

واکاوی حقوقی حملات سایبری به زیرساخت‌های مالی و غیرنظامی ایران در شرایط جنگی

دفاع حقوقی در برابر «تهدیدات سایبری»



در جریان جنگ ۱۲روزه میان ایران و رژیم اشغالگر صهیونیستی، زیرساخت‌های بانکی ایران طی هفته‌های اخیر هدف حملات سایبری گسترده‌ای قرار گرفت، این حملات که شامل نفوذ به بانک‌های ملی، سپه، پاسارگاد و حتی صراف‌ی نوبیتکس بود، نه تنها موجب اخلال در خدمات حیاتی مالی کشور شد بلکه بحث‌های تازه‌ای را در خصوص وضعیت امنیت سایبری، مسئولیت دولت‌ها و جایگاه این اقدامات در حقوق بین‌الملل برانگیخت. این حملات شامل تخریب داده‌های بانکی، اختلال در خدمات عمومی و سرقت دارایی‌های دیجیتال بود. آ با حملات سایبری به زیرساخت‌های مالی یک کشور می‌تواند مصداق استفاده از زور یا اقدام خصمانه در حقوق بین‌الملل باشد؟ مسئولیت بین‌المللی اسرائیل در قبال این اقدامات چیست؟ و چگونه می‌توان از منظر حقوقی، پاسخ مناسبی برای این تهدیدات نوپنهور ترسیم کرد؟ این گزارش به دنبال یافتن پاسخ‌های دقیق و مستند برای این پرسش‌هاست.

■ ■ ■

زیرساخت‌های مالی مانند نظام‌های بانکی، سامانه‌های پرداخت بین‌المللی و مقررات ضد پولشویی، به عنوان ابزارهایی برای تحقق اهداف حقوق بین‌الملل از جمله حفظ صلح، امنیت و توسعه پایدار عمل می‌کنند. این زیرساخت‌ها همچنین پلی میان منافع ملی دولت‌ها و منافع مشترک جهانی هستند و نقش مهمی در ایجاد همکاری‌های چندجانبه دارند. اهمیت این موضوع به حدی است که همواره اصلاحات گسترده‌ای در ساختار مالی بین‌المللی صورت می‌گیرد تا ریسک‌های سیستمی کاهش یابند و استانداردهای مالی تقویت شوند. فلز قارغ از اهمیت این بخش، به طور کلی کنوانسیون چهارم ژنو (۱۹۴۹) و پروتکل الحاقی اول (۱۹۷۷)، کشورها را از هدف قرار دادن غیرنظامیان و زیرساخت‌های غیرنظامی منع می‌کنند. در ماده ۵۲ پروتکل اول از الحاقی به کنوانسیون ژنو، یک شیء تنها در صورتی هدف نظامی محسوب می‌شود که مشارکت مؤثر در عملیات نظامی داشته باشد و نابودی آن مزیت نظامی قطعی فراهم آورد، بنابر این مطابق ماده ۵۲ پروتکل اول الحاقی به کنوانسیون ژنو، اهداف غیرنظامی نباید مورد حمله قرار گیرند. بانک‌هایی که خدمات عمومی ارائه می‌دهند، از جمله بانک‌های سپه، ملی و پاسارگاد در اغلب موارد مشمول حمایت‌های حقوقی بیشتری هستند. حمله به این بانک‌ها با تأکید بر عدم مشارکت مستقیم در عملیات نظامی، مصداق نقض حقوق بین‌الملل است.

■ حملات سایبری چگونه رخ دادند؟

طبق گزارش‌های رسمی و اطلاعات منتشرشده حملات سایبری از سوی گروه‌های هکری‌ای که به اسرائیل نسبت داده شده‌اند، انجام گرفت. مهم‌ترین ویژگی‌ای این حملات عبارت بودند از:

- قطع کامل خدمات آنلاین بانک شامل اینترنت بانک، همراه بانک، سامانه‌های خودپرداز و در برخی موارد سامانه‌های پرداخت حقوق دولتی
- نفوذ به دیتابیس‌های حساس که به حذب تراکنش‌ها، از دست رفتن اطلاعات حساب‌ها و

گزارش ۲

در دنیای امروز که برنده‌ها با سرعتی بی‌سابقه در حال رشد و رقابت هستند، علائم تجاری به عنوان یکی از مهم‌ترین ابزارهای شناسایی، تمایز و حفاظت از هویت تجاری شناخته می‌شوند. این علائم نه تنها نقش کلیدی در بازار باایی و جذب مشتری دارند، بلکه در حقوق مالکیت فکری نیز جایگاه ویژه‌ای به خود اختصاص داده‌اند و از حمایت‌های قانونی گسترده‌ای برخوردارند.

■ ■ ■

■ منظور از علائم تجاری چیست؟

مطابق ماده ۳۰ قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری ایران، علامت تجاری عبارت است از هر نشان قابل رؤیتی که بتواند کالاها یا خدمات اشخاص حقیقی یا حقوقی را از یکدیگر متمایز سازد. این نشان می‌تواند شامل واژه‌ها، حروف، اعداد، تصاویر، اشکال، رنگ‌ها، بسته‌بندی‌ها و حتی صدا یا بو باشد، به شرط آنکه قابل رؤیت و دارای قدرت تمایز باشد.

■ چرا علائم تجاری در حقوق مالکیت فکری

حقوق مالکیت فکری به دو شاخه اصلی تقسیم می‌شود، شاخه اول مالکیت صنعتی است که شامل اختراعات، علائم تجاری، طرح‌های صنعتی، نشانه‌های جغرافیایی و اسرار تجاری می‌شود. دسته دوم نیز مالکیت ادبی و هنری است که متشکل است از کپی رایت، حقوق مرتبط آثار هنری و نرم‌افزارها. علامت تجاری در بخش مالکیت صنعتی قرار دارد و هدف آن حمایت از نشانه‌هایی است که هویت کالا یا خدمات را مشخص می‌کنند.

■ اهمیت حقوقی ثبت علامت تجاری

ثبت علامت تجاری در ایران از طریق سامانه مالکیت معنوی انجام می‌شود و مزایای زیر را به همراه دارد:

- حق انحصاری استفاده از علامت
- امکان اقامه دعوی علیه نقض‌کنندگان
- جلوگیری از سوءاستفاده رقیبا
- افزایش اعتبار برند در بازار داخلی و بین‌المللی.

■ بررسی پرونده‌های حقوقی مرتبط با علائم تجاری پرونده «ADIDAAS» در ایران

در این پرونده، یک تولیدکننده داخلی از علامت «ADIDAAS» برای کفش‌های ورزشی استفاده کرده بود. شرکت آدیداس با استناد به شباهت ظاهری و تلفظی، شکایت کرد. دادگاه با بررسی قدرت تمایز و احتمال گمراهی مصرف‌کننده، رأی به ابطال علامت داخلی داد.

داده‌ها بازنگری و تقویت شد. نتیجه این تجربه برای ما این است که ایران نیازمند تصویب قانون جامع حفاظت از داده‌های شخصی است تا در صورت افشای اطلاعات بانکی، امکان پیگیری حقوقی و جبران خسارت فراهم باشد.

کره جنوبی و حمله به 2013 Darkseoul: طی این حمله در ۳۲ هزار سرور بانکی و رسانه‌ای اختلال ایجاد شد. کره جنوبی با استناد به منشور ملل متحد، حمله را مصداق اقدام خصمانه دانست و در مجامع بین‌المللی مطرح کرد. نتیجه این تجربه برای ما این است که ایران می‌تواند با استناد به دستورالعمل تالین و منشور ملل متحد، حملات سایبری را در قالب نقض اصل عدم‌مداخله با استفاده از زور مطرح کند.

عربستان و حمله گروه شمعون ۲۰۱۶: به موجب این حمله داده‌های بانکی به طور کامل حذف و خدمات متوقف شدند. عربستان به سرعت زیرساخت‌های پشتیبان را فعال کرد و تیم‌های واکنش سریع تشکیل داد. نتیجه این تجربه برای ما این است که اهمیت لزوم ایجاد سامانه‌های پشتیبان آفلاین و تیم‌های واکنش سریع در بانک‌ها برای کاهش خسارات و بازیابی اطلاعات را افزایش دهیم.

اتحادیه اروپا و مقررات DORA2022: در نتیجه افزایش حملات به مؤسسات مالی در اروپا، این مقرره تصویب شد. تصویب مقررات DORA برای الزام بانک‌ها به تاب‌آوری سایبری و گزارش‌دهی حملات است. نتیجه این تجربه برای ما این است که ایران می‌تواند با الگوبرداری از DORA، مقرراتی برای الزام بانک‌ها به امنیت سایبری، گزارش‌دهی حملات و پاسخگویی قانونی تدوین کند.

■ جمع‌بندی راه‌حل‌های حقوقی قابل اجرا برای ایران

تجربه بین‌المللی، راه حل حقوقی، پیشنهاد برای ایران، حمله به سوئیت، پیگیری دیپلماتیک و اصلاح شکایات رسمی به مجامع حقوقی مانند دیوان بین‌المللی دادگستری یا شورای امنیت

۴. تشویق به تشکیل کنوانسیون جهانی امنیت سایبری تحت‌نظارت سازمان ملل برای تعیین خطوط قرمز و پاسخ‌های مشروع

۵. شفاف‌سازی عمومی از سوی نهادهای دولتی برای حفظ اعتماد عمومی و جلوگیری از شایعات.

■ بررسی تجربه‌های جهانی

بنگلادش و حمله به شبکه سوئیفت ۲۰۱۶: در این حمله ۱۰۱ میلیون دلار از حساب بانک مرکزی در نیویورک به سرقت رفت. بنگلادش با همکاری بانک فدرال نیویورک و سوئیفت، پیگیری قضایی و دیپلماتیک را آغاز کرد. این پرونده باعث شد سوئیفت استانداردهای امنیتی خود را به‌روزرسانی کند. نتیجه این تجربه برای ما این است که ایران باید در تعامل با نهادهای بین‌المللی مانند سوئیفت، چارچوب‌های امنیتی خود را تقویت و در صورت حمله از مسیرهای دیجیتال یک موضوع می‌تواند جزو مصداق تهدید امریکا و حمله به 2017 Equifax: این حمله به افشای اطلاعات ۱۴۷ میلیون نفر منجر شد. شرکت مذکور مجبور به پرداخت ۷۰۰ میلیون دلار خسارت شد، با این حال قوانین فدرال در زمینه حفاظت از

حتماً برات سؤال شده که:



شرکت‌های سهامی عام و خاص چه تفاوت‌هایی باهم دارند؟

در نظام حقوقی ایران، شرکت‌های تجاری به انواع مختلفی تقسیم می‌شوند که یکی از مهم‌ترین آنها شرکت‌های سهامی هستند. این شرکت‌ها به دو دسته اصلی تقسیم می‌شوند: شرکت سهامی عام و شرکت سهامی خاص. هر یک از این دو نوع شرکت، ویژگی‌ها، مزایا و محدودیت‌های خاص خود را دارند که شناخت آنها برای فعالان اقتصادی، حقوق‌دانان و سرمایه‌گذاران ضروری است.

■ ■ ■

■ تعریف شرکت سهامی

شرکت سهامی، شرکتی است که سرمایه آن به سهام تقسیم شده و مسئولیت صاحبان سهام محدود به مبلغ اسمی سهام آنهاست. این نوع شرکت‌ها برای فعالیت‌های بزرگ اقتصادی و تجاری مناسب هستند و ساختار آنها به گونه‌ای طراحی شده که امکان جذب سرمایه از طریق فروش سهام فراهم باشد.

■ شرکت سهامی عام چیست؟

شرکت سهامی عام شرکتی است که بخشی از سرمایه آن از طریق فروش سهام به عموم مردم تأمین می‌شود.

این شرکت‌ها معمولاً در پروژه‌های بزرگ، مانند بانک‌ها، شرکت‌های بیمه، یا صنایع سنگین فعالیت و سهام آنها در بورس اوراق بهادار قابل معامله است.

برای مثال شرکت ملی صنایع مس ایران، با ناماد «فملی» یک شرکت سهامی عام است که سهام آن در بورس تهران معامله می‌شود و هزاران سهامدار حقیقی و حقوقی دارد.

■ شرکت سهامی خاص چیست؟

شرکت سهامی خاص شرکتی است که تمام سرمایه آن از سوی مؤسسان تأمین می‌شود و سهام آن قابل عرضه عمومی نیست.

این شرکت‌ها معمولاً در کسب و کارهای خانوادگی، استارت‌آپ‌ها یا پروژه‌های متوسط فعالیت دارند و کنترل بیشتری بر ساختار مدیریتی خود دارند.

برای مثال شرکت ملی تولید ساعت‌های دیواری لوکس که از سوی سه طراح تأسیس شده است و سرمایه اولیه را خودشان تأمین کرده‌اند، نمونه‌ای از شرکت سهامی خاص است.

■ مزایا و معایب هر ۲ نوع شرکت

مزایای شرکت سهامی عام:

۱. امکان جذب سرمایه‌های کلان

۲. نقدشوندگی بالای سهام

۳. افزایش اعتبار برند در بازار

۴. قابلیت توسعه سریع کسب و کار

معایب شرکت سهامی عام:

۱. تشریفات قانونی پیچیده‌تر

۲. الزام به شفافیت مالی و گزارش‌دهی عمومی

۳. کاهش آزادی عمل مدیران به دلیل تعدد سهامداران

مزایای شرکت سهامی خاص:

۱. کنترل بیشتر مؤسسان بر تصمیمات

۲. فرآیند ثبت ساده‌تر

۳. مناسب برای کسب و کارهای خصوصی و خانوادگی

معایب شرکت سهامی خاص:

۱. محدودیت در جذب سرمایه

۲. نقدشوندگی پایین سهام

۳. عدم امکان ورود به بازار سرمایه

■ نکات حقوقی مهم در ثبت و اداره شرکت‌ها

در شرکت سهامی عام، تشکیل مجمع عمومی مؤسس الزامی است، اما در شرکت سهامی خاص چنین الزامی وجود ندارد، همچنین در شرکت سهامی عام، انتخاب هیئت مدیره حداقل پنج نفره الزامی است، در حالی که در شرکت سهامی خاص این تعداد می‌تواند کمتر باشد.

در هر دو نوع شرکت، مسئولیت سهامداران محدود به مبلغ اسمی سهام آنهاست، به این معنا که در صورت ورشکستگی شرکت، سهامداران فقط تا سقف سرمایه پرداخت شده مسئولند.

■ نتیجه‌گیری

شرکت‌های سهامی عام و خاص هر یک برای اهداف و شرایط خاصی طراحی شده‌اند.

اگر هدف شما جذب سرمایه‌های کلان و ورود به بازار بورس است، شرکت سهامی عام گزینه مناسبی خواهد بود، اما اگر به دنبال کنترل بیشتر، فرایند ساده‌تر و حفظ ساختار خصوصی هستید، شرکت سهامی خاص انتخاب مناسب‌تری است.

شناخت تفاوت‌های این دو نوع شرکت نه تنها برای ثبت شرکت بلکه برای تحلیل حقوقی، سرمایه‌گذاری و مدیریت کسب و کار اهمیت دارد. در نهایت، انتخاب نوع شرکت باید بر اساس اهداف تجاری، میزان سرمایه، تعداد شرکا و چشم‌انداز توسعه صورت گیرد.

تفاوت‌های کلیدی شرکت سهامی عام و خاص

ویژگی	سهامی عام	سهامی خاص
تأمین سرمایه	از طریق مؤسسان و سایر موسسات عمومی	فقط توسط مؤسسان
حداقل سرمایه اولیه	شصت میلیون ریال	یک میلیون ریال
تعداد مؤسسان	حداقل پنج نفر	حداقل سه نفر
عرضه سهام	قابل عرضه در بورس	غیرقابل عرضه عمومی
انتقال سهام	آزادانه و بدون محدودیت	ممکن است مشروط به موافقت مدیران باشد
مدیر اوراق عرضه	مجاز	غیرمجاز
الزامات گزارش‌دهی	باید گزارش‌های مالی عمومی ارائه دهد	الزامی به انتشار عمومی ندارد

مفهوم	تفاوت با علامت تجاری
نام تجاری	معرف شخص یا شرکت است نه محصول
برند	مفهوم گسترده‌تر شامل اعتبار تجریه مشتری و هویت بصری است
لوگو	ممکن است علامت تجاری باشند اما همیشه نیستند
طرح صنعتی	مربوط به ظاهر محصول است، نه تمایز تجاری