

مسئولیت کیفری در فضای سایبر در حقوق ایران

بهزاد رضوی فرد* سید نعمت‌اله موسوی**

(تاریخ دریافت: ۹۵/۶/۱۴ تاریخ پذیرش: ۹۵/۶/۲۷)

چکیده

محیط سایبر یا محیط مجازی مفهومی است که اخیراً از سوی جرم‌شناسان و حقوق‌دانان مورد توجه قرار گرفته و همزمان با خلق این محیط جرایمی نیز در آن و با استفاده از آن به وقوع می‌پیوندد. مبارزه حقوقی با این جرایم مستلزم برداشتن چند گام اساسی بود: نخست جرم-انگاری رفتارهای مجرمانه بود، البته جرم‌انگاری بدون ایجاد و احراز مسئولیت کیفری عملی تقریباً بی‌سرانجام تلقی می‌شود، شاید بر همین اساس بوده که قانون‌گذار ایران در قانون جرایم رایانه‌ای بر مسئولیت کیفری اشخاص حقوقی تأکید زیادی نموده و مسئولیت کیفری این اشخاص را برای نخستین بار در حقوق ایران صراحتاً مورد توجه قرار داده است، به‌هرحال موضوع مسئولیت کیفری و تبیین گستره آن در حقوق جرایم رایانه‌ای از اهمیت بسیار زیادی برخوردار است، ممکن است سؤالات زیادی در رابطه با گستره مسئولیت افراد در محیط مجازی مطرح شود، قانون‌گذار ایران فصل ششم از قانون جرایم رایانه‌ای را به موضوع مسئولیت کیفری اختصاص داده است و تغییری که قانون فوق‌الذکر ایجاد نموده شناسایی و ایجاد مسئولیت کیفری برای اشخاص حقوقی در محیط مجازی است.

واژگان کلیدی: فضای سایبری، جرایم سایبری، مسئولیت کیفری، عوامل رافع مسئولیت کیفری.

* دانشیار حقوق جزا و جرم‌شناسی دانشگاه علامه طباطبائی (نویسنده مسئول): Razavi1351@yahoo.com

** دانشجوی مقطع دکتری حقوق جزا و جرم‌شناسی دانشگاه علامه طباطبائی: Snm.1396@yahoo.com

درآمد

امروزه استفاده از وسایل نوین الکترونیک ارتباطی تغییرات گسترده‌ای در تمام جنبه‌های زندگی انسان ایجاد نموده است، بدیهی است عرصه حقوق جزاء نیز دچار تغییرات زیادی شده است، مهم‌ترین تأثیری که تکنولوژی بر حقوق جزا گذاشته، ایجاد فرصت‌های جدید ارتکاب جرم برای بزهکاران و در نتیجه افق‌های نوینی از حمایت کیفری و ایجاد مسئولیت کیفری است، جرایم مختلفی ممکن است در محیط اینترنت به وقوع پیوندند و در نتیجه مجرمین متعددی اقدام به ارتکاب جرم در محیط اینترنت می‌نمایند، عدم هماهنگی حقوق جزاء با این پدیده‌ها یعنی عدم جرم‌انگاری جرایمی که در محیط اینترنت به وقوع می‌پیوندند، عدم ایجاد مسئولیت برای بزهکارانی که از این محیط برای انجام رفتارهای بزهکارانه خویش بهره‌ی جویند و ... مطمئناً راه را برای ارتکاب جرایم بسیار زیادی در محیط اینترنت و سایر فراهم خواهد نمود، بر این اساس باید اذعان داشت که پیشرفت فن‌آوری نباید بتواند جلوی جلوگیری و مقابله با جرایم را در حقوق جزا بگیرد، بنابراین مهم‌ترین مسئله‌ای که در پیش روی نظام‌های کیفری مختلف وجود دارد ایجاد و پذیرش تغییرات در راستای مبارزه و مقابله با جرایم مختلفی است که با استفاده از اینترنت و یا در محیط مجازی به وقوع می‌پیوندند، مبحث شناخت مسئولیت کیفری برای مجرمینی که در این محیط اقدام به ارتکاب رفتارهای بزهکارانه می‌نمایند از مهم‌ترین موضوعاتی است که باید پس از جرم‌انگاری یک رفتار مورد توجه قرار بگیرد که در ادامه تحقیق خود این موضوع مورد بررسی قرار خواهد گرفت.

۱. مفهوم محیط سایبری

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 فن آوری اطلاعات تنها اطلاعات یا تصاویر خانوادگی اشخاص را مورد تهدید قرار نداده، بلکه از این دانش ممکن است برای نقض سایر موضوعات مورد حمایت قانون گذار نیز استفاده شود، به طور مثال دشنام و فحاشی از جریان های همیشگی جوامع است و انگیزه ارتکاب آن از سوی اشخاص تحقیر دیگران از طریق خرد کردن ارزش فرهنگی آنها محسوب می شود (Jeff 2011: 849)، به موجب ماده ۳۱ قانون مطبوعات فحاشی نه تنها در روابط فردی شایسته نیست، بلکه از طریق مطبوعات و رسانه های 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 می شود و می توان آن را از طریق رایانه و سیستم های شبکه اینترنت مرتکب شد، در تمام این موارد استفاده از دانش فن آوری اطلاعات و اینترنت منجر به آن خواهد شد که ارزش های مورد حمایت قانون گذار نقض شود، اما محیط سایبری یا مجازی چیست و چگونه ارتکاب این قبیل جرایم را تسهیل می نماید؟ تاکنون تعاریف متعددی از محیط مجازی ارائه و ابراز شده است. برخی از این تعاریف مفهوم محیط مجازی را محدود کرده و برخی دیگر آن را توسعه بخشیده اند، به موجب یکی از این تعاریف محیط سایبر به اطلاعات الکترونیکی اطلاق می شود که از طریق اینترنت جابجا می شوند، البته تعاریف دیگر سعی نموده اند تا به بیان موارد افتراق محیط سایبری (Activities 2011: 28) از موضوعات مجازی^۱ و شبکه^۲ پردازند و از دیدگاه آنها محیط مجازی مجموعه اطلاعاتی است که در رایانه ذخیره سازی شده و از طریق اینترنت به یکدیگر متصل هستند (Ploug 2009: 70)، این در حالی است که شبکه یا نت دارای تعریف مخصوص به خود است، اینترنت مجموعه ای بسیار گسترده از رایانه های موجود در شبکه های رایانه ای سراسر جهان است که از طریق خطوط ارتباطی به یکدیگر متصل شده و با استفاده از پروتکل های معینی به تبادل اطلاعات می پردازند. بسیاری از رایانه های 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 روش های مختلفی ذخیره شده و در نتیجه با روش های گوناگونی قابل ارائه و انتقال هستند، «صفحات وب»^۳ یکی از روش های خاص ذخیره و ارائه اطلاعات در بین روش های متعدد ذخیره و ارائه اطلاعات در اینترنت هستند (دیانا هولمز ۱۳۷۷: ۵).

^۱ - virtual

^۲ - net

^۳ - Webpage

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»^۱ کار می‌کند. فرارسانه ترکیبی از «فرامتن» و «چندرسانه‌ای»^۲ است، اکنون اگر می‌گوییم جرایم سایبری واقع می‌شوند منظور این است که بزهدکار 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 محیط 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: «هر کس 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: «هر کس 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: «هر کس 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 نود و یک 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 محیط سایبری به وقوع بپیوندند و نوع جرم در تعریف محیط سایبر یا جرایم سایبری تأثیری ندارد.

۲. تعریف و تاریخچه جرایم رایانه‌ای

۲.۱. تاریخچه شکل‌گیری جرایم رایانه‌ای

نخستین کامپیوتر در سال ۱۹۳۷ در آمریکا اختراع شد. با پیشرفت فن‌آوری به تدریج در ساخت

^۱- Hyper

^۲- Multimedia

رایانه تغییراتی به وجود آمد، به اندازه‌ای که اصطلاح نسل‌های مختلف رایانه برای نامیدن این تغییرات مورد استفاده قرار گرفت، امروزه ارتباط با کامپیوتر از طریق صوت و تصویر نیز امکان‌پذیر خواهد بود. اطلاعات از همان زمان پیدایش به صورت مناسب برای کامپیوتر ذخیره شده و در هنگام لزوم، از طریق سیستم‌های کامپیوتری مورد استفاده قرار خواهد گرفت. استفاده از حافظه‌های نوری حافظه‌هایی با حجم کم و گنجایش غیرقابل تصور 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 در نهایت تأثیر آن بر حقوق کیفری جامعه چه خواهد بود؟

در یک اظهار نظر کلی می‌توان گفت که جرایم رایانه همزاد خود رایانه تلقی می‌شوند و با شروع استفاده از رایانه این 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، به عنوان مثال پس از مظنون شدن پلیس انگلستان به یک جوان ۲۳ ساله که با تماس با یک شرکت بزرگ رایانه‌ای پیشنهاد کرده بود که در عوض گرفتن وجوهی، طریقه گرفتن اطلاعات سری از رایانه‌های سایر مراکز را به آن‌ها آموزش دهد و دستگیری وی به عنوان باج‌خواهی یک باند سرقت بین‌المللی کشف شد، پس از تحقیقات به عمل آمده 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 به صورت 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 قابل ملاحظه‌ای که بر بحث امنیت ملی انگلستان داشته است در آن زمان جرم به حساب نمی‌آمد (طاهری ۱۳۷۲:۱۱۷) و جوان مورد ذکر به راحتی 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 (Atul 2005: 121)، البته سابق قانون‌گذاری در عرصه داخلی در خصوص جرایم رایانه‌ای به مدت‌زمانی قبل‌تر از سال ۲۰۰۱ بازمی‌گردد در آمریکا که یکی از پیشگامان در این عرصه محسوب می‌شود میان‌سال‌های 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 (W.Brenner 2012: 21). درنهایت 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 جرائم رایانه‌ای در ۲۷ آبان ۱۳۸۷ با رأی ۱۷۶ 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 جرائم رایانه‌ای به تأیید شورای نگهبان رسید (www.itna.ir). درنهایت مسئله‌ای که در این رابطه می‌تواند موردتوجه قرار بگیرد موضوع تأثیر جرم‌انگاری جرایم رایانه از پیشرفت علم رایانه در کشورهای مختلف است، همان‌طور که مشاهده شد جرم‌انگاری جرایم رایانه در ایالات‌متحده آمریکا که مهد ظهور دانش رایانه است بسیار زودتر از سایر مناطق جهان شروع شده و به‌تدریج برخی مناطق دیگر دنیا مانند ایران را نیز درنوردیده است.

۲. ۴. 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 (نامی، ۱۳۸۳: ۵۳)، البته باید توجه داشت که تعاریف ارائه‌شده از جرایم رایانه‌ای با توجه به تعریف مبتنی بر سوءاستفاده از رایانه امروز دگرگون‌شده 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 به‌وسیله اشخاصی خاص مرتکب خواهند شد (McEwen, 1989: 1)، درنهایت تعریف مبتنی بر استفاده از رایانه جایگزین تعریف فوق‌الذکر شد و درنهایت 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

(op.cit)، 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 شماره حسابی 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 پیوندد (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 غیرقانونی به داده‌های رایانه‌ای برای تسهیل سایر جرایم

پ: ایجاد تغییر غیرقانونی در داده‌های رایانه‌ای^۱

بندهای یک و دو ماده یک و شقوق سه گانه آن میان جرایم رایانه‌ای دستیابی غیرمجاز به داده‌های رایانه‌ای که نیاز به احراز سوءنیت در بزهدار 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 دانش‌محور از جرایم رایانه‌ای محسوب می‌شود (Madhava 2011: 21). به‌عبارت‌دیگر 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.

²- Unauthorised modification

۳. مسئولیت کیفری در محیط سایبری

۳.۴. 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 گاه‌تحت عنوان حقوق حمایتی جمعی و به‌منظور دفاع از جامعه ارائه می‌شود را مسئولیت کیفری قلمداد کرده است (شامبیاتی ۱۳۸۸: ۲۲). 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 محرمانه 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 (رحمان بور ۱۳۹۲: ۱۲). مسئولیت کیفری در محیط سایبر نیز به معنای تقبل آثار ناشی از فعل مجرمانه فرد است که در محیط اینترنت به وقوع پیوسته بنابراین مسئولیت در محیط سایبر مفهومی جدای از سایر موارد مسئولیت ندارد.

در رابطه با مسئولیت کیفری اشخاص حقوقی نظرات مختلفی ارائه شده است، برخی از نویسندگان در صدد نفی آن برآمده‌اند و برخی دیگر با استناد به اینکه اشخاص حقوقی وجود واقعی دارند، بزه ارتكابی در برابر ایشان قابلیت استناد دارد و در نهایت اینکه برخی کیفرها را می‌توان در ارتباط این اشخاص مورد استفاده قرارداد معتقدند که اشخاص حقوقی مسئولیت کیفری دارند (روح‌الامینی ۱۳۸۷: ۱۳۳). 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 ماده‌واحده مربوط به ضبط اموال متعلق به احزابی که منحل می‌شوند نمونه دیگری از پذیرش مسئولیت کیفری اشخاص حقوقی در نظام حقوقی ایران است (دامغانی ۱۳۸۸: ۱۵) و در نهایت 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 سازمان یافته 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 مشارکت کننده در ارتکاب جنایات شدیدی که یک گروه مجرم سازمان یافته 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 مورد پذیرش قرارداد، مهم‌ترین مجازات قابل اعمال در نظام حقوقی این کشور در برابر اشخاص حقوقی جریمه است (کیوتو ۱۳۸۲: ۱۸۰). در حقوق جزای آمریکا، به خاطر پیچیدگی بیشتر حیات اجتماعی، شرکت‌های بزرگ صنعتی و تجارتنی نمود و اهمیت فوق‌العاده‌ای به دست آورده‌اند؛ به همین خاطر مسئولیت جزایی اشخاص حقوقی از دیرباز پذیرفته شده است (گلدوزیان ۱۳۹۱: ۱۳). اما مسئولیت کیفری به‌عنوان یک مفهوم حقوقی چه ارتباطی با سایر موارد مسئولیت دارد؟ پاسخ این سؤال در گرو 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 وارد کردن زیان، مخاطب پاسخ نیز یا جامعه است یا زیان دیده و هدف از آن هم یا بازدارندگی و تنبیه شخص مسئول است یا به حالت اول برگرداندن وضعیت زیان دیده. 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 (بادینی ۱۳۸۴: ۵۹) 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

تفکیک شده‌اند، به طور 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: 173). 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 (گلدوزیان ۱۳۸۷: ۴۰) علاوه بر این قلمرو آن در مسئولیت نیز باهم متفاوت است، پاره‌ای از جرایم باینکه 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

به موجب ماده ۲ طرح ارائه شده از جانب کمیسیون حقوق بین‌الملل در زمینه مسئولیت بین‌المللی دولت‌ها تخلف بین‌المللی یک دولت زمانی محرز می‌شود که فعل یا ترک فعل تشکیل دهنده 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 آن که اقدام خاصی به عنوان 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. (مارینا، ۱۳۸۵: ۷۷). در واقع باید توجه داشت که ویژگی جنایات بین‌المللی به گونه‌ای است که اشخاص حقوقی به ویژه دولت‌ها در انجام آن‌ها توانا ترند، 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 (عالی پور، ۱۳۹۰: ۲۳۷)، به‌رحال 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 نه 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 در واقع 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 محیط 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، به هر حال 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, 2009: 24). البته این دو مسئولیت عواقب یکسانی ندارند، به هر حال 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 (op.cit: 24). در هر حال شناخت اشتراکات و ارتباط میان مسئولیت اشخاص بررسی مبانی مسئولیت در این زمینه است.

۵. عوامل رافع مسئولیت کیفری در محیط سایبری

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 شده‌است، 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 (حیب زاده، ۱۳۸۴: ۴۲-۴۱)، 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 (جعفری لنگرودی، ۱۳۸۶: ۶۴۲)، 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 موجه 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. درحالی‌که علل مشروعیت ناشی از عوامل و شرایط خارجی است و قائم بر واقعه‌ای است که باعث حذف وصف مجرمانه از عمل مرتکب خواهد شد، ضمن آنکه خصوصیات جسمی و روانی مجرم در آن نقشی ندارد (شامبیاتی، ص ۳۱۴)، 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 درحالی‌که علل مشروعیت نسبت به کلیه شرکت‌کنندگان در جرم قابل‌اعمال 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 نه تنها 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 (رحمان پور، ص ۹۲-۹۱).

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 محیط سایبری 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 محیط سایبری همان عوامل کلی رافع مسئولیت جزایی هستند که معمولاً در متون حقوق کیفری عمومی موردبررسی قرار می‌گیرند.

برآمد

استفاده از ابزارها و وسایل نوین ارتباطی خصوصاً محیط سایبر و اینترنت، فرصت‌های جدید برای ارتکاب جرم مجرمین به وجود آورده است، در همین راستا چنانچه حقوق کیفری در درون هر جامعه‌ای نتواند متناسب با این پیشرفت‌ها تغییر پیدا کند، تبعاً جرایم و

بزهکاری‌های زیادی به وجود می‌آید که بدون مجازات باقی خواهند ماند، شاید بتوان گفت که مهم‌ترین ابزارهایی که برای مبارزه با جرایم نوین در برابر حقوق جزا وجود دارد. راهکارهایی مانند جرم‌انگاری، ایجاد و توسعه مسئولیت کیفری، استفاده از راهکارهای نوین حل اختلاف و مجازات‌های نوین و... است، در رابطه با مسئولیت کیفری در جرایم سایبری قانون‌گذار ایران اقدام به توسعه و گسترش مسئولیت کیفری در برابر اشخاص حقوقی نموده است. تا قبل از تصویب قانون فوق‌الذکر بحث مسئولیت کیفری اشخاص حقوقی در قوانین کیفری ایران چندان مطرح نشده بود و قانون جرایم رایانه‌ای نخستین بار این موضوع یعنی مسئولیت کیفری اشخاص حقوقی را مورد پذیرش قرار داده است، می‌دانیم بسیاری از جرایم رایانه‌ای معمولاً توسط اشخاص حقوقی واقع می‌شوند و این اقدام قانون‌گذار ایران در رابطه با ایجاد مسئولیت کیفری برای این اشخاص امری کاملاً طبیعی بوده و در واقع استفاده از ابزار گسترش مسئولیت کیفری برای مبارزه با جرایم جدید است، البته باید اذعان داشت که:

الف: مسئولیت کیفری اشخاص حقوقی به معنای نفی مسئولیت اشخاص حقیقی نیست.

ب: مسئولیت کیفری شخص حقوقی مانعی بر سر راه اعمال مجازات بر اشخاص حقیقی ایجاد نمی‌کند.

و در نهایت باید گفت در باب عوامل رافع مسئولیت کیفری در محیط سایبر این علل تابع عوامل کلی رافع مسئولیت می‌باشند، عواملی مانند کودکی و جنون از این موارد محسوب می‌شوند.

منابع

- اردبیلی، محمدعلی (۱۳۸۷)، حقوق جزای عمومی، ج ۲، تهران، میزان، چاپ نوزدهم.
- بادینی، حسن (۱۳۸۴)، فلسفه مسئولیت مدنی، تهران، شرکت سهامی انتشار.
- جعفری لنگرودی (۱۳۸۶)، محمدجعفر، ترمینولوژی حقوق، تهران، گنج دانش، ش ۵۱۲۰.
- حبیب زاده، محمدجعفر، فخربناب، حسین (۱۳۸۴)، «مقایسه عوامل موجه جرم و عوامل رافع مسئولیت کیفری»، تهران، نشریه مدرس علوم انسانی، پائیز، ش ۴۰.
- حلمی، نصرت اله (۱۳۹۰)، مسئولیت بین‌المللی دولت و حمایت سیاسی، تهران، میزان، چاپ.
- دیانا هولمز (۱۳۷۷)، آشنایی با تکنولوژی اطلاعاتی، ترجمه دکتر مجید آذرخش و دکتر جعفر مهرداد، انتشارات سمت، تهران، چاپ اول.
- رحمان پور، ابوطالب (۱۳۹۲)، مسئولیت کیفری اشخاص حقوقی، تهران، دانشگاه امام حسین. شامبیاتی، هوشنگ (۱۳۸۸)، حقوق جزای عمومی، تهران، مجد، چاپ پانزدهم.
- طاهری جبلی، محسن (۱۳۷۲)، «جرم و رایانه»، تهران، مجله حقوقی دادگستری، زمستان، شماره ۹.
- عالی پور، حسن (۱۳۹۰)، «دیوان کیفری بین‌الملل و چالش مسئولیت اشخاص حقوقی»، مجموعه مقالات حقوق کیفری بین‌الملل فرایند نظریات و چشم‌اندازها، تهران، میزان.
- کاتوزیان، ناصر (۱۳۸۷)، الزام‌های خارج از قرارداد مسئولیت مدنی، ج ۱، تهران، انتشارات دانشگاه تهران، چاپ هشتم.
- مارینا، اسپیندی (۱۳۸۵)، «پیرامون امکان ارتکاب جرم از سوی دولت و مسئولیت کیفری او» مترجم، هنجی، علی، تهران، محله تحقیقات قانونی دانشگاه شهید بهشتی، پائیز و زمستان، شماره ۴۴.
- خامی، محسن (۱۳۸۳)، «نگاهی کلی به جرم‌های رایانه‌ای»، تهران، مجله اصلاح و تربیت، سال سوم، دی، شماره ۳۴.
- هاشمی، محمد (۱۳۸۴)، حقوق بشرو آزادی‌های اساسی، تهران، انتشارات میزان.

- Bonafe, Beatric, *The Relationship Between State and Individual Responsibility for International Crimes* Hague, martinus nijhoff pub: 2009, p ۲۴.
- Wilson, Luke Andrew, *Theaters of intention: drama and the law in early modern England*, Stanford University Press, 2000, p 173.
- Madhava Soma, Umarhathab, Sundaram, Syed, *Cyber Crime and Digital Disorder*, New Delhi Tamil nadu, K. Jaishankar pub: 2011, p 21.
- McEwen, J. Thomas, *Dedicated Computer Crime Units*, DIANE Publishing, 1989, p1.
- Section 202c, *Acts preparatory to data espionage and phishing*, (1) Whosoever
- Atul, Jain, *Cyber Crime: Cyber crime: issues and threats*, Gyan Publishing House, 2005, p 121.
- W. Brenner, Susan, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, University Press of New England, 2012, p21.
- Jeff B. Zhang, *Accusing the American Judicial System of Rampant Corruption*, Pittsburg Pennsylvania, Dorrance Publishing, 2011, p 489.
- Davi D'Agostino, Greg Wilshusen, *Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities*, DIANE Publishing, 2011, p 28.
- Ploug, Thomas, *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction*, Ballerup Denmark, Springer pub: 2009.
- <http://www.modiryar.com>
- <http://penology.blogfa.com/post-208.aspx>
- <http://www.itna.ir/vdcdsj0f.yt0xz6a22y.html>