در نشستی با حضور کارشناسان بررسی شد؛

مبانی فقهی-حقوقی جرم‌انگاری انواع هک

بهمن ۹, ۱۴۰۰ آخرین اخبار, دیدگاه (گفت‌وگو/یاداشت), فرهنگ و ارتباطات

در مسئله هک با توجه به شرایطی سایت مورد مطالعه که مورد حمله هکری قرار می‌گیرد همچون عمومی یا خصوصی بودن، داخلی یا خارجی بودن، قانونی یا غیرقانونی بودن فعالیت‌های سایت، مسلمان و یا نامسلمان بودن صاحب سایت و مسائل دیگر می‌توان ۸۴ حالت مختلف را متصور شد که هر یک از این حالات باید به صورت تک به تک مورد بررسی حقوقی و فقهی قرار گیرد. به عنوان نمونه نمی‌توان همه اقسام هک سیاه را از لحاظ حقوقی، غیرقانونی تلقی کرد چرا که حمله هکرها به سامانه‌های رژیم صهیونیستی عملی غیرقانونی نیست.

به گزارش شبکه اجتهاد، یکصد و هفتمین نشست از سلسله نشست‌های علمی-پژوهشی دین و فضای مجازی با موضوع بررسی مبانی فقهی-حقوقی جرم‌انگاری انواع هک و با حضور حجت‌الاسلام دکتر سید علیرضا طباطبایی، عضو هیئت علمی دانشگاه علوم قضایی، حجت‌الاسلام ابوالحسن حسنی، کارشناس دفتر مطالعات اسلامی فضای مجازی و مهندس امیررضا قاضی‌پور، کارشناس حوزه نفوذ و تست نفوذ به صورت مجازی برگزار شد.

مهندس قاضی‌پور در ابتدای این نشست، به تعریف «هک» پرداخت و اظهار داشت: مجموعه کارهایی که بر روی سرور، سایت و افراد یک مجموعه در جهت نفوذ و کسب اطلاعات انجام می‌شود را هک می‌گویند و هکرها به سه دسته کلاه سفید، کلاه خاکستری و کلاه سیاه تقسیم می‌شوند.

وی ادامه داد: رنگ کلاه هکرها به عملی که انجام می‌دهند، بستگی دارد؛ چنانچه یک هکر با سازمانی قرارداد ببندد و به صورت قانونی فعالیت کند، هکر کلاه سفید نام می‌گیرد. اما اگر بدون قرارداد، باگ‌های سیستم‌های مختلف را پیدا کند و آن را به صاحب سازمان مربوطه بفروشد، هکر کلاه خاکستری اطلاق می‌شود و اگر هکری با کشورهای خارجی همکاری و اعمال خرابکارانه انجام دهد، هکر کلاه سیاه نامگذاری می‌شود.

این کارشناس حوزه نفوذ افزود: از سال ۹۲ در ایران، هکرهای کلاه خاکستری از بین رفتند چرا که تست نفوذ سایت‌ها نادیده گرفته شده و یا سیستم‌های امنیتی دستگاه‌ها در انحصار برخی مراکز قرار گرفته است و چنانچه یک هکر خاکستری به سازمانی بگوید که سیستم شما فلان باگ را دارد و این را از من بخرید، اگر ارتباط لازم را نداشته باشد، بلافاصله با برخورد امنیتی مواجه می‌شود در نتیجه هکرها باگ سیستم‌ها را بررسی نمی‌کنند چون چنانچه این اقدام را به صورت شخصی انجام دهند، مجرم تلقی می‌شوند. از طرفی اگر فردی بخواهد با سازمان مربوطه قرارداد ببندد به دلیل اینکه این موضوع به صورت انحصاری در اختیار برخی مراکز قرار گرفته است، تنها ده درصد مبلغ قرارداد به هکر کلاه خاکستری که عامل اصلی کشف این باگ بوده می‌رسد و ما بقی مبلغ در اختیار شرکت مذکور -که رابطه دارد- قرار می‌گیرد. در نتیجه این اتفاق و عدم فعالیت، هکرهای کلاه خاکستری یا در برابر باگ‌ها سکوت می‌کنند و یا متاسفانه آن را به کشورهای خارجی می‌فروشند.

حجت‌الاسلام دکتر طباطبایی، استاد حقوق، در این نشست با اشاره به اینکه "هک مادر همه جرایم رایانه‌ای است"، عنوان کرد: هک به معنای شکافتن پوسته‌های امنیتی سایت می‌باشد و چنانچه هکر با نیت دسترسی غیرمجاز، پوسته‌ها را بشکافد، حتی اگر به اطلاعات لازم دسترسی پیدا نکند اما بازهم عمل مجرمانه‌ای انجام داده است.

وی ادامه داد: در مسئله هک با توجه به شرایطی سایت مورد مطالعه که مورد حمله هکری قرار می‌گیرد همچون عمومی یا خصوصی بودن، داخلی یا خارجی بودن، قانونی یا غیرقانونی بودن فعالیت‌های سایت، مسلمان و یا نامسلمان بودن صاحب سایت و مسائل دیگر می‌توان ۸۴ حالت مختلف را متصور شد که هر یک از این حالات باید به صورت تک به تک مورد بررسی حقوقی و فقهی قرار گیرد. به عنوان نمونه نمی‌توان همه اقسام هک سیاه را از لحاظ حقوقی، غیرقانونی تلقی کرد چرا که حمله هکرها به سامانه‌های رژیم صهیونیستی عملی غیرقانونی نیست.

این استاد دانشگاه افزود: ما در قانون اساسی موردی با عنوان هک نداریم و مبنای حقوقی برای جرم‌انگاری هک، ماده یک و دو جرایم رایانه‌ای می‌باشد اما در قانون این موضوع به صورت عام آمده است و فقها بایست فروض مختلف هک را استخراج کنند.

طباطبایی با اشاره به فعالیت هکرهای کلاه خاکستری در کشف باگ‌های دستگاه‌های مختلف دولتی، عنوان کرد: امر به معروف یکی از فرایض دینی است و یکی از تکالیف مردم، امربه معروف و نهی از منکر دولت می‌باشد. چنانچه بخواهیم این فریضه دینی را در عمل هک کردن پیاده کنیم، با شقوق مختلفی مواجه خواهیم شد اما به نظر می‌رسد قانون‌گذار با به کار بردن عبارت «دسترسی غیرمجاز» در قانون، دایره امر به معروف را در این حوزه محدود کرده است.

وی گفت: اگر چه بایست با نظام‌مند کردن فعالیت‌های هکرهای کلاه سفید و عقد قرارداد سازمان‌های مختلف با چنین افرادی، باگ‌های دستگاه‌های مربوطه رفع شود نه اینکه همه گونه فعالیت‌های هکری را در کشور آزاد کنیم.

این استاد دانشگاه با اشاره به قانون یک جرایم رایانه‌ای اظهار داشت: از جمله نقاط ضعف ماده یک جرایم رایانه‌ای این است که قانون‌گذار عنوان کرده "هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده‌است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد." در حالی که در این ماده استفاده از واژه «هرکس» اشتباه می‌باشد چرا که می‌توان از این واژه استنباط کرد که منظور قانون‌گذار اشخاص حقیقی هستند و اشاره‌ای به اشخاص و شرکت‌های حقوقی نشده است.

حجت‌الاسلام ابوالحسن حسنی، کارشناس دفتر مطالعات اسلامی فضای مجازی با اشاره به مبحث جرم در قاعده فقهی، عنوان کرد: در قاعده فقهی، هر گناهی مجازات و تعزیر دارد اما هک ذیل این قاعده تعریف نمی‌شود.

وی ادامه داد: قاعده فقهی دیگر، نقض حق است به این معنا که چنانچه حقی از فردی ضایع شود، مجازات اقتضا پیدا می‌کند و چنانچه فردی سایتی را هک کند، به این معناست که حریم خصوصی یک شهروند را نقض کرده است.

نگارنده کتاب «جرم‌انگاری از منظر فقه» با اشاره به قانون جرایم رایانه‌ای، عنوان کرد: در سال ۸۸(سال تصویب قانون) فضای مجازی همانند عصر کنونی، یه فضای زیست مردم تبدیل نشده بود در نتیجه این قانون با عنوان جرایم سایبری نابهنجار است.

وی ادامه داد: باید بررسی کرد که آیا در جرم‌انگاری فعالیت هکرهای کلاه خاکستری، مصلحت‌ها در نظر گرفته شده و یا برخی دست‌های پشت پرده در این قانون‌گذاری نقش داشته‌اند اما بایست توجه کرد که چنانچه هکرهای کلاه خاکستری -که خودی محسوب می‌شوند- باگ‌های دستگاه‌های داخلی را بررسی و کشف نکنند در نتیجه فضای مجازی کشور ناامن خواهد شد و این قانون که برای افزایش امنیت کشور، در نظر گرفته شده دقیقا در عکس هدف خود عمل می‌کند.

این کارشناس حوزه فضای مجازی خاطرنشان کرد: با بررسی‌های کنونی مشخص شده که در نتیجه جرم‌انگاری فعالیت هکری و قانون جرایم رایانه‌ای، امنیت سایبری ایران در جهان کاهش پیدا کرده است چرا که هکرها از ترس برخوردهای امنیتی، جرأت نمی‌کنند تا باگ‌ها را شناسایی کرده و به دستگاه‌ها اطلاع دهند. ما باید توجه کنیم که با صرف قانون نمی‌توان امنیت فضای مجازی را حفظ کرد چرا که عرصه فضای مجازی، عرصه‌ای آشکار در جهان است به این معنا که فضای مجازی کشور ما به صورت عیان زیر رصد دشمنان قرار دارد و نمی‌توان قانون‌های داخلی را بر هکرهای خارجی وضع کرد.