

شرکت آب منطقه‌ای گلستان

نشریه داخلی شرکت آب منطقه‌ای گلستان / شماره ششم / شهریور ماه ۱۴۰۴



قانون سایبری ایران خط قرمزهایی که نمی بینید

14 <

یک شوخی کوچک که
به ۶ ماه حبس کشید...

6 <

قانون‌گریزی دیجیتال
ناآگاهی به قیمت مجازات



CYBER LAW OF IRAN



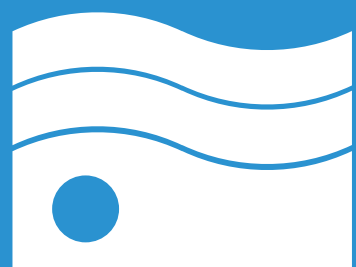
BRUCE SCHNEIER

برای امنیت سایبری، هیچ راه حل
قطعی وجود ندارد؛ اما راه حل‌ها
پله‌ای و لایه‌ای هستند.



نشریه داخلی شرکت
آب منطقه ای گلستان

شماره ششم — شهریور ماه ۱۴۰۴



فهرست

سرمقاله	06
قانون‌گریزی دیجیتال ناآگاهی به قیمت مجازات	
مقاله اصلی	08
جرایم رایانه‌ای در قانون ایران؛ چه چیزی جرم حساب می‌شود؟ و چه چیزی نه؟	
راهنمای عملی	11
چه کارهایی در فضای مجازی جرم محسوب می‌شوند؟ (بدون آنکه بدانیم!)	
مطالعه موردی	14
یک شوخی کوچک که به ۶ ماه حبس کشید...	
مصاحبه	16
از فوروارد تا فیلتر؛ گفت‌وگو با کارشناس حقوق سایبری	
راهنمای دفاع	18
راهنمای عملی اقدامات لازم در مواجهه با شکایت‌های سایبری	
چک‌لیست	20
هفت رفتار رایج در فضای مجازی که می‌تواند موجب مسئولیت کیفری شود	
قانون به زبان ساده	22
شرح ساده قانون جرایم رایانه‌ای؛ ماده به ماده	
سناریو	24
یک پست اشتباهی، مسیری به سوی مشکلات حقوقی	
آزمون دانشی	26
آزمون دانشی جرایم رایانه‌ای تشخیص رفتار مجرمانه در فضای مجازی	



دکتر امیرحسین رحیمیان

قانون‌گریزی دیجیتال ناآگاهی به قیمت مجازات

وقتی صحبت از «قانون» می‌شود، ذهن بسیاری از ما به سرعت به خیابان، رانندگی، مالیات یا دادگاه‌های حقوقی و کیفری می‌رود. کمتر کسی از همان ابتدا به رفتارهای آنلاین و فعالیت‌های دیجیتال خود فکر می‌کند. اما حقیقت این است که امروز، بخش بزرگی از زندگی ما به فضای مجازی گره خورده و درست همان‌طور که در دنیای واقعی قوانین و مقررات وجود دارد، در دنیای دیجیتال هم خط قرمزهایی هست که عبور از آن‌ها می‌تواند تبعات سنگینی داشته باشد.

در ایران، «قانون جرایم رایانه‌ای» مجموعه‌ای از مقررات است که به‌طور مشخص برای برخورد با تخلفات، سوءاستفاده‌ها و جرایم در فضای مجازی تدوین شده است. این قانون که در سال‌های اخیر به‌روز و تکمیل شده، مصادیق متعددی را در بر می‌گیرد؛ از هک و نفوذ غیرمجاز گرفته تا انتشار تصاویر خصوصی، از کلاهبرداری اینترنتی تا جعل داده‌های دیجیتال، و حتی موضوعاتی که شاید در نگاه اول «بی‌ضرر» به نظر برسند.

اما نکته نگران‌کننده اینجاست: بخش زیادی از مردم اصلاً از وجود این قوانین اطلاع ندارند یا اگر هم شنیده‌اند، جزئیات آن را نمی‌دانند. نتیجه؟ کارهایی که در نظر ما شاید یک شوخی یا حتی یک اقدام «عادی» محسوب شود، ممکن است از نظر قانون، جرم باشد و مجازات در پی داشته باشد.

ناآگاهی؛ دشمن شماره یک امنیت حقوقی در فضای مجازی
در فضای دیجیتال، ناآگاهی شاید از خودِ تخلف خطرناک‌تر باشد. فرض کنید فردی برای سرگرمی، عکس یکی از همکارانش را ویرایش کرده و در یک گروه خصوصی منتشر کند. شاید نیت او فقط شوخی باشد، اما از نظر قانون، این عمل می‌تواند «تغییر غیرمجاز داده‌های شخصی» یا «انتشار محتوای خلاف عفت عمومی» تلقی شود. در چنین شرایطی، اگر شکایتی مطرح شود، همین شوخی کوچک ممکن است به

احضاریه دادگاه و حتی حکم کیفری ختم شود.

مشکل اینجاست که قوانین سایبری معمولاً به زبان تخصصی نوشته شده‌اند و مطالعه آن‌ها برای عموم مردم ساده نیست. بسیاری از افراد هم به‌طور کلی، پیشگیری را جدی نمی‌گیرند؛ تا زمانی که حادثه‌ای رخ دهد و کار از کار بگذرد. این غفلت، همان نقطه‌ای است که «قانون‌گریزی دیجیتال» آغاز می‌شود؛ نه به این معنا که فرد عمداً قانون را دور زده، بلکه به این دلیل که اصلاً نمی‌دانسته رفتارش خلاف قانون است. زندگی دیجیتال، مسئولیت دیجیتال

وقتی حساب بانکی باز می‌کنیم، می‌دانیم که چک بی‌محل یا برداشت غیرمجاز، پیگرد قانونی دارد. اما آیا همه می‌دانیم که ورود به یک حساب ایمیل بدون اجازه صاحب آن، حتی اگر رمز عبور را خود او یک روز به ما داده باشد، می‌تواند مصداق «دسترسی غیرمجاز» و جرم تلقی شود؟ یا مثلاً، آیا آگاهیم که ذخیره‌سازی یا انتشار هرگونه فیلم و عکس خصوصی بدون اجازه صاحب اثر، حتی در یک گروه خانوادگی، می‌تواند تحت عنوان «نقض حریم خصوصی» پیگیری شود؟ زندگی در دنیای دیجیتال، یعنی هر کاربر - چه یک مدیر ارشد سازمان باشد، چه یک کارمند یا حتی یک نوجوان - مسئولیت مستقیم نسبت به رفتار آنلاین خود دارد. همان‌طور که رانندگی بدون گواهینامه جرم است، «گردش در فضای مجازی بدون آگاهی از قوانین» هم می‌تواند عواقب غیرقابل جبرانی داشته باشد.

چرا آگاهی حقوقی در فضای مجازی ضروری‌تر از همیشه است؟

با گسترش شبکه‌های اجتماعی، افزایش خرید و فروش آنلاین، و دیجیتالی شدن بخش بزرگی از تعاملات ما، مرز میان دنیای واقعی و مجازی تقریباً محو شده است. امروزه بخش قابل توجهی از روابط کاری، خانوادگی، و حتی سیاسی، در بسترهای دیجیتال شکل می‌گیرد. همین موضوع باعث شده که جرایم سایبری نه تنها بیشتر شوند، بلکه شکل‌های جدید و پیچیده‌تری به خود بگیرند. از طرف دیگر، ابزارهای فناوری آن‌قدر در دسترس و ساده شده‌اند که هر کاربر، حتی بدون دانش فنی، می‌تواند اقداماتی انجام دهد که از دید قانون، تخلف یا جرم محسوب می‌شود. ارسال یک لینک آلوده، فرورورد یک ویدئوی جعلی، دستکاری یک تصویر و انتشار آن، یا حتی درج یک نظر توهین‌آمیز، همه و همه می‌توانند تبعات حقوقی داشته باشند.

مسئولیت اجتماعی کاربران

آگاهی از قانون تنها برای حفاظت شخصی نیست؛ بلکه جنبه اجتماعی هم دارد. وقتی کاربر یک سازمان، به قوانین و مقررات دیجیتال پایبند باشد، ریسک امنیتی کل سازمان کاهش پیدا می‌کند. به همین ترتیب، اگر شهروندان یک جامعه قوانین فضای مجازی را رعایت کنند، امنیت سایبری عمومی ارتقا پیدا می‌کند. در این میان، نقش مدیران ارشد سازمان‌ها بسیار کلیدی است. آن‌ها باید نه تنها خودشان با این قوانین آشنا باشند، بلکه فرهنگ پایبندی به قوانین را در تیم‌ها و کارکنانشان تقویت کنند. قانون‌گریزی؛ انتخاب یا پیامد؟

در بسیاری از پرونده‌های جرایم رایانه‌ای، متهمان ادعا می‌کنند که «نمی‌دانستیم این کار جرم است». اما همان‌طور که در قوانین کلی کشور آمده، ندانستن قانون، مانع از اجرای آن نمی‌شود. به بیان ساده‌تر، اگر حتی بی‌خبر باشید که عملی جرم است، باز هم مسئولیت آن بر عهده شماست. بنابراین، قانون‌گریزی دیجیتال همیشه یک انتخاب آگاهانه نیست؛ گاهی پیامد ندانستن است. اما از منظر قانون، تفاوتی ندارد که ناآگاه باشید یا آگاهانه قانون را نقض کرده باشید؛ نتیجه نهایی می‌تواند جریمه، محرومیت از حقوق اجتماعی، یا حتی حبس باشد.

جمع‌بندی

دنیای دیجیتال فرصت‌های بزرگی برای رشد، یادگیری، و تعامل فراهم کرده است. اما این فرصت‌ها بدون شناخت قوانین، می‌توانند به تهدید تبدیل شوند. همان‌طور که یاد می‌گیریم از ابزارهای دیجیتال استفاده کنیم، باید یاد بگیریم در این فضا چگونه قانونی رفتار کنیم. قانون‌گریزی دیجیتال، هزینه دارد؛ و این هزینه را معمولاً کسانی می‌پردازند که تصور می‌کردند برای من اتفاقی نمی‌افتد.

در شماره ششم ماهنامه، تلاش ما این است که به زبان ساده، این قوانین را برای شما باز کنیم، مصادیق رایج را توضیح دهیم، و کمک کنیم تا با دانستن این خطوط قرمز، حضور امن‌تری در فضای مجازی داشته باشید.

MAIN ARTICLE



... مقاله اصلی



جرایم رایانه‌ای در قانون ایران؛ چه چیزی جرم حساب می‌شود؟ و چه چیزی نه؟

وقتی از «جرایم رایانه‌ای» یا همان «جرایم سایبری» صحبت می‌کنیم، خیلی‌ها تصور می‌کنند این موضوع فقط مربوط به هکرها، نفوذ به سرورهای بانکی یا سرقت‌های پیچیده اینترنتی است. اما واقعیت این است که قانون جرایم رایانه‌ای در ایران دامنه بسیار گسترده‌ای دارد و بخش زیادی از رفتارهای روزمره کاربران اینترنت، شبکه‌های اجتماعی و حتی پیام‌رسان‌ها می‌تواند در این دسته قرار گیرد.



قانون جرایم رایانه‌ای ایران که نخستین بار در سال ۱۳۸۸ به تصویب رسید و در سال‌های بعد نیز اصلاح و تکمیل شد، با هدف شفاف‌سازی مصادیق تخلفات و ایجاد ضمانت اجرایی برای مقابله با آن‌ها شکل گرفته است. این قانون نه تنها شامل جرایم آشکار و بزرگ، بلکه شامل مواردی می‌شود که شاید در نگاه اول بی‌ضرر یا حتی «عادی» به نظر برسند.

«۱. دسترسی غیرمجاز»

یکی از مهم‌ترین و شناخته‌شده‌ترین بخش‌های قانون، «دسترسی غیرمجاز» است. هرگونه ورود به سیستم‌های رایانه‌ای یا مخابراتی دیگران بدون اجازه صاحب آن، حتی اگر صرفاً برای «دیدن» اطلاعات باشد، جرم محسوب می‌شود.

نمونه‌ها:

«ورود به ایمیل یا شبکه اجتماعی شخصی همکار یا دوست، حتی اگر رمز عبور را در گذشته خودش داده باشد.
«مشاهده فایل‌های اشتراکی در یک شبکه سازمانی که برای شما مجوز دسترسی صادر نشده است.
«استفاده از حفرة‌های امنیتی برای ورود به وب‌سایت یا سامانه‌های داخلی یک سازمان.
مجازات در این بخش بسته به شدت و نتیجه کار، از جریمه نقدی تا حبس پیش‌بینی شده است.

«۲. شنود غیرمجاز»

طبق قانون، هرگونه شنود یا دسترسی به محتوای در حال انتقال در سیستم‌های ارتباطی بدون اجازه، ممنوع است. این شامل شنود مکالمات، پیام‌ها و حتی داده‌های منتقل‌شده در بستر اینترنت یا شبکه‌های داخلی می‌شود.

برای مثال:

«شنود تماس‌های اینترنتی در یک شبکه وای‌فای عمومی با استفاده از ابزارهای نرم‌افزاری.
«نصب بدافزار بر روی گوشی یا کامپیوتر شخصی فردی برای دسترسی به پیام‌ها و فایل‌ها.
«رهگیری و ضبط بسته‌های داده در شبکه سازمانی بدون مجوز.

«۳. جعل رایانه‌ای»

جعل رایانه‌ای یعنی تغییر، ساخت یا دستکاری داده‌های دیجیتال به گونه‌ای که به نظر برسد داده‌ها اصلی و معتبر هستند. این بخش از قانون برای جلوگیری از سوءاستفاده در حوزه اسناد دیجیتال، تراکنش‌های بانکی و مدارک هویتی آنلاین بسیار مهم است.

نمونه‌ها:

«تغییر اطلاعات موجود در یک فایل یا پایگاه داده به قصد فریب دیگران.
«تولید اسناد جعلی مانند کارت ملی یا گواهینامه دیجیتال.
«دستکاری اطلاعات مالی یا حساب کاربری برای دریافت وجه یا خدمات.

«۴. تخریب و اختلال در داده‌ها و سامانه‌ها»

هرگونه اقدام عمدی برای از بین بردن داده‌ها، تخریب نرم‌افزارها یا ایجاد اختلال در عملکرد سامانه‌های رایانه‌ای و مخابراتی، تحت

این عنوان جرم‌انگاری شده است.

مثال‌ها:

«حذف یا تغییر عمدی فایل‌های یک سیستم سازمانی.
«حملات DDoS برای از کار انداختن یک وب‌سایت یا سرویس.

«آلوده کردن شبکه با بدافزار به قصد مختل کردن عملیات.

«۵. کلاهبرداری رایانه‌ای»

این بخش، نسخه دیجیتالی همان کلاهبرداری سنتی است. استفاده از بسترهای الکترونیکی برای فریب دیگران و کسب منافع مالی یا غیرمالی، جرم محسوب می‌شود.

نمونه‌ها:

«ایجاد صفحات جعلی بانکی برای سرقت اطلاعات کارت بانکی.
«فروش کالا یا خدمات غیرواقعی در وب‌سایت‌ها یا شبکه‌های اجتماعی.

«ارسال پیام‌های دروغین برای دریافت وجه یا اطلاعات حساس.

«۶. جرایم علیه عفت و اخلاق عمومی»

یکی از بخش‌هایی که بیشترین شکایت‌ها در آن ثبت می‌شود، مربوط به انتشار یا تولید محتوای مستهجن یا مغایر با عفت عمومی در فضای مجازی است.

مثال‌ها:

«انتشار تصاویر یا فیلم‌های خصوصی افراد بدون رضایت آن‌ها.
«تولید یا بازنشر محتوای مبتذل در شبکه‌های اجتماعی.

«راه‌اندازی یا مدیریت وب‌سایت‌ها و کانال‌های توزیع محتوای غیراخلاقی.

«۷. نقض حریم خصوصی»

این بخش، از اساسی‌ترین اصول قانون جرایم رایانه‌ای است. هرگونه جمع‌آوری، ذخیره یا انتشار اطلاعات خصوصی افراد بدون رضایت آن‌ها، جرم است.

برای مثال:

«ذخیره و انتشار عکس‌های شخصی بدون اجازه.
«انتشار اطلاعات محل سکونت یا شماره تماس فردی در گروه‌ها و صفحات عمومی.

«استفاده از موقعیت مکانی یک فرد برای رهگیری یا مزاحمت.

«۸. انتشار اکاذیب و تشویش اذهان عمومی»

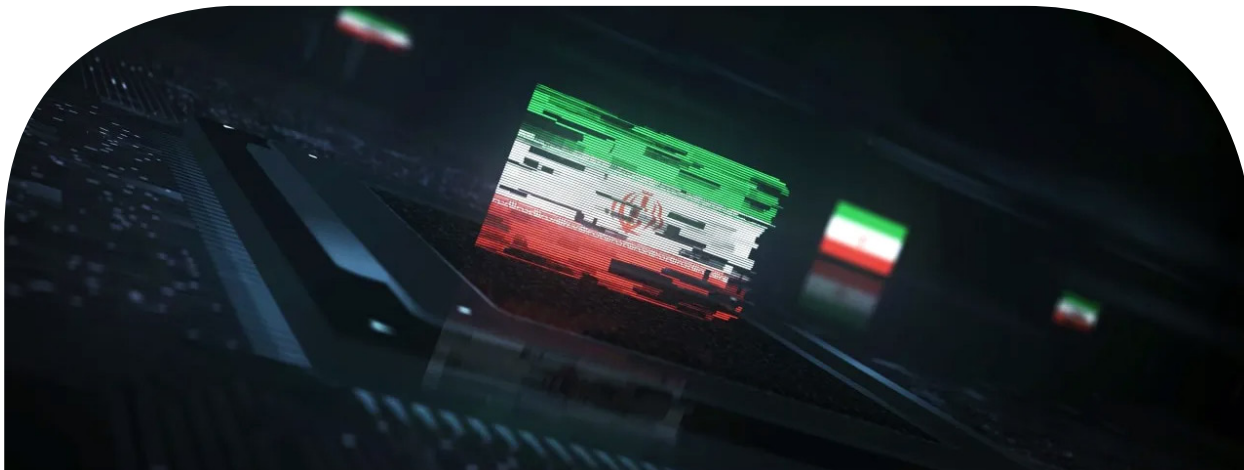
در فضای مجازی، انتشار اخبار و اطلاعات نادرست که باعث نگرانی یا آسیب به حیثیت افراد یا امنیت عمومی شود، جرم است.

نمونه‌ها:

«انتشار شایعات بی‌اساس درباره یک فرد یا سازمان.
«پخش اطلاعات نادرست درباره رویدادهای امنیتی یا اجتماعی.
«جعل بیانیه یا خبر منتسب به نهادها و سازمان‌های رسمی.

«۹. جرایم سازمان‌یافته و امنیتی»

در مواردی که اقدامات سایبری منجر به آسیب به امنیت ملی، زیرساخت‌های حیاتی یا اطلاعات محرمانه کشور شود، این بخش از قانون فعال می‌شود. مجازات‌ها در این حوزه بسیار سنگین است



یک گروه واتس‌آپ منتشر کرد. به ظاهر شوخی بود، اما به اتهام نقض حریم خصوصی شکایت شد و منجر به جریمه نقدی شد.

«دسترسی با رمز قدیمی: یک کارمند سابق با استفاده از رمز عبور قدیمی خود وارد ایمیل سازمان شد و تعدادی از مکاتبات را کپی کرد. حتی اگر این اطلاعات برای سوءاستفاده استفاده نشد، خود ورود غیرمجاز جرم بود.

«شایعه در کانال محلی: در یک شهر کوچک، ادمین یک کانال تلگرامی خبر فوت یکی از چهره‌های محلی را منتشر کرد بدون اینکه صحت آن را بررسی کند. خبر کذب بود و خانواده فرد شکایت کردند.

۲. مرز باریک بین شوخی و جرم

گاهی کاربر فکر می‌کند «فقط یک شوخی» کرده، اما قانون چنین نگاهی ندارد. فرستادن پیام‌های تهدیدآمیز، انتشار اطلاعات بدون اجازه یا حتی استفاده از تصویر دیگران در پروفایل بدون رضایت، می‌تواند در دسته جرایم سایبری قرار گیرد.

۳. جرایم رایانه‌ای در محل کار

سازمان‌ها هم محیطی پرریسک برای این جرایم هستند: «ذخیره‌سازی داده‌های محرمانه شرکت روی فلش شخصی و گم شدن آن.» «ارسال فایل‌های داخلی به ایمیل شخصی برای «کار در خانه» بدون اجازه مافوق.

«ورود به فولدرهای شبکه که دسترسی رسمی به آن‌ها ندارد.»

۴. چطور از خودمان محافظت کنیم؟

«قبل از ارسال هر فایل یا پیامی، فکر کنید که آیا صاحب آن رضایت دارد یا نه.

«رمز عبورهای قدیمی را تغییر دهید و به کسی واگذار نکنید.» «در گروه‌ها و شبکه‌های اجتماعی، از بازنشر مطالب بدون منبع معتبر خودداری کنید.

«در سازمان، مقررات امنیت اطلاعات را رعایت کنید و به دیگران هم یادآوری کنید.

نتیجه نهایی:

فضای مجازی همان‌قدر که فرصت ایجاد می‌کند، خطر هم دارد. شناخت مصادیق جرم و رعایت قوانین، تنها راه اطمینان از این است که حضور ما در این فضا امن، قانونی و بی‌دردسر باشد.

و ممکن است شامل حبس‌های طولانی یا حتی محرومیت‌های اجتماعی جدی باشد.

مثال‌ها:

«حملات به سامانه‌های زیرساختی مانند شبکه برق، آب یا حمل‌ونقل.

«سرقت یا افشای اطلاعات طبقه‌بندی شده دولتی.

«همکاری با گروه‌های هکری معاند یا تروریستی.

چه چیزهایی «جرم» محسوب نمی‌شود؟

برای اینکه مرز بین جرم و رفتار قانونی مشخص شود، باید به چند نکته توجه کرد:

«استفاده شخصی و قانونی: ورود به سامانه یا داده‌ها با اجازه رسمی صاحب آن جرم نیست.

«انتقاد یا اظهار نظر سازنده: بیان نظرات شخصی در چهارچوب قانون و بدون توهین یا نشر اکاذیب جرم محسوب نمی‌شود.

«انتشار اطلاعات عمومی: بازنشر داده‌هایی که به صورت رسمی و عمومی منتشر شده‌اند، جرم نیست.

چرا باید این موارد را بدانیم؟

نادیده گرفتن قانون جرایم رایانه‌ای می‌تواند برای هر کاربر عواقب جدی داشته باشد. حتی اگر نیت بدی نداشته باشید، باز هم قانون نسبت به نقض حقوق دیگران بی‌تفاوت نیست.

به همین دلیل، آگاهی از این قوانین نه تنها برای متخصصان IT، بلکه برای تمام کاربرانی که روزانه از اینترنت و فضای مجازی استفاده می‌کنند، ضروری است.

جرایم رایانه‌ای از پشت‌صحنه تا زندگی واقعی

وقتی درباره قانون جرایم رایانه‌ای صحبت می‌کنیم، ذهن خیلی‌ها می‌رود سمت فیلم‌های هالیوودی، هک‌هایی با مانیتورهای پر از کد، یا نفوذ به سرورهای بین‌المللی. اما واقعیت این است که بیشتر پرونده‌های سایبری که در دادگاه‌های ایران مطرح می‌شوند، ماجراهایی ساده و حتی «روزمره» هستند. ماجراهایی که می‌توانستند به راحتی اتفاق نیفتند، اگر افراد کمی دقت می‌کردند.

۱. پرونده‌های واقعی، عبرت‌های واقعی

«یک عکس شخصی، یک دردسر بزرگ: خانمی در تهران بدون اجازه دوستش، یک عکس قدیمی از دوران دانشگاه را در



... راهنمای عملی



چه کارهایی در فضای مجازی جرم محسوب می‌شوند؟ (بدون آنکه بدانیم!)

در دنیای امروز، اینترنت و شبکه‌های اجتماعی بخشی جدایی‌ناپذیر از زندگی روزمره شده‌اند. اما همان‌طور که در دنیای واقعی قوانین و محدودیت‌هایی وجود دارد، فضای مجازی نیز تابع قوانین خاص خود است. بسیاری از کاربران، به دلیل عدم آگاهی کافی از این قوانین، ناخواسته مرتکب رفتارهایی می‌شوند که در چارچوب (قانون جرایم رایانه‌ای) و سایر مقررات مرتبط، جرم تلقی می‌شود.



شناخت این مصادیق نه تنها از بروز مشکلات حقوقی پیشگیری می‌کند، بلکه به ایجاد محیطی امن‌تر و مسئولانه‌تر در فضای مجازی کمک می‌نماید. در ادامه، با مهم‌ترین مواردی که هر کاربر باید بداند آشنا می‌شویم.

«۱. نقض حریم خصوصی افراد

حریم خصوصی در فضای مجازی، به همان اندازه حریم خصوصی در محیط واقعی ارزشمند و مورد حمایت قانون است. هرگونه دسترسی، ذخیره، انتشار یا استفاده از اطلاعات شخصی افراد بدون رضایت آن‌ها، مصداق نقض حریم خصوصی و جرم محسوب می‌شود.

نمونه‌های رایج:

«انتشار عکس یا فیلم خصوصی دیگران بدون کسب اجازه، حتی اگر در محیط‌های محدود مانند گروه‌های خانوادگی یا کاری باشد.

«ضبط یا بازنشر مکالمات خصوصی در پیام‌رسان‌ها بدون اطلاع و رضایت طرف مقابل.

«ذخیره و اشتراک‌گذاری صدا یا تصویر جلسات آنلاین بدون مجوز رسمی.

مثال واقعی:

در یک پرونده حقوقی، کارمندی جلسه آنلاین داخلی سازمان را ضبط و برای دوستانش ارسال کرد تا بخشی از اشتباه یکی از همکاران را نشان دهد. این اقدام، با شکایت فرد مذکور مواجه شد و دادگاه، کارمند را به پرداخت جریمه نقدی محکوم کرد.

«۲. انتشار اخبار کذب و شایعات

طبق قانون، نشر اکاذیب و انتشار اخبار یا اطلاعات دروغ که موجب تشویش اذهان عمومی یا لطمه به حیثیت و اعتبار افراد یا سازمان‌ها شود، جرم است.

موارد شایع:

«پخش شایعه درباره مرگ، بیماری یا اتهام به اشخاص حقیقی یا حقوقی.

«انتشار خبرهای بی‌اساس درباره تعطیلی سازمان‌ها، بحران‌های اقتصادی یا اجتماعی.

«بازنشر محتوای بدون منبع معتبر در گروه‌ها و شبکه‌های اجتماعی.

نکته حقوقی: حتی اگر شما تولیدکننده اصلی خبر نباشید، ولی آن را بازنشر کنید، از نظر قانون می‌توانید مسئول شناخته شوید.

«۳. تهدید، توهین و مزاحمت اینترنتی

هرگونه تهدید به افشای اطلاعات شخصی یا وارد کردن خسارت، حتی اگر به شوخی بیان شود، می‌تواند از نظر قانونی جرم باشد. علاوه بر این، مزاحمت و آزار آنلاین نیز در قوانین پیش‌بینی شده است.

نمونه‌ها:

«ارسال مکرر پیام‌های ناخواسته به فرد یا سازمانی که تمایلی به دریافت آن ندارد.

«استفاده از الفاظ توهین‌آمیز، تحقیرکننده یا تمسخرآمیز در کامنت‌ها، پیام‌ها یا شبکه‌های اجتماعی.

«ایجاد حساب کاربری جعلی برای تخریب یا تمسخر شخصیت یک فرد.

«۴. دسترسی غیرمجاز به داده‌ها

و حساب‌های کاربری

ورود به حساب کاربری، سیستم یا فایل‌های شخصی و سازمانی دیگران بدون مجوز، حتی اگر صرفاً از روی کنجکاوی باشد، مصداق «دسترسی غیرمجاز» و جرم است.

نمونه‌های متداول:

«استفاده از رمز عبور قدیمی برای ورود به ایمیل یا حساب کاربری شخص دیگری.

«باز کردن پوشه یا فایل‌های سازمانی که به شما دسترسی رسمی برای مشاهده آن داده نشده است.

«تلاش برای حدس زدن رمز عبور یک حساب کاربری. توضیح مهم: نیازی نیست که داده‌ای را حذف یا تخریب کنید؛ صرف عمل ورود غیرمجاز، جرم‌انگاری شده است.

«۵. نقض حقوق مالکیت فکری و معنوی

قانون ایران، حق مؤلف، مصنف و هنرمند را در فضای مجازی به رسمیت می‌شناسد. کپی و انتشار آثار بدون اجازه یا ذکر منبع، می‌تواند منجر به پیگرد قانونی شود.

موارد رایج:

«دانلود، نصب یا فروش نرم‌افزارهای کرک‌شده یا نسخه‌های غیرقانونی.

«استفاده از تصاویر، ویدئوها یا مقالات بدون ذکر منبع و کسب اجازه.

«پخش غیرمجاز آثار سینمایی یا موسیقی دارای حق نشر. مثال: صفحه‌ای در شبکه اجتماعی که ویدئوهای آموزشی

یک مؤسسه را بدون مجوز منتشر می‌کند، ممکن است با شکایت صاحب اثر روبه‌رو شود.

«۶. سوءاستفاده از داده‌های شخصی و سازمانی

اطلاعات شخصی و سازمانی، مانند شماره کارت بانکی، کد ملی، آدرس، شماره تماس و داده‌های مالی، دارای ارزش قانونی و اقتصادی هستند. هرگونه سوءاستفاده از این داده‌ها جرم محسوب می‌شود.

موارد نمونه:

«فروش یا انتشار لیست مشتریان یک شرکت.

«نگهداری داده‌های سازمانی بر روی تجهیزات شخصی بدون مجوز.

«استفاده از داده‌های شخصی برای بازاریابی یا تبلیغات بدون رضایت صاحبان آن‌ها.



« ۷. فعالیت‌های تجاری غیرقانونی در فضای مجازی هرگونه خرید و فروش یا تبلیغ کالاها و خدمات غیرقانونی در فضای مجازی، جرم است. نمونه‌ها:

«فروش کالاهای قاچاق یا محصولات ممنوعه مانند داروهای بدون مجوز.
«تبلیغ خدمات غیرمجاز، مثل جعل مدارک یا فروش گواهینامه‌های جعلی.
«قمار یا شرط‌بندی آنلاین.

« ۸. نفوذ، تخریب و اختلال در داده‌ها یا سامانه‌ها اقداماتی که باعث از بین رفتن داده‌ها، تغییر غیرمجاز یا اختلال در عملکرد سیستم‌های رایانه‌ای شود، جرم است. موارد رایج:

«حذف یا تغییر اطلاعات یک پایگاه داده بدون مجوز.
«ارسال بدافزار یا ویروس برای آسیب به سیستم دیگران.
«ایجاد حملات منع سرویس برای از کار انداختن یک وب‌سایت یا سرویس.

« ۹. مسئولیت ویژه کارکنان سازمان‌ها کارکنان سازمان‌ها، به دلیل دسترسی به اطلاعات حساس، مسئولیت بیشتری دارند و تخلفات آن‌ها می‌تواند هم پیگرد اداری و هم کیفری داشته باشد.

موارد مهم:

«ارسال یا افشای اسناد داخلی سازمان به افراد یا رسانه‌های غیرمجاز.
«استفاده از ایمیل سازمانی برای مکاتبات شخصی غیرمرتبط یا مشکوک.
«اشتراک‌گذاری رمزهای عبور سازمانی با دیگران.

« ۱۰. توصیه‌های کلیدی برای پیشگیری از مشکلات قانونی

۱. قبل از ارسال یا انتشار هر محتوا، اطمینان حاصل کنید که مجاز به این کار هستید.
۲. اخبار و اطلاعات را فقط از منابع معتبر و رسمی دریافت و بازنشر کنید.
۳. حریم خصوصی دیگران را در هر شرابطی رعایت کنید.
۴. به قوانین کپی‌رایت و حقوق مالکیت فکری احترام بگذارید.
۵. از رمزهای عبور قوی و منحصر به فرد برای حساب‌های کاربری استفاده کنید.
۶. از ذخیره‌سازی اطلاعات حساس در تجهیزات یا فضاهای ناامن خودداری کنید.
۷. به یاد داشته باشید که «نادانی از قانون» مانع مجازات نخواهد شد.

CASE STUDY



... مطالعه موردی



یک شوخی کوچک که به ۶ ماه حبس کشید...

در نگاه اول، ماجرا فقط یک «شوخی» ساده بود. حداقل این طور که «امیر» تعریف می‌کرد. اما این شوخی، به دلیل بی‌اطلاعی از قوانین فضای مجازی، سرانجام به پرونده قضایی، بازجویی، و حکمی ختم شد که زندگی کاری و شخصی او را برای مدت‌ها تحت تأثیر قرار داد.





« شروع ماجرا

امیر، ۲۸ ساله، کارمند بخش فروش یک شرکت بازرگانی بود. روزی در گروه واتس‌اپی همکاران، یکی از دوستانش در شرکت، پیام خنده‌داری درباره یکی از مدیران ارسال کرد؛ محتوایی که به‌وضوح ساختگی بود، اما لحنش به‌گونه‌ای بود که اگر کسی مدیر را نمی‌شناخت، ممکن بود حرف‌ها را واقعی تصور کند. امیر که همیشه در جمع به‌عنوان «آدم شوخ» شناخته می‌شد، تصمیم گرفت «شوخی را کمی جالب‌تر» کند. او با استفاده از یک اپلیکیشن رایگان ویرایش تصویر، عکس مدیر را برداشت و متن طنزی زیر آن گذاشت که وانمود می‌کرد مدیر درگیر پرونده‌ای عجیب شده است. سپس، این تصویر را در همان گروه کاری ارسال کرد و حتی برای چند دوست دیگر هم فرستاد.

« انتشار ناخواسته

همه چیز از همین نقطه تغییر کرد. یکی از همکاران، بدون اطلاع امیر، تصویر را برای شخص دیگری خارج از شرکت ارسال کرد. ظرف کمتر از ۴۸ ساعت، تصویر در چند گروه محلی تلگرام منتشر شد و حتی به دست خود مدیر رسید. مدیر که از دیدن این محتوای تمسخرآمیز و ساختگی عصبانی شده بود، تصمیم گرفت موضوع را از طریق بخش حقوقی شرکت پیگیری کند. شکایت رسمی به دادسرای جرایم رایانه‌ای ثبت شد؛ اتهام: نشر اکاذیب و توهین از طریق سامانه‌های رایانه‌ای.

« مسیر قانونی

امیر که تصور می‌کرد «شوخی» است و کسی آن را جدی نمی‌گیرد، به محض دریافت احضاریه شوکه شد. او هرگز با دادگاه یا پلیس سر و کار نداشت و حتی نمی‌دانست دقیقاً چه جرمی به او نسبت داده شده است. در بازجویی اولیه، مأمور پرونده از او خواست محتوای منتشرشده را توضیح دهد. امیر گفت: این فقط یک شوخی بود، همه هم می‌دانستند که واقعی نیست. اما مأمور پاسخ داد: شما نمی‌توانید تشخیص دهید که همه مخاطبان درک می‌کنند این محتوا شوخی است. قانون بر اساس اثر و پیامد قضاوت می‌کند، نه صرف نیت شما.

« قوانین چه می‌گویند؟

طبق ماده ۱۸ قانون جرایم رایانه‌ای، هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی، اکاذیبی را از طریق سامانه‌های رایانه‌ای یا مخابراتی منتشر کند یا در دسترس دیگران قرار دهد، به حبس یا جزای نقدی محکوم می‌شود. همچنین، طبق ماده ۶۰۸ قانون مجازات اسلامی، توهین به

اشخاص حقیقی از طریق هر وسیله‌ای، حتی در فضای مجازی، می‌تواند مجازات حبس یا جزای نقدی داشته باشد. در این پرونده، ترکیب انتشار مطالب کذب، توهین و استفاده از تصویر شخص بدون اجازه، باعث شد اتهامات امیر سنگین‌تر شود.

« نتیجه دادگاه

پس از چند جلسه بررسی و ارائه دفاعیات، دادگاه با توجه به اینکه انتشار اولیه در گروه کاری صورت گرفته و سپس به بیرون درز کرده، مسئولیت اصلی را بر عهده امیر گذاشت. قاضی با در نظر گرفتن اینکه امیر سابقه کیفری نداشت و انگیزه مالی هم در کار نبوده، مجازات را به حداقل رساند: شش ماه حبس تعزیری که با قید تعلیق به مدت دو سال همراه شد، به‌علاوه پرداخت جزای نقدی و عذرخواهی رسمی از شاکی.

« پیامدهای فراتر از حکم

گرچه حکم زندان تعلیقی بود و امیر به زندان نرفت، اما این ماجرا پیامدهای دیگری داشت:

- « از دست دادن اعتبار شغلی در شرکت
- « قطع همکاری و اخراج از محل کار
- « خدشه‌دار شدن روابط اجتماعی و خانوادگی
- « نگرانی از سابقه قضایی در پرونده کاری

امیر بعدها می‌گفت: فکر نمی‌کردم یک تصویر ادیت‌شده بتواند چنین فاجعه‌ای درست کند. حالا فهمیدم که در فضای مجازی، شوخی هم باید حد و مرز داشته باشد.

« درس‌هایی برای همه:

- « شوخی بدون رضایت طرف مقابل، می‌تواند مصداق توهین یا نشر اکاذیب باشد، حتی اگر در جمعی کوچک منتشر شود.
- « فضای مجازی خصوصی مطلق ندارد؛ هر محتوایی به‌راحتی می‌تواند از یک گروه محدود خارج و گسترده شود.
- « نیت شما تضمین‌کننده بی‌ضرر بودن عملتان نیست؛ قانون به اثر و پیامد نگاه می‌کند.
- « استفاده از تصویر و نام افراد بدون مجوز، به‌خصوص در محتوای منفی، ریسک بالایی دارد.

« توصیه نهایی

در دنیای دیجیتال، قبل از انتشار هر محتوا، یک سؤال ساده از خود بپرسید اگر این پیام یا تصویر به دست همه برسد، آیا می‌توانم پاسخگویش باشم؟ گاهی یک ثانیه مکث، می‌تواند از ماه‌ها دردسر و هزینه جلوگیری کند.

INTERVIEW



... مصاحبه



از فوروارد تا فیلتر؛ گفت‌وگو با کارشناس حقوق سایبری

در سال‌های اخیر، جرایم رایانه‌ای به بخشی جدانشدنی از زندگی دیجیتال ما تبدیل شده‌اند. با گسترش شبکه‌های اجتماعی، پیام‌رسان‌ها و ابزارهای ارتباطی آنلاین، مرز بین «استفاده عادی» و «ارتکاب جرم» به طرز نگران‌کننده‌ای باریک شده است. برای روشن‌تر شدن این موضوع، با «دکتر نادر کیانی» وکیل پایه یک دادگستری و کارشناس حقوق سایبری گفت‌وگو کرده‌ایم.



« آقای دکتر، به طور کلی جرایم رایانه‌ای را چطور تعریف می‌کنید؟

پاسخ: قانون جرایم رایانه‌ای، هر عمل مجرمانه‌ای که با استفاده از سامانه‌های رایانه‌ای یا مخابراتی انجام شود را در بر می‌گیرد. این یعنی از هک و نفوذ گرفته تا انتشار محتوای مستهجن، جعل اسناد دیجیتال، یا حتی ارسال یک پیام توهین‌آمیز در شبکه اجتماعی می‌تواند زیر این چتر قرار بگیرد. مهم است بدانیم که در این حوزه، هم «وسیله ارتکاب جرم» و هم «ماهیت عمل» در تعیین عنوان مجرمانه نقش دارند.

« خیلی‌ها فکر می‌کنند فقط هکرها یا مجرمان حرفه‌ای مشمول این قانون می‌شوند. آیا این درست است؟

پاسخ: خیر. این یکی از بزرگ‌ترین سوء تفاهم‌هاست. آمار نشان می‌دهد که بخش قابل توجهی از پرونده‌های جرایم رایانه‌ای علیه افراد عادی تشکیل می‌شود. مثلاً فردی که یک ویدئوی خصوصی را بدون اجازه در گروه خانوادگی منتشر می‌کند، یا کارمندی که ایمیل محرمانه سازمان را برای دوستش فوروارد می‌کند، بدون آنکه قصد آسیب داشته باشد. قانون در بسیاری موارد به «نتیجه عمل» توجه دارد، نه نیت.

« یعنی حتی یک فوروارد ساده هم ممکن است جرم باشد؟

پاسخ: بله، بسته به محتوا. اگر مطلبی که فوروارد می‌کنید حاوی توهین، افترا یا نشر اکاذیب باشد، شما در گسترش آن نقش داشته‌اید و می‌توانید پاسخگو باشید. حتی باز نشر یک شایعه محلی درباره یک شخص یا کسب و کار کوچک، در صورت ایجاد ضرر، قابل پیگیری قضایی است.

« در فضای مجازی گاهی شوخی‌های تصویری با دوستان می‌کنیم. این هم ممکن است مشکل ساز شود؟

پاسخ: قطعاً. انتشار یا ویرایش تصاویر اشخاص بدون رضایت آن‌ها می‌تواند مصداق نقض حریم خصوصی و حتی افترا باشد، حتی اگر نیت شما صرفاً شوخی باشد. قانون به نیت خیر یا بد کمتر توجه می‌کند و بیشتر به اثر و آسیب وارده اهمیت می‌دهد.

« استفاده از فیلترشکن یا VPN چه وضعیتی دارد؟

پاسخ: قانون فعلی ایران استفاده شخصی از VPN را جرم‌انگاری نکرده، اما این موضوع خاکستری است. اگر از VPN برای دسترسی به سرویس‌های غیرقانونی یا ارتکاب جرم استفاده کنید، عمل شما مشمول مجازات می‌شود. به علاوه، برخی فعالیت‌ها حتی با ابزارهای امن، قابل ردیابی است. تصور ناشناس ماندن کامل، اشتباه خطرناکی است.

« برخی کاربران فکر می‌کنند گروه‌های خصوصی یا پیام‌های پاک‌شده، امن هستند. این تصور درست است؟

پاسخ: خیر. هیچ بستری در فضای مجازی صد درصد امن نیست. داده‌ها ممکن است روی سرورهای خارجی ذخیره شوند یا توسط

اعضای گروه اسکرین‌شات گرفته شود. حتی پیام‌های حذف‌شده در برخی موارد قابل بازیابی فنی هستند.

« مهم‌ترین اشتباهات رایج کاربران که باعث تشکیل پرونده می‌شود چیست؟

- پاسخ:
۱. باز نشر بدون تحقیق محتوا.
 ۲. ورود به حریم خصوصی دیگران بدون رضایت.
 ۳. ذخیره و اشتراک‌گذاری فایل‌های حساس در فضای ابری بدون رمزگذاری.
 ۴. شوخی‌های متنی یا تصویری که بار حقوقی دارد.
 ۵. اعتماد بیش از حد به پیام‌رسان‌ها و گروه‌های «به ظاهر» امن.

« آیا ناآگاهی از قانون می‌تواند به عنوان دفاع مطرح شود؟

پاسخ: در نظام حقوقی ایران، «جهل به قانون» عذر موجه نیست. یعنی اگر بگویید «نمی‌دانستم این کار جرم است»، معمولاً پذیرفته نمی‌شود. اینجاست که اهمیت آموزش عمومی قوانین سایبری خودش را نشان می‌دهد.

« اگر فردی ناخواسته محتوای مجرمانه را منتشر کند و بعد متوجه شود، باید چه کند؟

پاسخ: باید فوراً انتشار را متوقف کند، محتوای منتشرشده را حذف کند و اگر لازم بود، عذرخواهی عمومی یا شخصی انجام دهد. نگهداری نسخه اصلی محتوا برای ارائه به وکیل یا مقام قضایی هم مهم است تا ثابت کند اقدام اصلاحی سریع انجام شده است.

« آیا کارفرما می‌تواند بابت فعالیت‌های آنلاین کارمندش، حتی خارج از ساعت کاری، اقدام قانونی کند؟

پاسخ: بستگی دارد. اگر فعالیت آن کارمند به اعتبار یا اسرار تجاری شرکت لطمه بزند، حتی خارج از ساعات کاری، کارفرما می‌تواند از مسیر حقوقی یا کیفری پیگیری کند. این موضوع در قراردادهای کاری شفاف‌تر مشخص می‌شود.

« در مورد محتوای انتقادی، مرز بین آزادی بیان و جرم کجاست؟

پاسخ: نقد سازنده و مستند، جرم نیست. اما وقتی انتقاد به توهین، افترا یا نشر اکاذیب تبدیل شود، وارد حوزه جرم می‌شود. مستند بودن، بی‌طرفی و پرهیز از الفاظ تحقیرآمیز، سه اصل کلیدی هستند.

« نقش ادله دیجیتال در این پرونده‌ها چقدر مهم است؟

پاسخ: بسیار زیاد. پیام‌ها، ایمیل‌ها، تصاویر و لاگ‌های سیستم می‌توانند به عنوان سند در دادگاه پذیرفته شوند. البته این ادله باید به روش قانونی جمع‌آوری شوند تا اعتبار داشته باشند. بسیاری از پرونده‌ها صرفاً به خاطر ارائه یا نبود یک اسکرین‌شات معتبر، نتیجه متفاوتی گرفته‌اند.



... راهنمای دفاع



راهنمای عملی اقدامات لازم در مواجهه با شکایت‌های سایبری

امروزه بخش زیادی از ارتباطات، معاملات، کار و حتی تفریحات ما به فضای مجازی منتقل شده است. همین موضوع باعث شده تا احتمال درگیر شدن با مسائل حقوقی و شکایت‌های مرتبط با جرایم رایانه‌ای، برای هر فردی - حتی کسانی که خودشان را کاربر ساده می‌دانند - وجود داشته باشد. تصور کنید یک روز صبح، پیامکی از سامانه ابلاغ الکترونیک قضایی (ثنا) دریافت می‌کنید که نشان می‌دهد علیه شما شکایتی در حوزه سایبری ثبت شده است. شوک، نگرانی و حتی ترس طبیعی است، اما مهم‌تر از همه، واکنش درست و به‌موقع است.



در ادامه، گام به گام توضیح می‌دهیم که در چنین شرایطی باید چه کارهایی انجام دهید تا از حقوق خود دفاع کنید و اشتباهات رایج را تکرار نکنید.

« ۱. اول از همه، آرامش خود را حفظ کنید

اولین واکنش اغلب افراد، ترس شدید یا انکار ماجراست. اما این واکنش می‌تواند باعث شود کارهای اشتباهی انجام دهید، مثل پاک کردن پیام‌ها یا حذف حساب کاربری، که بعدها ممکن است به عنوان امحای ادله تلقی شود و به ضررتان تمام شود.

به جای این کار، چند نفس عمیق بکشید و به خاطر داشته باشید که تا زمان صدور حکم، شما مجرم محسوب نمی‌شوید و قانون به شما حق دفاع کامل داده است.

« ۲. بررسی دقیق ابلاغیه یا پیام دریافتی

اگر از طریق سامانه ثنا یا پیامک رسمی قوه قضاییه، اطلاعیه‌ای دریافت کرده‌اید:

«وارد حساب کاربری ثنای خود شوید و متن کامل ابلاغیه را بخوانید.

«تاریخ جلسه یا مهلت ارائه دفاعیه را یادداشت کنید.

«بررسی کنید موضوع شکایت چیست و تحت کدام ماده یا عنوان قانونی ثبت شده است.

گاهی اوقات، موضوع به یک سوء تفاهم یا اختلاف ساده برمی‌گردد که با مذاکره قابل حل است.

« ۳. جمع‌آوری و نگهداری ادله دیجیتال

در پرونده‌های سایبری، مدارک دیجیتال اهمیت حیاتی دارند. هر چیزی که بتواند ادعای شما را ثابت کند، باید به شکل امن نگهداری شود:

«اسکرین‌شات‌های پیام‌ها، ایمیل‌ها یا محتوای منتشرشده.

«فایل‌های اصلی بدون تغییر.

«لاگ‌های فعالیت (در صورت دسترسی).

«رسید یا سندی که نشان دهد شما مالک حساب یا دستگاه نبوده‌اید.

توجه کنید: تغییر، دستکاری یا حذف این داده‌ها می‌تواند بر علیه شما استفاده شود.

« ۴. مشورت با وکیل متخصص جرایم رایانه‌ای

قوانین سایبری پیچیدگی‌های خاص خود را دارند. یک وکیل آشنا با این حوزه می‌تواند:

«اتهام را دقیق برایتان توضیح دهد.

«بگوید که شاکی باید چه مدارکی ارائه کند.

«راهکارهای قانونی برای دفاع ارائه دهد.

«در جلسه بازجویی با دادگاه همراه شما باشد تا از بیان مطالبی که ممکن است بر علیه شما تفسیر شود، جلوگیری کند.

حتی اگر نمی‌توانید وکیل بگیرید، بهتر است با یک مشاور حقوقی یا مرکز معاضدت قضایی مشورت کنید.

« ۵. پاسخ به احضاریه یا دعوت بازپرسی

بی‌توجهی به احضاریه می‌تواند منجر به صدور حکم جلب شود. پس:

«در تاریخ تعیین‌شده حاضر شوید.

«با آرامش و صداقت صحبت کنید، ولی تنها در محدوده‌ای که وکیل یا مشاور توصیه کرده توضیح دهید.

«اگر سوالی را نمی‌دانید یا مطمئن نیستید، بگویید «نیاز به

بررسی دارم» به جای اینکه حدس بزنید یا چیزی بگویید که بعداً خلافش ثابت شود.

« ۶. پرهیز از هرگونه تماس مستقیم با شاکی

در بسیاری از پرونده‌ها، تلاش برای تماس مستقیم با شاکی (برای توضیح یا عذرخواهی) می‌تواند وضعیت را بدتر کند، چون ممکن است به عنوان تهدید، تطمیع یا مزاحمت تفسیر شود. در صورت لزوم، هرگونه مذاکره باید از طریق وکیل یا به صورت رسمی در مرجع قضایی انجام شود.

« ۷. استفاده از فرصت صلح و سازش

اگر موضوع پرونده از نوع قابل گذشت باشد، می‌توان با شاکی به توافق رسید و پرونده را مختومه کرد. بسیاری از شکایات ناشی از سوء تفاهم یا عصبانیت لحظه‌ای است و با یک گفت‌وگوی رسمی یا عذرخواهی، قابل حل است. اما این کار باید با ثبت رسمی توافق و رضایت در دادسرا یا شورای حل اختلاف انجام شود تا از نظر قانونی معتبر باشد.

« ۸. مراقب رفتار آنلاین خود بعد از شکایت باشید

تا زمان پایان پرونده:

«از انتشار هرگونه مطلب مرتبط با پرونده در فضای مجازی خودداری کنید.

«درباره شاکی یا موضوع پرونده، هیچ‌گونه اظهار نظر عمومی نکنید.

«امنیت حساب‌های کاربری خود را افزایش دهید تا از ورود غیرمجاز و انتشار محتوای مشکوک جلوگیری شود.

« ۹. حضور در دادگاه یا جلسه رسیدگی

در جلسه دادگاه:

«لباس و ظاهر آراسته داشته باشید، چون اولین برداشت قاضی می‌تواند ناخودآگاه تأثیرگذار باشد.

«با احترام صحبت کنید و اجازه دهید قاضی یا بازپرس صحبت شما را قطع یا هدایت کند.

«در ارائه مدارک، نظم داشته باشید و نسخه چاپی یا الکترونیکی منظم ارائه دهید.

« ۱۰. پیگیری نتیجه و مراحل بعدی

پس از پایان جلسه:

«رأی دادگاه یا نظر بازپرس را به دقت مطالعه کنید.

«اگر نتیجه به ضررتان بود و حق تجدیدنظر دارید، سریعاً اقدام کنید چون مهلت محدود است.

«در صورت برائت یا مختومه شدن پرونده، ابلاغیه رسمی را نزد خود نگه دارید.

« ۱۱. یادگیری برای آینده

حتی اگر بی‌گناه باشید، این تجربه می‌تواند درس بزرگی برای آینده باشد:

«محتاط‌تر در فضای مجازی رفتار کنید.

«قوانین پایه‌ای جرایم رایانه‌ای را یاد بگیرید.

«اطلاعات شخصی و کاری را با امنیت بیشتری نگه دارید.

« جمع‌بندی:

در پرونده‌های سایبری، سرعت و دقت در واکنش اهمیت زیادی دارد. عجله در تصمیم‌گیری یا بی‌توجهی به مراحل قانونی می‌تواند خسارت‌های جبران‌ناپذیری به همراه داشته باشد. به یاد داشته باشید که دفاع موفق، ترکیبی از آرامش، مستندسازی، مشورت حقوقی و رعایت کامل فرآیند قضایی است.

CHECKLIST



... چک لیست



هفت رفتار رایج در فضای مجازی که می‌تواند موجب مسئولیت کیفری شود

با گسترش استفاده از اینترنت و شبکه‌های اجتماعی، بسیاری از رفتارهایی که شاید در نگاه اول بی‌ضرر یا حتی عادی به نظر برسند، می‌توانند در قالب «جرم رایانه‌ای» یا «تخلف سایبری» قرار بگیرند. نکته مهم این است که در حقوق کیفری، ناآگاهی از قانون، مانع مجازات نیست؛ یعنی حتی اگر نیت بدی نداشته باشید، باز هم ممکن است مسئولیت کیفری پیدا کنید. در ادامه، هفت رفتار رایج را بررسی می‌کنیم که انجام آن‌ها می‌تواند شما را در معرض پیگرد قانونی قرار دهد.



« ۱. انتشار یا بازنشر محتوای توهین‌آمیز یا افترا بسیاری از کاربران، بدون دقت کافی، پیام‌ها یا پست‌هایی را که حاوی توهین، افترا یا مطالب خلاف واقع درباره افراد است، بازنشر می‌کنند.

« مثال: فوروارد یک پیام در گروه خانوادگی که به شخصیت یک فرد یا مقام رسمی توهین می‌کند.
« پیامد حقوقی: مطابق قانون جرایم رایانه‌ای و مواد قانون مجازات اسلامی، انتشار یا بازنشر چنین محتواهایی می‌تواند منجر به تعقیب کیفری شود.
« نکته: حتی اگر شما نویسنده پیام نباشید، ولی آن را منتشر یا بازنشر کنید، مسئولیت قانونی دارید.

« ۲. ذخیره و انتشار تصاویر یا ویدئوهای خصوصی دیگران بدون اجازه

« ذخیره یا ارسال فایل‌های خصوصی دیگران، حتی اگر از طریق یک دوست یا گروه به دست شما رسیده باشد، می‌تواند جرم محسوب شود.
« مثال: دریافت یک عکس خصوصی و ارسال آن برای یک دوست به شوخی.
« پیامد حقوقی: طبق قانون، این عمل «انتشار محتوای مستهجن یا خصوصی» تلقی می‌شود و می‌تواند شامل مجازات حبس و جزای نقدی باشد.
« نکته: رضایت صاحب تصویر یا ویدئو شرط اصلی برای هرگونه انتشار است.

« ۳. استفاده غیرمجاز از تصاویر یا محتوای تولیدی دیگران

« بسیاری از کاربران فکر می‌کنند چون یک تصویر یا متن در اینترنت وجود دارد، استفاده از آن آزاد است.
« مثال: برداشتن عکس یک عکاس حرفه‌ای از اینترنت و استفاده در تبلیغات یا شبکه اجتماعی شخصی بدون ذکر منبع یا اجازه.
« پیامد حقوقی: این کار نقض «حقوق مالکیت فکری» محسوب می‌شود و می‌تواند منجر به شکایت مدنی یا کیفری شود.
« نکته: همیشه منبع و مالک اثر را ذکر کنید و در موارد تجاری، حتماً اجازه رسمی بگیرید.

« ۴. دسترسی غیرمجاز

به حساب‌های کاربری دیگران

« گاهی افراد برای کنجکاوی یا شوخی، به حساب کاربری ایمیل، اینستاگرام یا حتی سیستم‌های داخلی محل کار دیگران وارد می‌شوند.
« مثال: استفاده از رمز عبور همکار که قبلاً روی سیستمش ذخیره شده است.
« پیامد حقوقی: این رفتار مصداق «دسترسی غیرمجاز»

است که طبق قانون جرایم رایانه‌ای جرم‌انگاری شده و مجازات سنگینی دارد.
« نکته: حتی اگر اطلاعات را تغییر ندهید، صرف ورود بدون مجوز هم جرم است.

« ۵. ایجاد یا انتشار اخبار و اطلاعات نادرست انتشار شایعات یا اطلاعات تأییدنشده، مخصوصاً درباره مسائل حساس، می‌تواند پیامد قانونی جدی داشته باشد.
« مثال: پخش خبر جعلی درباره وضعیت یک بانک، که باعث نگرانی عمومی می‌شود.
« پیامد حقوقی: این عمل تحت عنوان «تشویش اذهان عمومی» یا «انتشار اکاذیب» پیگرد دارد.
« نکته: قبل از انتشار هر خبر، صحت آن را از منابع معتبر بررسی کنید.

« ۶. دانلود و استفاده از نرم‌افزارهای کرک‌شده یا محتوای غیرمجاز

« گرچه بسیاری از کاربران نرم‌افزارها یا فیلم‌های کرک‌شده را استفاده می‌کنند، اما این کار نقض قوانین حق مؤلف و مالکیت معنوی است.
« مثال: دانلود نسخه کرک‌شده یک نرم‌افزار و استفاده در محیط کاری.
« پیامد حقوقی: علاوه بر جنبه کیفری، ممکن است مجبور به پرداخت خسارت به صاحب اثر شوید.
« نکته: استفاده از نسخه‌های قانونی، حتی اگر هزینه‌بر باشد، ریسک‌های حقوقی و امنیتی را کاهش می‌دهد.

« ۷. ورود به حریم خصوصی افراد در فضای آنلاین

« حتی پرس‌وجو یا جمع‌آوری اطلاعات شخصی افراد بدون اجازه، می‌تواند مصداق نقض حریم خصوصی باشد.
« مثال: استفاده از شماره موبایل یا ایمیل فردی که بدون رضایتش در اختیار شما قرار گرفته، برای ارسال پیام تبلیغاتی یا شخصی.
« پیامد حقوقی: این کار می‌تواند منجر به شکایت به دلیل مزاحمت یا نقض حریم خصوصی شود.
« نکته: حریم خصوصی در فضای مجازی همان‌قدر مهم است که در دنیای واقعی.

« جمع‌بندی:

« در فضای مجازی، مرز بین یک رفتار عادی و یک جرم، گاهی بسیار باریک است. آگاهی از قوانین و رعایت اصول اخلاقی و حقوقی، بهترین راه برای جلوگیری از مشکلات احتمالی است. به یاد داشته باشید که «نیت خیر» یا «شوخی» توجیه قانونی محسوب نمی‌شود و مسئولیت هر آنچه منتشر یا انجام می‌دهید، بر عهده خود شماست.

LAW



... قانون به زبان ساده



شرح ساده قانون جرایم رایانه‌ای؛ ماده به ماده

قانون جرایم رایانه‌ای در ایران با هدف مقابله با تخلفات و جرایمی تدوین شده که از طریق ابزارها و بسترهای دیجیتال صورت می‌گیرند. این قانون، همانند هر متن قانونی دیگر، با اصطلاحات تخصصی و ادبیات رسمی نگارش شده که ممکن است برای عموم مردم پیچیده باشد. هدف ما در این مطلب، ساده‌سازی و توضیح روان مواد اصلی این قانون است تا هر فرد بتواند بفهمد چه اعمالی جرم محسوب می‌شوند و چه پیامدهایی دارند.



« بخش اول: دسترسی غیرمجاز (ماده ۱)

متن ساده‌شده: هرگونه وارد شدن به سیستم‌ها، شبکه‌ها یا حساب‌های کاربری بدون اجازه صاحب آن‌ها، حتی اگر تغییر یا خرابکاری انجام نشود، جرم است.

مثال: اگر به ایمیل دوستان وارد شوید چون رمز عبورش را حدس زده‌اید، حتی بدون تغییر دادن اطلاعات، مرتکب جرم شده‌اید.

مجازات: طبق قانون، این عمل می‌تواند منجر به حبس یا جزای نقدی شود.

« بخش دوم: شنود غیرمجاز (ماده ۲)

متن ساده‌شده: اگر بدون اجازه، مکالمات، پیام‌ها یا داده‌های در حال انتقال بین دو نفر را ضبط یا شنود کنید، جرم مرتکب شده‌اید.

مثال: نصب نرم‌افزار جاسوسی روی گوشی فردی بدون اطلاع او.

مجازات: حبس یا جریمه نقدی، بسته به نوع و میزان جرم.

« بخش سوم: دستکاری و تخریب داده‌ها (ماده ۳)

متن ساده‌شده: تغییر، پاک کردن یا خراب کردن داده‌ها یا اختلال در کارکرد سیستم‌ها، بدون مجوز، جرم محسوب می‌شود.

مثال: پاک کردن فایل‌های محل کار یا تغییر اطلاعات در یک پایگاه داده.

مجازات: بسته به خسارت وارده، از جزای نقدی تا حبس چندساله.

« بخش چهارم: جعل رایانه‌ای (ماده ۴)

متن ساده‌شده: ساخت یا تغییر داده‌های دیجیتال به گونه‌ای که به عنوان اصل شناخته شوند، جرم است.

مثال: ساخت یک گواهی‌نامه جعلی به صورت فایل PDF که ظاهراً معتبر به نظر می‌رسد.

مجازات: مشابه جعل اسناد فیزیکی، شامل حبس و جزای نقدی.

« بخش پنجم: سرقت و کلاهبرداری رایانه‌ای (مواد ۱۲ و ۱۳)

متن ساده‌شده: استفاده از ابزار دیجیتال برای گرفتن مال یا امتیاز دیگران به صورت غیرقانونی، جرم است.

مثال: فیشینگ و سرقت اطلاعات بانکی برای برداشت غیرمجاز از حساب.

مجازات: بازگرداندن اموال + حبس + جزای نقدی.

« بخش ششم: انتشار محتوای مجرمانه (مواد ۱۴ تا ۱۸)

متن ساده‌شده: انتشار یا در دسترس قرار دادن هرگونه محتوای مجرمانه مانند تصاویر مستهجن، تبلیغات تروریستی، یا محتوای حاوی توهین به مقدسات، جرم است.

مثال: انتشار ویدئوی غیراخلاقی یا پست‌های حاوی محتوای نفرت‌پراکن.

مجازات: از جزای نقدی تا چند سال حبس، بسته به نوع محتوا.

« بخش هفتم: نقض حریم خصوصی (مواد ۱۶ و ۱۷)

متن ساده‌شده: هرگونه افشا یا انتشار اطلاعات شخصی دیگران بدون رضایت، حتی اگر اطلاعات حساس نباشند، جرم است.

مثال: انتشار شماره تلفن یا آدرس یک شخص در شبکه‌های اجتماعی بدون اجازه او.

مجازات: بسته به شرایط، شامل حبس و جزای نقدی.

« بخش هشتم: مسئولیت مدیران سایت‌ها و اپلیکیشن‌ها

متن ساده‌شده: اگر شما مدیر یک سایت یا پلتفرم هستید و از محتوای مجرمانه کاربران اطلاع پیدا کنید و اقدامی برای حذف آن نکنید، مسئولیت قانونی خواهید داشت.

مثال: عدم حذف محتوای توهین‌آمیز یا غیراخلاقی منتشرشده توسط کاربر.

مجازات: مسئولیت کیفری مشابه فرد منتشرکننده محتوا.

« بخش نهم: همکاری در جرم

متن ساده‌شده: حتی اگر خودتان جرم را مستقیماً انجام ندهید اما ابزار، اطلاعات یا راهنمایی برای ارتکاب آن به دیگری بدهید، شریک جرم محسوب می‌شوید.

مثال: دادن نرم‌افزار هک به فردی که می‌داند قصد سوءاستفاده دارد.

مجازات: مشابه مجازات فرد مجرم اصلی.

« بخش دهم: جمع‌بندی و توصیه‌ها

قانون جرایم رایانه‌ای به‌طور مستقیم بر رفتار ما در فضای مجازی تأثیر می‌گذارد. دانستن این مواد قانونی نه تنها باعث می‌شود از مشکلات احتمالی جلوگیری کنیم، بلکه به ما کمک می‌کند حریم خصوصی و حقوق دیگران را نیز رعایت کنیم. یادمان باشد که فضای مجازی «بی‌قانون» نیست و همانند دنیای واقعی، مرزها و قواعد مشخصی دارد.

SCENARIO



... سناریو



یک پست اشتباهی، مسیری به سوی مشکلات حقوقی

فضای مجازی فرصتی بی‌نظیر برای ارتباط، بیان عقاید و اشتراک‌گذاری لحظات زندگی است. اما همین فضا که در نگاه اول بی‌خطر و سرگرم‌کننده به نظر می‌رسد، می‌تواند به بستری برای مشکلات جدی حقوقی و حتی مجازات‌های سنگین تبدیل شود. در بسیاری از پرونده‌ها، تنها یک اقدام ساده و بی‌فکرانه مانند ارسال یک تصویر، ویدئو یا متن، منجر به شکایت، احضار و حتی محکومیت شده است.



این سناریو داستانی، بر اساس اتفاقات واقعی اما با تغییر جزئیات و اسامی، تلاش دارد نشان دهد که چگونه یک پست به ظاهر بی اهمیت، می تواند آغازگر زنجیره ای از دردها باشد.

« بخش اول - شروع ماجرا

امیر، کارمند یک شرکت خصوصی، علاقه زیادی به حضور فعال در شبکه های اجتماعی داشت. او در طول روز بارها از لحظات زندگی، محیط کار و حتی صحبت های دوستانه اش پست و استوری منتشر می کرد.

یک روز بعد از ظهر، در جریان یک گفت و گوی خودمانی با همکاران، شوخی ای درباره یکی از مدیران شرکت مطرح شد. شوخی ای که به نظر امیر بی ضرر بود و فقط باعث خنده جمع می شد. او بدون فکر زیاد، همین شوخی را در قالب یک پست طنز به همراه تصویری دستکاری شده از آن مدیر در صفحه شخصی اش منتشر کرد. امیر تصور می کرد که این پست فقط توسط دوستان نزدیکش دیده می شود و هرگز به دست شخص مدیر یا افراد خارج از حلقه دوستانش نمی رسد. اما در کمتر از ۲۴ ساعت، پست از طریق اسکرین شات و بازنشر به گروه ها و صفحات مختلف راه یافت.

« بخش دوم - گسترش واکنش ها

ابتدا واکنش ها طنزآمیز و همراه با شوخی بود. اما خیلی زود عده ای این محتوا را توهین آمیز و خلاف شأن کاری دانستند. برخی حتی در بخش نظرات، به آن مدیر و عملکردش در شرکت حمله کردند. چند روز بعد، امیر احضاریه ای از پلیس فتا دریافت کرد. اتهام او «توهین و نشر اکاذیب در فضای مجازی» عنوان شده بود. امیر شوکه شد. او هرگز تصور نمی کرد که یک شوخی شخصی بتواند رنگ و بوی جرم بگیرد.

« بخش سوم - ورود قانون

در مرکز پلیس فتا، به امیر توضیح داده شد که طبق قانون جرایم رایانه ای، هرگونه انتشار محتوایی که به شخصیت حقیقی یا حقوقی افراد لطمه بزند یا باعث خدشه دار شدن اعتبار آن ها شود، می تواند جرم محسوب شود، حتی اگر نیت بدی در کار نبوده باشد. مأمور پرونده به او یادآوری کرد که در فضای مجازی، گستره انتشار محتوا غیرقابل کنترل است و یک پست کوچک می تواند به سرعت میان هزاران کاربر منتشر شود. همین گسترش غیرقابل پیش بینی، پایه بسیاری از شکایت های سایبری است.

« بخش چهارم - روند رسیدگی

پرونده امیر به دادسرا ارجاع شد. شاکی، همان مدیر شرکت، مدعی شد که پست منتشر شده باعث خدشه به اعتبار حرفه ای و جایگاه سازمانی او شده است. در دفاعیات، امیر توضیح داد که قصد توهین نداشته و پست را صرفاً در فضای دوستانه منتشر کرده است. با این حال، قاضی به استناد شواهد و گستره انتشار محتوا، استدلال کرد که حتی اگر قصد بدی وجود نداشته، نتیجه انتشار، آسیب به اعتبار فرد و سازمان بوده و این امر طبق قانون قابل پیگیری است. در نهایت، امیر با تخفیف مجازات به دلیل فقدان سابقه کیفری و ابراز پشیمانی، به جزای نقدی و الزام به

عذرخواهی رسمی محکوم شد.

« بخش پنجم - پیامدهای غیرقابل پیش بینی

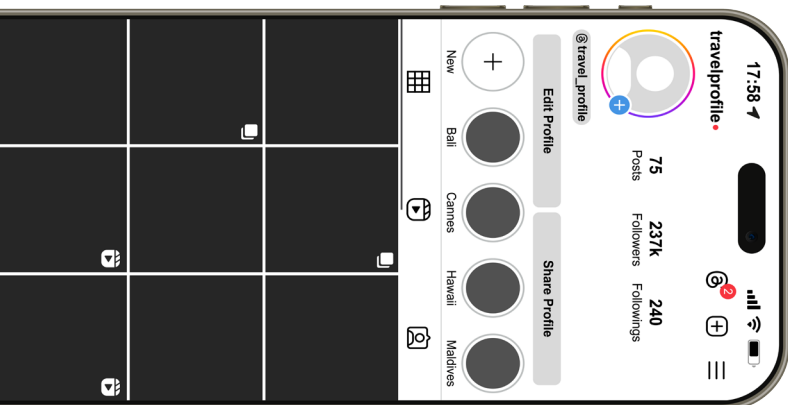
مجازات قضایی تنها بخشی از ماجرا بود. امیر پس از این اتفاق، روابط کاری پرتنشی با برخی همکاران پیدا کرد. مدیران شرکت اعتماد قبلی را نسبت به او نداشتند. حتی برخی دوستانش در شبکه های اجتماعی، ارتباط خود را کاهش دادند. امیر تازه فهمید که پیامدهای یک اشتباه در فضای مجازی، تنها به جریمه یا حبس محدود نمی شود، بلکه می تواند سال ها بر اعتبار شخصی و حرفه ای فرد اثر بگذارد.

« بخش ششم - درس هایی که باید گرفت

۱. هیچ محتوایی در فضای مجازی خصوصی نیست. حتی پیام هایی که در گروه های بسته یا بین دوستان منتشر می شوند، ممکن است به خارج از آن محیط راه پیدا کنند.
۲. قانون نیت را نمی سنجد، بلکه به اثر عمل نگاه می کند. حتی اگر نیت شوخی باشد، اگر نتیجه آن آسیب به دیگری باشد، می تواند جرم تلقی شود.
۳. انتشار محتوای توهین آمیز یا تحقیرکننده درباره افراد حقیقی یا حقوقی همیشه ریسک دارد.
۴. قبل از انتشار، یکبار دیگر فکر کنید. آیا حاضرید همین حرف یا تصویر را در حضور فرد مقابل بزنید؟ اگر پاسخ منفی است، منتشر کردن آن هم خطرناک خواهد بود.
۵. آگاهی حقوقی، بهترین سپر دفاعی است. شناخت مواد قانونی مرتبط با فضای مجازی به ما کمک می کند پیش از عمل، پیامدهای احتمالی را در نظر بگیریم.

« جمع بندی

ماجرای امیر نشان می دهد که فضای مجازی همان قدر که فرصتی برای ارتباط و بیان آزاد است، به همان اندازه نیازمند احتیاط و مسئولیت پذیری است. هر کلیک و هر پست می تواند تأثیری فراتر از تصور ما داشته باشد. قانون جرایم رایانه ای در ایران، چارچوب مشخصی برای رفتارهای مجاز و غیرمجاز در فضای دیجیتال تعیین کرده است. احترام به این چارچوب ها نه تنها ما را از مشکلات حقوقی دور نگه می دارد، بلکه به ایجاد فضایی سالم تر و ایمن تر برای همه کاربران کمک می کند.



KNOWLEDGE TEST



... آزمون دانشی



آزمون دانشی جرایم رایانه‌ای تشخیص رفتار مجرمانه در فضای مجازی

یکی از چالش‌های مهم کاربران فضای مجازی این است که نمی‌دانند مرز بین رفتار مجاز و رفتار مجرمانه دقیقاً کجاست. بسیاری از ما فکر می‌کنیم چون نیت بدی نداریم یا چون فضای مجازی «آزاد» است، پس عمل ما مشکل قانونی ندارد. اما قانون جرایم رایانه‌ای و سایر مقررات مرتبط، معیارهایی مشخص دارد که صرف‌نظر از نیت شخصی، می‌تواند یک عمل را جرم تلقی کند.



برای سنجش آگاهی شما، در این آزمون دانشی چند سناریوی واقعی یا شبیه‌سازی شده مطرح شده است. شما باید تشخیص دهید که آیا این عمل طبق قوانین ایران «جرم» محسوب می‌شود یا خیر. سپس در ادامه، پاسخ درست و توضیح مختصر ارائه شده است.

« سناریو ۱

شخصی در یک گروه خانوادگی، تصویری قدیمی و ویرایش شده از یکی از اقوام را با هدف شوخی ارسال می‌کند. تصویر، وضعیت نامناسبی را نشان می‌دهد که باعث خجالت فرد در جمع می‌شود.

سؤال: آیا این کار جرم است یا خیر؟

پاسخ: بله.

توضیح: انتشار تصویر یا ویدئویی که موجب هتک حیثیت یا تحقیر فرد شود، حتی در محیط‌های خصوصی مانند گروه خانوادگی، طبق قانون می‌تواند مصداق «نشر اکاذیب» یا «هتک حیثیت» در فضای مجازی باشد.

« سناریو ۲

دانشجویی برای کمک به دوستانش، نسخه PDF یک کتاب دارای حق نشر را در کانال تلگرامی عمومی منتشر می‌کند.

سؤال: آیا این کار جرم است یا خیر؟

پاسخ: بله.

توضیح: انتشار و توزیع آثار دارای حق نشر (کپی‌رایت) بدون اجازه صاحب اثر، نقض حقوق مؤلف است و طبق قوانین ایران، قابل پیگرد قضایی است.

« سناریو ۳

فردی در صفحه شخصی اینستاگرام خود، خبری بدون منبع معتبر درباره تعطیلی یک بانک منتشر می‌کند.

سؤال: آیا این کار جرم است یا خیر؟

پاسخ: بله.

توضیح: انتشار اخبار کذب که باعث تشویش اذهان عمومی یا اختلال در نظم اقتصادی شود، جرم محسوب می‌شود و حتی بدون نیت بد، قابل پیگیری است.

« سناریو ۴

کارمندی رمز عبور حساب کاربری همکارش را که روی یک برگه روی میز رها شده، می‌بیند و بدون اطلاع او وارد ایمیلش می‌شود.

اما هیچ تغییری ایجاد نمی‌کند.

سؤال: آیا این کار جرم است یا خیر؟

پاسخ: بله.

توضیح: دسترسی غیرمجاز به داده‌ها یا حساب‌های کاربری دیگران، حتی بدون تغییر یا حذف اطلاعات، مصداق «دسترسی غیرمجاز» در قانون جرایم رایانه‌ای است.

« سناریو ۵

شخصی برای تبلیغ یک محصول، از عکس یک فرد مشهور

بدون کسب اجازه او استفاده می‌کند.
سؤال: آیا این کار جرم است یا خیر؟
پاسخ: بله.

توضیح: استفاده تجاری از تصویر یا نام افراد بدون مجوز، نقض حقوق شخصی و تجاری آنهاست و می‌تواند پیگرد قانونی داشته باشد.

« سناریو ۶

فردی در صفحه شخصی خود، فیلم کوتاهی از یک تجمع خیابانی را منتشر می‌کند که چهره عده‌ای مشخص است.

سؤال: آیا این کار جرم است یا خیر؟

پاسخ: بستگی دارد.

توضیح: اگر انتشار فیلم باعث شناسایی و آسیب به افراد حاضر شود یا قوانین امنیتی و اجتماعی را نقض کند، جرم است. در غیر این صورت، ممکن است مشمول حریم خصوصی نباشد.

« سناریو ۷

شخصی برای دریافت کد تخفیف یک سایت، آدرس ایمیل جعلی ایجاد می‌کند و آن را به سیستم وارد می‌کند.

سؤال: آیا این کار جرم است یا خیر؟

پاسخ: در اغلب موارد بله.

توضیح: استفاده از هویت جعلی یا اطلاعات نادرست برای کسب منفعت یا فریب سیستم، می‌تواند مصداق «فریب در رایانه» یا «کلاهبرداری رایانه‌ای» باشد.



« نتیجه‌گیری

این سناریوها نشان می‌دهد که حتی رفتارهایی که به ظاهر ساده یا بی‌ضرر به نظر می‌رسند، می‌توانند طبق قانون، جرم محسوب شوند. بنابراین، آگاهی از قوانین سایبری و رعایت آنها نه تنها برای متخصصان، بلکه برای تمام کاربران فضای مجازی ضروری است.

