

گفت و گو

امروزه هستند انسان هایی که بیش از آن چه در فضای حقیقی زندگی می کنند، اوقات خود را در فضای مجازی می گذرانند. زندگی در این فضا، ارتباط انسان ها را در پی دارد و به نظم درآوردن روابط افراد، مقررات، ضوابط و ضمانت اجراهای خاص خود را می طلبد. تدوین این مقررات یکی از مسایل بیش زوی نظام های حقوقی دنیا است. قانون گذار ایران نیز در سال های اخیر قوانینی در این زمینه تصویب کرده است؛ قانون تجارت الکترونیکی در سال ۱۳۸۲ به تنظیم روابط تجاری در فضای سایبر پرداخت و قانون جرایم رایانه ای مصوب ۱۳۸۸ جرم انگاری رفتارهای قابل ارتکاب در این فضا و آیین دادرسی خاص این جرایم را مد نظر قرار داد. تازگی ناشناخته بودن و جذابیت فضای مجازی در ارتباط با حقوق، موجب شد به بررسی و تحلیل گام های قانون گذار ایران در مقایسه با سایر کشورها و اسناد بین المللی در این زمینه بپردازیم.

دکتر علی حسین نجفی ابرندآبادی، عضو هیات علمی دانشکده حقوق دانشگاه شهید بهشتی، جنبه ی جرم شناسی بحث را توضیح می دهند و بخش تجارت الکترونیکی را نیز از زبان دکتر ستار زر کلام و آقای سیامک قاجار قبولو می شنویم.



پریاره

بزه کاری و جرم شناسی سایبری

جرم انگاری نقض ارزش های جدیدی است که اختراعات و اکتشافات بشری برای جوامع انسانی به ارمغان آورده است. به تعبیر استاد دلماس-مارتی، جرم انگاری نقض این ارزش ها که در حقیقت حمایت کیفری از ارزش های فنی محسوب می شود، حاکی از مدرن و متحول شدن جامعه است. حقوق کیفری به ویژه در بخش حقوق کیفری اختصاصی، حقوق ارزش ها، باورها و اعتقادات هر جامعه ی بشری است. قانون گذار، به منظور حفظ مصالح اجتماعی، سیاسی، اقتصادی و فرهنگی جامعه ی متحول، ناگزیر از تصویب قوانین کیفری است. بی جهت نیست که گفته اند، چنان چه می خواهید بینید یک جامعه در چه مرحله ای از تحول قرار دارد و باورها و ماهیت آن جامعه چیست، به بخش اختصاصی حقوق کیفری آن جامعه رجوع کنید. بر این اساس می توان گفت وضع جرایم فنی در هر جامعه حکایت از مدرن شدن آن جامعه و ورود فن آوری ها و علوم جدید در آن دارد. بدین ترتیب، فضای مجازی (سایبری) نیز در فنی شدن بزه کاری نقش مهمی دارد. در جرایم فنی عنصر معنوی یا سوء نیت مستتر است. در واقع، یک جرم مادی مطلق محسوب می شود. زیرا صاحبان مشاغل صنعتی و فنی - یعنی مرتکبان بالقوه ی جرایم فنی - همگی متخصص و دوره دیده هستند و فرض بر این است که آموزش ها و کارآموزی های تخصصی لازم را گذرانده اند. به همین جهت گفته می شود که فنی شدن حقوق کیفری اختصاصی با مادی شدن جرایم آن همراه است.

**تعالی حقوق: آیا فنی شدن جرایم با ایجاد و توسعه ی فضای سایبر مرتبط است؟
دکتر نجفی ابرندآبادی: از نشریه تعالی حقوق تشکر می کنم که زمینه ی گفت و گو درباره ی موضوع هایی را فراهم کرده است که بحث روز حقوق کیفری و جرم شناسی نه تنها در ایران، بلکه در اغلب کشورهای جهان است. قانون گذار ایران در خرداد ۱۳۸۸، یعنی حدود سه ماه پیش، با تصویب قانون جرایم رایانه ای زمینه ی مبارزه ی کیفری با مظاهر بزه کاری سایبری را از نظر شکلی (مقررات آیین دادرسی خاص از مواد ۲۸ تا ۵۱) و ماهوی (جرایم سایبری و مجازات های مربوط از مواد ۱ تا ۲۷) فراهم نمود. به موازات گسترش فن آوری های نوین اطلاعات و ارتباطات و گسترش استفاده از آن ها، کشورها شاهد ظهور نسل جدیدی از جرایم، بزه کاران و بزه دیدگان هستند که شناخت آن ها، مطالعات جرم شناختی جدیدی را می طلبد. بدین ترتیب، حقوق کیفری سایبری و جرم شناسی سایبری در قلمروارشته مطالعاتی نوپا به ویژه در کشور ما هستند. تصویب قانون جرایم رایانه ای مصوب ۱۳۸۸ و رویه قضایی که به تدریج به استناد مفاد این قانون ایجاد و صادر خواهد شد، بی تردید، فصل های پژوهشی نوینی را در حقوق کیفری اختصاصی و عمومی، آیین دادرسی کیفری و حتی جرم شناسی و بزه دیده شناسی سایبری در ایران خواهد گشود. اما در مورد پرسش شما، فنی شدن جرایم در واقع ناظر به

۷
تاریخچه حقوق کیفری

جرم سایبری، اما، یک وصف یا عنوان کیفری وسیع است. اصطلاحی است که شامل جرائم ارتكابی در محیط مجازی اینترنتی و تاثیراتی می‌شود. این اصطلاح حدود دو دهه است که وارد ادبیات حقوق جزایی شده است. در سطح بین‌المللی، مهم‌ترین سند در این زمینه، کنوانسیون جرائم سایبری شورای اروپا است که در سال ۲۰۰۱ به تصویب رسیده است. بخش مهمی از این سند به تعریف انواع جرائم سایبری اختصاص داده شده است و تا آن جا که اطلاع دارم، تهیه کنندگان قانون جرائم رایانه‌ای از متن و وصف‌های کیفری این کنوانسیون نیز الهام گرفته‌اند. جرائم سایبری، از یک سو جرائم ویژه فضای مجازی را دربرمی‌گیرد و از سوی دیگر، شامل جرائم متعارض می‌شود که در فضای مجازی، از جمله با کمک رایانه و اینترنت ارتکاب می‌یابد.

تعبیر دیگری که در این خصوص، بیشتر در جرم‌شناسی، به کار برده می‌شود، بزهکاری سایبری یا بزهکاری الکترونیکی است که در حقیقت شامل جرایمی می‌شود که امکان ارتکاب در شبکه‌های رایانه‌ای و انفورماتیک - به ویژه شبکه‌ی اینترنتی - را پیدا می‌کنند. این نوع بزهکاری معمولاً به دو شاخه تقسیم می‌شود:

۱- جرایمی که سامانه‌ی فن آوری‌های اطلاعات و رایانه موضوع آن‌ها هستند؛

۲- جرائم عادی و کلاسیک که توسط شبکه‌های الکترونیکی یا از طریق و به کمک آن‌ها ارتکاب می‌یابند (مانند توهین، افتراء، جرائم علیه کرامت انسانی، جرائم علیه قوانین و مقررات مربوط به مالکیت فکری و هنری، جرائم مطبوعاتی). لذا بزهکاری سایبری اعم از جرائم اینترنتی است.

تعالی حقوق: به طور کلی، در خصوص جرائم و حقوق کیفری سایبری توضیح دهید.

دکتر نجفی ابرندآبادی: اصولاً با دسترسی به فضای مجازی یا سایبر، انسان‌های سده بیست‌ویکم در دو جهان زندگی می‌کنند؛ جهان واقعی یا حقیقی و جهان مجازی یا سایبری.

امروزه انسان‌ها، بسته به میزان پیشرفت و ترقی جوامع، گاه بیشتر در فضای مجازی زندگی می‌کنند تا در فضای حقیقی، چندان که اگر از نسل انسان‌های سایبری صحبت کنیم، اغراق نکرده‌ایم. انسان‌هایی که بخشی از فرایند اجتماعی شدن و جامعه‌پذیری آن‌ها - در قالب کارتر اینترنت و به طور کلی فضای سایبر - محقق شده است، انسان‌هایی که همسر آینده، دوست، اوقات فراغت، مطالعات، منابع تحصیلی و حتی پایان‌نامه‌ی خود را در فضای سایبر جست‌وجو می‌کنند، انسان‌هایی که خرید و فروش، مسافرت‌ها، جابه‌جایی‌ها، بلیت‌ها، پرداخت پول و بسیاری از فعالیت‌های دیگر خود (از جمله آموزش) را از طریق اینترنت انجام می‌دهند و تهیه می‌کنند. کافی است، نسل انسان‌های سایبری را از نظر رفتار، گفتار، آداب و رسوم و عادات روزانه با نسل انسان‌هایی که بیشتر محصول تربیت و آموزش دنیای واقعی هستند، مقایسه کنیم، آن گاه تفاوت‌ها آشکار می‌شود. بنابراین، یکی از محیط‌های موثر در جامعه‌پذیری انسان‌های امروزی، فضا یا جهان سایبری است.

از نظر جامعه‌شناسی، انسان‌های قرن بیست‌ویکم پیوندها و محیط‌های معاشرتی خود را در دو جهان واقعی و مجازی جست‌وجو

می‌کنند و فرایند جامعه‌پذیری آنان در این دو محیط محقق می‌شود. بدین ترتیب، فضای محاری همان طور که فرصت‌ها و موقعیت‌های مستقر و سارنده‌ی برای بشریت سر سده‌ی سست و یکم - وجود آورده است، ارتباطات و زندگی را تسهیل کرده است، به همان میزان نیز می‌تواند وسیله‌ای برای ارتکاب جرائم متعارف، فضایی برای محرم شدن یا بزه‌دیده واقع شدن، و محیطی برای ارتکاب جرائم جدید (سایبری) نیز شده است. به همین جهت، همان‌طور که پیش‌تر بیان شد، امروزه در سطح بین‌المللی و نیز در حقوق داخلی قوانین و مقررات کیفری شکلی ماهوی خاص جرائم سایبری تصویب شده و می‌شود که عنوان «حقوق کیفری سایبری» رایانه‌ای یا حقوق کیفری فن آوری‌های نوین اطلاعات و ارتباطات» به آن داده شده است.

تعالی حقوق: تاثیر اینترنت به عنوان رایج ترین و شناخته شده ترین فضای سایبری بر بزهکاری چیست؟

دکتر نجفی ابرندآبادی: این سؤال ما را به طرح بحث‌های جرم‌شناختی هدایت می‌کند. همان‌طور که می‌دانیم نظریه‌ها، اصول و راهکارهای جرم‌شناسی در ستر، فضا و جهان واقعی و انسان‌های محصول این فضا و جهان شکل گرفته و متحول شده است به عنوان مثال، وقتی ادوین ساترلند، جامعه‌شناس آمریکایی، برای تبیین بزه‌کاری، نظریه‌ی «معاشرت‌های ترجیحی» را ارائه نمود، او به اقتضای زمان خود (اواسط سده‌ی بیستم) از محیط‌هایی چون خانواده، مدرسه، محله، پارک، کلوب ورزشی و غیره یاد می‌کند و معتقد است که چنانچه محیط‌های معاشرتی ترجیحی فرد، محیط‌های متحرک‌تر باشد، یعنی شخص رفت‌وآمد به این محیط‌ها را به بیوند با محیط‌های متعارف ترجیح دهد، به سمت انحراف و جرم خواهد رفت. آیا در آغاز هزاره‌ی سوم، این نظریه برای تبیین بزه‌کاری هم‌چنان اعتبار دارد؟ یا باید آن را با توجه به دوگانه شدن محیط‌ها مورد بازبینی قرار داد؟

پیش‌تر از انسان‌های سایبری سخن به میان آمد، یعنی انسان‌هایی که در پرتو فضاهای مجازی رشد کرده و شکل گرفته‌اند. با توجه به این واقعیت، نظریه‌های جرم‌شناختی نیز باید در چارچوب محیط‌های سایبری و تاثیر آن‌ها بر جرم، بررسی شوند. به طور کلی، دو دیدگاه راجع به تاثیر اینترنت و به طور کلی محیط سایبری بر جرم مطرح شده است.

دیدگاه اول: بر اساس این دیدگاه، اینترنت که از اواسط دهه‌ی ۱۹۹۰ میلادی گسترش یافته و امروزه در سطح وسیعی رایج شده است، می‌تواند دست کم به سه دلیل موجب کاهش جرائم متعارف و کلاسیک به ویژه جرائم خرد که بیشتر توسط نوجوانان ارتکاب می‌یابد، شود:

دلیل اول: اینترنت، شیوه و عادت زندگی انسان امروزی را عمیقاً تغییر داده است، چندان که در خانواده‌ها، معمولاً اعضای خانواده، هر یک رایانه‌ی خود را دارد؛ در هر خانه، حداقل یک رایانه وجود دارد. مطالعات نشان داده است که اینترنت بیش از پیش موجب کاهش ساعات اختصاص یافته‌ی به سایر فعالیت‌ها مانند تماشای تلویزیون، خواندن روزنامه، گوش دادن به رادیو، مطالعه (به طور کلی)، خواب و غیره شده است. اینترنت موجب شده است که افراد، به تعبیر جامعه‌شناسان، تحرک کمتری داشته باشند و بیش از گذشته یک‌جا نشین شوند. اشخاص از طریق اینترنت عمده‌ی نیازهای خود را برآورده



می‌کنند بنابراین به رفت‌وآمد و تحرک تیزی ندارند. نمود خرابه‌جایی و تحرک سب می‌شود که از یک سو، مناسبت بزه دیده واقع شدن آن‌ها در سطح جامعه کمتر شود و از سوی دیگر، فرصت تعارض و اصطکاک متوقع با دیگران و بنابراین مجرم شدن کاهش یابد، چون عمدی وقت روزانه‌ی خود را در خانه کافی‌نت، محیط کار و حتی پس از پایان ساعات کار در برابر صفحه‌ی رایانه و سایت‌های اینترنتی سپری می‌کنند.

دلیل دوم: غالباً این احساس در کاربر اینترنت وجود دارد که در جهان مجازی ناشناخته باقی می‌ماند و بنابراین می‌تواند هر کاری را بدون بیم از شناخته شدن و تحمل آثار آن انجام دهد. اما بر خلاف این احساس، کاربر در محیط سایبر در نهایت قابل ردیابی و نظارت است. بدین معنا که در صورت لزوم کارشناسان رایانه و اینترنت می‌توانند رفتارهای کاربر را در فضای اینترنت ردیابی نموده و شناسایی کنند. در فضای سایبر هیچ اثر و ردی نماند نمی‌شود. لذا اگر چه احساس ناشناختگی در فضای سایبر برای فرد به‌وجود می‌آید اما از آن جا که در واقع امکان ردیابی و شناسایی وجود دارد افراد با کسب اطلاع تدریجی از این واقعیت کمتر ریسک ارتکاب جرم در این فضا را می‌پذیرند به عبارت دیگر، شناسایی و ردیابی شدن، به رغم ناشناختگی ظاهری، تا اندازه‌ای نقش بارز دارند.

دلیل سوم: فضای سایبر، به طور کلی و اینترنت به طور خاص، فضای اطلاعات و ارتباطات است. در این فضا کاربر می‌تواند بسته به نوع علاقه و نیاز خود، هرگونه اطلاعات را سریع به دست آورد. از جمله از طریق این فضا است که کاربران بیش از پیش با هشدارهای پیشگیرانه، به ویژه پیشگیری فنی، وضعی از وقایع مجرمانه آشنا می‌شوند. ما توجه به این هشدارها است که خود را در مقابل جرایم سایبری مصون می‌کنند به عبارت دیگر، فضای ارتباطی - اطلاعاتی اینترنت، به لحاظ تنوع، می‌تواند به کاربران خود اطلاعات جرم شناختی (فرایند بزهکاری و بزهکار شدن، فرایند بزه‌بینی و واقع شدن، تدبیرهای پیشگیرنده و چگونگی پیشگیری از جرم و...) را به زبان ساده ارائه دهد.

دیدگاه دوم: در مقابل دیدگاه نخست، عده‌ای از جرم‌شناسان معتقدند که فضای اینترنت زمینه‌ی ارتکاب جرایم جنینی تحت عنوان جرایم خاص سایبری را فراهم کرده و به طور کلی، شکل و نحوه‌ی ارتکاب جرایم را تغییر داده است. از جمله جرایم خاصی که در فضای اینترنت ارتکاب می‌راند، می‌توان به استeganography یا «لایه پوششی» اشاره کرد. مرتکب، یک پیام مجرمانه یا اطلاعات مجرمانه و مهم را به صورت غیرمجاز در لایه‌ی یک تصویر، یک پیام یا سند قلبونی و مجز پنهن و ارسال می‌کند. به گونه‌ای که مخاطب بتواند با اطلاعات کلی که در در روی تصویر، پیام، نامه یا سند، اطلاعات و پیام مخفی شده را شناسایی کند و آن‌ها را که به صورت پراکنده پخش شده

است، کنار هم بگذارد و در نهایت متن پیام را دریافت کند.

جرم دیگری که خاص فضای سایبر است، رخنه کردن و ورود غیر مجاز به فضای دیگری یا هکینگ است که نوع شدیدتر آن کراکینگ نام دارد. در عمل رخنه کردن، افراد با ورود غیرمجاز به فضاها، حساب‌ها و اطلاعات خصوصی افراد و اشخاص حقوقی در دنیای مجازی، مرتکب جرم علیه آن‌ها می‌شوند. نمونه‌ی دیگر جرایم سایبری به معنای موسع و ازه، حمله‌های سایبری و میکرسی علیه پایگاه‌های (سایت‌های) خدماتی در فضای مجازی است. چنان‌که پایگاه هدف حمله در ارائه‌ی خدمات به کاربران و متقاضیان خود دچار مشکل عمده شوند مرتکب با ارسال تقاضاهای صوری به سایت ارائه دهنده‌ی خدمات سایبری موجب ایجاد ترافیک و شلوغی صوری می‌شود و از این رهگنر ظرفیت خدمات دهی سایت را به متقاضیان، مشتریان و کاربران واقعی خود خنثی و دست کم کند و محدود می‌کند. این حمله یا تعرض مجرمانه ممکن است از طریق منابع مختلف و متعدد علیه یک سایت صورت گیرد و در نهایت مانع از جریان عادی کار آن شود. بدین ترتیب، می‌توانیم در کنار نسل انسان‌های سایبری، از نسل مجرمین سایبری یاد کنیم که نظریه‌های جرم‌شناسی کلاسیک هنوز از تبیین و گونه‌شناسی آن‌ها ناتوان است. به عنوان مثال در برخورد با مجرمین سایبری این سؤال مطرح است که آیا بزهکاران سایبری، بقیه‌ای هستند یا بقیه سفید؟ آیا بزهکاران سایبری متعلق به طبقات بالای جامعه هستند یا متعلق به همه طبقات جامعه؟ آیا همه بزهکاران سایبری دارای تحصیلات دانشگاهی هستند؟ آیا بیشتر بزهکاران سایبری نوجوان و جوان هستند؟ انگیزه‌ی ارتکاب جرایم سایبری همان انگیزه‌ی متعارف مجرمانه است؟ آیا برنامه‌های بالینی بازپروری بزهکاران کلاسیک و سنتی نسبت به بزهکاران سایبری نیز قابل اعمال است؟ آیا برنامه‌های کلاسیک پیشگیری از جرم، به شرحی که با آن آشنا هستیم، در قبال جرایم سایبری، به ویژه جرایم اینترنتی، قابل اعمال است؟ بزه‌دیدگان جرایم سایبری از چه قشری از جامعه هستند؟ آیا در بزه دیدگی خود نقش دارند؟ ...

این‌ها، سوالات عمده‌ای هستند که مطالعات جرایم سایبری باید به آن‌ها پاسخ دهند. همان‌طور که امروزه ما بی‌نیاز از حقوق کیفری سایبری یا حقوق کیفری فن‌آوری‌های اطلاعات و ارتباطات نیستیم، از جرم‌شناسی و بزه دیده شناسی سایبری نیز بی‌نیاز نخواهیم بود. مفاهیمی چون امنیت، آزادی، اعتماد، فرصت، رفتار و ... در فضا و محیط مجازی در مقایسه با فضای عادی، معانی و ابعاد متفاوتی به خود می‌گیرند. به این ترتیب است که فضای سایبری دست کم تحت سه عنوان در جرم‌شناسی قابل مطالعه است: ۱- فرصت‌های جنایی (تأمین وسایل جدید ارتکاب جرم و نیز آماج‌های جدید برای مجرمان)، ۲- فرصت‌های کنترل و پیشگیری از جرم (گونه‌های فنی

1- steganography

2- Hacking

3- Cracking

هکرها و کراکرها معمولاً به سه انگیزه مرتکب اعمال مجرمانه می‌شوند: انگیزه‌های تفریحی و ماجراجویانه، انگیزه‌های سودجویانه و انگیزه‌های راهبردی. منظور از انگیزه‌های اخیر (راهبردی) این است که جرم معمولاً به حساب و به نفع یک موسسه‌ی خصوصی، عمومی و حتی یک دولت یا نهاد خاص دولتی ارتکاب می‌یابد. یعنی مرتکب به دنبال یک سفارش، عمل مجرمانه سایبری را مرتکب می‌شود.

4- Denial of Services Attacks Distributed Denial of Services Attacks (DOS/DDOS)

۱۲۸

سایبر

نظارت و پیشگیری و کسب اطلاعات پلیسی)، و ۳- امنیت-نامنی. یک جرم شناس هندی به نام «کارویانان جایشانکار»^۱ که مجله بین‌المللی جرم‌شناسی سایبری^۲ را نیز اخیراً تاسیس کرده است، با طرح نظریه «تغییر و گذر محیطی»^۳ معتقد است که رفتار و کردار افراد با گذر از محیط واقعی به فضای سایبری تغییر می‌کند و این تفاوت رفتار با تغییر فضا و محیط است که علل بزهکاری در فضای مجازی را تشکیل می‌دهد. به عبارت دیگر، این تغییر محیط و فضا است که موجب تغییر رفتار افراد می‌شود. «جایشانکار» هفت رکن را برای این نظریه برشمرده است: ۱- اشخاصی که گرایش‌های مجرمانه‌ی خود را در فضای حقیقی مهار و کنترل کرده‌اند، تمایل به ارتکاب جرم با جرایمی در فضای سایبری دارند که، به لحاظ موقعیت و جایگاه اجتماعی خود، نتوانسته‌اند در محیط حقیقی مرتکب شوند؛ ۲- تغییر هویت، ناشناختگی در فضای سایبری که شناسایی فرد را دشوار می‌کند و نبود عوامل بازدارنده در این فضا، به بزهکار اجازه می‌دهد تا ارتکاب جرم در چنین محیطی را برگزیند؛ ۳- رفتار مجرمانه‌ی بزهکاران در فضای سایبری مستعد انتقال به فضای واقعی و بر عکس، از این فضا به محیط مجازی است؛ ۴- ویژگی نامستمر رفتار مجرمانه‌ی بزهکاران در فضای سایبری و ماهیت مکانی-زمانی پویای این فضا می‌تواند موجب فرار بزهکاران سایبری از تعقیب کیفری و مجازات بشود؛ ۵- اشخاص بیگانه نسبت به یکدیگر، می‌توانند در فضای سایبری-به منظور ارتکاب جرم در فضای حقیقی- دوست و متحد شوند و برعکس، بزهکاران در محیط واقعی می‌توانند برای ارتکاب جرم در فضای مجازی با هم متحد گردند و مشارکت کنند؛ ۶- اشخاص متعلق به «جوامع بسته» بیشتر از مردمان متعلق به جوامع باز مستعد ارتکاب جرم در فضای مجازی هستند؛ ۷- تعارض میان هنجارها و ارزش‌های محیط واقعی و فضای مجازی می‌تواند منجر به بزهکاری سایبری شود.

فرصت نقد این نظریه، در گفت‌وگوی ما وجود ندارد، ولی آن‌چه قابل تأکید است، «فرصت‌های مجرمانه‌ی جدیدی» است که فضای مجازی برای بزهکاران فراهم می‌کند. این امر، خود تأییدی بر دیدگاه دوم در جرم‌شناسی سایبری است. نظریه «عبور و گذر از یک فضا به فضای دیگر» با نظریه «تغییر فضا و مکان»، خود نمودی از این جرم‌شناسی است که در حال شکل‌گیری می‌باشد.

✽✽✽ تعالی حقوق: اینترنت و فضای سایبر می‌تواند هم فرصت و هم تهدید باشد. چگونه می‌توان اینترنت را از تهدید به فرصت تبدیل کرد؟

دکتر نجفی ابرندآبادی: سوال جالبی است، ولی پاسخ به آن، در عین حال دشوار. اگر بیست سال پیش صحبت از دهکده‌ی جهانی و جهانی شدن بود، امروزه به لطف فن‌آوری‌های جدید ارتباطات و اطلاعات، فضای سایبر و به ویژه اینترنت، صحبت از انسان‌های جهانی شده می‌شود. اصطلاح انسان‌های جهانی شده در بحث ما به این معنا است که جمعیت کره‌ی زمین که بیش از یک چهارم آن به اینترنت وصل هستند و از خدمات آن استفاده می‌کنند، می‌توانند از طریق فضاهای سایبری در هر لحظه از آن چه که در آن سوی دنیا می‌گذرد

مطلع و متأثر شوند و واکنش نشان دهند، فضای مجازی، به ویژه اینترنت، مرز سیاسی نمی‌شناسد. اینترنت، فضای جهانی است که به رغم ایجاد بنسب سایبری و اینترنتی، به رغم ایجاد انواع وسایل نظارتی، هم چنان محل رویت و خواندن و پیدا کردن انواع تصاویر و اطلاعاتی است که در دنیای واقعی سانسور شده است. اینترنت، بی‌گمان انسان‌های دارای تابعیت و فرهنگ مختلف را به هم نزدیک کرده است. این نیز یک واقعیت جهانی است که شهروندان کشورها، بسته به نوع جامعه و میزان ارتباط آن‌ها با فضای سایبری، در معرض آثار مضر و مخاطره‌آمیز این فضا نیز قرار دارند. به عنوان مثال، در ارتباط با پیامدهای مخاطره‌آمیز استفاده از اینترنت برای کودکان و نوجوانان، می‌توان گفت که یک مادر انگلیسی به همان میزان نگران تربیت و آینده‌ی فرزند کاربر اینترنت خود است که یک مادر هندی. نوجوان امروز به عنوان کاربر اینترنت، روزانه ساعتی را که باید در کنار والدین و اعضای خانواده‌ی خود بگذراند و از این طریق به طور ملموس و واقعی جامعه پذیر و اجتماعی شود، در برابر اینترنت سپری می‌کند و مطالب و تصاویری را می‌خواند و می‌بیند که خود دوست دارد و نسبت به آن‌ها علاقه پیدا می‌کند، بدون این که لزوماً از تأثیر آن پیام‌ها و تصاویر آگاه باشد. در چنین بستری است که آموزش همراه با نظارت به کودکان و نوجوانان می‌تواند کارساز باشد. آموزش، یک نوع پیشگیری اجتماعی از مجرم شدن است و نظارت، در واقع کنترل سایت‌هایی است که مطالب و تصاویر منحرفانه و گمراه کننده را ترویج می‌کنند. اما کارسازترین روش برای مصون کردن نسل سایبری در برابر آثار سوء، اینترنت، آموزش آنان است، نه محدود کردن کردن استفاده از فن‌آوری نوین اطلاعات و ارتباطات، چنان‌که پیش بینی یک ماده‌ی درسی در دوره‌های تحصیلی راهنمایی و دبیرستان تحت عنوان «آشنایی با فرهنگ و فضای اینترنت»، یا «کاربری در فضای فرهنگی اینترنت» می‌تواند مفید واقع شود. امروزه، غالب کودکان و نوجوانان به ویژه در جوامع بسته- به صورت خودجوش و به دور از نگاه و مراقبت والدین، کنجکاو‌ها، سوال‌ها و نیازهای اطلاعاتی خود را در فضای اینترنت جست‌وجو، مطرح و تأمین می‌کنند. این آموزش، باید به صورت شفاف و ملموس با نمایش جنبه‌های مثبت و منفی اینترنت همراه باشد. همان‌طور که برای هر حرفه‌ای نوعی اخلاق فنی و خاص آن حرفه تعریف و آموزش داده می‌شود، در چارچوب این ماده‌ی درسی نیز می‌توان ضمن آموزش رایانه، فضای سایبر و به ویژه فرهنگ و نوع داده‌ها و اطلاعات در اینترنت، سلوک اخلاقی استفاده از اینترنت، یعنی «مدنیّت اینترنتی» را نیز آموزش داد. این اقدام، به تعبیر جرم‌شناسی، یک گونه پیشگیری اجتماعی تخصصی از مجرم شدن در پیوند، معاشرت و تعامل با محیط‌های مجازی است. با این کار، هم کودکان و هم نوجوانان از مزایای اینترنت بهره می‌برند و هم تهدیدهایی که در کمین آن‌ها است، خنثی می‌شود. به طور کلی، از آن جا که بزهکاری سایبری بدون مرز است، جنبه‌ی فراملی دارد و یک تهدید جهانی برای کشورها و شهروندان آن‌ها است، مبارزه با مظاهر آن به همکاری بین‌المللی و هماهنگ سازی اقدام‌های پلیسی، قضایی و به طور کلی قوانین و مقررات دولت‌ها نیز نیاز دارد.

1- K. Jaishankar
 2- International Journal of Cyber Criminology/ www.cybercrimejournal.co.nr
 3- Spatial transition Theory (گذر عبور به فضا و محیط جدید)

۵۵ تعالی حقوق: بین جرایم کلاسیک و رایانه‌ای چه

تفاوتی است؟ آیا جرایم رایانه‌ای همان جرایم کلاسیک هستند که صرفاً با وسیله کامپیوتر و تلفن همراه ارتکاب می‌یابند یا این که تفاوت‌های دیگری بین این جرایم وجود دارد؟

دکتر نجفی ابرندآبادی: به مناسبت پاسخ به پرسش‌های

قبلی به این سوال به طور کلی پاسخ داده شد، اما از منظر جرم‌شناسی گاه جرایم کلاسیک مانند کلاهبرداری، جعل یا سرقت نسبت به مالکیت‌های ادبی و هنری از طریق اینترنت ارتکاب می‌یابد. در این حالت، اینترنت یک وسیله است. اینترنت با ایجاد این احساس که شخص در فضای آن ناشناخته است و هویت مشخصی ندارد، می‌تواند فرایند گذر از اندیشه و وسوسه مجرمانه به عمل مجرمانه را تسهیل نماید. گاه جرایم علیه داده‌ها، اطلاعات، خلوت و زندگی اشخاص در اینترنت ارتکاب می‌یابد (مانند رخنه‌گری - کراکینگ-هکینگ با حمله سایبری به منظور جلوگیری از ارائه خدمات به سایت یا برای از کار انداختن آن‌ها) به این ترتیب، رکن مادی جرم همراه با خشونت و زور نیست، بلکه بیش‌تر یک عمل فکری و فنی است. به همین جهت است که ادله اثبات این جرایم با ادله اثبات جرایم سنتی متفاوت است و آیین رسیدگی این جرایم از مقررات تخصصی و فنی پیروی می‌کند.

نکته قابل توجه دیگر در واقع بزه‌دیدگان جرایم خاص

اینترنتی هستند که ممکن است از اتباع کشورهای مختلف باشند، در کشورهای مختلف زندگی کنند و از نظر کمیت، شمار زیاد و توده‌ای از مردم را در برگیرند و برای مرتکب ناشناخته باشند. از همه مهم‌تر، بر خلاف جرایم کلاسیک، بزه‌دیدگان بسیاری از جرایم اینترنتی و به طور کلی سایبری، از مراتب بزه‌دیدگی و زیان‌دیدگی خود مطلع نمی‌شوند یا آن که ماه‌ها یا سال‌ها بعد از ارتکاب جرم، در جریان آن قرار می‌گیرند. بدین ترتیب اعلام جرم یا طرح شکایت مدت‌ها بعد از وقوع جرم صورت می‌گیرد. ضمن این که رقم سیاه این جرایم، یعنی تعداد جرایمی که از چشمان فرشته‌ی عدالت مخفی می‌ماند و تحت تعقیب رسیدگی کفیری قرار نمی‌گیرد بسیار بیشتر از جرایم متعارف است. امروزه فضای سایبر تبدیل به فرصتی برای ارتکاب جرایم تروریستی نیز شده است، چندان که به تعبیر کارشناسان در کنار جنگ‌های کلاسیک، امروزه دولت‌ها در قالب جنگ‌های اطلاعاتی سایبری و اینترنتی در مقابل یکدیگر قرار می‌گیرند. نمونه‌ای که این روزها در مطبوعات از آن صحبت می‌شود، جنگ سایبری و اینترنتی روسیه علیه گرجستان است که در تابستان ۱۳۸۷ رخ داد. بدین ترتیب روسیه بسیاری از مراکز و پایگاه‌های اینترنتی دولت گرجستان را از فعالیت و سرویس‌دهی خارج کرد، به گونه‌ای که فعالیت بعضی از نهادهای آن دولت با مشکل روبه‌رو شد. بنابراین، اینترنت افزون بر تغییر دادن رفتار و عادات روزانه و به طور کلی زندگی مردم، شکل و کیفیت روابط بین دولت‌ها و به طور کلی روابط بین‌المللی را نیز تحت الشعاع قرار داده است.

*** تعالی حقوق: امنیت اخلاقی اطلاعات در

فضای سایبر دغدغه‌ای است که امروزه در حوزه سایبر وجود دارد. به نظر جناب عالی این امنیت چگونه می‌تواند تامین گردد؟

دکتر نجفی ابرندآبادی: این سوال نیز جالب و پاسخ آن

نیز مشکل است. از این جهت جالب است که دغدغه‌ی مطرح شده در سوال، در فضای حقیقی نیز موضوعیت دارد. حریم خصوصی و خلوت افراد، امنیت یک کشور و سرزمین همواره توسط مجرم یا توسط دولت دیگر در معرض تهدید است. پاسخ به این سوال نیز مشکل است، چون فضای سایبر فضای جدیدی است. فضای حقیقی، عمر طولانی دارد و راهکارهایی برای خنثی کردن تهدیدهای آن به دست آمده و تجربه شده است، اما فضای سایبری و به ویژه اینترنت، عمری کوتاه دارد و جوان است. اینترنت در بیست سال اخیر گسترش یافته، همه گیر و استفاده‌ی از آن جهانی شده است، لذا در خصوص رفع و خنثی کردن تهدیدهای موجود در این فضا هنوز در آغاز کار قرار داریم. انسان سده‌ی بیست و یکم به تدریج در حال آشنا شدن با تهدیدها و فرصت‌های این فضا است. به همین جهت دولت‌ها به موارات استفاده از این فضا، به ویژه اینترنت، با وضع قوانین و مقررات، ایجاد پلیس و تربیت قضات ویژه، به دنبال راهکارهای خنثی‌کننده‌ی این تهدیدها هستند، اما نکته‌ای که باید روی آن تاکید کرد این است که اینترنت و اصولاً فن‌آوری‌های نوین اطلاعات و ارتباطات مثل خیلی از فن‌آوری‌های دیگر در کشور ما جنبه‌ی وارداتی دارد و ما آن را از کشورهای دیگر گرفته‌ایم. اگر چه امروزه در این زمینه پیشرفت‌های قابل توجهی در کشور صورت گرفته، اما به هر حال این فن‌آوری در بستر فرهنگی، اجتماعی و سیاسی خاص دنیای صنعتی غرب-دنیای باز، مردم سالار، پویا و متحول - متولد شده و در حال تکامل است. اما در کشور ما این فن‌آوری‌ها به صورت آماده و به صورت یک تولید قابل مصرف و بهره برداری وارد و عرضه شده است. اگر چه سعی کرده‌ایم بر این فن‌آوری‌ها اشراف پیدا کنیم، اما از نظر فرهنگی، هم‌چنان به تطبیق این فن‌آوری‌ها با جامعه‌ی ایرانی و به ویژه با فرهنگ سیاسی-اجتماعی ایران نیاز داریم.

آیا می‌توان از تجربه و دست‌آورد‌های کشورهای دیگر برای مهار این تهدیدها استفاده کرد؟ به عبارت دیگر، آیا راهکارهای مهار تهدیدهای سایبری، جهانی است یا این که پژوهشگران ایرانی باید با توجه به فرهنگ ایرانی، راهکارهای منطبق با شرایط سیاسی جامعه‌ی ایران را پیدا کنند؟

اینترنت یک فضای جدید است و به نظر می‌رسد که برای مهار همه تهدیدهای ناشی از آن، در قالب اشکال پیش گفته، نیاز به مطالعه و تجربه است. کشورهایی مانند آمریکا و انگلستان که در معرض تهدیدهای تروریستی بوده و جرایم سایبری بیشتری را شاهد هستند، همواره در حال مطالعه و تجربه اندوزی برای مصون سازی آماج‌های بالقوه و اتخاذ راه‌کارهای مناسب در مقابل این تهدیدها هستند. سوال قابل طرح که پاسخ به آن به مطالعه نیاز دارد، این است که آیا دولت‌ها به عنوان متولیان تامین امنیت می‌توانند در مسابقه‌ی جاری بین خود و مجرمین سایبری، پیروز شوند؟ به تعبیر بهتر، آیا دولت‌ها می‌توانند همواره یک گام جلوتر از بزهکاران سایبری باشند، به گونه‌ای که با دستیابی به راهکارهای مؤثر، اعمال و برنامه‌های بزهکاران سایبری را پیشگیری، پیش‌بینی و خنثی کنند؟

پاسخ به این پرسش‌ها بی‌گمان به سرمایه‌گذاری علمی و مادی در پژوهش‌ها و مطالعات جرم‌شناسی و بزه‌دیده‌شناسی سایبری نیاز دارد.

۱- رک: پاکزاد، بتول، تروریسم سایبری، پایان‌نامه‌ی دکتری، دانشکده‌ی حقوق دانشگاه شهید بهشتی، در دست‌دفاع (پاییز ۱۳۸۸)