

Executive Guarantees for Compliance with International and National Regulations in Virtual Platforms Regarding the Commission of Crimes and the Dissemination of Criminal Content

1. Samira Asadi*: MA, Department of Criminal Law and Criminology, South Tehran Branch, Islamic Azad University, Tehran, Iran. Email: Adrin.sys@gmail.com (Corresponding Author)

ABSTRACT

Military crimes against national security in the laws of Iran and Iraq have various legal, material, and moral elements. The criminalization of such crimes in Iranian law is stipulated in the Islamic Penal Code and the Law on the Crimes of the Armed Forces, while in Iraqi law it is codified in the Iraqi Penal Code enacted in 1969. Accordingly, military crimes against national security constitute one of the highly significant subjects that can be examined in various instances. Regarding the foundations of criminalization of military crimes in Iranian and Iraqi law, various jurisprudential, legal, and criminological bases have been adopted, which reveal both commonalities and differences. Therefore, the present study aims to conduct a comparative analysis of military crimes against national security in the laws of Iran and Iraq, using an analytical–descriptive and comparative method. The findings indicate that, despite certain similarities, military crimes against national security in Iran and Iraq differ in some conditions, elements, foundations, consequences, scope of criminalization, and instances.

Keywords: *cyberspace, virtual platforms, commission of crimes, dissemination of criminal content*

How to cite: Asadi, S. (2025). Executive Guarantees for Compliance with International and National Regulations in Virtual Platforms Regarding the Commission of Crimes and the Dissemination of Criminal Content. *Comparative Studies in Jurisprudence, Law, and Politics*, 7(4), 1-20.

© 2025 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 03 December 2024

Revise Date: 21 January 2025

Accept Date: 30 January 2025

Publish Date: 11 August 2025



ضمانت اجرایی برای رعایت ضوابط جهانی و ملی در پلتفرم‌های مجازی در قبال ارتکاب جرم و انتشار محتوای مجرمانه

۱. سمیرا اسدی*: کارشناس ارشد، گروه حقوق جزا و جرم‌شناسی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران. پست الکترونیک: Adrin.sys@gmail.com (نویسنده مسئول)

چکیده

با گسترش اینترنت و شبکه‌های اجتماعی، این بسترها به محیطی برای تبادل آزاد اطلاعات تبدیل شده‌اند، اما به مرور زمان به دلیل بروز چالش‌های امنیتی، حقوقی و اجتماعی، دولت‌ها و شرکت‌های ارائه‌دهنده این پلتفرم‌ها مقرراتی را برای کنترل محتوا و حفاظت از حقوق کاربران وضع کردند. هدف اصلی این مقررات، جلوگیری از انتشار محتوای مضر و مجرمانه، شامل تروریسم، نقض کپی‌رایت، ترویج خشونت، نژادپرستی، نفرت‌پراکنی و سوءاستفاده از کودکان است. یکی از چالش‌های اصلی، نحوه نظارت بر محتوای تولیدی کاربران است. اگرچه این نظارت ابزاری برای حفظ امنیت عمومی محسوب می‌شود، اما می‌تواند با آزادی بیان و حریم خصوصی در تعارض باشد. تفاوت‌های فرهنگی و قانونی بین کشورها نیز بر این موضوع اثرگذار است؛ برخی کشورها آزادی بیان را اولویت می‌دانند، در حالی که برخی دیگر کنترل محتوای مجرمانه را سخت‌گیرانه‌تر دنبال می‌کنند. ویژگی ناشناس‌ماندن در فضای مجازی امکان سوءاستفاده مجرمان را افزایش داده و شناسایی هویت واقعی آن‌ها را دشوار کرده است. این موضوع چالش‌هایی برای شفافیت و پاسخگویی ایجاد می‌کند و بسیاری از سیستم‌های نظارتی قادر به واکنش سریع و مؤثر نیستند. در ایران، نبود چارچوب قانونی جامع و نارسایی در قوانین کیفری موجب شده مجازات انتشار محتوای ممنوعه در پلتفرم‌های مجازی به‌طور کامل و مؤثر اجرا نشود. بنابراین، با وجود تلاش‌ها برای تنظیم مقررات و کنترل محتوا، اجرای موفق آن‌ها همچنان با موانع حقوقی، فرهنگی و سیاسی مواجه است.

واژگان کلیدی: فضای مجازی، پلتفرم‌های مجازی، ارتکاب جرم، انتشار محتوای مجرمانه

نحوه استناددهی: اسدی، سمیرا. (۱۴۰۴). ضمانت اجرایی برای رعایت ضوابط جهانی و ملی در پلتفرم‌های مجازی در قبال ارتکاب جرم و انتشار محتوای مجرمانه. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۷(۴)، ۲۰-۱.

© ۱۴۰۴ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۱۳ آذر ۱۴۰۳

تاریخ بازنگری: ۲ بهمن ۱۴۰۳

تاریخ پذیرش: ۱۱ بهمن ۱۴۰۳

تاریخ چاپ: ۲۰ مرداد ۱۴۰۴

رسانه‌های الکترونیکی آزادی بیشتری برای ابراز عقیده فراهم می‌کنند، اما متوجه می‌شویم که برخی از افراد از این آزادی‌ها و حقوق سوءاستفاده کرده‌اند و از مرز بین آزادی عقیده و توهین به خود و ناموس انسان یا حرمت نهادهای دولتی و نهادهای آن‌ها یا به خطر انداختن آن عبور کرده‌اند. اعتقادات مذهبی و تشریفات مذهبی افراد این امر منجر به ظهور انواع جدیدی از جرایم مجازی شده و به تسریع گسترش آن‌ها کمک کرده است، زیرا مکانی مناسب برای گسترش جرایم به ویژه در کشورهایی است که در آن‌ها وجود دارد. وجود این جرایم مستلزم ایجاد چارچوب قانونی مبتنی بر طبقه‌بندی و کنترل و ایجاد مجازات‌های بازدارنده لازم برای محافظت از انسان در برابر نفوذ آن و حفاظت از انواع فعالیت‌ها است. با توجه به توسعه شگرفی که از طریق وسایل ارتباطی و فناوری مدرن به ویژه اینترنت رخ داده است که امروزه بزرگترین، مهم‌ترین و سریع‌ترین وسیله کسب اطلاعات، نمایش و تبادل نظر و بیان آزادانه آن‌ها در این فضای وسیع الکترونیکی به شمار می‌رود. به نام اینترنت و عرفاً دنیای مجازی نامیده می‌شود و به ستون فقرات انقلاب اطلاعاتی تبدیل شده است که امروزه شاهد آن هستیم و برجسته‌ترین وسیله تبلیغاتی و مهم‌ترین وسیله ارتباطی است (Rahmanpour, 2013).

امروزه با توسعه و گسترش روزافزون اینترنت، شبکه‌های اجتماعی در حال تبدیل شدن به بستر اصلی ارتباطات و تبادل اطلاعات هستند. اگرچه در ابتدای ظهور این شبکه‌ها، آن‌ها برخلاف رسانه‌های سنتی بستری کاملاً آزاد تصور می‌شدند، اما به مرور مقررات تعیین شده توسط دولت‌ها و شرکت‌ها محدودیت‌هایی برای انتشار محتوا در این شبکه‌ها ایجاد کرده است. چنین محدودیت‌هایی در عرصه جهانی بیشتر با هدف مبارزه با جرایم تروریستی، نقض کپی رایت، ترویج نژادپرستی، نفرت پراکنی، ترویج خشونت و نقض حقوق کودکان وضع شده اند. این موارد که عموماً برگرفته از فهرست جرایم هر کشور است، چارچوب کلی محتوای قابل انتشار را در این شبکه‌ها تعیین می‌کند (Resende, 2020). به طور کلی، علی‌رغم اینکه آزادی به عنوان یک ارزش جهان شمول درباره اینترنت و شبکه‌های اجتماعی نیز مورد تأکید است، اما تقریباً همه کشورهای دنیا و مطلقاً همه شبکه‌های اجتماعی برجسته، دارای سازوکارهای نظارتی برای انتشار محتوا هستند؛ هرچند میزان و گستره‌ی این نظارت‌ها در کشورهای مختلف بسته به وضعیت فرهنگی، موازین قانونی و ارزش‌های هر کشور متفاوت است (Habibzadeh & Fakhr Bonab, 2005). با این حال ذات اینترنت که دربرگیرنده دو خصیصه آزادی عمل کاربران و پنهان ماندن هویت آن‌ها است، در عمل چالش‌هایی را برای سزادهی جرایم ارتكابی و حاکمیت قانون در شبکه‌های اجتماعی به همراه داشته است. به علاوه در مسئولیت کیفری ناشی از انتشار محتوای ممنوعه نیز ابهامات و نارسایی‌های قانونی (به ویژه در ایران) وجود دارد. در واقع می‌توان گفت که مجموعه این شرایط نشان می‌دهد راه حل‌های سنتی نظام‌های کیفری پاسخگوی مسائل جدید فضای مجازی و شبکه‌های اجتماعی نیست. از سوی دیگر برخی مقررات گذاری‌های منجر به ایجاد سانسور، چالش‌هایی جهانی برای آزادی بیان در این شبکه‌ها رقم زده است. البته از آنجا که این شبکه‌ها غالباً خصوصی هستند، اختلاف نظر جدی وجود دارد که آیا ضمانت‌هایی همچون متمم اول قانون اساسی آمریکا برای محتوای منتشر شده در شبکه‌های اجتماعی نیز وجود دارد یا خیر. در کل، این ابهامات و نارسایی‌ها تا حدی است که گاهی به واقع می‌توان گفت ما در این عرصه وارد یک طیف خاکستری جدیدی شده ایم که هنوز قوانینی برای آن نوشته نشده است. مشخصاً آنچه امروز کشور ما در این عرصه با آن مواجه است، مجموعه‌ای از چالش‌ها و سوالات بی پاسخ است که به دلیل فقدان پیش بینی‌های لازم روز به روز شرایط پراشوب تری را رقم می‌زند. از یک طرف در این شبکه‌ها به سادگی قوانین و حاکمیت ملی ایران نقض می‌شود و از طرف دیگر آزادی دسترسی کاربران به شبکه‌های اجتماعی در معرض تهدید است (Shambayati, 2009).

به علاوه، برخلاف دیگر کشورها، هیچ گونه ارتباط موثری بین حاکمیت ملی ما و پلتفرم‌های خارجی وجود ندارد که ضمانت اجرایی برای رعایت ضوابط جهانی و ملی در این پلتفرم‌ها در قبال ارتکاب جرم و انتشار محتوای مجرمانه ایجاد شود. اساساً از منظر تاریخی اینترنت در دهه ۱۹۶۰ میلادی توسط آژانس پروژه‌های تحقیقاتی پیشرفته در وزارت دفاع ایالات متحده‌ی آمریکا ابداع شد. اگرچه اینترنت امروزه دیگر یک بستر فراملی و جهانی تلقی می‌شود، اما کشورهای غربی و به‌ویژه آمریکا با حفظ نفوذ و سلطه‌ی خود نسبت به این بستر، بیش از سایر کشورها توانایی نظارت و اعمال حاکمیت بر اینترنت را دارند؛ مثلاً از طریق حفظ کنترل وزارت بازرگانی آمریکا بر شرکت آیکان که وظیفه‌ی مدیریت پروتکل اینترنت جهانی را دارد؛ یا از طریق رصد پهنای باند جهانی توسط آژانس امنیت ملی آمریکا یا همین‌طور از طریق شرکت‌های اصلی حوزه‌ی فناوری مانند گوگل، اپل و مایکروسافت که همگی آمریکایی بوده و در این کشور مستقرند. همین‌طور شبکه‌های اجتماعی اصلی مانند فیسبوک، اینستاگرام، توییتر و یوتیوب نیز همگی آمریکایی بوده و تحت قوانین آمریکا و در راستای سیاست‌های آن فعالیت می‌کنند. عملکرد این شبکه‌ها، حاکی از غلبه حاکمیت ملی ایالات متحده و ارزش‌هایش بر سایر حاکمیت‌های ملی و ارزش‌های جهانی است. امری که برای کشوری مانند ایران که تحت تحریم و سیاست‌های خصمانه آمریکاست باعث شده حتی از فرصت و شرایط عمومی همکاری‌های مشابهی که این شبکه‌ها با سایر کشورهای جهان دارند، محروم شود (Ardito, 2013). در نتیجه، برخلاف دیگر کشورها، مانند کشورهای اتحادیه اروپا یا هند و ترکیه، هیچ گونه امکانی برای احترام به حاکمیت ملی و قوانین ایران در این شبکه‌ها وجود نداشته و عملاً هیچ جرم و محتوای مجرمانه‌ای در این شبکه‌ها قابلیت حذف یا پیگرد را نیافته‌اند. در نتیجه این شبکه‌های اجتماعی عملاً به یک بستر آناشستی مطلقاً آزاد در ایران تبدیل شده‌اند. حال آنکه در خود آمریکا شبکه‌های اجتماعی نه فقط در قبال جرایم بلکه حتی با ساده‌ترین مصادیق انتشار اخبار کذب یا محتوای مخل آرامش و امنیت عمومی برخورد می‌کنند. به شکل مشابهی پلتفرم‌های غیرآمریکایی مانند تلگرام نیز از همکاری با ایران خودداری می‌کنند. در نتیجه همین شرایط تلگرام در ایران فیلتر شد هرچند به دلیل عدم همراهی افکار عمومی و دسترسی گسترده به فیلترشکن‌ها همچنان نزدیک به ۴۰ درصد کاربران از آن استفاده می‌کنند. یک گزارش رسمی حاکی از این است که در ایران ۱۰ تا ۱۲ میلیون نفر با استفاده از وی‌پی‌ان‌ز فیلترینگ عبور می‌کنند (Hintz, 2015). مجموعه این مسائل، به اندازه کافی ضرورت انجام پژوهشی کامل از وضعیت کلی انتشار جرم در شبکه‌های اجتماعی را جهت شناسایی دقیق نواقص و ارائه راهکارهای عملی برای برون رفت از تنگنای کنونی روشن می‌سازد (Jafari Langeroudi, 2007). پلتفرم‌های مجازی معمولاً دارای سیاست‌ها و ضوابطی برای مدیریت محتوا هستند، که شامل رعایت قوانین محلی و جلوگیری از انتشار محتوای مجرمانه است. این پلتفرم‌ها معمولاً از الگوریتم‌ها و تیم‌های انسانی برای مانیتورینگ و حذف محتوای ناقض استفاده می‌کنند. همچنین، آن‌ها ممکن است همکاری با مقامات قضایی محلی برای شناسایی و پیگیری فعالیت‌های مجرمانه داشته باشند.

۱. مفهوم فضای مجازی

یکی از حقوق اساسی اشخاص حق بر داشتن اطلاعات خصوصی و مراوده این قبیل اطلاعات با دیگران است، افراد در زندگی خود ناگزیر از داشتن یک سلسله روابط خصوصی، عمومی شغلی و خانوادگی می‌باشند، طبیعت این روابط نوعاً به گونه‌ای است که از کسی پوشیده نمی‌ماند و دانستن آن اصولاً بلااشکال است، اما هر کس برای خود مسائل صد در صد خصوصی دارد که شرط لازم، سری بودن و عدم افشای آن است، عدم افشای مسائل خصوصی و اطلاعات شخصی در اجتماعی به صورت حق متجلی شده است و افراد مکلف به رعایت آن می‌باشند، ورود به زندگی خصوصی افراد به هر شکل از نظر اخلاقی مذموم و از نظر قانون موجب مسئولیت است (هاشمی، ۱۳۸۴: ۲۸۶)، امروزه پیشرفت

فن‌آوری اطلاعات وضعیتی را به وجود آورده که بحث امنیت شخصی و اطلاعاتی افراد را بیش از هر زمان دیگری مورد تهدید قرار داده است، دانش کامپیوتر و فن‌آوری اطلاعات تنها اطلاعات یا تصاویر خانوادگی اشخاص را مورد تهدید قرار نداده، بلکه از این دانش ممکن است برای نقض سایر موضوعات مورد حمایت قانون‌گذار نیز استفاده شود، به‌طور مثال دشنام و فحاشی از جریان‌های همیشگی جوامع است و انگیزه ارتکاب آن از سوی اشخاص تحقیر دیگران از طریق خرد کردن ارزش فرهنگی آن‌ها محسوب می‌شود (Jafari Langeroudi, 2007)، به موجب ماده ۳۱ قانون مطبوعات فحاشی نه تنها در روابط فردی شایسته نیست، بلکه از طریق مطبوعات و رسانه‌های گروهی نیز بیانگر یک فرهنگ منحط است، به همین ترتیب افشاگری و برملا کردن نقاط ضعف دیگران از موارد دیگری است که در هتک حیثیت افراد بکار گرفته می‌شود و می‌توان آن را از طریق رایانه و سیستم‌های شبکه اینترنت مرتکب شد، در تمام این موارد استفاده از دانش فن‌آوری اطلاعات و اینترنت منجر به آن خواهد شد که ارزش‌های مورد حمایت قانون‌گذار نقض شود، اما فضای مجازی یا مجازی چیست و چگونه ارتکاب این قبیل جرایم را تسهیل می‌نماید؟ تاکنون تعاریف متعددی از فضای مجازی ارائه و ابراز شده است. برخی از این تعاریف مفهوم فضای مجازی را محدود کرده و برخی دیگر آن را توسعه بخشیده‌اند، به‌موجب یکی از این تعاریف فضا سایر به اطلاعات الکترونیکی اطلاق می‌شود که از طریق اینترنت جابجا می‌شوند، البته تعاریف دیگر سعی نموده‌اند تا به بیان موارد افتراق فضای مجازی (Madhava Soma & Sundaram, 2011) از موضوعات مجازی و شبکه پردازند و از دیدگاه آن‌ها فضای مجازی مجموعه اطلاعاتی است که در رایانه ذخیره‌سازی شده و از طریق اینترنت به یکدیگر متصل هستند (Ploug, 2009)، این در حالی است که شبکه یا نت دارای تعریف مخصوص به خود است، اینترنت مجموعه‌ای بسیار گسترده از رایانه‌های موجود در شبکه‌های رایانه‌ای سراسر جهان است که از طریق خطوط ارتباطی به یکدیگر متصل شده و با استفاده از پروتکل‌های معینی به تبادل اطلاعات می‌پردازند. بسیاری از رایانه‌های موجود در عرصه اینترنت اطلاعات زیادی در خود ذخیره کرده و در مجموع حجم عظیمی از اطلاعات در اینترنت انباشته شده است. اطلاعات موجود در اینترنت به روش‌های مختلفی ذخیره شده و در نتیجه با روش‌های گوناگونی قابل ارائه و انتقال هستند، «صفحات وب» یکی از روش‌های خاص ذخیره و ارائه اطلاعات در بین روش‌های متعدد ذخیره و ارائه اطلاعات در اینترنت هستند (Holmes, 1998).

برخلاف روش‌های قدیمی ذخیره و ارائه اطلاعات که معمولاً اطلاعات را در قالب متن ذخیره و منتقل می‌کنند، صفحه وب یک صفحه گرافیکی ذخیره اطلاعات است که بر اساس نظام «فرارسانه‌ای» کار می‌کند. فرارسانه ترکیبی از «فرامتن» و «چند رسانه‌ای» است، اکنون اگر می‌گوییم جرایم مجازی واقع می‌شوند منظور این است که بزهکار با استفاده از رایانه یا هر ابزار دیگری که دسترسی به شبکه اینترنت را برای ایشان فراهم می‌سازد اقدام به ایجاد اختلال در اطلاعات موجود در فضای مجازی نموده تا منافی برای خود کسب نماید، اکنون مصداق این جرم می‌تواند از جرایم مختلف باشد، می‌تواند دسترسی غیرمجاز باشد، چنانچه ماده یک قانون جرایم رایانه‌ای مقرر داشته: «هرکس به‌طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد»؛ می‌تواند جعل باشد، چنانچه ماده ۶ قانون فوق‌الذکر مقرر داشته: «هرکس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر داده‌ای قابل استناد یا ایجاد یا وارد کردن متقلبانه داده‌ها،

ب) تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل‌پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علایم به آن‌ها؛ یا می‌تواند جرم خلاف عفت عمومی باشد، چنانچه ماده ۱۴ قانون جرایم رایانه‌ای مقرر می‌دارد: «هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را تولید، ارسال، منتشر، توزیع یا معامله کند یا به‌قصد ارسال یا انتشار یا تجارت تولید یا ذخیره یا نگهداری کند، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد»؛ بنابراین باید اذعان داشت اکثر جرایم می‌توانند در فضای مجازی به وقوع بپیوندند و نوع جرم در تعریف فضا سایبر یا جرایم مجازی تأثیری ندارد.

۲. تعریف و تاریخچه جرایم رایانه‌ای

۱-۲. تاریخچه شکل‌گیری جرایم رایانه‌ای

نخستین کامپیوتر در سال ۱۹۳۷ در آمریکا اختراع شد. با پیشرفت فن‌آوری به‌تدریج در ساخت رایانه تغییراتی به وجود آمد، به‌اندازه‌ای که اصطلاح نسل‌های مختلف رایانه برای نامیدن این تغییرات مورداستفاده قرار گرفت، امروزه ارتباط با کامپیوتر از طریق صوت و تصویر نیز امکان‌پذیر خواهد بود. اطلاعات از همان زمان پیدایش به‌صورت مناسب برای کامپیوتر ذخیره‌شده و در هنگام لزوم، از طریق سیستم‌های کامپیوتری مورداستفاده قرار خواهد گرفت. استفاده از حافظه‌های نوری حافظه‌هایی با حجم کم و گنجایش غیرقابل‌تصور ویژگی مهم این نسل است. استفاده از هوش مصنوعی و قدرت تفکر و استنتاج کامپیوتری، از دیگر ویژگی‌های کامپیوترهای این نسل است، تغییرات گسترده در ساخت رایانه‌های مطمئناً به تغییرات تکنولوژیکی ختم نخواهد شد و تغییرات فرهنگی را نیز به دنبال خواهد داشت، اما تغییرات فرهنگی چیست و چه تأثیری بر زندگی اجتماعی انسان خواهد گذاشت و درنهایت تأثیر آن بر حقوق کیفری جامعه چه خواهد بود؟

در یک اظهارنظر کلی می‌توان گفت که جرایم رایانه هم‌زاد خود رایانه تلقی می‌شوند و با شروع استفاده از رایانه‌این جرایم نیز پا به عرصه وجود گذاشتند، این تعریف با تعاریفی که طرفداران مکتب عدالت مطلق و تعریف جامعه‌شناختی (جرم هر عملی است که نظم جامعه را مختل نماید) جرایم رایانه‌ای همخوانی دارد، اما از دیدگاه حقوق جزاء جرم عملی است که قانون‌گذار آن را جرم شناخته باشد، به‌عنوان مثال پس از مظنون شدن پلیس انگلستان به یک جوان ۲۳ ساله که با تماس با یک شرکت بزرگ‌رایانه‌ای پیشنهاد کرده بود که در عوض گرفتن وجوهی، طریقه گرفتن اطلاعات سری از رایانه‌های سایر مراکز را به آن‌ها آموزش دهد و دستگیری وی به‌عنوان باج‌خواهی یک باند سرقت بین‌المللی کشف شد، پس از تحقیقات به‌عمل‌آمده معلوم شد که این جوان با سیستمی آشناست که می‌تواند از رایانه‌های حساس نظامی و تجاری کشور اطلاعات کسب کند، بعلاوه این جوان با چند باشگاه اطلاعاتی در آلمان و آمریکا سروکار داشته و ظرف چند سال اطلاعات را به‌صورت رمز با آن‌ها مبادله می‌کرده است، این جوان با استفاده از سیستم عقل رایانه‌ای کیلفورد توانسته است از سیستم‌های اطلاعاتی موجود در وزارت دفاع انگلستان و نیز ناسا اطلاعات زیادی کسب نماید، مسئله اساسی در رابطه با او این بود که عمل او علیرغم تأثیر قابل‌ملاحظه‌ای که بر بحث امنیت ملی انگلستان داشته است در آن زمان جرم به‌حساب نمی‌آمد (Taheri Jabali, 1993) و جوان مورد ذکر به‌راحتی از اعمال مجازات گریخت، بر این اساس بدون توجه به تعریف جامعه‌شناختی جرم در مبحث قصد داریم ببینیم پیشینه شناخت جرم رایانه‌ای به کجا بازمی‌گردد.

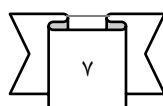
از دیدگاه بین‌المللی امضای کنوانسیون جرایم رایانه‌ای که به‌وسیله شورای اروپا در ۸ نوامبر ۲۰۰۱ صورت گرفت نخستین قدم در راه مبارزه بین‌المللی قانونی با پدیده جرایم رایانه‌ای بود (Ardito, 2013)، البته سابق قانون‌گذاری در عرصه داخلی در خصوص جرایم رایانه‌ای به

مدت زمانی قبل‌تر از سال ۲۰۰۱ بازمی‌گردد در آمریکا که یکی از پیشگامان در این عرصه محسوب می‌شود میان سال‌های ۱۹۷۸ تا ۱۹۸۶ تعداد ۴۵ ایالت از ایالات این کشور قانون جرایم رایانه‌ای را موردپذیرش قرار دادند، متن این قانون با متن پیشنهادی قانون‌گذار فدرال مطابقت داشت (Brenner, 2012). در نهایت در رابطه با سابقه قانون‌گذاری در ایران در رابطه با جرایم رایانه‌ای باید گفت سابقه تدوین قانون در کشورمان در رابطه با جرایم رایانه به سال‌های اخیر یعنی سال ۱۳۸۸ بازمی‌گردد، کلیات لایحه قانون جرایم رایانه‌ای در ۲۷ آبان ۱۳۸۷ با ۱۷۶ رأی موافق، ۳ رأی مخالف و ۲ رأی ممتنع به تصویب رسید. پس از رفع ایراداتی که شورای نگهبان به این قانون وارد کرده بود. در ۷ تیر ۱۳۸۸ قانون جرایم رایانه‌ای به تأیید شورای نگهبان رسید (www.itna.ir). در نهایت مسئله‌ای که در این رابطه می‌تواند موردتوجه قرار بگیرد موضوع تأثیر جرم انگاری جرایم رایانه از پیشرفت علم رایانه در کشورهای مختلف است، همان‌طور که مشاهده شد جرم انگاری جرایم رایانه در ایالات متحده آمریکا که مهد ظهور دانش رایانه است بسیار زودتر از سایر مناطق جهان شروع شده و به تدریج برخی مناطق دیگر دنیا مانند ایران را نیز درنوردیده است.

۲-۲. تعریف جرم رایانه‌ای

در رابطه با تعریف جرایم رایانه‌ای باید گفت در قانون ایران تعریفی کلی از جرم رایانه‌ای ارائه نشده است، قانون‌گذار ایران تنها دامنه مصداقی جرایم رایانه‌ای را مشخص نموده است، این در حالی است که در تعریفی که پلیس فدرال آمریکا از جرایم رایانه‌ای ارائه نموده، جرم رایانه‌ای هر جرمی است که در انجام آن از رایانه کمک گرفته شده باشد (Nami, 2004)، البته باید توجه داشت که تعاریف ارائه شده از جرایم رایانه‌ای با توجه به تعریف مبتنی بر سوءاستفاده از رایانه امروز دگرگون شده و حوزه‌های دیگری را نیز در بر گرفته است، توضیح اینکه در ابتدای پیدایش تعریف جرایم رایانه‌ای برخی این جرایم را نوعی جرم یقه‌سفید تلقی می‌نمودند که تنها به وسیله اشخاصی خاص مرتکب خواهند شد (McEwen, 1989)، در نهایت تعریف مبتنی بر استفاده از رایانه جایگزین تعریف فوق‌الذکر شد و در نهایت امروزه اعتقاد بر این است که هر جرمی که در ارتکاب آن به‌نوعی دانش و فن‌آوری رایانه به‌کار رفته باشد از جرایم رایانه‌ای تلقی می‌شود (McEwen, 1989)، این تعریف دامنه استناد به جرایم رایانه‌ای را گسترش داده است، به‌عنوان مثال در حال حاضر ممکن است شخص در ارتکاب جرم رایانه‌ای مشخصاً از خود رایانه استفاده نکند. مثلاً بدون استفاده از رایانه و با استفاده از امواج الکترومغناطیس به داده‌های رایانه‌ای خسارت وارد سازد یا آن‌ها را پاک نماید بدون آنکه حتی نزدیک به رایانه مورد تخریب شود یا حتی با استفاده از این امواج شماره‌حسابی را تغییر داده و اقدام به کلاهبرداری رایانه‌ای نماید، بدون آنکه در این راه رایانه استفاده نموده باشد. بر این اساس تعریف مبتنی بر استفاده از رایانه نمی‌تواند چندان معتبر باشد، ضمن اینکه در قوانین برخی کشورهای دیگر، تعاریفی از جرایم رایانه‌ای ارائه شده که بنا به مورد بسته به سیاست جنایی قانون‌گذاران آن کشورها در برابر این جرایم دامنه تعریف این جرم را گسترش می‌دهد یا محدود می‌کند. در کد کیفری آلمان بخش ۲۰۲ قانون‌گذار جرایم رایانه‌ای را جرایمی تعریف می‌کند که با اخذ شماره رمز ورود یا تغییر در برنامه و سیستم نرم‌افزاری یک رایانه به وقوع بپیوندد (Section 202c, 1998)، البته در قانون آلمان نیز به‌مانند قانون کشورمان قانون‌گذار جرایم رایانه‌ای را در ارتباط با جرایم مختلف تعریف کرده است. به‌عنوان مثال به‌موجب بخش ۲۶۳ A این قانون کلاهبرداری رایانه‌ای تعریف شده و یا در ماده ۳۰۳ b اخلال در نظم عمومی رایانه‌ای تعریف شده است. در انگلستان نیز ماده ۱ قانون سوءاستفاده از رایانه مصوب ۱۹۹۰ تعریف کامل و تقسیم‌بندی جالبی از جرایم رایانه‌ای ارائه نموده است، به‌موجب بخش یک این قانون، یعنی سه ماده اولیه جرایم رایانه‌ای به سه دسته زیر تقسیم شده‌اند:

الف: دستیابی غیرقانونی به داده‌های رایانه‌ای



ب: دستیابی غیر قانونی به داده‌های رایانه‌ای برای تسهیل سایر جرایم

پ: ایجاد تغییر غیرقانونی در داده‌های رایانه‌ای

بندهای یک و دو ماده یک و شقوق سه‌گانه آن میان جرایم رایانه‌ای دستیابی غیرمجاز به داده‌های رایانه‌ای که نیاز به احراز سوءنیت در بزه‌کار دارند و جرایم رایانه‌ای مطلق تفکیک قائل شده‌اند. درنهایت با توجه به تعاریف فوق‌الذکر می‌توان جرایم رایانه‌ای را جرایمی دانست که با استفاده از دانش یا فن‌آوری رایانه صورت می‌پذیرند. این تعریف دانش محور از جرایم رایانه‌ای محسوب می‌شود ([Madhava Soma](#) & Sundaram, 2011). به عبارت دیگر بر ضرورت استفاده از دانشی خاص در ارتکاب جرایم رایانه‌ای تأکید می‌نماید؛ زیرا همان‌طور که گفتیم این قبیل جرایم می‌توانند بدون استفاده از رایانه واقع شوند.

۳. مسئولیت کیفری در فضای مجازی

۳-۱. مفهوم مسئولیت کیفری

تعاریف بسیار زیادی از آن ارائه داده‌اند. یکی از نویسندگان حقوق جزای کشورمان به‌طور کلی الزام شخص به پاسخگویی در قبال تعرض به دیگران یا نقض حقوقی که تحت عنوان حقوق آزادی‌های غربی و گاهاً تحت عنوان حقوق حمایتی جمعی و به‌منظور دفاع از جامعه ارائه می‌شود را مسئولیت کیفری قلمداد کرده است (Shambayati, 2009). یکی دیگر از نویسندگان با توجه به تعریف لغوی مسئولیت که به معنای موظف بودن به انجام کار معنا شده مسئولیت را نوعی التزام دانسته و معتقد است در قلمرو حقوق کیفری محتوای این التزام تقبل آثار و عواقب افعال مجرمانه است، به عبارت صحیح‌تر تحمل مجازات که در قوانین کیفری سزای افعال سرزنش‌آمیز بر نظام به شمار می‌آید (اردبیلی ۱۳۸۷: ۷۴). البته مسئولیت کیفری را می‌توان از دیدگاه دیگری نیز معنا کرد و آن نه التزام به تقبل آثار و عواقب افعال مجرمانه که استحقاق و سزاواری تحمل این عواقب است (Rahmanpour, 2013). مسئولیت کیفری در فضا سایر نیز به معنای تقبل آثار ناشی از فعل مجرمانه فرد است که در فضا اینترنت به وقوع پیوسته بنابراین مسئولیت در فضا سایر مفهومی جدای از سایر موارد مسئولیت ندارد. در رابطه با مسئولیت کیفری اشخاص حقوقی نظرات مختلفی ارائه شده است، برخی از نویسندگان درصدد نفی آن برآمده‌اند و برخی دیگر با استناد به اینکه اشخاص حقوقی وجود واقعی دارند، بزه ارتكابی در برابر ایشان قابلیت استناد دارد و درنهایت اینکه برخی کیفرها را می‌توان در ارتباط این اشخاص مورد استفاده قرارداد معتقدند که اشخاص حقوقی مسئولیت کیفری دارند (Rahmanpour, 2013). در ایران موارد متعددی می‌توان ذکر نمود که بیانگر تمایل قانون‌گذار ایران در پذیرش مسئولیت کیفری برای اشخاص حقوقی است، شاید بتوان ماده ۲۲۰ قانون تجارت را به‌عنوان نخستین گام از پذیرش مسئولیت برای اشخاص حقوقی نام برد که به‌موجب آن مسئولیت تضامنی برای شرکت‌های ثبت‌نشده و عملی در نظر گرفته شده است، متن ماده واحده مربوط به ضبط اموال متعلق به احزابی که منحل می‌شوند نمونه دیگری از پذیرش مسئولیت کیفری اشخاص حقوقی در نظام حقوقی ایران است و درنهایت می‌توان به قانون جرایم رایانه‌ای استناد نمود که در این قانون مسئولیت کیفری اشخاص حقوقی صراحتاً مورد پذیرش قرار گرفته است، از دیدگاه تطبیقی ماده ۱۰ کنوانسیون پالرمو که در رابطه با جرایم سازمان‌یافته فراملی به تصویب کشورهای عضو رسیده است، در این رابطه مقرر داشته: «۱ هر دولت عضو، منطبق با اصول حقوقی خود، تدابیر لازم جهت برقراری مسئولیت اشخاص حقوقی مشارکت‌کننده در ارتکاب جنایات شدیدی که یک گروه مجرم سازمان‌یافته نیز در آن‌ها دخالت دارد و نیز جرایم موضوع ۵، ۶، ۸ و ۳۲ این کنوانسیون اتخاذ خواهد نمود. مسئولیت اشخاص حقوقی می‌تواند کیفری، مدنی یا اداری باشد. این مسئولیت‌ها، به مسئولیت کیفری اشخاص حقیقی که مرتکب این جرایم شده‌اند، خدشه‌ای وارد نخواهد کرد.

در ژاپن تا سال ۱۹۳۲ تنها مدیران اشخاص حقوقی به نیابت از آن مسئول قلمداد می‌شدند، از سال ۱۹۳۲ نظام مسئولیت دوگانه یا ریوباتسوکایتی مسئولیت مشترک شخص حقوقی و مدیر را موردپذیرش قرارداد، مهم‌ترین مجازات قابل‌اعمال در نظام حقوقی این کشور در برابر اشخاص حقوقی جریمه است (Marina, 2006). در حقوق جزای آمریکا، به خاطر پیچیدگی بیشتر حیات اجتماعی، شرکت‌های بزرگ صنعتی و تجارتي نمود و اهمیت فوق‌العاده‌ای به دست آورده‌اند؛ به همین خاطر مسئولیت جزایی اشخاص حقوقی از دیرباز پذیرفته‌شده است (Habibzadeh & Fakhr Bonab, 2005) اما مسئولیت کیفری به‌عنوان یک مفهوم حقوقی چه ارتباطی با سایر موارد مسئولیت دارد؟ پاسخ این سؤال درگرو بررسی مفهوم مسئولیت کیفری در کنار سایر موارد مسئولیت است.

الف- مسئولیت کیفری و مسئولیت مدنی

مسئولیت اعم از کیفری و مدنی، مستلزم پاسخگویی شخص مسئول است و این پاسخگویی یا به دلیل تقصیر است یا به دلیل واردکردن زیان، مخاطب پاسخ نیز یا جامعه است یا زیان‌دیده و هدف از آن‌هم یا بازدارندگی و تنبیه شخص مسئول است یا به حالت اول برگرداندن وضعیت زیان‌دیده. البته در نظام‌های حقوقی قدیمی، موارد و هدف‌های فوق‌الذکر از هم تفکیک نشده بود و مجازات فرد مسئول هم هدف بازدارندگی داشت و هم موجب جبران خسارت (Badini, 2005) و همین گذشته مشترک تنها نقطه عطف مفاهیم مسئولیت مدنی و کیفری است، از اواخر قرن هجدهم در اکثر نظام‌های حقوقی مسئولیت کیفری و مدنی هم از لحاظ مقررات و هم از لحاظ هدف‌ها و مبانی از هم تفکیک‌شده‌اند، به‌طور مثال مهم‌ترین مبنای ایجاد مسئولیت کیفری حمایت از حقوق جمعی، در کامن‌لا اصطلاحاً گفته می‌شود مسئولیت کیفری در ارتباط میان افراد و پادشاه اتفاق می‌افتد (Wilson, 2000). این در حالی است که هدف حقوق مسئولیت مدنی حمایت از افراد در برابر زیان‌هایی است که ممکن است در روابط اجتماعی از افعال سایرین متوجه آن‌ها شود، علاوه بر این از جمعیت منبع مسئولیت نیز جرم ناشی از قانون است و نمی‌توان هر کار ناپسند و زیان‌بار را جرم شناخت، ضمن اینکه در امور کیفری قیاس روا نیست و اصل قانونی بودن مجازات‌ها ضامن حفظ حقوق فردی در برابر دولت‌هاست، اما در مسئولیت مدنی دادرسی نیازی ندارد که برای هر مسئولیت مبنای قانونی و شروطی به دست آورد (Habibzadeh & Fakhr Bonab, 2005). علاوه بر این قلمرو آن در مسئولیت نیز باهم متفاوت است، پاره‌ای از جرایم با اینکه مجازات‌های سنگین دارند به دلیل اینکه برای اشخاص خسارت ایجاد نمی‌کنند با مسئولیت مدنی همراه نیستند، به همین ترتیب وجود و احراز مسئولیت مدنی نیز به مفهوم وجود و ارتکاب یک جرم نیست.

ب: مسئولیت کیفری و مسئولیت بین‌المللی

به‌موجب ماده ۲ طرح ارائه‌شده از جانب کمیسیون حقوق بین‌الملل در زمینه مسئولیت بین‌المللی دولت‌ها تخلف بین‌المللی یک دولت زمانی محرز می‌شود که فعل یا ترک فعل تشکیل‌دهنده اقدام مطابق حقوق بین‌الملل قابل انتساب به آن دولت باشد و موجب نقض یک تعهد بین‌المللی آن دولت باشد، بنابراین مسئولیت بین‌المللی تنها با احراز دو شرط فوق قابل ایجاد است، بنابراین برای آن‌که اقدام خاصی به‌عنوان یک تخلف بین‌المللی توصیف شود، باید در درجه اول قابل انتساب به دولت باشد و دومین شرط آن نیز این است که اقدام منتسب به دولت باید موجب نقض یک تعهد بین‌المللی دولت شده باشد (حلمی ۱۳۹۰: ۳۶-۳۷). در مقابل، مسئولیت بین‌المللی دارای چند تفاوت اساسی با آن است. نخست اینکه برخلاف مسئولیت کیفری که معمولاً برای اشخاص حقیقی ایجاد می‌شوند، مسئولیت بین‌الملل اساساً برای دولت‌ها که کامل‌ترین موجودیت حقوقی در عرصه حقوق بین‌الملل محسوب می‌شود ایجاد می‌شود. از سویی دیگر، برای ایجاد مسئولیت بین‌الملل کافی است رفتار یا تخلف دولت برخلاف قواعد حقوق بین‌الملل محسوب شوند و الزاماً معاهدات موجود مسئولیت بین‌المللی برای دولت‌ها نیستند.

باید توجه داشت موضوعی که پیرامون مسئولیت بین‌المللی دولت در بیست سال گذشته بیش از هر چیز دیگری مورد بحث و مناقشه قرار گرفته است، ارتکاب برخی اعمال غیرقانونی است که باید در مقوله دیگری غیر از اعمال ایجادکننده ایجاد کنند. مسئولیت بین‌المللی او جای گیرند، چنین اعمال غیرقانونی را جنایات بین‌المللی دولت نام نهاده‌اند (Marina, 2006). درواقع باید توجه داشت که ویژگی جنایات بین‌المللی به‌گونه‌ای است که اشخاص حقوقی به‌ویژه دولت‌ها در انجام آن‌ها تواناترند، ولی اساسنامه دیوان کیفری بین‌الملل راه بزهکاری را بر این اشخاص مسدود نموده و بر پایه رویکرد سنتی، تنها اشخاص حقیقی را مسئول قلمداد کرده است (Alipour, 2011)، به‌هرحال تفاوت مسئولیت کیفری و بین‌المللی در شخصی است که در این مواقع مسئول قلمداد می‌شود.

۴. مسئولیت کیفری در قانون جرایم رایانه‌ای ایران

قانون‌گذار ایران در قانون جرایم رایانه‌ای فصل ششم از قانون را به موضوع مسئولیت کیفری اختصاص داده است، شاید بتوان گفت مهم‌ترین تغییری که قانون فوق‌الذکر در رابطه با مسئولیت کیفری ایجاد نموده، شناسایی و ایجاد مسئولیت کیفری برای اشخاص حقوقی است، ماده ۱۹ و ۲۰ قانون فوق‌الذکر در رابطه با مسئولیت کیفری اشخاص حقوقی است. ماده ۱۹ مقرر می‌دارد: «در موارد زیر، چنانچه جرایم رایانه‌ای 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 جرم رایانه‌ای را صادر کند و جرم به وقوع پیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی بااطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

ماده ۲۰ نیز اشعار داشته: «اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم شخص حقوقی منحل خواهد شد.

در این رابطه ممکن است این سؤال مطرح شود که تأکید قانون‌گذار ایران بر بحث مسئولیت کیفری اشخاص حقوقی چه معنایی در پی دارد؟ و آثار آن چیست؟

یکی از مهم‌ترین سؤالاتی که ممکن است در این زمینه مطرح شود درواقع بحث شناخت مسئولیت کیفری برای اشخاص حقوقی و تأثیر آن بر مسئولیت افراد حقیقی است، آیا رویه قانون‌گذار ایران بر این بوده که اصل را بر مسئولیت کیفری اشخاص حقوقی قرار دهد؟ یا به دنبال نفی مسئولیت کیفری اشخاص حقیقی در فضا سایبر بوده است؟ پاسخ مطمئناً منفی است، با توجه به اینکه تبصره دو ماده ۱۹ مقرر می‌دارد: «مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود»، بنابراین اینکه قانون‌گذار ماده نخست از مبحث ششم قانون جرایم رایانه‌ای را به بحث مسئولیت کیفری اختصاص داده، به معنای نفی مسئولیت کیفری اشخاص حقیقی نیست.

مسئله دیگری که باید در این مقوله مورد بررسی قرار بگیرد بحث تناسب مسئولیت‌ها و رابطه مسئولیت کیفری اشخاص حقیقی و حقوقی است، همان‌طور که گفتیم تبصره دو ماده ۱۹ مسئولیت کیفری اشخاص حقوقی را مانعی برای مجازات اشخاص حقیقی ندانسته، اما متن ماده فوق تا اندازه‌ای گمراه‌کننده است، زیرا عملاً صحبتی از ارتباط دو مسئولیت با یکدیگر نشده است، به‌هرحال باید اذعان داشت تا زمانی که کسی مسئولیت نداشته باشد اعمال مجازات بر ایشان امکان‌پذیر نیست، بنابراین متن تبصره ۲ فوق‌الذکر به معنای امکان وجود مسئولیت همزمان برای شخص حقوقی و اشخاص حقیقی عضو آن مجموعه است. بحث ارتباط میان مسئولیت اشخاص حقیقی و مسئولیت اشخاص حقوقی، به اشکال ارتباط میان این دو نوع مسئولیت می‌پردازد، باید توجه داشت که این دو مسئولیت از پیشینه و ریشه‌ی مشترکی برخوردارند، آن‌ها بر اثر نقض جدی تعهداتی که به‌طور کلی در برابر جامعه وجود دارند ایجاد می‌شوند (Bonafe. Beatric, 2009). البته این دو مسئولیت عواقب یکسانی ندارند، به‌هرحال باید گفت که وجود مبنای مشترک به معنای آن نیست که قواعد کلی مسئولیت اشخاص حقیقی در رابطه با مسئولیت اشخاص حقوقی قابلیت کاربرد دارند، در اینجا تنها می‌توانیم به این مسئله اشاره کنیم که یکسان بودن این دو نوع مسئولیت در قواعد اولیه به معنای آن است که هر دو بر اثر نقض هنجارهای اساسی که مورد حمایت جامعه است ایجاد می‌شوند، البته در قواعد ثانویه این ارتباط کمرنگ خواهد شد (Bonafe. Beatric, 2009). در هر حال شناخت اشتراکات و ارتباط میان مسئولیت اشخاص بررسی مبانی مسئولیت در این زمینه است.

۵. عوامل رافع مسئولیت کیفری در فضای مجازی

مسئولیت کیفری «التزام به تقبل آثار عواقب افعال مجرمانه یا تحمل مجازاتی است که سزای افعال سرزنش‌آمیز بزهکار به‌شمار می‌آید؛ لکن به‌صرف ارتکاب جرم نمی‌توان بار مسئولیت را یک‌باره بر دوش مقصر گذاشت، بلکه پیش از آن باید بتوان او را سزاوار تحمل این بار سنگین دانسته، تقصیری را که مرتکب شده است، نخست به حساب او گذاشت و سپس او را مؤاخذه کرد. توانایی پذیرفتن بار تقصیر را در اصطلاح حقوقدانان «قابلیت انتساب» می‌نامند و آن را به برخورداری فاعل از قدرت ادراک و اختیار تعریف کرده‌اند؛ بنابراین اگر مجرم مُدرک یا مختار نباشد مسئول اعمال خود نیست. برای اینکه مسئولیت جزایی به معنای اخص کلمه وجود داشته باشد باید مجرم مرتکب تقصیری شده مجرمیت و این تقصیر قابل اسناد به او باشد (Habibzadeh & Fakhr Bonab, 2005)، در این قبیل علل مسئولیت جزایی برای اعمال مجرم وجود ندارد، برای درک این مفهوم باید ابتدا معنای مسئولیت جزایی را درک نمود، مسئولیت جزایی را مسئولیت مرتکب جرمی از جرایم مصرح در قانون را گویند و شخص مسئول به یکی از مجازات‌های مقرر در قانون خواهد رسید، متضرر از جرم در این موارد اجتماع است (Jafari Langeroudi, 2007)، به هر صورت علل رافع مسئولیت جزایی موجبات سلب مسئولیت بزهکار را فراهم می‌سازند در این موارد علیرغم آنکه جرم به وقوع پیوسته است اما به واسطه وجود شرایطی در خود شخص بزهکار مجرم مسئولیت نداشته و در نتیجه مجازاتی بر وی اعمال نخواهد شد، در رابطه با تفاوت ماهوی این علل با علل موجهه جرم باید گفت: عوامل رافع مسئولیت جزایی، جنبه خصوصی و شخصی و یا به عبارتی درونی دارند، دارد و ناشی از اهلیت و خصوصیات جسمی یا روانی مرتکب جرم است و دارای مظهر و منشأ درونی است. در حالی که علل مشروعیت ناشی از عوامل و شرایط خارجی است و قائم بر واقع‌ای است که باعث حذف وصف مجرمانه از عمل مرتکب خواهد شد، ضمن آنکه خصوصیات جسمی و روانی مجرم در آن نقشی ندارد (Shambayati, 2009)، عوامل رافع مسئولیت جزایی همچون یک امر شخصی است که قلمرو آن محدود به شخص مرتکب جرم است یعنی وجود آن تنها باعث عدم مسئولیت جزایی مجرم می‌شود و تأثیری در عدم مسئولیت جزایی شرکا و معاونین جرم ندارد در حالی که علل مشروعیت نسبت به کلیه شرکت‌کنندگان در جرم

قابل اعمال است یعنی مشروعیت آن شامل شرکا و معاونین جرم نیز می‌شود. از دیگر تفاوت‌های این دو باید گفت که در علل رافع مسئولیت درواقع عنصر معنوی جرم محقق نشده و بدین ترتیب اصولاً جرمی تحقق نیافته است درحالی‌که در علل موجهه جرم عدم جرم شناختن عمل مجرمانه به علت رفع عنصر قانونی آن توسط متن دیگری از قانون است و درنهایت از دیدگاه هدف شناسی باید گفت علل رافع مسئولیت مدنی مرتکب را رفع نمی‌نماید زیرا هدف از وضع قواعد مربوط به عوامل رافع مسئولیت جزایی همان‌طوری که از عنوان آن برمی‌آید، برای از بین رفتن مسئولیت جزایی مرتکب جرم است. زیرا لازمه اعمال مجازات که فرع بر اثبات مسئولیت جزایی است، به‌منظور حفظ نظم و دفاع اجتماعی است و نمی‌تواند مسئولیت مدنی مرتکب جرم را از بین ببرد. درحالی‌که علل مشروطیت نه‌تنها موجب زوال مسئولیت جزایی و مسئولیت مدنی مرتکب جرم خواهد شد. یعنی عمل مجرمانه او را مشروع می‌سازد و باعث عدم مسئولیت جزایی و مدنی شرکا و معاونین جرم نیز خواهد شد (Rahmanpour, 2013).

قانون‌گذار ایران در قانون جرایم رایانه‌ای اشاره‌ای به عوامل رافع مسئولیت کیفری ننموده است بند ب ماده ۱۹ اشاره به دستور مدیر و نقش این دستور در ارتکاب جرم دارد که درواقع اشاره به علل موجهه جرم دارد نه عوامل رافع مسئولیت کیفری، به‌هرحال باید اذعان داشت عوامل رافع مسئولیت در فضای مجازی تابع عوامل کلی رافع مسئولیت کیفری است، می‌توان این عوامل را در موضوعاتی مانند کودکی، جنون، اجبار معنوی و... دانست، بنابراین باید اذعان داشت که عوامل رافع مسئولیت در فضای مجازی همان عوامل کلی رافع مسئولیت جزایی هستند که معمولاً در متون حقوق کیفری عمومی موردبررسی قرار می‌گیرند.

۶. بررسی تطبیقی افترا در فضای سایبری

یکی از جرائم علیه شخصیت معنوی و شرافت، افراد افترا است که به وسیله گفتار رفتار یا کردار فرد واقع می‌شود. بدگویی از دیگران اگر راست باشد، غیبت است و اگر دروغ باشد افترا است که گاهی "بهتان" نیز نامیده می‌شود. افترا از کارهای حرام و از گناهان بزرگ به شمار می‌آید در قرآن آیات فراوانی وجود دارد که این عمل را زشت و ناپسند شمرده است؛ از جمله در سوره نحل آیه ۱۰۵ می‌فرماید: «إنما یفتی الکذب الذین لا یؤمنون... کسانی که افترا می‌بندند ایمان ندارند همچنین روایات بسیاری بر حرمت آن دلالت دارند. افترا» در لغت به معنای دروغ بستن چیزی را به دروغ گفتن و بهتان زدن آمده است. هنگامی که امری غیر واقعی را به کسی نسبت می‌دهیم در حقیقت به او افترا بسته و بهتان زده‌ایم این واژه در اصطلاح حقوقی عبارت است از نسبت دادن صریح عمل مجرمانه و برخلاف حقیقت و واقع به شخص یا اشخاص معین، به یکی از شیوه‌های یاد شده در قانون مشروط به این که صحت عمل مجرمانه نسبت داده شده در نظر مراجع و مقامات قضایی ثابت نشود. به عبارت دیگر انتساب امری مجرمانه یا انتشار جرم انتسابی به یکی از طرق قانون و امثال آن از همین جاست که فرق بین غیبت و افترا روشن می‌شود؛ زیرا اگر بدگویی از دیگران راست باشد، غیبت و اگر دروغ باشد، افتراست. با توجه به اطلاق تعریف فوق می‌توان گفت ارتکاب جرم افترا از طریق رایانه قابل تحقق است و چه بسا اتفاق افتاده است در ادامه به عناصر تشکیل دهنده این جرم می‌پردازیم.

۶-۱. عنصر قانونی

پیرامون افترا در فضای مجازی تا پیش از تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ دادگاهها از روی ناچاری از اطلاقات موجود در مواد قانونی استفاده کرده و این جرم را با استفاده از قوانین سنتی بررسی می‌کردند برای مثال عنصر قانونی جرم افترای اینترنتی از اطلاق ماده ۶۹۷ قانون مجازات اسلامی استفاده میشد ماده فوق مقرر میدارد: هر کس به وسیله اوراق چاپی یا به وسیله درج در روزنامه و جراید یا نطق در مجامع یا به هر وسیله دیگر، به کسی امری را صریحاً نسبت دهد یا آن‌ها را منتشر نماید که مطابق قانون آن امر جرم محسوب میشود و نتواند

صحت آن اسناد را ثابت نماید جز در مواردی که موجب حد است به یک ماه تا یک سال حبس و تا ۷۴ ضربه شلاق یا یکی از آن‌ها حس مورد محکوم خواهد شد. تبصره در مواردی که نشر آن، امر اشاعه فحشا محسوب، گردد هر چند بتواند صحت اسناد را ثابت نماید مرتکب به مجازات مذکور محکوم خواهد شد.» بنابراین بر اساس کلمه کلیدی یا به هر وسیله دیگر در ماده مذکور که مقرر می‌دارد: «هر کس به وسیله اوراق چاپی... یا به هر وسیله دیگر به کسی امری را صریحا نسبت دهد یا آن‌ها را منتشر نماید... محکوم خواهد شد، وسیله را شرط نداشته است؛ لذا افترا به هر وسیله‌ای که، باشد اگر چه با رایانه و در فضای مجازی صورت، بگیرد مشمول همین حکم است؛ زیرا اطلاق ماده بیان میکند که نوشته چه به صورت چاپی (تایپی) یا خطی و دست نوشته باشد یا به صورت عکسبرداری از نوشته دیگر باشد تفاوتی ندارد بنابراین، نوشتن روی صفحه مانیتور رایانه یا صفحه اینترنت نیز مشمول ماده فوق میشود. با تصویب قانون جرایم رایانه‌ای توسط مجلس شورای اسلامی در خرداد ماه ۱۳۸۸ افترا در فضای مجازی و اینترنت به عنوان یک جرم شناخته شد و در بخشی از ماده ۱۸ این قانون به جرم افترای رایانه‌ای اشاره شد. بنابراین ماده: هر کس... یا با همان، مقاصد اعمالی را برخلاف حقیقت راسا یا به عنوان نقل قول به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد اعم از این که از طریق یاد شده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود افزون بر اعاده حیثیت در صورت (امکان به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج میلیون (۵۰۰۰۰۰۰) ریال تا چهل میلیون (۴۰۰۰۰۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

۲-۶. عنصر مادی

در بحث عنصر مادی چند نکته بسیار مهم وجود دارد نکته اول: از شرایط تحقق جرم افترا معین بودن شخص طرف اسناد است؛ یعنی شخص مسندالیه در جرم افترا باید به شکل روشن و بدون ابهام مشخص شده باشد بنابراین اگر در سایت یا وبلاگ یا به طور کلی در اینترنت چنین بنویسد یکی از اعضای دولت مختلس است یا یکی از مدیران کل وزارت کشور مرتکب اختلاس شده است نمیتوان او را مفتری به حساب آورد. مگر آنکه همراه با آن، خبر صفات و مشخصاتی بیاورد که بر فرد مورد نظر منطبق باشد که در این صورت میتوان گفت این فرد مفتری است البته در صورتی که سایر شرایط را نیز داشته باشد. حال این تعیین ممکن است صریح باشد مثلا با گفتن نام و مشخصات او صورت گیرد یا با اشاره و علامت مشخص، شود یا این که از طریق انتشار خبری در اینترنت الف) را به کلاهبرداری متهم. کند یا این که از طریق انتشار عکس یا کاریکاتور که مشخص کننده «الف» است وی را به ارتکاب عملی متهم نماید یا این که ابتدا به ذهن می‌رسد که عکس نقاشی و کاریکاتور نمیتوانند معین باشند؛ ولی از آنجا که خط با توجه به تاریخ و سیر تحول و تکامل، آن خلاصه شده تصاویر است و تصویر و نقاشی و کاریکاتور گاهی ممکن است گویاتر از خط باشند و با توجه به این که در ماده ۱۸ قانون جرایم رایانه‌ای واژه تلویحا نیز به کار برده شده، میتوان گفت که در همه این موارد اگر صراحت در افترا، نباشد دست کم تلویحا به افترا اشاره دارد همچنین شخص معین ممکن است حقیقی یا حقوقی باشد؛ هر چند برخی قانون مجازات اسلامی را با توجه به عبارت هر کس» و «کسی شامل اشخاص حقوقی نمیدانند؛ زیرا معتقدند عبارت هر کس و همچنین کلمه کسی برای منتسب الیه یا مجنی علیه در ماده، قانون حاکی از ارتکاب جرم به وسیله شخص حقیقی است.

بدین ترتیب شخص حقیقی معین به عنوان مجنی علیه در جرم افترا همانند جرم توهین مورد توجه است و مزبور شامل، اداره سازمان شرکتهای دولتی و تجاری و به طور کلی اشخاص حقوقی نمیشود. اما با توجه به ماده ۱۸ قانون جرایم رایانه‌ای که صراحت دارد: «هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر کند یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت راسا یا به عنوان نقل قول به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت

دهد اعم از اینکه از طریق یاد شده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود افزون بر اعاده حیثیت در صورت امکان به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد باید گفت افترا در فضای مجازی شامل تمامی اشخاص حقیقی و حقوقی میشود و این که بعضی افترا را تنها به اشخاص حقیقی منتسب میدانند با توجه به قوانین سنتی است از این رو برخی از حقوقدانان در توجیه این موضوع اظهار داشته اند که اگر شخصی در ظاهر، یک شرکت تجاری یعنی شخصیت حقوقی معینی را طرف افترا قرار دهد ولی منظور او اعضای هیئت مدیره یا مدیر عامل آن شرکت باشد عمل او جرم است. البته پذیرفتن این دیدگاه یا بیان چنین توجیهاتی برای شمول افترا زمانی صحیح خواهد بود که نص صریح قانونی در این باره موجود نباشد؛ در حالی که پیرامون افترا در فضای مجازی به اشخاص حقوقی ماده ۱۸ قانون جرایم رایانه‌ای به صراحت به آن اشاره دارد هر چند میتوان گفت این که بعضی افترا را به اشخاص حقیقی منتسب می‌دانند مرادشان افترا در محیط و فضای طبیعی است. هر چند باز هم باید گفت افترا در فضای واقعی نیز با توجه به تصریح ماده ۳۰ قانون مطبوعات مصوب ۱۳۶۴ و تبصره ذیل آن که افترا را شامل اشخاص حقیقی و حقوقی میداند منحصر دانستن تحقق جرم افترا به اشخاص حقیقی و جاهت نخواهد داشت. در نتیجه می‌توان چنین گفت: چون شخصیت‌های حقوقی به وسیله شخص یا اشخاصی به نام هیئت مدیره یا مدیر عامل یا هیئت عامل اداره میشوند میتوان اسناد و افترا را با توجه به اقتضا و قرائن، امر متوجه آنان دانست (Nami, 2004).

بنابراین با توجه به این که قانونگذار برخلاف قوانین سابق پیرامون افترا از طریق رایانه و سامانه‌های مخابراتی قیدی به کار نبرده و قائل به توسعه شده است میتوان گفت ارتکاب این جرم اگرچه پیش از تصویب قانون جرایم رایانه‌ای با نارسایی‌هایی همراه بود، ولی با تصویب این قانون مرتفع گردید. در نتیجه جرم افترا با هر نوع وسیله، چه به صورت تصریحی یا تلویحی و چه به شخص حقیقی یا حقوقی و چه موجب ضرر مادی یا معنوی بشود یا نشود مشمول این ماده خواهد بود. نکته دوم ملاک تحقق جرم افترا این است که عمل انتسابی در زمان انتساب جرم باشد بنابراین اگر عمل انتسابی به موجب قانون لاحق جرم شناخته شود تحقق جرم افترا منتفی است (Rahmanpour, 2013). نکته سوم در قانون جرایم رایانه‌ای برخلاف قانون مجازات اسلامی اشاره‌ای به صورت دوم جرم افترا که همان انتشار نسبت دادن امر مجرمانه است نشده است؛ زیرا قانونگذار این امر را مفروض گرفته که طبیعت رایانه و اینترنت انتشار اخبار و اطلاعات است، لذا به آن اشاره نکرده است از این رو میتوان یکی از مصادیق انتشار امر افترا آمیز در فضای مجازی را به این صورت بیان کرد اگر شخصی مطالب افترا آمیز را تایپ کند و در رایانه خود نگهداری کند ولی فعلاً هیچگونه قصد و سونیتی در این باره نداشته باشد اگرچه شاید در آینده و در موقع مناسب بخواهد آن را انتشار دهد ولی شخص دیگری آن را انتشار دهد، شخص دوم اگر با علم و اطلاع این کار را انجام دهد مرتکب جرم افترا شده است و نمیتوان فرد نویسنده را به جرم افترا مجازات کرد؛ زیرا افترا باید علنی باشد؛ به گونه‌ای که دیگران از آن آگاه شوند و کار نویسنده مانند موردی است که افترای نوشته شده را در صندوقچه شخصی خود نگه داشته و مطلبی برای خود نوشته است بنابراین باید گفت علنی شدن نوشته افترا آمیز ناشی از فعل نویسنده نیست و لذا نباید مجازات شود اما در صورتی که نویسنده با این قصد که دیگری آن را منتشر کند اقدام به نوشتن مطالب افترا آمیز کرده باشد و شخص دوم بدون اطلاع و آگاهی اقدام به انتشار آن کند، میتوان گفت که نویسنده باید به جرم افترا مجازات شود؛ زیرا در اینجا سبب، اقوا از مباشر است.

۳-۶. عنصر معنوی

هر جرم ارتكابی که عمدی باشد یکی از ارکان اصلی، آن قصد یا سوءنیت است در نتیجه افترا که از جمله جرایم عمدی شمرده می‌شود همراه با سوءنیت عام است؛ یعنی مفتری باید، بالغ عاقل مختار و قاصد باشد. به بیان دیگر مفتری در به کار بردن الفاظ و انتساب عمل مجرمانه و در انتشار آن اراده آزاد داشته باشد. همچنین مرتکب باید در انتساب عمل مجرمانه و کذب بودن موارد استناد علم و آگاهی داشته باشد (گلدوزیان ۱۳۸۸: ۱۴۴). یعنی مفتری با آگاهی از بی گناهی مفتری علیه آن جرم را به دروغ و برخلاف واقع به او نسبت دهد. بنابراین هرگاه مرتکب در نتیجه اشتباه یا سهل انگاری عمل مجرمانه‌ای را از طریق اینترنت منتشر کند و چنین امری ثابت شود چنین شخصی به عنوان مفتری قابل مجازات نیست؛ زیرا فاقد سوء نیت است. همچنین اگر کسی با قصد مزاح و شوخی امری مانند کلاهبرداری یا اختلاس را به دیگری (مثلاً دوست یا همکار خودش نسبت دهد، قابل تعقیب نیست. همچنین اگر مفتری معنای لفظی را نداند مانند این که کارگر ساده جوان و بیسواد شهرداری که وظیفه جمع آوری زباله‌ها را برعهده دارد به راننده کامیون شهرداری که مبلغی پول از یکی از شهروندان بابت حمل زباله‌ها گرفته است بگوید مختلس یا سارق و در جریان تحقیق مطلع نبودن او از مفهوم این واژه احراز گردد، نمیتوان او را به عنوان افترا تعقیب کرد؛ یا اینکه شخص معنای مجرمانه را مدنظر نداشته باشد یا با این تصور که لفظ یا نوشته مزبور دارای معنای صواب و غیر مجرمانه، است به کار برده باشد نمیتوان او را به جرم افترا مجازات کرد؛ زیرا در این موارد میتوان از اصل تفسیر مضیق قوانین جزایی و تفسیر به نفع متهم استفاده کرد بنابراین، افترا در فضای مجازی از جرایم عمد و مطلق است و در نتیجه تحقق ضرر مادی و معنوی در آن شرط نیست.

۷. چالش‌های فراوی اثبات جرایم فضای مجازی

دستگاه قضایی و مجریان قانون، در راه اثبات جرایم فضای مجازی نیز ممکن است کار دشواری را در پیش داشته باشند. بحث اثبات جرایم فضای مجازی همواره یکی از چالش‌های اساسی قضات بوده است که برخی از دلایل آن را میتوان در موارد ذیل خلاصه کرد:

۱. بزهکاران فضای مجازی به دلیل تخصصی که در ارتکاب جرایم سایبری دارند به راحتی میتوانند از طرق مختلف مانند از بین بردن مدارک جرم یا تغییر و جابه جایی، آن اثری از خود بر جای نگذاشته یا حداقل باعث عدم شناسایی خود شوند. همچنین آنان میتوانند با روشهایی مانند کدگذاری مدارک یا انتقال آن به قسمتی دیگری از شبکه اینترنت مانند دارکوبها عملاً دسترسی ادله به جرم و در نتیجه اثبات جرم را مختل سازند همچنین زمانی که جرمی تخصصی و فنی شود، بزهکاران آن به راحتی در جامعه جولان داده و با سوء استفاده از ناآگاهی مردم یا مقامات قضایی و ضابطین ایشان جرایم خود را مخفی نگه دارند.

۲. به دلیل پایین آمدن هزینه‌های استفاده از تکنولوژی و فضای مجازی جرایم این حوزه نیز افزایش یافته و اشخاصی که اطلاعات و آگاهی لازم را نسبت به ماهیت آن نداشته باشند، ممکن است بزه دیدگان این فضا قرار بگیرند همچنین سهولت و ارزانی استفاده از اسناد دیجیتال نیز منجر به توسعه آن شده که این امر با اینکه مزایای فراوانی دارد اما در زمان ارتکاب جرایم سایبری و رایانه ای، جمع آوری و استناد پذیری آن توسط ضابطین و مقام قضایی دشوار خواهد بود. همچنین به دلیل سهولت در تغییر و امحاء اینگونه اسناد قابلیت استناد یا اثبات جرایم فضای مجازی، نیز به چالش کشیده خواهد شد.

۳. مورد بعدی سرعت بالای پیشرفت تکنولوژی و ابزارهای نوین میباشد که در نتیجه آن جرایم نوین و مرتبط با فضای مجازی نیز روز به روز متحول شده و دیگر قابل شناسایی با استفاده از ابزارها و مقررات سنتی نمیشود؛ در نتیجه زمانی که کشوری مهمترین سلاح خود در برابر جرم یعنی قانون را قدرتمند و کارآمد نکرده و به قوانین قدیمی اتکاء داشته باشد نمیتوان انتظار داشت نتایج مطلوبی در مقابله با اینگونه جرایم

کسب کند؛ بنابراین قوای قانون گذاری کشور وظیفه دارد نسبت به جرم انگاری جرایم نوین و تدوین قوانین و مجازتهای متناسب با آن تلاش و دقت مضاعفی را در مقایسه با، جرایم سنتی به خرج دهد.

۴. برخی از جرایم فضای مجازی مانند جرایم منافی عفت، اغلب در لیست ارقام سیاه جرایم قرار می گیرند دلایل این موضوع نیز به چند چیز باز می گردد. نخست؛ برخی از بزه دیدگان این فضا به دلیل ترس از از بین رفتن حیثیت فردی یا جایگاه اجتماعی خود هیچگاه این جرایم را افشاء نخواهند کرد و حتی در این راه ممکن است شواهد و مدارک جرم را از بین ببرند؛ لذا اینگونه جرایم معمولاً اثبات نخواهند شد دوم؛ بزهکاران این فضا نیز به راحتی آثار و ادله جرم را از بین برده و محلی برای اثبات برجای نمیگذارند سوم زنانی که بزه دیده جرایم منافی عفت هستند اغلب به دلیل دوری از برچسب زنی یا انگشت نما شدن در خانواده یا جامعه ارتکاب این جرایم را علیه خود گزارش نکرده و چه بسا انکار نیز میکنند بنابراین مشخصاً بسیاری از جرایم منافی عفت در فضای مجازی ممکن است در بطن این فضا دفن شده و هیچگاه برملا یا اثبات نشوند (Nami, 2004).

نتیجه گیری

فضای مجازی در عصر امروز گسترش زیادی پیدا کرده است زیرا بستری را برای اتصال جهانی فراهم می کند و به افراد از نقاط مختلف جهان اجازه می دهد به راحتی با یکدیگر ارتباط برقرار کنند، همکاری کنند و اطلاعات را به اشتراک بگذارند. این به هم پیوستگی تبادل فرهنگی، اشتراک دانش و نوآوری را در مقیاس جهانی تقویت می کند. همچنین فضای مجازی فرصتهایی را برای کسب و کارها فراهم می کند تا به مخاطبان گسترده تری دست یابند، محصولات یا خدمات خود را به بازار عرضه کنند، و معاملات آنلاین انجام دهند. با این حال، فضای مجازی چالش هایی مانند نگرانی در مورد حفظ حریم خصوصی، امنیت مجازی و انتشار اطلاعات نادرست را نیز به همراه دارد. از آنجایی که جامعه به طور فزاینده ای به فناوری های دیجیتال متکی می شود، باید به این مسائل و اطمینان از اینکه فضای مجازی فضای امن و فراگیر برای همه کاربران باقی می ماند پرداخت. قوانین و مقررات در فضای مجازی به چارچوب قانونی حاکم بر فعالیت ها، تعاملات و تراکنش های آنلاین اشاره دارد. این قوانین برای تضمین حفاظت از حقوق، حریم خصوصی و امنیت افراد در حوزه دیجیتال ضروری هستند. آن ها همچنین به ایجاد دستورالعمل هایی برای رفتار اخلاقی، جلوگیری از جرایم مجازی، و تنظیم محتوای آنلاین برای حفظ یک فضا آنلاین امن و منصفانه کمک می کنند. ارتکاب جرایم در فضای مجازی که به عنوان جرایم مجازی نیز شناخته می شود، در عصر دیجیتال امروزی یک تهدید قابل توجه است. با انجام اقدامات پیشگیرانه و ترویج بهترین شیوه های امنیت مجازی، می توانیم خطرات مرتبط با تهدیدات مجازی را کاهش دهیم. جرم انگاری بی ضابطه و گسترده در قوانین کیفری علاوه بر اینکه موجبات بروز آثار و تبعات سوء تورم کیفری را فراهم میکند با اهداف حقوق جزا نیز مغایرت دارد. وجود ضمانت اجرایی خاص در حقوق جزا همچون سلب حیات، محدود کردن آزادی و تنبیه بدنی ضرورت جرم انگاری مضیق و بر مبنای اصول را روشن میسازد. جرائم مجازی به اقتضای ویژگیهایی از قبیل سهولت ارتکاب جرم، کثرت بزه دیدگان و کم سن بودن اغلب مجرمان آن، در کنار اصول عمومی، اصول جرم انگاری خاصی را می طلبد. عرصه حقوق جزاء تحت تاثیر گسترش وسایل نوین الکترونیک و مشخصاً گسترش فضاهای مجازی نیز دچار تغییرات زیادی شده است، مهمترین تاثیری که تکنولوژی بر حقوق جزا گذاشته، ایجاد فرصت های جدید ارتکاب جرم برای بزهکاران و در نتیجه افقهای نوینی از حمایت کیفری و ایجاد مسئولیت کیفری است. اشخاص حقیقی و حقوقی یکی از موضوعات وقوع و ارتکاب جرم در فضاهای مجازی و فضای مجازی است. ارائه غیرمجاز داده های سری به افراد فاقد صلاحیت یکی از گونه های جرایم رایانه ای است که دارای رکن قانونی، مادی و معنوی است. سیاست جنایی ایران جرم ارائه غیرمجاز

داده‌های سری به افراد فاقد صلاحیت را جرم انگاری کرده و برای مرتکبان این جرم حبس و تعطیلی فعالیت را در نظر گرفته است. یافته‌های پژوهش نشان می‌دهد در این ارتباط، مجازات عادی مرتکبین اشخاص حقیقی این جرم محکومیت به حبس از دو تا ده سال خواهد بود. برای اشخاص حقوقی مبنای مجازات ماده ۱۹ قانون جرایم رایانه‌ای است. لذا اگر دادگاه بر اساس شرایط مندرج در ماده ۱۹ قانون جرائم رایانه‌ای شخص حقوقی را در ارائه غیرمجاز داده‌های سری به افراد فاقد صلاحیت از نظر کیفری مسئول بشناسد، به استناد ماده ۲۰ قانون جرائم رایانه‌ای و با لحاظ صدر و بند ب ماده ۳ قانون مذکور مجازات شخص حقوقی برای بار اول تعطیلی نموقت شخص حقوقی از یک تا سه سال خواهد بود.

رعایت ضوابط در پلتفرم‌های مجازی در قبال ارتکاب جرم و انتشار محتوای مجرمانه موضوعی پیچیده و بسیار مهم است که با توجه به گسترش روزافزون استفاده از فضای مجازی و رسانه‌های اجتماعی، اهمیت آن به شدت افزایش یافته است. پلتفرم‌های مجازی مانند شبکه‌های اجتماعی، سایت‌ها، و اپلیکیشن‌ها به عنوان ابزارهای ارتباطی و اطلاعاتی، تأثیرات زیادی در زندگی اجتماعی و فردی کاربران دارند. این فضاها نه تنها امکانات ارتباطی و تفریحی را فراهم می‌کنند، بلکه به عنوان بسترهایی برای تبادل اطلاعات، فعالیت‌های تجاری، و حتی فعالیت‌های سیاسی و اجتماعی به شمار می‌آیند. اما این بسترهای دیجیتال با تمام مزایای خود، به دلیل عدم نظارت کافی و نبود سازوکارهای مناسب، زمینه‌ساز ارتکاب انواع مختلف جرم‌ها نیز شده‌اند. انتشار محتوای مجرمانه یکی از مهم‌ترین مسائلی است که در این پلتفرم‌ها به وجود می‌آید. محتوای مجرمانه می‌تواند شامل انواع مختلفی از جمله نشر اطلاعات نادرست، هتک حرمت افراد، تهدیدات خشونت‌آمیز، و حتی فعالیت‌های تروریستی و فساد مالی باشد. در بسیاری از موارد، مجرمان از طریق هویت‌های جعلی و به صورت ناشناس اقدام به انتشار این نوع محتوا می‌کنند که این خود به پیچیدگی موضوع می‌افزاید. همچنین، گستردگی این پلتفرم‌ها به گونه‌ای است که محتوای مجرمانه می‌تواند به سرعت در سطح جهانی منتشر شود و افراد زیادی را تحت تأثیر قرار دهد. در مواجهه با این مشکلات، رعایت ضوابط و مقررات در این پلتفرم‌ها امری ضروری است. قوانین مختلفی در کشورهای مختلف به تصویب رسیده‌اند که هدف آن‌ها کاهش جرم‌انگاری و نظارت بر فعالیت‌های آنلاین است. این قوانین معمولاً بر اساس حقوق بشر، حفاظت از حریم خصوصی و امنیت عمومی تنظیم می‌شوند و نیازمند تعادل میان آزادی بیان و جلوگیری از سوءاستفاده‌های احتمالی هستند. در بسیاری از کشورها، پلتفرم‌ها موظف به رعایت قوانین مربوط به انتشار محتوا هستند و باید مکانیزم‌های نظارتی برای شناسایی و حذف محتوای مجرمانه و همچنین مسدود کردن کاربران متخلف ایجاد کنند. یکی از مسائل مهم در این راستا، چالش‌های فنی و عملیاتی است که پلتفرم‌ها در پیاده‌سازی این ضوابط با آن‌ها مواجه هستند. نظارت بر محتوای منتشر شده در فضای آنلاین به دلیل حجم بالای اطلاعات و پیچیدگی‌های مربوط به هوش مصنوعی و داده‌های حجیم، به یک معضل جدی تبدیل شده است. بسیاری از پلتفرم‌ها سعی کرده‌اند با استفاده از الگوریتم‌ها و هوش مصنوعی، محتوای مجرمانه را شناسایی کنند، اما هنوز این فناوری‌ها قادر به شناسایی همه نوع محتوای مجرمانه نیستند. در این میان، همچنین باید به موانع فرهنگی، سیاسی و اجتماعی در کشورهای مختلف اشاره کرد که بر نحوه مدیریت و نظارت بر این پلتفرم‌ها تأثیر می‌گذارد. علاوه بر این، پلتفرم‌های مجازی باید در قبال کاربران خود مسئولیت‌پذیر باشند. این مسئولیت‌ها شامل حفاظت از حریم خصوصی کاربران، جلوگیری از انتشار محتوای مجرمانه، و شفافیت در فرآیندهای نظارتی می‌شود. در برخی کشورها، مسئولیت‌پذیری پلتفرم‌ها به حدی است که در صورت عدم رعایت ضوابط، ممکن است به جریمه‌های سنگین یا مسدود شدن خدمات آن‌ها منجر شود. این اقدام‌ها نه تنها برای جلوگیری از انتشار محتوای مجرمانه بلکه برای ایجاد فضای امن و قابل اعتماد برای کاربران نیز ضروری است.

در نهایت، رعایت ضوابط در پلتفرم‌های مجازی باید به گونه‌ای باشد که حقوق کاربران به‌ویژه حقوق بشر، آزادی بیان و حریم خصوصی مورد احترام قرار گیرد. این مسأله نیازمند همکاری میان دولت‌ها، شرکت‌های فناوری و سازمان‌های حقوق بشری است تا به ایجاد یک فضای آنلاین امن و عادلانه کمک کند. در این راستا، قوانین و مقررات باید به‌طور مداوم بازنگری شوند تا با تغییرات سریع فناوری و شرایط اجتماعی و سیاسی هماهنگ باشند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid development of the internet and social media has transformed these platforms into primary arenas for communication, information exchange, and public discourse. Initially envisioned as completely open spaces compared to traditional media, these networks quickly became subject to regulation by both governments and platform operators. These regulatory frameworks, often shaped by cultural, legal, and political contexts, aim to prevent the dissemination of harmful and criminal content such as terrorism, copyright violations, racism, hate speech, incitement to violence, and child exploitation (Resende de Mendonça et al., 2020). However, the inherent nature of the internet—characterized by user anonymity and transnational accessibility—creates substantial challenges for law enforcement and judicial authorities. In countries like Iran, the absence of comprehensive legislative frameworks and deficiencies in criminal law exacerbate enforcement issues, allowing the proliferation of prohibited content without effective sanctions (Shambayati, 2009). Unlike many other nations that maintain collaborative relationships with major international platforms, Iran lacks formal mechanisms to ensure compliance with domestic laws, particularly due to geopolitical tensions and sanctions (Ardito, 2013). This disconnect results in the inability to remove or prosecute criminal content effectively, turning many platforms into anarchic digital spaces within the Iranian context (Hintz, 2015). These conditions necessitate systematic research into the structural deficiencies of legal enforcement on virtual platforms to develop pragmatic solutions (Jafari Langeroudi, 2007).

Understanding the concept of cyberspace is crucial in addressing its legal implications. Cyberspace encompasses electronically stored and transmitted information, distinct from but interconnected with computer networks (Madhava Soma & Sundaram, 2011). The internet, as a massive interlinked network of computers, serves as the backbone for storing and disseminating vast quantities of information in diverse formats (Holmes, 1998; Ploug, 2009). The rise of cybercrimes—offenses facilitated by or targeting computer systems—has paralleled technological advancement. Examples include unauthorized access, data forgery, and distribution of obscene materials, all codified under Iran's Computer Crimes Law. The historical trajectory of computer crimes reveals that such offenses emerged alongside the advent of computing technology, with early cases in the 20th century

highlighting the absence of legal frameworks to address them (Taheri Jabali, 1993). Internationally, the Council of Europe's 2001 Convention on Cybercrime marked a milestone in coordinated legal responses (Brenner, 2012). In the Iranian context, formal criminalization occurred with the 2009 enactment of the Computer Crimes Law, aligning with global trends in addressing cyber threats (McEwen, 1989; Nami, 2004).

Central to the regulation of online criminal behavior is the concept of criminal liability. Defined as the obligation to bear the consequences of unlawful acts, criminal liability applies equally within cyberspace (Rahmanpour, 2013). Iranian law has progressively recognized the criminal responsibility of legal persons, codified in the Computer Crimes Law through provisions that hold organizations accountable for cyber offenses committed in their name or for their benefit. Comparative legal perspectives, such as Japan's dual responsibility model and long-standing U.S. acceptance of corporate criminal liability, provide relevant insights (Habibzadeh & Fakhr Bonab, 2005; Marina, 2006). Criminal liability must be distinguished from civil and international responsibility, as each operates under different objectives, legal bases, and enforcement mechanisms (Alipour, 2011; Badini, 2005; Wilson, 2000). While both natural and legal persons may bear liability, the relationship between these responsibilities requires nuanced interpretation, as shared foundational principles do not imply identical procedural or substantive rules (Bonafe, Beatric, 2009).

Exemptions from criminal liability, or defenses, operate similarly in cyberspace as in other domains. These include incapacity due to age, mental illness, or coercion, which negate the necessary mental state for criminal responsibility (Habibzadeh & Fakhr Bonab, 2005; Jafari Langeroudi, 2007; Rahmanpour, 2013; Shambayati, 2009). However, Iran's Computer Crimes Law does not explicitly address these defenses, implying the application of general criminal law principles. A notable cyber-specific offense is online defamation (eftira), which—prior to 2009—was prosecuted under general provisions such as Article 697 of the Islamic Penal Code. The Computer Crimes Law now explicitly criminalizes false attributions made via computer or telecommunications systems to both natural and legal persons (Nami, 2004; Rahmanpour, 2013). The offense requires a clearly identifiable victim, intent, and knowledge of falsity, while mistakes, jokes, or lack of awareness may negate culpability. Importantly, the law's inclusive language extends protections to corporate entities, reflecting the evolving nature of reputational harm in digital contexts.

Proving cybercrimes presents unique evidentiary and procedural challenges. Skilled offenders often erase or manipulate digital traces, employ encryption, or exploit anonymization technologies to evade detection (Nami, 2004). The low cost and widespread accessibility of digital tools expand the pool of potential offenders, many of whom operate across jurisdictions. Technological advances outpace legislative adaptation, leaving outdated legal frameworks ill-equipped to address novel forms of cyber offending. Moreover, crimes such as those involving sexual morality frequently go unreported due to stigma, fear of reputational damage, or victim reluctance, creating "dark figures" in crime statistics. These factors, combined with the transnational and intangible nature of cyberspace, demand proactive legislative reform, enhanced technical capacity for law enforcement, and international cooperation to improve investigative and prosecutorial effectiveness.

In conclusion, the intersection of cyberspace, criminal behavior, and regulatory enforcement underscores the urgent need for coherent, adaptable, and balanced legal frameworks. While digital platforms offer unparalleled opportunities for communication, commerce, and cultural exchange, they also facilitate the rapid dissemination of harmful and criminal content. Addressing these issues requires integrating technological tools such as artificial intelligence for content moderation with robust procedural safeguards to protect rights and freedoms. Iran's current legal regime, though

incorporating significant advances such as recognizing corporate criminal liability, remains hindered by structural, political, and operational limitations. The path forward necessitates harmonizing domestic laws with international standards, fostering cooperative relationships with global platforms, and continuously refining legal responses to match the evolving landscape of cyber threats.

References

- Alipour, H. (2011). The International Criminal Court and the Challenge of Responsibility of Legal Persons. In *Proceedings of International Criminal Law: The Process of Theories and Perspectives*. Mizan Publishing.
- Ardito, A. (2013). Social Media, Administrative Agencies, and the First Amendment. *Admin. L. Rev.*, 65, 301.
- Badini, H. (2005). *The Philosophy of Civil Liability*. Sherkat Sahami Enteshar.
- Bonafe, Beatrix. (2009). *The Relationship Between State and Individual Responsibility for International Crimes*. Hague, martinus nijhoff pub. <https://doi.org/10.1163/ej.9789004173316.i-284.45>
- Brenner, S. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. University Press of New England.
- Habibzadeh, M. J., & Fakhr Bonab, H. (2005). Comparison of Justifying Factors of Crime and Exemptions from Criminal Responsibility. *Modares Journal of Humanities*(40).
- Hintz, A. (2015). Social media censorship, privatized regulation and new restrictions to protest and dissent. In *Critical perspectives on social media and protest: Between control and emancipation* (pp. 109-126).
- Holmes, D. (1998). *Introduction to Information Technology*. SAMT Publications.
- Jafari Langeroudi, M. J. (2007). *Legal Terminology*. Ganj-e Danesh.
- Madhava Soma, U., & Sundaram, S. (2011). *Cyber Crime and Digital Disorder*. K. Jaishankar pub.
- Marina, S. (2006). On the Possibility of Committing Crime by the State and Its Criminal Responsibility. *Translated by Ali Hanji*(44).
- McEwen, J. T. (1989). *Dedicated Computer Crime Units* PB - DIANE Publishing.
- Nami, M. (2004). An Overview of Computer Crimes. *Correction and Rehabilitation Journal*, 3(34).
- Ploug, T. (2009). *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction*. Springer pub. <https://doi.org/10.1007/978-90-481-2370-4ER> -
- Rahmanpour, A. (2013). *Criminal Responsibility of Legal Persons*. Imam Hossein University.
- Resende de Mendonça, R., Felix de Brito, D., de Franco Rosa, F., dos Reis, J. C., & Bonacin, R. (2020). A framework for detecting intentions of criminal acts in social media: A case study on Twitter. *Information*, 11(3), 154. <https://doi.org/10.3390/info11030154>
- Shambayati, H. (2009). *General Criminal Law*. Majd Publications.
- Taheri Jabali, M. (1993). Crime and Computer. *Judiciary Law Journal*(9).
- Wilson, L. A. (2000). *Theaters of intention: drama and the law in early modern England*. Stanford University Press.