پلیـــــــس ســـــــایبر، ضرورت عصر اطلاعات

سید علی اکرمی‌فر[1]

دفتر همکاری‌های فناوری ریاست جمهوری، تهران صندوق پستی ۴۶۷۱-۱۴۱۵۵، تلفن: ۶۵۰۰۰۶۵

akrami@ictr.ir

همه روزه با اخبار متعددی راجع به سوء استفاده از محیطهای رایانه‌ای و شبکهٔ اینترنت، نفوذ ویروس‌ها و هکرها، سرقت اطلاعات و هتک حرمت افراد در اینترنت مشاهده می‌کنیم و به جز ابراز تاسف و یا نگرانی چارهٔ دیگری نداریم. آیا با این شرایط که روز به روز پیچیده تر می شود، فناوری اطلاعات در کشور توسعه خواهد یافت؟ به راستی چه باید کرد؟

مقدمه

در اواخر قرن بیستم، جهتگیری گسترش فناوری اطلاعات و ارتباطات به گونه‌ای بود که در هر کجای زندگی انسان، نمودی از آن پیدا می‌شد؛ اکثر فعالیت‌های اجتماعی به نوعی به آن وابسته شده بودند. بدون فناوری اطلاعات، حداقل در جوامع پیشرفته زندگی دشوار به نظر می‌رسید و گاهی ناممکن بود. فناوری اطلاعات یک نیاز اساسی جامعه بود. این روند به قرن بیست و یکم نیز منتقل شد؛ در سال‌های آغازین قرن جدید، حرکت باز هم ادامه یافته؛ و درنتیجه دنیای مجازی آرام آرام رو به شکل‌گیری گذاشت. دنیایی که پدیدهٔ فناوری اطلاعات و ارتباطات از همان ابتدا به دنبال تحقق آن بود. به عبارت دیگر جامعه مجازی در اثر توسعهٔ فناوری اطلاعات و ارتباطات در حال پیدایش است. در این جامعه مجازی که *فضای سایبر* نامیده می‌شود تعاملات اجتماعی نیز به شکل دیگری انجام می‌شود.

اساس و بنیاد هر جامعه چه کوچک و چه بزرگ بر اصولی استوار است که بدون آن شیرازهٔ جامعه از هم گسیخته خواهد شد. مهمترین قاعده اجتماعی نظم و قانون است . هر تعامل اجتماعی باید ذاتاً با مفهوم جامعه سازگار باشد و تیشه به ریشه آن نزد. از این روست که برخی از فعالیت‌ها در جامعه جرم محسوب می‌شوند و خشکاندن ریشه آن آرزوی هر عضو جامعه است. جامعه مجازی نیز از این قاعده مستثنی نیست.

ویژگیهاي فضاي سایبر

فضای سایبر محیطی مجازی برای فعالیت‌های اجتماعی است. مهمترین ویژگی فضای سایبر استقلال از زمان و مکان است. به عنوان مثال، کلاس درس نمونه‌ای از یک فعالیت اجتماعی در محیط واقعی است . دانشجویان و استاد باید به طور همزمان در این مکان مشترک به تعامل علمی و آموزشی بپردازند. اما در فضای سایبر کلاس به صورت مجازی برگزار می‌شود. دانشجویان از هر مکان نامشخص به کلاس می‌آیند. حتی در حالت کاملتر هروقت که فرصت داشتند و شرایط روحی و روانیشان مناسبتر بود به یادگیری و مباحثه غیرمستقیم می‌پردازند، خواه روز باشد و یا شب. با شکل‌گیری فضای سایبر اثر مرزها کم‌رنگ‌تر شده و جهانی شدن در کلیه امور اجتماعی با وضوح بیشتری دیده می‌شود. سرعت و ارزانی، کیفیت، نزدیکی و در دسترس بودن، شفافیت و تنوع برخی ویژگی‌های فضای سایبر هستند.

در فضای سایبر به همان دلیل که فعالیتها سریعتر و ارزانتر انجام پذیرند، جرایم نیز می‌توانند پیچیده‌تر، سریعتر و کم‌هزینه‌تر صورت گیرند. در دنیای واقعی، فیزیکی بودن محیط، محدودیتها و موانع بزرگی را برای

---

[1] دبیر کمیتهٔ مطالعات فناوری اطلاعات

مجرمین و تبهکاران ایجاد می‌کند که در عوض در فضای سایبر این مهم برقرار نیست و نتیجه آن به سود مجرمین می‌تواند باشد. البته لازم به ذکر است یکی از ویژگی‌های مثبت فضای سایبر ایجاد شفافیت در امور است که به نوعی با ذات جرم در تضاد است.

نظم و برقراری جامعه مجازی در فضای سایبر از یک منظر به قوانین کارآمد و قابل قبول نیاز دارد. این نیاز برای کشور ما که ایدئولوژی دینی خاص خود را دارد، مسلما باید سریعتر نهادینه شود وگرنه تنها ترجمه‌ای از قوانین دیگران بر فضای سایبر ما حاکم خواهد شد. از سوی دیگر اجرای قانون نیازمند یک سیستم نظارتی بر فعالیتهای شبکه و تعقیب و دستگیری مجرمین و سرکوب و امحای امور مجرمانه در محیط سایبر است که به آن «پلیس سایبر» گوییم.

ویژگی‌های پلیس سایبر

پلیس سایبر باید بتواند به ردیابی، شناسایی، ایجاد محدودیت برای مجرمین در فضای سایبر و ... اقدام کند. این امر مستلزم داشتن وجاهت قانونی، حرفه‌ای بودن و تسلط بر فنون نفوذگری و هکری و همچنین داشتن ابزارهای پیشرفته عملیات در فضای سایبر و در نهایت نیازمند همکاری است.

دامنه فعالیت پلیس سایبر متناسب با پیوستگی ذاتی فضای سایبر، سرتاسر جهان است و احتمالاً در آینده این پلیس زیرنظر سازمان ملل یا احتمالاً کشورهای غربی تشکیل خواهد شد. پلیس‌های دنیای واقعی وابسته به یک منطقه فیزیکی خاصی هستند که به آن کشور می‌گوییم. این پلیس‌ها اگرچه در سطح بین‌الملل با یکدیگر ارتباط دارند و پلیس بین‌الملل (Interpol) نیز وجود دارد اما فعالیتهای بین‌المللی آنها معمولاً تابع سیاست و روابط کشورها است.

یکی از کارهایی که پلیس سایبر می‌تواند انجام دهد محدود کردن حق فعالیت و یا زندگی برای مجرمین در فضای سایبر است. هم‌اکنون شرایطی فراهم شده که آدرس‌های اینترنتی افراد که از طریق آن به فعالیت‌های خرابکارانه مثل ارسال ویروس، نفوذ غیرمجاز و ارسال پیغامهای مزاحم می‌پردازند، توسط کامپیوترهای خاصی شناسایی شده و در لیست سیاه آنان قرار می‌گیرد. هرگونه فعالیت از طریق این آدرس‌ها با محدودیت‌های بسیار روبرو است. ورود یک آدرس به این پایگاه‌های داده به منزلهٔ تعطیلی فعالیت از طریق آن آدرس در سرتاسر دنیاست. برای مثال امروزه سرورهای پست الکترونیک به صورت خودکار با این مراکز برای دریافت یا حذف پیغامهای ورودی مشورت می‌کنند.

پلیس سایبر[۲] با اسامی مختلفی چون پلیس شبکه[۳]، پلیس وب[۴] و ... در کشورهای مختلف شکل گرفته و حتی برخی از کشور این وظیفه را به CERT[۵] (تیم واکنش سریع به مشکلات رایانه‌ای) واگذار کرده‌اند. ازجمله کشورهای پیشرو در ایجاد پلیس سایبر می‌توان به آمریکا، فرانسه، چین، ژاپن، هند و کره اشاره کرد. کره تا قبل از سال ۲۰۰۰ فقط به جرایم رایانه‌ای اهمیت می‌داد، اما در این سال CTRC[۶] را برای مقابله با جرایم سایبری ایجاد کرد.

---

[۲] Cyber Police

[۳] Network Police

[۴] Web Police

[۵] Computer Emergency Response Team

[۶] Korea National Police Cyber Terror Response Center

- **تجربة سایر کشورها**

هند نیز اولین ایستگاه پلیس سایبر خود را در سال ۲۰۰۱ در بنگلور ایجاد نمود. پلیس سایبر هند یا CCPS[۷] وظیفه دارد با جرایم فضای سایبر از قبیل نفوذ غیرمجاز، خرابکاری اطلاعات و کلاهبرداری اینترنتی مقابله نماید. ایجاد پلیس سایبر در هند در شرایطی است که این کشور در سال ۲۰۰۰ قانونی را برای مقابله با جرایم رایانه‌ای تصویب کرده بود.

- **تجربة کشور**

در کشور ما نیز چندسالی است که اداره‌کل مبارزه با جرایم رایانه‌ای معاونت آگاهی در نیروی انتظامی ایجاد شده است. پرواضح است که رویکرد جرایم فضای سایبر محدود به جرایم رایانه‌ای نبوده و ابزارها، نیروی انسانی و اختیارات خود را می‌طلبد. *پلیس سایبر* قطعه‌ای از پازل گمشدهٔ توسعه فناوری اطلاعات در کشور است. با توجه به این نکته که نیروی انتظامی مسؤول برقراری نظم در جامعه می‌باشد، این ارگان می‌تواند درصورت در دست گرفتن ابتکار عمل و از دست ندادن فرصت‌ها، مسؤولیت نظم و امنیت در این حوزه بزرگ اجتماعی را نیز برعهده بگیرد. البته پر واضح است که باید برای مقابله قانونی با جرایم فضای سایبر، قوانین لازم و شایسته تدوین گردد.

- **راه‌کارهاي پيشنهادي**

برای برقراری نظم و امنیت در محیط شبکه‌های رایانه‌ای، پلیس سایبر یک ضرورت ملی است. ایجاد چنین نهادی به مراحل زیر نیاز دارد:

۱- عناوین مجرمانه در فضای سایبر ملی مشخص گردد.

۲- قانون جرایم فضای سایبر و مجازات‌های مربوطه متناسب با در نظر گرفتن تاثیرنمایی شبکه در گسترش شایعات، اتهامات، خرابکاری‌ها و ... تعیین گردد. مسلماً مجازات جرم در محیط شبکه‌های رایانه‌ای به دلیل گسترش آن بسیار بیشتر از فضای خارج باید باشد.

۳- پلیس سایبر رسماً در نیروی انتظامی تاسیس گردد.

۴- پلیس سایبر برای مقابله با جرایم طبق اولویتی مشخص برنامه داشته باشد.

۵- پلیس سایبر در مراکز استان‌ها و سایر نقاط کشورگسترش یابد.

۶- پلیس سایبر بر مبارزه با تروریست و تهدیدکنندگان خارجی و داخلی فضای سایبر ملی تاکید کند.

۷- پلیس سایبر ملی همکاری با کشورهای دیگر را آگاهانه و فعالانه آغاز نماید.

---

[۷] Cyber Crime Police Station