات (۲۶۵ الف) را جرم‌انگاری نموده است به‌طوری که هر یک دارای مجازات متفاوت بوده و شرایط ارتکاب آن‌ها نیز متفاوت است. در باب تعیین مجازات نیز، قانون‌گذار آلمان ضمن رعایت تناسب میان جرم و مجازات، برای جرائم رایانه‌ای (به‌ویژه جرم کلاهبرداری رایانه‌ای) در قیاس با جرائم کلاسیک مجازات بیشتری تعیین نموده است، زیرا هزینهٔ کمتر و خسارت بیشتری نسبت به جرائم کلاسیک دارد. قانون‌گذار آلمان مطابق پاراگراف ۳۶ گزارش توجیهی کنوانسیون جرائم سایبر و در راستای اصل تمایز در تعیین قلمرو و محدودهٔ عناوین مجرمانه تلاش نموده به دلیل ماهیت فنی و پیچیدهٔ جرائم ارتکابی در فضای سایبر تا حد امکان با تفکیک در نوع جرائم، عناصر تشکیل‌دهندهٔ هر یک از جرائم

را با عباراتی روشن و دقیق، مشخص و تعریف نماید. به دلیل آنکه استفاده از الفاظ و عبارات موسع و دارای معانی، مفاهیم و حتی کاربردهای متنوع و یا قابل اطلاق بر وضعیت یا رفتارهای متعدد توسط قانون‌گذار منجر به ابهام مادهٔ قانونی می‌شود و لاجرم مقصود قانون‌گذار از مصادیق موردنظر را مشخص نمی‌نماید و راه را بر تفسیرهای گوناگون و صدور احکام متفاوت می‌گشاید. قانون‌گذار ایران در باب کلاهبرداری مرتبط با رایانه با الگوبرداری از مادهٔ ۸ کنوانسیون جرائم سایبر در مادهٔ ۶۷ قانون تجارت الکترونیک مقرر می‌دارد: «هرکس در بستر مبادلات الکترونیکی، با سوءاستفاده و یا استفاده غیر مجاز از «داده‌پیام» برنامه‌ها و سامانه‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده‌پیام» مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیر دیگران را بفریبد و یا سبب گمراهی سامانه‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود». مادهٔ ۶۷ قانون تجارت الکترونیک اگرچه با الگوبرداری از مادهٔ ۸ کنوانسیون جرائم سایبر تدوین‌شده است لیکن دارای تفاوت‌های محسوسی است. بدین نحو که رفتارهای مجرمانه‌ای که منجر به کلاهبرداری رایانه‌ای در مادهٔ ۶۷ قانون تجارت الکترونیک می‌شوند تمثیلی هستند. لیکن در مادهٔ ۸ کنوانسیون جرائم سایبر، رفتارهای مجرمانه‌ای که منجر به کلاهبرداری رایانه‌ای می‌شوند حصری هستند. زیرا عنصر فریب و یا گمراه کردن سیستم، جزء عناصر جرم کلاهبرداری موضوع مادهٔ ۸ کنوانسیون جرائم سایبر نیست.

مطابق مادهٔ ۶۷ قانون تجارت الکترونیک ایران فریب دیگران و یا گمراهی سامانه‌های پردازش خودکار، جزء رفتارهای مجرمانه در جرم کلاهبرداری رایانه‌ای محسوب می‌شود. این در شرایطی است که در جرم کلاهبرداری رایانه‌ای، جرم بدون نیاز به فریب یک انسان تحقق می‌یابد، زیرا از نظر علمی اگر شخصی مداخله در عملکرد سامانه رایانه‌ای نماید و بدین لحاظ سامانه در پردازش به‌طور خودکار پاسخ محاسبات را غلط ارائه نماید در اینجا سامانه گمراه نشده بلکه سامانه پاسخ را با توجه به وضعیتی که داشته ارائه نموده است. بر مبنای مادهٔ ۶۷ قانون تجارت الکترونیک مرتکب باید اموال و امتیازات مالی را برای خود یا دیگران تحصیل نماید تا جرم کلاهبرداری رایانه‌ای تحقق یابد، لیکن بر مبنای مادهٔ ۸ کنوانسیون جرائم سایبر تحقق جرم کلاهبرداری مستلزم تحصیل وجوه، اموال یا امتیازات مالی نیست. لذا اگر مرتکب اقداماتی مانند ورود، محو، تغییر و توقف بدون حق داده‌های رایانه‌ای و یا اخلال بدون حق در عملکرد سیستم رایانه‌ای را به‌قصد تحصیل بدون حق و متقلبانه یک منفعت اقتصادی برای خود یا دیگری انجام داده باشد و موجب از دست رفتن اموال

دیگری گردد ولو مرتکب مالی تحصیل ننماید،جرم کلاهبرداری تحقق می‌یابد. در باب تعیین مجازات نیز به‌موجب مادهٔ ۶۷ قانون تجارت الکترونیکی، مجازات کلاهبرداری رایانه‌ای حبس از ۱ تا ۳ سال و پرداخت جریمهٔ نقدی معادل مال مأخوذه است این در حالی است که، به‌موجب مادهٔ ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء مجازات کلاهبرداری ۱ تا ۷ سال است.

قانون‌گذار ایران در مادهٔ ۱۳ قانون جرائم رایانه‌ای مقرر می‌دارد: «هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون تا یک‌صد میلیون ریال یا هر دو مجازات محکوم خواهد شد.» قانون‌گذار ایران در مصوبهٔ مورد اشاره به‌طورکلی اشکال مختلف کلاهبرداری (کسب وجه، مال، منفعت، خدمات، امتیاز مالی) را جرم‌انگاری نموده است و هیچ تفکیکی در اشکال مختلف جرم و میزان مجازات آن قائل نشده است و میزان مجازات آن نیز در قیاس با کلاهبرداری سنتی کمتر و فاقد تناسب است. با توجه به مصادیق پیش‌گفته، در دو نظام عدالت کیفری ایران و آلمان به نظر می‌رسد قانون‌گذار ایران به‌رغم الگوبرداری از کنوانسیون جرائم سایبر و پروتکل الحاقی ۲۰۰۱ میلادی در ایجاد تمایز در قلمرو و محدودهٔ عناوین مجرمانه همانند نظام عدالت کیفری آلمان دقت لازمه را در تفکیک و تمایز در تعریف، قلمرو و میزان مجازات در قیاس با جرائم سنتی اعمال ننموده است و اتخاذ چنین رویکردی برای نمونه در مبحث کلاهبرداری رایانه‌ای (مال، منفعت، امتیاز) و میزان مجازات تعیین‌شده در قیاس با کلاهبرداری سنتی موجب می‌شود تا مجرمان با توجه به منافع بیشتر و مجازات کمتر کلاهبرداری رایانه‌ای در قیاس با کلاهبرداری سنتی به ارتکاب این نوع از جرم مبادرت ورزند.

### ۴. اصل شناسایی مسئولیت کیفری اشخاص حقیقی و حقوقی

حقیقت غیرقابل‌انکار خطرات ناشی از جرائم اشخاص حقوقی، به‌ویژه جرائم اشخاص حقوقی در فضای سایبر، کشورهای مختلف را یکی پس از دیگری اقناع نموده تا فراتر از مضیقه‌های حاکم بر حقوق کیفری، به تبیین مسئولیت کیفری اشخاص حقوقی بپردازند و آن را با دیدگاهی واقع‌گرایانه موردپذیرش قرار دهند. (Hetzer, 2007: 403) کنوانسیون جرائم سایبر در مادهٔ ۱۲ به مسئولیت اشخاص حقوقی می‌پردازد و هدف از آن، مسئول دانستن شرکت‌ها، انجمن‌ها و دیگر اشخاص حقوقی به خاطر ارتکاب اعمال مجرمانهٔ اشخاص حقیقی است که در مقام مدیریت شخص حقوقی هستند و در جهت منافع آن مرتکب جرم می‌شوند. کنوانسیون جرائم سایبر دربند یک مادهٔ ۱۲، چهار شرط را برای مسئول شناختن اشخاص لازم می‌داند تا بتوان مسئولیت را به این اشخاص نسبت دهد:

الف) یکی از جرائم مندرج در کنوانسیون واقع‌شده باشد؛ فهرست جرائم مندرج در کنوانسیون جرائم سایبر در بخش نخست خود تحت حقوق جزای ماهوی در چهار گفتار شامل: ۱. جرائم علیه محرمانگی، تمامیت و دسترس‌پذیری سامانه‌ها و داده‌های رایانه‌ای (دسترسی غیرمجاز، شنود غیرمجاز، اخلال در داده‌ها و سامانه‌ها و سوءاستفاده از دستگاه‌ها)؛ ۲. جرائم مرتبط با رایانه (جعل و کلاهبرداری)، ۳. جرائم مرتبط با محتوا (هرزه‌نگاری کودکان)؛ ۴. جرائم مرتبط با نقض حق نشر و حقوق مرتبط به تصویب رسانده است.

ب) جرم باید به خاطر منافع شخص حقوقی ارتکاب یافته باشد. مقصود از منافع، همان انگیزه و ارتکاب جرائم رایانه‌ای است که سود مادی و معنوی شخص حقوقی را دربر می‌گیرد.

ج) می‌باید شخصی که مدیریت شخصی حقوقی را به‌عهده دارد، آن جرم را مرتکب شده باشد. مراد از مدیر شخص حقوقی به فردی اطلاق می‌گردد که سمت بالایی در سازمان داراست، مانند مدیرعامل.

د) اقدام فردی که پست مدیریت شخص حقوقی داراست، نیز باید بر اساس یکی از اختیارات مدیریتی، نظیر اختیار نمایندگی یا تصمیم‌گیری یا اعمال نظارت باشد، به‌نحوی‌که نشان دهد وی در چهارچوب اختیارات خود عمل نموده است تا بتوان مسئولیت را بر شخص حقوقی تحمیل نمود. (convention on Cyber crime, 2001: 123) لذا اگر مدیر شخص حقوقی، خارج از حیطهٔ اختیارات، مرتکب یکی از اقسام بزه‌های رایانه‌ای گردد، تمامی مسئولیت جزایی متوجه مدیر بوده و شخص حقوقی فاقد مسئولیت کیفری است. کنوانسیون جرائم سایبر در بند دو مادهٔ ۲ مقرر می‌دارد مسئولیت موردنظر در این ماده، می‌تواند کیفری، حقوقی و یا اداری و شامل جریمه‌های نقدی باشد که متناسب و بازدارنده است. بند چهارم مادهٔ ۲ کنوانسیون تصریح می‌نماید که مسئولیت اشخاص حقوقی موجب از بین رفتن مسئولیت فردی نمی‌گردد.

در نظام کیفری آلمان، این اصل که خلاف‌های انجمن قابل‌اعتراض نیست، برای مدت طولانی از تحمیل مسئولیت کیفری به شخص حقوقی به‌طورکلی جلوگیری می‌نمود. (Sun Beale & G, 2005: 105) اما ضرورت‌های اجتماعی و نقش فزایندهٔ اشخاص حقوقی در تحولات اجتماعی، دخالت گسترده در جرائم و عدم تکاپوی ضمانت‌اجراهای غیرکیفری در پیشگیری از این‌گونه رخدادها، پذیرش مسئولیت کیفری آن‌ها را اجتناب‌ناپذیر نمود. قانون‌گذار آلمان در مادهٔ ۱۴ قانون مجازات آلمان مقرر می‌دارد: «درصورتی‌که شخص در حوزه اختیارات به‌عنوان نماینده یک شخص حقوقی و یا به‌عنوان یکی از اعضای نهادی که به آن اختیارات نمایندگی واگذار گردیده و یا به‌عنوان شریکی که جهت نمایندگی یک مؤسسه تجاری، باصلاحیت حقوقی مستقل، به وی اختیاراتی

واگذارشده است و یا به‌عنوان نماینده قانونی شخص دیگری عمل نماید و به‌موجب هرگونه قانونی که بر طبق آن، خصوصیات، روابط یا ویژگی‌های خاص فردی مبنای مسئولیت کیفری را تشکیل می‌دهد، مسئولیت کیفری باید درخصوص نماینده مذکور اعمال گردد، اگرچه چنین خصوصیتی در خود شخص نماینده وجود نداشته باشد، بلکه نهاد، شرکت یا شخصی که وی نمایندگی آن را بر عهده دارد، واجد آن ویژگی‌ها باشد». مطابق مادهٔ ۱۴ قانون مجازات آلمان، عمل مجرمانهٔ تمامی کارکنان و مقامات اشخاص حقوقی به شرطی که ظاهراً در مقام انجام وظیفه برای شخص حقوقی و حداقل تا حدی به‌قصد تأمین منافع آن ارتکاب باید، حتی اگر با سیاست کلی شخص حقوقی مغایرت داشته باشد، به نام شخص حقوقی گذاشته و مسئولیت کیفری اعمال می‌گردد. (Beale & Safwat, 2005: 113) بر این مبنا، اشخاص حقوقی رکن‌های مادی و روانی جرائم منتسب به خود را برای مسئولیت یافتن، تنها از اشخاص حقیقی مذکور به عاریه می‌گیرند. مقصود از نماینده، شخص واجد قدرت و اختیاری مانند مدیرعامل است که به نام و به‌حساب شخص حقوقی ایفای نقش می‌کند و منظور از نهاد نیز مجمع‌های عمومی، هیئت‌مدیره و هیئت ناظران‌اند که از طریق خرد جمعی و تصمیم گروهی بر فعالیت شخص حقوقی اثر گذاشته و سیاست حاکم بر آن را ترسیم می‌کنند. لذا این مقام قضایی است که در عمل با اهتمام به‌جایگاه اعضای شخص حقوقی در سلسله‌مراتب اداری و تأثیرگذاری آن‌ها دست به تشخیص مسئولیت خواهد زد. (Belghoul, 2004: 17)

قانون‌گذار آلمان دربند ۲ مادهٔ ۱۴ قانون مجازات مقرر می‌دارد: «درصورتی‌که شخصی، خواه از طرف مالک شرکت و یا نماینده وی، اختیار یافته است تا شرکت را بعضاً یا کلاً، اداره نماید؛ یا به‌صراحت اختیار دارد وظایفی را به‌طور مستقل انجام دهد که در تصدی شرکت است و شخص موردنظر بر اساس این اختیارات عمل نماید قوانینی که به‌موجب آن ویژگی‌های فردی خاص منجر به مسئولیت کیفری می‌شود باید در مورد این شخص دارای اختیار نیز اعمال گردد اگرچه چنین ویژگی‌هایی نه در شخص وی، بلکه در شخصیت مالک شرکت وجود داشته باشد». مطابق این فرضیه در نمایندگی قانونی، اگر نماینده خارج از حدود اختیارات خود عمل کند و موجب ورود ضرر به شخصی شود، خود باید از عهدهٔ خسارت برآید و اصیل هیچ مسئولیتی ندارد. نظام کیفری آلمان برحسب مصادیق مورداشاره مسئولیت کیفری را به شخص حقوقی تحمیل نمی‌کند؛ بلکه به شخص نمایندگان و مدیران شرکت گسترش می‌دهد و کارکنان را به‌ویژه در چهارچوب مفهوم رژیم قانونی، کیفر می‌دهد و به‌منظور قاعده‌مند نمودن رفتار شرکت‌ها تا حد امکان از راهکارهای جبران حقوق اداری و مدنی و جزای نقدی مبتنی بر ضمانت‌اجراهای اداری بهره می‌گیرد و این رویکرد از جهت کارکردی دارای ارزش یکسان با مسئولیت کیفری است. (فرح‌بخش و فتازاده، ۱۳۹۵: ۱۴۹)

در نظام کیفری ایران، گسترش نقش اشخاص حقوقی در ارائهٔ خدمات اینترنتی قانون‌گذار را بر آن داشت تا مسئولیت کیفری آنان را درخصوص ارتکاب جرائمی چون دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی، جعل، تخریب و اخلال در داده‌ها با سامانه‌های رایانه‌ای با مخابراتی، سرقت، کلاهبرداری، جرائم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب با تصویب قانون جرائم رایانه‌ای به رسمیت بشناسد. قانون‌گذار ایران در مادهٔ ۱۹ قانون جرائم رایانه‌ای مقرر می‌دارد جرائم رایانه‌ای ذیل درصورتی‌که به نام شخص حقوقی و در راستای منافع آن، ارتکاب یابد، شخص حقوقی، دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی، مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی، دستور ارتکاب جرائم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد. بر این اساس مدیر شخص حقوقی قادر خواهد بود جرم رایانه‌ای را به شخص حقوقی منتسب کند، بی‌آنکه خود در تحقق مباشرت کرده باشد و آن زمانی است جرم منظور، به دستور او ارتکاب یابد.

ج) هرگاه یکی از کارمندان با اطلاع مدیر و یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود. مطابق این فرضیه کارمند بودن فرد شرط تحقق مسئولیت است. زیرا که حسب سلسله‌مراتب اداری، دستور مدیر شخص حقوقی صرفاً برای کارمند امری است مطاع. به‌موجب این نظریه، در مواردی که در اثر فقدان نظارت بر اعمال زیردستان، جرمی ارتکاب یابد و یکی از افرادی که در شخص حقوقی سمت ارشد داشته است بر اثر این فقدان نظارت یا مدیریت صحیح مقصر باشد، به‌گونه‌ای که مجموعهٔ ساختار و رویهٔ شخص حقوقی را بتوان در ارتکاب این جرم مقصر دانست، شخص حقوقی به خاطر جرائم این کارکنان مسئولیت کیفری خواهد داشت. بر اساس تئوری مسئولیت ناشی از عمل دیگری، هریک از کارکنان شخص حقوقی در هر درجه‌ای که باشند اگر مرتکب بعضی جرائم مادی صرف شوند، مسئولیت شخص حقوقی را به‌دنبال می‌آورند.(Tarelli, 2004: 4-5)

د) هرگاه تمام و یا قسمتی از فعالیت‌های شخص حقوق به ارتکاب جرم رایانه‌ای، اختصاص‌یافته باشد. ازجمله راه‌های انتساب جرم به شخص حقوقی، ارتکاب جرم رایانه‌ای توسط یکی از کارمندان آن است. مشروط به اینکه جرم مزبور با اطلاع مدیر یا در اثر عدم نظارت وی تحقق‌یافته باشد. پس ارتکاب جرم توسط کارمند بدون وجود اجتماع شرایط مذکور به مسئولیت کیفری شخص حقوقی دامن نخواهد زد. چندان‌که مسئولیت کیفری شخص حقوقی را متوقف بر احراز تقصیر از سوی مدیر یا هیئت‌مدیره نمی‌داند، زیرا گاه اصول اساسنامه و سیاست مأخوذ از خرد جمعی مجامع عمومی ترسیم‌کنندهٔ روند مجرمانه‌ای است که به مسئولیت کیفری شخص مزبور ختم می‌شود. مادهٔ ۱۹

قانون جرائم رایانه‌ای ایران نه‌فقط جرائم ارتکابی توسط یا به دستور مدیران، بلکه جرائم ارتکاب یافته از سوی کارمندان را نیز به‌شرط اطلاع یا عدم نظارت آن‌ها را نیز به شخص حقوقی منتسب کرده است (شریفی، ۱۳۹۶: ۸۹). مطابق این نظریه، افکار و اعمال مدیر، افکار و اعمال شخص حقوقی محسوب می‌شود. با این توصیف بر شخص حقوقی نه تعدد اراده، بلکه وحدت اراده حاکم است. (خدابخشی، ۱۳۸۷: ۱۳۰-۱۲۷) بر اساس این تعریف؛ مجامع عمومی و بازرسان شرکت نیز مدیر محسوب می‌شوند. اگر اشخاص تصمیم‌گیرنده بیش از یکی باشند، درصورتی‌که هر یک به‌تنهایی اختیار تصمیم‌گیری داشته باشد، انجام جرم از سوی یکی از آن‌ها برای تحقق مسئولیت کیفری شخص حقوقی، لازم است ولی اگر هیچ‌یک به‌تنهایی اختیار تصمیم‌گیری نداشته باشند باید جرم به مباشرت همه انجام شود (دیندار، ۱۳۸۹: ۳)

با وجود موانعی که پیرامون اسناد جرم به شخص حقوقی و مسئولیت کیفری آن وجود دارد؛ نظام‌های کیفری ایران و آلمان هدف‌های مشابهی را از راه رژیم‌های قانونی متفاوتی پی می‌گیرند. قانون‌گذار ایران مطابق کنوانسیون جرائم سایبر (بوداپست) در قانون جرائم رایانه‌ای با اشاره به انتساب اعمال کارمند و مدیر به شخص حقوقی نظریهٔ نمایندگی، موردتوجه قرار داده است تا به این‌سان احراز مسئولیت در صور مختلف میسر گردد. نظام کیفری آلمان برحسب مصادیق مورداشاره مسئولیت کیفری را به شخص حقوقی تحمیل نمی‌کند، بلکه به شخص نمایندگان و مدیران شرکت گسترش می‌دهد و کارکنان را به‌ویژه در چهارچوب مفهوم رژیم قانونی، کیفر می‌دهد و به‌منظور قاعده‌مند نمودن رفتار شرکت‌ها تا حد امکان از راهکارهای جبران حقوق اداری و مدنی و جزای نقدی مبتنی بر ضمانت‌اجراهای اداری بهره می‌گیرد. بر این مبنا قصور در نظارت، قصور در انجام اقدامات مناسب و متعارف جهت پیشگیری از ارتکاب فعالیت‌های مجرمانه توسط کارمندان یا نمایندگان به نفع شخص حقوقی را شامل می‌شود و این شرط نباید به معنای الزامی بودن اعمال یک نظام نظارتی عام بر ارتباطات کارمندان تلقی نمود؛ زیرا تحمیل وظایف سنگین به ارائه‌کنندهٔ خدمات و مسئول دانستن آن نسبت به داده محتوای ارائه‌شده توسط کاربران، با اهداف کنوانسیون جرائم سایبر در تعارض است و هدف حکومت‌ها در حفظ بازار آزاد و رقابت موجود در ارائه خدمات را دچار اختلال می‌نماید.

**نتیجه**

اصول بین‌المللی حاکم بر حمایت کیفری از داده با هدف ایجاد تعامل و راهبردی مؤثر در همکاری بین‌المللی و به‌منظور هماهنگی ارکان تشکیل‌دهندهٔ جرم در حقوق جزای ماهوی داخلی کشورها به‌عنوان الگو و راهنما مشخص می‌نماید که با احتساب ماهیت بین‌المللی شبکه‌های

اطلاعاتی، چه اعمالی باید از حیطهٔ اقتدار نظام عدالت کیفری خارج شوند. چگونگی تعیین این گزینش مبتنی بر اصول و مؤلفه‌هایی است، ازجمله اصل تعامل مداخله‌های کیفری با مداخله‌های حمایتی، اصل تمایز در تعیین قلمرو و محدودهٔ عناوین مجرمانه، اصل تمایز در حمایت از اشخاص حقیقی و حقوقی که در اسناد بین‌المللی همچون کنوانسیون جرائم سایبر، پروتکل الحاقی به کنوانسیون جرائم سایبر به‌عنوان تدابیری که باید در سطح ملی اتخاذ شوند. تمرکز این پژوهش بر تحلیل نظام جرم‌انگاری در فضای سایبر در دو نظام کیفری ایران و آلمان از منظر اصول بین‌المللی جرم‌انگاری بوده است. با واکاوی و بررسی میزان تأثیرپذیری دو نظام کیفری ایران و آلمان از اصول بین‌المللی جرم‌انگاری در فضای سایبر و مقایسهٔ این دو نظام کیفری با یکدیگر می‌توان بر نتایج ذیل تأکید نمود. با توجه به اینکه فضای سایبر مبتنی بر داده‌های فناورانه است. بنابراین اسناد بین‌المللی استفاده از فناوری‌های نوین حمایتی همچون رمزنگاری داده‌ها، کدهای رفتاری، ابزارهای گزینش محتوا در حمایت از اشخاص و داده‌های شخصی را به‌عنوان یک اولویت در مقابله با جرائم سایبر پیشنهاد نموده و مقرر می‌دارند کارکرد مجازات در فضای سایبر صرفاً می‌بایست حمایت فرعی و جانبی و نه حمایت گسترده و همه‌جانبه از منافع، ارزش‌ها را شامل شود.

قانون‌گذار آلمان مطابق اسناد بین‌المللی به‌منظور ایجاد تعامل میان ضمانت‌اجراهای کیفری و حمایتی در فضای سایبر با اتخاذ سیاست‌های حمایتی صنعت را به نوآوری به‌ویژه به ایجاد محصولات امنیتی جدید، کدهای رفتاری و ابزارهای گزینش محتوا که می‌تواند مکملی برای حمایت کیفری به شمار آیند ترغیب می‌نمایند و در جرم‌انگاری نیز مطابق کنوانسیون جرائم سایبر و پروتکل الحاقی تقدم را به ضمانت‌اجراهای غیرکیفری معطوف داشته است. به‌ویژه هنگامی‌که روابط طرفین به‌وسیلهٔ یک قرارداد تنظیم می‌شود و مقررات جزایی فقط در جرائم خطرناکی که مقررات اداری یا مدنی توان مقابله با آن را ندارند، اعمال می‌نماید. لیکن قانون‌گذار ایران به‌رغم توصیهٔ اسناد بین‌المللی تمایل کمتری به استفاده از روش‌های حمایتی ازجمله ایجاد محصولات امنیتی و ابزارهای گزینش محتوا نشان داده است و بدون توجه به‌پیش شرط‌های جرم‌انگاری که شامل اصل صدمه و سرزنش است، تمرکز بر جرم‌انگاری رفتارهایی را نموده است که فاقد مبانی روشن و توجیهات کارشناسی است و این رویکرد با اصل مداخلهٔ حداقلی دولت‌ها در فضای سایبر که مورد تأکید اسناد بین‌المللی ازجمله کنوانسیون جرائم سایبر می‌باشد در تعارض است.

بر مبنای اصل تمایز در تعیین قلمرو و محدودهٔ عناوین مجرمانه، موارد مختلف نقض حریم خصوصی کاربران رایانه در فضای سایبر مطابق کنوانسیون جرائم سایبر، نباید در یک مادهٔ کلی جرم‌انگاری شود و می‌بایست معیارهای مادی و روانی مختلف که باعث تغییر در اوصاف جرائم

می‌شوند و جرائم مهم از غیرمهم، جرائم عمدی از جرائم مبتنی بر تقصیر تفکیک شوند و در میزان مجازات آن‌ها نیز تفاوت ایجاد گردد. بر این مبنا قانون‌گذار آلمان مطابق کنوانسیون جرائم سایبر تلاش نموده ضمن تفکیک عناصر قانونی، مادی و معنوی هر جرم به‌طور واضح و شفاف، بدون هرگونه ابهام و کلی‌گویی؛ محدوده و قلمرو عناوین مجرمانه را مشخص نماید و متناسب با اعمال ارتکابی اقدام به جرم‌انگاری و تعیین مجازات نماید تا مصادیق جرم‌انگاری شده با توجه به اسناد بین‌المللی در حد امکان قابلیت پیش‌بینی مناسب نوع رفتاری که منجر به محکومیت کیفری می‌شود را فراهم آورد. لیکن قانون‌گذار ایران به‌رغم الگوبرداری از اسناد بین‌المللی دقت لازمه را در تفکیک قلمرو عناوین مجرمانه اعمال ننموده است و این عدم تمایز در تعیین قلمرو جرائم ارتکابی و عدم تناسب مجازات تعیین‌شده موجب شده تا مجرمان به دلیل منافع بیشتر و مجازات کمتر به ارتکاب جرائم سنتی در فضای سایبر متمایل شوند.

اصل شناسایی مسئولیت کیفری اشخاص حقوقی بر مبنای کنوانسیون جرائم سایبر درصدد مسئول شناختن اشخاص حقوقی و مسئول دانستن شرکت‌ها، انجمن‌ها و دیگر اشخاص حقوقی به خاطر ارتکاب اعمال مجرمانه اشخاص حقیقی است که در مقام مدیریت شخص حقوقی هستند و در جهت منافع آن مرتکب جرم می‌شوند. مطابق این رویکرد قانون‌گذار ایران مسئولیت کیفری برای اشخاص حقوقی را به‌شرط اینکه به نام و در راستای منافع آن، ارتکاب یابد، مورد شناسایی قرار داده است و این رویکرد مطابق نظریهٔ نمایندگی بنا نهاده شده است. لیکن نظام قانون‌گذاری آلمان به دلیل صنعتی بودن کشور آلمان و لزوم حمایت کیفری متناسب با ماهیت فضای مجازی و ایجاد شفافیت در تعیین مصادیق مسئولیت و به‌منظور ایجاد انگیزه برای سرمایه‌گذاری و مبادلهٔ مطمئن داده‌ها و فناوری‌های بین‌المللی، مسئولیت کیفری را به شخص حقوقی تحمیل نمی‌کند بلکه به شخص نمایندگان و مدیران شرکت گسترش می‌دهد و کارکنان را به‌ویژه در چهارچوب مفهوم رژیم قانونی کیفر می‌دهد و به‌منظور قاعده‌مند نمودن رفتار شرکت‌ها از راهکارهای جبران حقوق اداری و مدنی و جزای نقدی بهره می‌گیرد. با توجه به مصادیق پیش‌گفته به نظر می‌رسد بهره‌برداری از تجربهٔ نظام کیفری آلمان به دلیل جامعیت و سابقهٔ طولانی این نظام کیفری در تدوین مقررات کیفری حاکم بر فضای سایبر در مقایسه با نظام کیفری ایران در حوزه‌های اصل تعامل میان ضمانت‌اجراهای کیفری و حمایتی، اصل تفکیک عناوین مجرمانه، اصل شناسایی مسئولیت کیفری اشخاص حقیقی و حقوقی به دلیل داشتن ظرفیت‌هایی همچون تقویت نظام حاکم بر پیشگیری از وقوع جرم، شفافیت در تعیین قلمرو و محدوده عناوین مجرمانه، تناسب مجازات‌های تعیین‌شده و پیشبرد اهداف جامعهٔ مدنی، ازجمله پیشگیری از وقوع جرم و توسعهٔ عدالت قضایی، قابلیت بهره‌برداری و انتقال به حقوق

کیفری ایران را دارد. با عنایت به‌مراتب فوق و داده‌های تحقیق پیشنهادهای زیر به‌منظور تدوین سیاست‌های قانون‌گذاری ارائه می‌شود:

۱. اتخاذ سیاست‌های حمایتی به‌منظور ایجاد محصولات امنیتی جدید، رمزنگاری داده‌ها، کدهای رفتاری، ابزارهای گزینش محتوا و پالایه استفاده از پروکسی به‌عنوان یک اولویت در مقابله باجرائم سایبر به‌منظور کاهش هزینه‌های دستگاه قضایی و پیشگیری از وقوع جرم.

۲. پیش‌بینی و اعمال ضمانت‌اجراهای غیرکیفری (اداری و مدنی) به‌خصوص در مواردی که قراردادهای میان موضوع داده و سازمان‌های دخیل در پردازش داده رهگشا است و مقررات اداری و مدنی امکان مقابله با این جرائم را فراهم می‌نمایند.

۳. کاهش پرونده‌های ورودی به‌نظام قضایی، با تمسک به راهکارهایی چون جرم‌زدایی.

## منابع

### فارسی


- الهی منش، محمدرضا و ابوالفضل سدره‌نشین (۱۳۹۵)، **محشای قانون جرائم رایانه‌ای**، تهران: انتشارات مجد.
- پیکا، ژرژ و علی حسین نجفی ابرندآبادی (۱۳۹۳)، **جرم‌شناسی**، تهران: نشر میزان.
- رضوی، محمد (۱۳۸۶)، «جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آن‌ها»، **دانش انتظامی**، شماره ۳۲.
- خدابخشی، عبدالله (۱۳۸۷)، «نقش قواعد مدنی در شناسایی مسئولیت کیفری شخص حقوقی»، **پژوهشگاه فرهنگ و اندیشه اسلامی**، شماره ۵.
- شمس ناتری، محمدابراهیم، سید وحید ابوالمعالی الحسینی و زهرا سادات علیزاده طباطبایی (۱۳۹۰)، «ویژگی‌های جرم‌انگاری در پرتو اسناد و موازین حقوق بشر»، **فصلنامه راهبرد**، شماره ۵۸.
- شریفی، محسن (۱۳۹۶)، «مسؤولیت کیفری اشخاص حقوقی در نظام کیفری ایران و فرانسه»، **فصلنامه دیدگاه‌های حقوق قضایی**، شماره ۷۵.
- عبدالفتاح، عزت و اسماعیل رحیمی نژاد (۱۳۸۱)، «جرم چیست و معیارهای جرم‌انگاری کدام است؟»، **مجله حقوقی دادگستری**، شماره ۴۱.
- کوشا، جعفر (۱۳۸۰)، «کارکردهای حقوق جزا»، **مجله الهیات و حقوق‌دانشگاه رضوی (آموزه‌های حقوقی)**، شماره ۲.
- فرجیها، محمد و علی علمداری (۱۳۹۶)، «مطالعه تطبیقی مبانی جرم‌انگاری جرائم سایبر در نظام کیفری ایران و آلمان»، **پژوهش‌های حقوق تطبیقی**، دوره ۲۱، شماره ۴.
- فرح‌بخش، مجتبی و نصیب الله فتازاده (۱۳۹۵)، «مطالعه تطبیقی مسؤولیت کیفری شخص حقوقی در کشورهای آمریکا و آلمان»، **مدیریت آموزش دادگستری استان تهران**، شماره ۱۶.
- نوبهار، رحیم (۱۳۹۰)، **اهداف مجازات در جرائم جنسی: چشم‌اندازی اسلامی**، قم: نشر پژوهشکده علوم و فرهنگ اسلامی.


### غیرفارسی


- **Bundesdatenschutzgesetz**. (1990), BGBl.I.S.2954, as amended by the law of 14 September, 1994, available at:
  < http:// www. iuscomp.org/gla/statutes/BDSG.html >. 2013/08/16.
- Belghoul, Fabrice. (2004). **L'extension de la Responsabilité Pénale des Personnes Moral**. Mémoire du Dea de Droit Economique et des Affaires d'orléams.
- Clarkson, Christopher M. V. (1995). **Understanding criminal law** (2nd ed). London: Fontana Press of Harper-Collins.
- Convention on Cybercrime, Budapest. (2001). available at:
  <html://www.covention.coe.int/ Treaty/en/Treaties/Html/185. html>. 2006/06/19.

- Concil of Europe, (2001), **Explanatory report to the Convention on Cybercrime**.
- Duff, Antony; & Garland, David (eds). (1994). **A reader on punishment**. Oxford; New York: Oxford University Press.
- European Committee on Crime Problems; & Council of Europe (eds). (1990). Computer-related crime: recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg: Croton, N.Y: Council of Europe, Pub. and Documentation Service; Manhattan Pub. Co.
- European Committee on Crime Problems. Strasbourg (2001). Croton, N.Y: Council of Europe, Pub. and Documentation Service; Manhattan Pub. Co.
- Faure, Michael; & Visser, Marjolein. (1995). **How to Punish Environmental Pollution-Some Reflections on Various Models of Criminalization of Environmental Harm**. Eur. J. Crime Crim. L. & Crim. Just, 3, 316.
- Jescheck, Hans-Heinrich. (1996). **Lehrbuch des Strafrechts Allgemeiner Teil**. Berlin: Duncker & Humblot.
- Jareborg, Nils. (1995). "What Kind of Criminal Law Do We Want? On Defensive and Offensive Criminal Law Policy". **Scandinavian Studies in Law**. In: Beware of Punishment: On the Utility and Futility of Criminal Law, 14, 19.
- Hetzer, Wolfgang. (2007). "Corruption as Business Practice? Corporate Criminal Liability in the European Union. European Journal of Crime", **Criminal Law and Criminal Justice**, 15.
- Personal Data protection Code, (2003), sction 4, (1) (b), 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.
- Sun Beale, Sara; & Safwat, adam. (2005). What Developments in Western Europe Tell Us About American Critiques of Corporate Criminal Liability. **Buffalo Criminal Law Review**.
- Sieber, Ulrich (ed). (1994). Information technology crime: national legislations and international initiatives. Köln.
- Sieber.Ulrich, (2000), **Information Technology Crime**, vo l.
- Sieber.Ulrich, (2001), Responsibility of Internet-providers, In Law, Information and Information Technologhy, E. Lederman, R. shapira (eds.) The Hague, Kluwer International.
- Tarelli, Elis. (2004). "A Brief Introduction to the Principles and Rules for Determining Corporate Criminal Liability". **SSRN Electronic Journal**.
- Nations, United. (1994). **United Nations Manual on the Prevention and Control of Computer Related Crime**. UN,14.