

Original Article

The Role of Judicial Officers in the Prevention and Control of Cybercrime in Iranian and British Law

Ali Zallaghi¹, Mahmoud Malmir^{2*}

1. Department of Criminal Law and Criminology, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

2. Department of Criminal Law, Isfahan Branch (Khorasgan), Islamic Azad University, Isfahan, Iran. (Corresponding author) Email: dr.malmir1@gmail.com

Received: 16 Jan 2019 Accepted: 8 Sep 2020

Abstract

Background and Aim: The Inefficiency and Criticisms of the Traditional Model in Curbing the Criminal Phenomenon, As Well as the Achievements of Criminal Science in Particular in Recent Decades, Have Led to a Fundamental and New Change in the Ideas, Patterns and Tools of the Judiciary and This Development has Led to a Change in Judicial Approaches and the Formation of new Structures and Types of Criminal Response.

Materials and Methods: This Research is of Theoretical Type and the Research Method is Descriptive-Analytical and the Method of Data Collection is Library and has Been Done by Referring to Documents, Books and Articles.

Findings: Due to the Fact That Cyberspace is Becoming More and More Widespread, and at the Same Time, the Methods of Committing Crime Also Take on a Different Color and Smell With the Advancement of Technology. In the Face of Crime, the Judicial System in Iran Uses the Various Elements and Institutions of the Criminal Justice System. At the Beginning of Dealing With Crime, it is the Prosecutor's Office and the Prosecutor Who, as the First Judicial Institution, are the Factors Influencing the Quality of the Trial Process and Also Play an Important Role in Achieving the Goals of the Criminal Justice System. Suffice it to Say That the Success or Failure of Criminal Policies Wes Much to the Performance of the Judiciary and the Prosecutor.

Ethical Considerations: In Order to Organize This Research, While Observing the Authenticity of the Texts, Honesty and Fidelity have Been Observed.

Conclusion: In Iranian law, All Forces, Including the Police, the Prosecutor, The Dispute Resolution Council, and Finally the Prosecutor's Office, Are Involved in the Entire Cybercrime Process. In the UK Legal System, The Prosecution is Not Involved in the Investigation and Inspection Phase; As it is the Duty of the Regional Police Unit to Deal With Most Crimes at the Micro and Macro Levels. While in Other European Countries, the Opposite Method is Common. The Purpose of This Study is to Investigate the Role of Judicial Officers in the Prevention and Control of Cybercrime in Iranian and British law.

Keywords: Cybercrime; Judicial Officers; Prevention and Control; Iranian and British Law

Please cite this article as: Zallaghi A, Malmir M. The role of judicial officers in the prevention and control of cybercrime in Iranian and British law. *Iran J Med Law, Special Issue on Human Rights and Citizenship Rights 2018; 93-106.*

نقش ضابطان قضایی در پیشگیری و کنترل جرائم فضای سایبری در حقوق ایران و انگلستان

علی زلفی^۱، محمود مالمیر^{۲*}

۱. گروه حقوق جزا و جرم‌شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.

۲. گروه حقوق جزا و جرم‌شناسی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران. (نویسنده مسؤول) Email: dr.malmir1@gmail.com

دریافت: ۱۳۹۷/۱۰/۲۶ پذیرش: ۱۳۹۹/۰۶/۱۸

چکیده

زمینه و هدف: جرائم سایبری جزء جرائمی هستند که جدید و ناشی از تکنولوژی مدرن هستند. توجه به این دو نکته یعنی جدید بودن و ناشی از تکنولوژی مدرن بودن، در هرگونه آنالیز جنایی اثر فراوان دارد. رایانه ممکن است ابزار جرم باشد مانند قتل عمد یا کلاهبرداری، وسیله جرم مانند سرقت، و یا موضوع جرم مانند سرقت رایانه‌ای (هک) و پخش ویروس باشد. با این حال اینترنت محیطی است که در حال حاضر بر بحث رایانه‌ها و استفاده از آنها غلبه کرده است. هدف از این تحقیق بررسی نقش ضابطان قضایی در پیشگیری و کنترل جرائم فضای سایبری در حقوق ایران و انگلستان است.

مواد و روش‌ها: این تحقیق از نوع نظری بوده روش تحقیق به صورت توصیفی تحلیلی می‌باشد و روش جمع‌آوری اطلاعات به صورت کتابخانه‌ای است و با مراجعه به اسناد، کتب و مقالات صورت گرفته است.

یافته‌ها: با توجه به اینکه فضای مجازی روز به روز گسترده‌تر می‌شود و در عین حال شیوه‌های ارتکاب جرم نیز با پیشرفت تکنولوژی، رنگ و بوی دیگری می‌گیرد. در رویارویی با وقوع جرم، سیستم قضایی در ایران، ارکان و نهادهای مختلف نظام عدالت کیفری امکانات خود را به کار می‌گیرد. در ابتدای مواجهه با جرم، دادسرا و دادستان هستند که به عنوان اولین نهاد قضایی، عامل تأثیرگذاری در کیفیت روند دادرسی هستند و در تحقق اهداف نظام عدالت کیفری نیز نقش مهمی دارند. در میزان اهمیت این نهاد همین بس که به صراحت می‌توان گفت موفقیت یا ناکامی سیاست‌های کیفری تا حد زیادی مرهون عملکرد نهاد دادسرا و دادستان است.

ملاحظات اخلاقی: در تمام مراحل نگارش پژوهش حاضر، ضمن رعایت اصالت متون، صداقت و امانت‌داری رعایت شده است.

نتیجه‌گیری: در حقوق ایران کلیه نیروها از پلیس، دادستان، شورای حل اختلاف و در نهایت دادگاه دادسرا در کلیه فرآیند جرائم سایبری نقش دارند. در سیستم حقوقی انگلستان، دادستانی در مرحله تحقیق و بازرسی دخیل نیست؛ به طوری که رسیدگی به اکثر جرائم در سطح خرد و کلان، وظیفه یگان پلیس منطقه‌ای است. در حالی که در سایر کشورهای اروپایی، برخلاف این روش معمول است. هدف از این تحقیق بررسی نقش ضابطان قضایی در پیشگیری و کنترل جرائم فضای سایبری در حقوق ایران و انگلستان است.

واژگان کلیدی: جرائم فضای سایبری؛ ضابطان قضایی؛ پیشگیری و کنترل؛ حقوق ایران و انگلستان

مقدمه

آنچه امروز تحت عنوان جرائم رایانه‌ای شناخته می‌شود، مجموعه‌ای از همین تخلفات و بزهکاری‌هاست که از طریق رایانه و یا مؤثر بر رایانه اتفاق می‌افتد. همچنین می‌توان گفت جرائم رایانه‌ای، جرائم سنتی هستند که با فناوری اطلاعات از طریق رایانه صورت می‌گیرد، لذا برای رسیدگی به آن و اعمال مجازات، ناگزیر از وضع اعمال و مقرراتی هستیم که متفاوت از شکل سنتی آن است. نوین و ممتاز بودن جرائم رایانه‌ای و خصوصیات منحصر به فرد آن، همچون عدم لزوم حضور مرتکب در محل جرم در کنار شیوه ارتکاب این‌گونه جرائم و گاهاً داشتن جنبه بین‌المللی آن، نحوه رسیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش‌هایی روبه‌رو کرده است (۱).

در سیستم حقوقی انگلستان جرائم رایانه‌ای مورد توجه قانون‌گذار است. به طوری که قوانینی منحصر به فردی در سیستم قضایی انگلستان برای مقابله با جرائم اینترنتی تعیین کرده‌اند. در کشور انگلستان به دلیل اینکه فضای سایبری قدمت بیشتری نسبت به حقوق ایران دارد، جرائم جدید سنگین‌تری در آن به وقوع می‌پیوندد، ولی در سیستم قضایی ایران چون بیشتر قربانیان فضای سایبری به دلیل عدم آشنایی با این فضاست جرائم با شدت کمتری انجام می‌گیرد (۲).

در ارتباط با اهمیت پژوهش حاضر باید دقت داشت که، جرائم رایانه‌ای (cyber crime) یکی از پیش‌رونده‌ترین جرائمی است که با سرعت زیاد در حال گسترش و بلای جان بشر امروز شده است. جهان امروز جهان علم و فناوری است و بی‌شک پیشرفت را نمی‌توان از آن جدا کرد. این در حالی است که همگام با پیشرفت‌های علمی به‌ویژه در زمینه رایانه و اینترنت، عده‌ای برخلاف خدمت‌گزاران بشریت که به فکر استفاده‌های مثبت از فناوری‌ها هستند به فکر سوءاستفاده‌اند (۳). جرائم رایانه‌ای جرائمی سازمان‌یافته می‌باشند که از طریق اشخاص حرفه‌ای و باسواد انجام می‌شوند و همیشه و مجازات‌ها قوانین رایانه‌ای امروزه برای مجازات مجرمین کافی اما کامل نمی‌باشد چون هر روز جرائم جدیدی به وجود می‌آید که برای مجازات آن‌ها نیاز به قوانین جدید داریم همان‌گونه که جرائم اینترنتی همیشه در حال به روز شدن هستند

بایستی تلاش کرد تا بتوان با نو شدن جرائم هر ساله قوانینی را که در زمینه جرائم جدید قابل اعمال باشد ارائه کرد چون رایانه و اینترنت همیشه شکل‌های مختلفی به خود می‌گیرند (۴). در ارتباط با محدودیت‌های پژوهش حاضر نیز باید به این نکته دقت داشت که فضای مجازی در فرایند ارتکاب تمام جرائم، امکان نقش‌آفرینی دارد. در نتیجه برای تبیین آثار این دسته از جرائم عملاً با قلمرو بسیار گسترده‌ای مواجه هستیم، اما در اینجا صرفاً هدف ما، تحلیل نقش ضابطان قضایی در پیشگیری و کنترل جرائم می‌باشد؛ در نتیجه سایر آثار و حوزه‌های مرتبط، موضوع بحث ما نخواهد بود. همچنین مباحث مطروحه صرفاً در چهارچوب نظام حقوقی ایران و انگلستان مورد بحث و بررسی قرار خواهند گرفت.

هدف از این مقاله پاسخ به پرسش‌های زیر است. در سیستم حقوقی ایران و سیستم حقوقی انگلیس مرجع تعقیب‌کننده رسیدگی به جرایم سایبری بر عهده چه کسانی است؟ در سیستم حقوقی ایران و سیستم حقوقی انگلیس در قبال جرائم سایبری علیه اطفال، بانوان و یا عفت عمومی چه مجازات‌هایی تعیین شده است؟ قوانین حاکم بر ارتکاب جرائم سایبری در سیستم حقوقی ایران و سیستم حقوقی انگلیس چیست؟

قانون حاکم بر ارتکاب جرائم عام سایبری

جرائم عام سایبری مانند کلاهبرداری، سرقت و جعل است که با استفاده از رایانه انجام می‌شود. قانون‌گذار در این دسته از جرائم میزان مجازات آنها را تعیین کرده است. به طور مثال قانون‌گذار جرائم کلاهبرداری اینترنتی از سوی اشخاص صاحب نفوذ در فضای سایبری متناسب با میزان جرمی که اتفاق افتاده بین ۶ ماه تا ۳ سال حبس و جریمه نقدی تعیین کرده است. نوع جرائم و میزان مجازات‌های تعیین شده در فضای سایبری به طور عام متفاوت است. در سیستم حقوقی انگلستان جرائم عام مانند سوء استفاده از هویت افراد، هک کردن اطلاعات و داده‌های شخصی افراد، و جرائم عام مانند کلاهبرداری، سرقت از افراد در محیط سایبری، میزان مجازات‌های آنها در دادگاه تعیین شده است. و متناسب با این میزان افراد مجازات می‌شود و حکم دادگاه در مورد آنها اجرا می‌شود. به طور مثال جرم

کلاهبرداری اینترنتی در دادگاه انگلستان با توجه به کیفیت جرم بین ۱ تا ۲ سال حبس در نظر گرفته‌اند (۵).

میزان مجازات جرائم در محیط سایبری

قانونگذار بر اساس جرائمی که در محیط سایبری اتفاق افتاده مجازاتی تعیین کرده است، البته میزان کمیت و کیفیت این مجازات‌ها بر اساس نوع جرمی که اتفاق افتاده توسط قاضی تعیین می‌شود. به طور مثال هرکس عمداً و بدون مجوز، با نقض تدابیر حفاظتی داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی، به آنها دسترسی یابد به ۹۱ روز تا ۱ سال حبس یا پرداخت جزای نقدی از ۲,۵۰۰,۰۰۰ ریال تا ۱۰,۰۰۰,۰۰۰ ریال محکوم خواهد شد. یا در ماده ۳ تعیین شده است که هر کس عمداً و بدون مجوز داده‌های در حال انتقال غیر عمومی در یک ارتباط خصوصی به، یا از یک یا چند سیستم رایانه‌ای یا مخابراتی یا امواج الکترو مغناطیسی را شنود یا دریافت نماید به ۹۱ روز تا ۱ سال حبس یا پرداخت جزای نقدی از ۲,۵۰۰,۰۰۰ ریال تا ۱۰,۰۰۰,۰۰۰ ریال محکوم خواهد شد. یا طبق ماده ۱۱ هر کس عمداً با انجام اعمالی از قبیل وارد کردن، انتقال دادن، ارسال، پخش، صدمه زدن، پاک کردن، ایجاد وقفه، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی، سیستم رایانه‌ای یا مخابراتی دیگری را غیر قابل استفاده کرده یا عملکرد آنها را مختل نماید به حبس از ۶ ماه تا ۲ سال و یا پرداخت جزای نقدی از ۵,۰۰۰,۰۰۰ ریال تا ۲۰,۰۰۰,۰۰۰ ریال محکوم می‌گردد (۶). قانون‌گذار میزان مجازات هر یک از جرائم اینترنتی را معین کرده است. میزان مجازات در سیستم حقوقی انگلستان براساس نوع کیفیت جرم تعیین می‌شود. در بعضی از جرائم مثل کلاهبرداری و سوء استفاده جعلی از هویت افراد بین ۶ ماه تا دو سال حبس و جریمه نقدی در نظر گرفته‌اند. در بعضی از جرائم که آثار سنگین‌تری از جرم نمود پیدا می‌کند مجازات سنگین‌تری در نظر می‌گیرند (۷).

تشدید مجازات مرتکبین جرائم سایبری

ارتباط جرم و مجازات رابطه لازم و ملزومی است، زیرا جرم، آن فعل یا ترک فعلی است که قانون برایش مجازات در

نظر گرفته، و مجازات نیز واکنشی است که دستگاه قضاء (به نیابت از جامعه) در برابر ارتکاب جرم از خود نشان می‌دهد. بنابراین مجازات بدون ارتکاب جرم قابل تصور نیست. از موارد فردی کردن مجازات، می‌توان به تشدید کیفر به هنگام تعدد و تکرار جرم اشاره کرد. فلسفه تشدید مجازات در مورد عدم تنبه و ترس مرتکب جرم از مجازات مقرر در قانون یا اصلاح نشدن او می‌باشد. به همین علت به قاضی اجازه داده می‌شود که در صورت ارتکاب مجدد جرم، نسبت به مجرم شدت عمل به خرج دهد. تشدید کیفر همیشه با مجوز قانون است، زیرا در غیر آن مغایر با اصل قانونی بودن مجازات‌ها خواهد بود (۸). در ارتباط با جرائم رایانه‌ای هم تشدید مجازات برای مرتکبین جرائم به همین منوال است. و با صلاحدید قاضی و با توجه به میزان جرمی که اتفاق افتاده مجازات در نظر می‌گیرند. تشدید مجازات در سیستم حقوقی انگلستان به صورتی تعیین شده است که مجرمینی که جرائم خود را تکرار می‌کنند مجازات آنها دو برابر نسبت به جرائم قبلی افزایش می‌یابد (۹).

مرجع کشف و شناسایی جرم در جرائم اینترنتی

۱- پلیس

به موجب ماده ۶۰۲ قانون آیین دادرسی جرائم نیروهای مسلح، ضابطان پلیس مأمورانی هستند که تحت نظارت و تعلیمات دادستان نظامی و دیگر مقامات قضایی مربوط در کشف جرم، حفظ آثار و علایم و جمع‌آوری ادله وقوع جرم، شناسایی و یافتن متهم و جلوگیری از فرار یا مخفی شدن او، تحقیقات مقدماتی، ابلاغ اوراق و اجرای تصمیمات قضایی به موجب قانون اقدام می‌کنند.

همچنین ماده ۶۰۳ قانون یاد شده بیان می‌دارد: مأموران زیر پس از کسب مهارت‌های لازم و اخذ کارت مربوط، ضابط نظامی می‌باشند:

(الف) مأموران دژبان نیروهای مسلح، (ب) مأموران حفاظت اطلاعات نیروهای مسلح در چارچوب مأموریت‌ها و وظایف قانونی، (پ) مأموران بازرسی و قضایی نیروهای مسلح، (ت) فرماندهان، افسران و درجه‌داران آموزش‌دیده نیروی انتظامی، (ث) افسران و درجه‌داران نیروهای مسلح در جرایم مشهود در صورت عدم

اغفال‌کننده و سؤالات بی‌ربط به موضوع اتهام در بازجویی‌ها و بازجویی و تحقیقات از بانوان و کودکان، حتی‌الامکان توسط ضابطان آموزش‌دیده خانم و با رعایت موازین شرعی، از دیگر وظایف ضابطان نظامی است (۱۱).

معنای ضابط در لغت عبارت است از نگهدارنده و مباشر، حاکم، محفوظ دارنده و کارگزار است و نظام حقوقی انگلستان در آیین دادرسی کیفری خود، اصطلاح ضابط قضایی را مأمورانی می‌داند که مکلفند: مطابق با قانون و اصول تعلیمی و آموزش‌هایی که دیده‌اند به اموری همچون کشف جرم، نگهداری آثار و ادوات و علائم و ضبط ادله وقوع جرم، شناسایی و دستگیری و جلوگیری از گریختن متهم، انجام تحقیقات اولیه، ابلاغ اوراق و اجرای تصمیمات قضایی، بپردازند.

در مقام اجرای وظایف و تکالیف قانونی ارجاعی به ضابطین، توسل به رفتار خشونت‌آمیز علیه متهمین و مرتکبین به جرم که در حال تعرض به جان و حیثیت افراد می‌باشند بدون دستور قضایی در دادگاه امری اجتناب‌ناپذیر است و نمی‌توان در جایز بودن آن تردید داشت. مثلاً اعمال خشونت‌آمیز، در حد رفع خطر و دستگیری فردی که در حال ارتکاب قتل است یا حمل مواد مخدر، بدون دستور قضایی امری منطقی بوده، زیرا که وقت‌کشی و استیذان منجر به وقوع قتل یا جرم دیگر می‌شود و از نظر عقلی مورد قبول است. پلیس در سیستم حقوقی انگلیس یکی مهم‌ترین ارکان حقوقی ضابطان به شمار می‌رود. در سیستم حقوقی انگلیس اختیارات متفاوتی به پلیس داده‌اند. حتی در بعضی از مواقع پلیس می‌تواند بدون ارجاع متهمین به دادگاه بازجویی‌های اولیه را انجام دهد.

در نظام حقوقی انگلستان وقتی یک جرمی واقع می‌شود، پیش از شروع به تعقیب، پلیس است که وظیفه تحقیق و جمع‌آوری دلایل مرتبط با جرم را دارد. درواقع محدوده وظایف پلیس از زمان کشف جرم شروع می‌شود. اگرچه در نتیجه تحقیقات یا مدرکی دال بر متهم بودن مظنون پیدا شود، پلیس به وی تفهیم اتهام می‌کند و پرونده را برای پیگیری قضایی شخص متهم، به اداره دادستانی سلطنتی ارسال می‌کند. همچنین رسیدگی به پرونده در حضور هیئت منصفه انجام می‌شود و قاضی پس از بررسی پرونده و صدور

حضور سایر ضابطان نظامی، (ج) مقامات و مأمورانی که به موجب قوانین خاص در حدود وظایف محوله ضابط نظامی محسوب می‌شوند. تبصره (۱) رؤسا، معاونان و مأموران زندان‌ها و بازداشتگاه‌های نظامی در امور مربوط به زندانیان نظامی و همچنین مأموران حفاظت اطلاعات وزارت اطلاعات نسبت به جرایم کارکنان وزارت مزبور که در صلاحیت رسیدگی سازمان قضایی است، ضابط نظامی محسوب می‌شوند (۱۰). از جمله وظایف ضابطان نظامی، جلوگیری از امحای آثار و دلایل جرم و فرار متهم؛ مکلف بودن به قبول شکایت شفاهی یا کتبی در تمام اوقات شبانه‌روز و ارائه رسید به شاکی و ارسال سریع پرونده به دادسرا؛ حفظ و جلوگیری از نشت اطلاعات هویتی و اقامتگاه بزه‌دیده و اطلاعات مربوط به شهود و مطلعان و سایر اشخاص مرتبط با پرونده به جز آنچه که قانون استثناء نموده؛ اجرای دستورهای مقام قضایی در اسرع وقت و در مدتی که مقام قضایی تعیین می‌کند؛ انجام تحقیق تحت نظارت و تعلیمات بازپرس یا مقام قضایی؛ ارائه اوراق هویت ضابط بودن و اصل دستور قضایی هنگام ورود به منازل، اماکن بسته و تعطیل؛ آگاه کردن شاکی از حق درخواست جبران خسارت و بهره‌مندی از خدمات مشاوره‌ای موجود و سایر معاضدت‌های حقوقی؛ تفهیم حقوق «شخص تحت نظر» به‌صورت مکتوب و دریافت رسید و ضمیمه کردن آن به پرونده و ثبت اظهارات «شخص تحت نظر» و سبب تعقیب و پیگرد، زمان دقیق شروع و پایان آن، بازه زمانی بازجویی‌ها و زمانبندی حفاصل بین آنها، زمان دقیق ارائه اطلاعات و معرفی متهم به دادرس، در صورت مجلس همراه با امضاء یا اثر انگشت متهم است. اخذ اجازه موردی از مقام قضایی برای ورود به اماکن تعطیل و منازل اشخاص حتی در جرائم مشهود؛ اقدام طبق مجوز مقام قضایی و پرهیز از بازرسی اشخاص، اشیاء و مکان‌های غیرمرتبط با موضوع در بازرسی؛ گزارش فوری مراتب به مرجع قضایی در صورت مشاهده ادله، وسایل و آثار جرم دیگری را که محل امنیت و نظم عمومی اجتماع است در موقع واکاوی مکان؛ انجام معاینات و تحقیقات محلی؛ ابلاغ اوراق قضایی؛ ممنوعیت اجبار یا اکراه متهم، استفاده از عبارات تحقیرآمیز، القاء سؤالات و مطالبی که به ضرر متهم است یا مطالب یا

در انجام وظایف خود موفق خواهد بود که دارای سیستمی کارآمد و ساختار مناسب باشد (۵).

طبق قانون یکی از راههای اطلاع دادستان‌ها از ارتکاب جرم یا شروع دستور تعقیب قضایی گزارشی است که ضابطان اعلام می‌کنند. اینکه ضابط قضایی به چه کسی می‌گویند و چه وظایفی برایش تعریف شده است در قانون آیین دادرسی کیفری جدید بیان شده است، اما آنچه همیشه محل بحث و اختلاف نظر و حتی اعتراض را در هر زمینه‌ای ایجاد می‌کند، رفتارهای غیر قانونی، خودسرانه و عمل نکردن به نص صریح قانون است (۱۴).

ماده ۳۳ این قانون در راستای تکلیف نظارتی دادستان مقرر داشته، دادستانی می‌بایست در فواصل زمانی و حدوداً دو ماهه عملکرد ضابطان زیرمجموعه خود را ارزیابی و نتایج آن را ثبت و ضبط نموده اقدامات و تدبیرات لازم را اتخاذ کند. مطابق ماده ۳۴ این قانون از دستورات مقام قضایی به ضابطان به استثنای موارد فوری که شفاهی انجام می‌شود، باید کتبی، سریع، روشن و مقید به مهلت باشد. موارد فوری که دستور آن شفاهی صادر می‌شود را ضابط قضایی باید در ضمن انجام آن، مراتب اقدامات مرتبط را در صورت‌مجلس قید و در ظرف ۲۴ ساعت آن را به امضای مقام قضایی برساند. تکلیف ضابطان درباره انجام سریع و به‌موقع و دقیق تکالیف محوله نیز در ماده ۳۵ آمده است که در موارد عدم تکمیل امور در موعد مقرر، ضابط باید گزارش آن را با ذکر دلایل و موانع شرح دهد (۱۵).

در نظام حقوقی انگلستان، که متفاوت از دیگر نظام‌های اروپایی است، دادستانی در پروسه‌های تحقیق و بازرسی دخیل نیست و رسیدگی به اکثر جرائم خرد و کلان بر عهده نیروی پلیس منطقه‌ای است، البته از این وجه که در این مرحله نیز قاضی تحقیق وجود ندارد، مشابه با حقوق فرانسه است. در ساختار پلیس نیز این‌گونه نیست که هر پلیسی صلاحیت پرداختن به تمام مراحل رسیدگی و تحقیق را داشته باشد، بلکه امور با تقسیم وظایف صورت می‌گیرد؛ مثلاً یک گروه، فقط مسئول تحقیقات هستند. همچنین پلیس انگلستان دارای واحد تحقیق و کشف جرم است که افسران این واحد، به جرائم مهمی همچون قتل عمد می‌پردازند؛ نام دیگر آن

حکم وضعیت متهم را روشن می‌سازد. لازم به ذکر است که دادستانی سلطنتی زمانی به تعقیب می‌پردازد که ادله کافی برای محکومیت متهم را در پرونده بیابد (۱۲).

در سیستم حقوقی انگلستان ضابط دارای درجه ضابط یا بالاتر باشند، دارای صلاحیت و اختیار قانونی هستند. صلاحیت افسران پلیس نیروهای پلیس سرزمینی در انگلستان و ولز از ماده ۳۰ قانون پلیس ۱۹۹۶ ناشی می‌شود. این ماده مشخص می‌کند که چه افسرانی دارای صلاحیت در سرتاسر انگلستان و ولز هستند. ضابطان خاص - که نیروهایی پاره‌وقت و سربازانی داوطلب هستند - دارای صلاحیت بسیار محدودی هستند که تنها مختص به مناطق خودشان بوده و با مرز نیروهای دیگر محدود می‌شود. با این وجود، از اول آوریل ۲۰۰۷ ضابطان خاص انگلستان و ولز، اختیارات تام پلیس را در این دو کشور به دست آوردند. بدین معنا که در مقایسه با اکثریت کشورها، امروزه همه سربازان داوطلب بریتانیای کبیر، دقیقاً همان اختیارات پلیس‌های تمام‌وقت را دارند. به طور کلی، ضابطان نیروهای پلیس سرزمینی انگلستان و ولز در اسکاتلند یا ایرلند شمالی صلاحیت ندارند و بالعکس. با این وجود، هنگامی که شخصی از مرز خارج شده و به اسکاتلند فرار کند، ضابطان اختیارات محدودی برای تعقیب و بازداشت او خواهند داشت که البته نیازمند شرایط خاصی است. قانون همچنین در جای خود برای معاضدت دوجانبه، مقرراتی پیش‌بینی می‌کند که صلاحیت ضابطان را به هر بخشی از بریتانیای کبیر گسترش می‌دهد، البته هنگامی که آنها تقاضای نیرو کنند (۱۳).

۲- دادستانی

نظام کیفری وظیفه دارد در زمان وقوع جرم برای اجرای عدالت از تمام نهادها و امکانات خود بهره گیرد. اولین نهادهایی که با پدیده مجرمانه درگیر می‌شوند دادسرا و دادستانی هستند که اتفاقاً تأثیرگذارترین عوامل در کیفیت رسیدگی و مثمر ثمر واقع شدن پرونده می‌باشند. به عبارت دیگر تأثیر دادسرا و دادستانی در تحقق اهداف سیاست کیفری امری غیر قابل انکار و بسیار موثر است، البته دادستانی زمانی

اداره تحقیقات کیفری است. این اداره همچنین واحدهایی نیز مختص رسیدگی به جرائمی همچون سرقت دارد (۱۶).
یک طبقه‌بندی در نظام حقوقی انگلستان جرائم را به سه دسته تقسیم می‌کند. نخست جرائمی که از میزان شدت و خطر کمتری برخوردارند که در اصطلاح جرائم اختصاری نام می‌گیرند و رسیدگی به این جرائم فقط در دادگاههای مجیستریت صورت می‌گیرد. دسته دیگر جرائمی هستند که به آنها صرفاً با کیفرخواست در دادگاه جزا و در حضور قاضی و هیئت‌منصفه رسیدگی می‌شود؛ مانند سرقت، قتل عمد و غیر عمد. دسته سوم جرائم دو وجهی هستند، که به آنها در قالب جرائم اختصاری رسیدگی می‌شود، مگر اینکه دادگاه مجیستریت رسیدگی به پرونده را در دادگاه جزا مناسب بداند و یا ترجیح متهم محاکمه در دادگاه جزا باشد (۱۷).

۳-۲- نهادهای عمومی و غیر دولتی

امروزه مشارکت سازمان‌های غیردولتی به عنوان یکی از عوامل حسن اداره کشور از جنبه‌های اقتصادی، اجتماعی و فرهنگی به شمار می‌رود. مشارکت مذکور در نظام حقوقی می‌تواند در کارآمدی و ایجاد اعتماد عمومی نقش برجسته‌ای ایفا کند. قانون جدید آیین دادرسی کیفری با هدف عملیاتی کردن اهداف فوق، تعقیب دعوی عمومی را در دست‌های خاص از جرائم توسط این سازمان‌ها به رسمیت شناخته است، هرچند در متن قانون از سمت این سازمان‌ها به عنوان یاد شده است، اختیارات گسترده‌ای از قبیل اقامه دلیل و اعتراض به آرای صادره « اعلام‌کننده جرم به آن‌ها واگذار شده است. این نهادها در سیستم حقوقی ایران شورای حل اختلاف شهرستان و در استان‌هاست. در سیستم حقوقی انگلستان نهادها غیر رسمی زیادی به عنوان ضابطان قضایی انجام وظیفه می‌کنند از جمله این ضابطان به شرح زیر است:

۳-۱- نهادهایی با صلاحیت اجرایی محدود: این

نهادهای پلیسی نیستند و اختیارات پلیس را ندارند. آنها دارای اختیارات اجرایی کاملاً مشخص هستند، هرچند در عمل، این سازمان‌ها در فهرست نیروهای قرار می‌گیرند که باید از نیروهای پلیس سرزمینی حمایت کرده و در انجام این پشتیبانی، باید وظایف بازرسی و بازداشت را از طریق

۳-۲- نهادهایی با صلاحیت انجام بازرسی و تحقیقات:

نهادهای زیر دارای صلاحیت بازرسی و تحقیقاتی شبه پلیسی هستند که به موجب به آنها تفویض شده آیین‌نامه اختیارات بازرسی و تحقیقات (داده‌های ارتباطی) است: شعبه تحقیقات پیرامون سوانح هوایی؛ کمیسیون نظارت بر پرونده‌های کیفری؛ کمیسیون (تحقیق پیرامون) قمار؛ مرجع صدور پروانه و مجوز برای مجرمان حرفه‌ای است.

۳-۳- کمیسیون مستقل رسیدگی به شکایات از

پلیس: این کمیسیون شکایات علیه پلیس و پرسنل ستادی نیروهای پلیس بریتانیا، اداره جرایم سازمان‌یافته شدید در انگلستان و ولز و دایره آژانس گمرک و عواید سلطنتی، مرزی بریتانیا را مورد رسیدگی قرار می‌دهد. کارمندان کمیسیون مستقل رسیدگی به شکایات از پلیس، به‌منظور انجام تحقیقات و وظایف خود، کلیه اختیارات و مصونیت‌های پلیس در سرتاسر انگلستان و ولز و آب‌های مرزی را دارند (۱۸).

۴- مؤسسات کنترل‌کننده حامل‌های الکترونیکی

شرکت‌ها و مؤسسات زیادی هستند که حامل ارائه خدمات اینترنتی در سایت‌های مختلف هستند. این مؤسسات تمامی داده‌های اشخاص حقیقی و حقوقی را در اختیار دارند و کنترل می‌کنند. با هک شدن این سایت‌ها توسط افراد سودجو ممکن خسارات جبران‌ناپذیری به شرکت حمایت‌کننده وارد کند. بنابراین در وهله اول این شرکت‌ها بایستی اطلاعات خود را به روز کرده و با رمزگذاری بر روی سایت‌های خود می‌توانند از این جرائم جلوگیری کنند. در کشور انگلستان نیز هم مانند کشور ایران نیز به همین شکل است. با این تفاوت که در کشور انگلستان تمامی اطلاعات شرکت‌ها و مؤسسات زیر نظر پلیس بررسی و نظارت می‌شود. و تمامی هویت افراد حقیقی و حقوقی در شرکت‌ها به وسیله ناظرین سایبری کنترل می‌شود (۱۹).

نقش مردم در پیشگیری از وقوع جرائم سایبری

مردم خودشان اطلاعات خود را در فضای مجازی فاش می‌کنند. به عبارتی اشخاصی هستند که از اینترنت اطلاع کافی ندارند و بدون اطلاع، اقدام به چت کردن با افراد ناآشنا می‌نمایند. این اشخاص، اطلاعات شخصی خودشان را در معرض دسترس این افراد قرار می‌دهند. به این‌گونه که توسط افراد متخصص هک شده و اطلاعات شخصی‌شان در اختیار آنها قرار می‌گیرد. همچنین گاهی اوقات اشخاص برای خرید یک محصول از یک سایت، رمز عبور کارت شتاب خود را در اختیار متصدیان سایت قرار داده و سبب می‌شوند که از کارت آنها پول برداشت شود که می‌بایست پس از اقدام به پرداخت‌های اینترنتی از جمله شهریه و قبوض، رمز خود را بر روی سیستم قرار ندهد و یا حذف نماییم که مورد سوء استفاده دیگران قرار نگیرد. نصب آنتی‌ویروس‌ها و نرم‌افزارهایی که وظیفه حذف یا جلوگیری از ورود کرم‌های اینترنتی دارند، برای جلوگیری از دزدی اطلاعات، خیلی از ویروس‌ها و کرم‌های اینترنتی هنگامی که وارد کامپیوتر می‌شوند سیستم امنیتی را از کار می‌اندازند و اقدام به دادن اطلاعات شخص دریافت‌کننده به شخص فرستنده ویروس می‌نمایند که از طریق آنتی‌ویروس‌ها و ضدکرم‌های اینترنتی که به روز شده‌اند می‌توان از ورود آن‌ها و سرقت داده‌ها جلوگیری کرد (۲۰).

جرائم سایبری علیه اطفال

بیشترین قربانیان فضای سایبری اطفال و زنان هستند. بالغ بر ۱۰ درصد جرائم اینترنتی در کشور مربوط به کودکان ۱۵ تا ۱۷ ساله است و همچنین بیش از ۴۰ درصد از جرائم را کودکان ۱۸ تا ۲۶ سال انجام می‌دهند. با توجه به این آمار در کشور نشان‌دهنده اهمیت دادن به این نوع جرائم است. اطفال با عضویت در گروه‌ها و کانال‌های شبکه‌های اجتماعی قربانی جرائم می‌شوند (۲۱). بعضی از سایت با نشان دادن فیلم بازی‌های کودکانه و عکس‌ها کودکان را جذب خود می‌کنند. ممکن است از کودکان سوء استفاده جنسی نیز شود. در سیستم حقوقی انگلستان مجازات‌های سنگینی برای جرائم علیه کودکان در فضای سایبری تعیین کردند. از حبس گرفته

تا پرداخت جریمه نقدی تا محروم از حقوق شهروندی است. بیشترین رنج سنی که اطفال در کشور انگلستان مرتکب جرائم فضای سایبری می‌شوند بین ۱۸-۱۲ سال است (۲۲).

جرائم سایبری علیه بانوان و یا عفت عمومی

موضوع جرائم علیه عفت و اخلاق عمومی عبارت است از حیثیت، اعتبار، آبروی فردی و خانوادگی اشخاص که از نظر اکثریت افرادی که در یک جامعه معین زندگی می‌کنند، رعایت آنها الزامی است و عرف و قانون از این ارزش‌ها با واژه‌های عصمت، عفت و اخلاق جنسی یاد می‌کند. رعایت و حرمت حیثیت و اعتبار افراد که با منطق و شعور اجتماعی انسان‌ها منطبق است، الزامی و بر این اساس است که هر رفتاری که مغایر با این‌گونه ارزش‌های معتبر اجتماعی باشد، به عنوان جرم علیه عفت و اخلاق عمومی مستحق تعقیب و مجازات خواهد بود. برخی از مصادیق جرائم علیه عفت و اخلاق عمومی در قوانین جزایی ایران، در زمره حدود جا می‌گیرند و بعضی دیگر نیز در زمره تعزیرات هستند. آن دسته از جرائم علیه عفت و اخلاق عمومی که در زمره حدود (مجازات‌هایی که کمیت و کیفیت آنها در شرع مشخص شده است) قرار دارند عبارتند از زنا، زنا با زنی مجرد، زنا با زنی متاهل یا زن متاهل، زنا با زنی مجرد، زنا با محارم نسبی، زنا با زنی پدر، لواط، تفخیز، مساحقه و ... هر یک از موارد فوق دارای مجازات‌های خاصی هستند، مثلاً مجازات زنا، زنی مجرد یا زن مجرد ۱۰۰ ضربه تازیانه است یا مجازات زنا، زنی با زنی با محارم نسبی یا زنی با زنی پدر کیفر اعدام را در پی خواهد داشت (۶). هرگاه روابط بین زن و مردی در خارج از حد و مرز متعارف ارزش‌های پذیرفته شده در جامعه برای ارضای تمایلات جنسی انجام گیرد، قانوناً جرم علیه عفت و اخلاق عمومی تلقی خواهد شد. به این ترتیب، جرم علیه عفت و اخلاق عمومی عبارت است از هرگونه رابطه ناشی از تمایل زن و مرد به یکدیگر که از حد و مرز متعارف جامعه فراتر باشد به نحوی که جامعه نتواند آن را غمض عین کند. بلکه آن را به عنوان یک عمل ضد عفت و اخلاق عمومی مردود شمرده و مستحق مجازات و کیفر بداند (۶).

پدوفیلی (کودک دوستی به منظور سوءاستفاده جنسی) و هرزه‌نگاری اطفال در اینترنت تشکیل شد، اعلامیه مورخه ۱۹۹۹/۱/۱۹ یونسکو که یک برنامه‌ی عملی برای مبارزه با جرائم اینترنتی علیه اطفال می‌باشد، صادر گردید.

۳- سازمان همکاری و توسعه اقتصادی

اولین کوشش بین‌المللی در مورد بحث و بررسی مشکلات حقوق جزا در برابر جرم سایبری توسط سازمان همکاری و توسعه اقتصادی صورت پذیرفت. این سازمان در سال ۱۹۷۷ شروع به اتخاذ رهنمودهایی ناظر به حمایت از حقوق فردی و جریان فراملی داده‌های شخصی کرد. کمیته تخصصی این سازمان، کار خود را در زمینه ایجاد هماهنگی بین‌المللی بین قوانین کیفری برای مبارزه با جرائم اقتصادی رایانه‌ای شروع کرد و در سال ۱۹۸۹ لیستی از سوءاستفاده‌های رایانه‌ای را ارائه داد. در سال ۱۹۸۹ این سازمان کارش را در خصوص امنیت سیستم‌های رایانه‌ای ادامه داد.

۴- سازمان ملل

در هفتمین کنگره سازمان ملل متحد در سال ۱۹۸۵ «جرم سایبری» از جمله موارد مطروحه در گزارش دبیر کل این سازمان بود. به‌عنوان برنامه تدارکاتی هشتمین کنگره سازمان ملل متحد، اجلاس مقدماتی منطقه‌ای آسیا و اقیانوس آرام، نگرانی خود را درباره آثار پیشرفت‌های تکنولوژی و انعکاس آن در جرائم سایبر اعلام داشت. در اجلاس مقدماتی منطقه‌ای اروپا پیشنهاد شد که مبارزه بین‌المللی با جرائم رایانه‌ای از سوی هشتمین کنگره سازمان ملل متحد و کنگره‌های پس از آن مورد حمایت و توجه قرار گیرد. در دوازدهمین اجلاس عمومی کنگره هشتم که در سال ۱۹۹۰ برگزار شد، نماینده کانادا پیش‌نویس قطعنامه‌ای را در مورد جرائم رایانه‌ای تسلیم کنگره کرد. در سیزدهمین اجلاس عمومی کنگره هشتم، قطعنامه مذکور پذیرفته شد. در این قطعنامه از کشورهای عضو خواسته شده است که به تلاش‌های خود در زمینه مبارزه با جرائم رایانه‌ای از طریق مدرنیزه کردن قوانین و دادرسی‌های ملی، ارتقاء ضوابط پیشگیرانه و امنیتی رایانه، اتخاذ تدابیری برای ایجاد حساسیت در مردم و قوه قضائیه برای جلوگیری از جرائم

جرائم رایانه‌ای علیه خانواده که در قانون جرائم رایانه‌ای، جرم‌انگاری شده است و در حوزه خانواده به حریم و عفت و اخلاق خانواده آسیب وارد می‌کند (۲۳).

فعالیت‌های سازمان‌های منطقه‌ای و بین‌المللی در خصوص جرائم سایبری

به لحاظ خصیصه فراملی جرائم سایبری، اقدامات بین‌المللی فراوانی برای دستیابی به سیاست جنایی بین‌المللی ناظر بر این جرائم انجام شده است.

۱- شورای اروپا

شورای اروپا در سال ۱۹۸۵ موضوع جرم رایانه‌ای را از طریق یک کمیته تخصصی مورد مطالعه و بررسی قرار داده است. کمیته منتخب کارشناسان جرم رایانه‌ای کار خود را در سال ۱۹۸۵ شروع و در سال ۱۹۸۹ یک توصیه‌نامه و یک گزارش به کمیته اروپایی مسائل ناشی از جرم ارائه کرد. کمیته نیز پس از تصویب، آن را به کمیته وزرای شورای اروپا فرستاد و در سپتامبر ۱۹۸۹ به‌عنوان یک توصیه‌نامه تحت عنوان ۹ (۸۹) R مورد تصویب نهایی قرار گرفت. توصیه‌نامه دیگری در زمینه آئین دادرسی جرائم فناوری اطلاعات در سال ۱۹۹۵ تحت عنوان توصیه‌نامه ۱۳ (۹۵) R توسط این شورا تصویب شده است. کمیته وزراء شورای اروپا در سال ۱۹۹۷ کمیته دیگری به نام کمیته متخصصان جرائم سایبر را تشکیل داد. این کمیته پیش‌نویس کنوانسیون جرائم سایبر و گزارش توجیهی آن را در سال ۲۰۰۰ تهیه کرد. کنوانسیون جرائم سایبر در سال ۲۰۰۱، در یک کنفرانس بین‌المللی که با شرکت کشورهای عضو شورای اروپا و چهار کشور دیگر (آمریکا، ژاپن، آفریقای جنوبی و کانادا) تشکیل گردید، به تصویب رسید که کامل‌ترین سند بین‌المللی در مورد جرائم رایانه‌ای است (۲۴).

۲- یونسکو

در اجلاس سال ۱۹۹۹ یونسکو در پاریس که با حضور ۳۰۰ نفر از متخصصان در حوزه مراقبت و محافظت از اطفال، متخصصان اینترنت و تهیه‌کنندگان خدمات اینترنتی و ... به‌منظور بررسی راه‌های مبارزه با سوءاستفاده جنسی از اطفال،

رایانه‌ای و ... شدت بخشند و از دبیر کل سازمان خواسته شد تا موضوع انتشار یک نشریه فنی در مورد جلوگیری و تعقیب جرائم رایانه‌ای را مد نظر قرار دهد.

۵- انجمن بین‌المللی حقوق جزا

انجمن بین‌المللی حقوق جزا که یک سازمان غیردولتی است در سال ۱۹۹۰ جرم سایبری را به‌عنوان یک موضوع مورد بحث برای اعضای خود مطرح کرد. در سال ۱۹۹۲ یک نشست مقدماتی پیرامون این جرم در دانشگاه ورتسبورگ آلمان برگزار و قطعنامه‌ای در مورد فهرست جرائم رایانه‌ای صادر کرد. در سال ۱۹۹۴ در نشست نهایی خود در ریودوژانیرو و در نشست‌های بعدی خود مصوباتی در این خصوص داشته است.

۶- کنوانسیون بوداپست

کنوانسیون بوداپست به نام «پیمان جرائم اینترنتی بین‌المللی» نیز معروف است و اولین پیمان بین‌المللی ایجادشده برای مقابله با جرائم اینترنتی است که حدود ۴۰ کشور مختلف در کنفرانس بین‌المللی بوداپست با موضوعیت جرائم اینترنتی، در ۲۳ نوامبر ۲۰۰۱ در مجارستان آن را امضا کردند که از آن پس این پیمان به نام «پیمان بوداپست» معروف شد. این پیمان شامل تعاریف دقیق برای همه نوع از جرائم اینترنتی است و کیفر مربوط به هر کدام نیز مشخص شده است. در این پیمان، سیستم کامپیوتری، دسترسی غیر قانونی به اطلاعات، نقض قانون مالکیت معنوی، تولید و پخش ویروس کامپیوتری و ترویج پورنوگرافی کودکان به‌عنوان یک عمل مجرمانه تعریف شده است و کشورها را موظف به الحاق به این قانون و ممنوعیت این‌گونه جرم‌ها در قوانین داخلی خود می‌سازد. همه کشورهایی که این پیمان را امضا کرده‌اند قانون و مقررات یکسانی برای کنترل جرائم اینترنتی داشته و جهت همکاری‌های بین‌المللی یک خط تلفن استاندارد برای این بخش فراهم کرده‌اند (۲۴).

سیاست‌های کلی نظام در خصوص شبکه‌های اطلاع‌رسانی رایانه‌ای

این سند از سوی دفتر مقام معظم رهبری ابلاغ شده است. سند مزبور دارای هفت بند بوده و طی آن برای ایجاد، سازماندهی

و تقویت نظام ملی اطلاع‌رسانی رایانه‌ای و اعمال تدابیر نظارتی لازم تأکید شده است. سیاست‌های مزبور پس از طرح و بررسی توسط مجمع تشخیص مصلحت نظام به مقام معظم رهبری پیشنهاد و با لحاظ نظرات معظم له ابلاغ شد. اهمیت این سیاست‌ها به گونه‌ای بود که بلافاصله موضوع در دستور کار شورای عالی فرهنگی قرار گرفت و پس از بحث و بررسی در جلسات متعدد شورای عالی انقلاب فرهنگی مجموعه‌ای با عنوان «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» به تصویب آن شورا رسید و پیرو ابلاغیه مقام معظم رهبری به مراجع ذی‌ربط ابلاغ شد. در این آیین‌نامه بر چهار نکته اساسی به شرح زیر تأکید شده است: (۱) حق دسترسی آزاد مردم به اطلاعات و دانش؛ (۲) مسئولیت مدنی و حقوقی افراد در قبال فعالیت‌های خود؛ (۳) رعایت حقوق اجتماعی و صیانت فرهنگی و فنی کشور در این قلمرو؛ (۴) ایجاد حداکثر سهولت در ارائه خدمات اطلاع‌رسانی و اینترنت به عمومی مردم (۲۵).

خلاءهای قانونی و اجرایی در جرائم سایبری

۱- نامعین بودن حیطه‌های جغرافیایی

قوانین و مقررات حاکم بر بستر عبور و مرور در فضای مبادلات اینترنتی بی‌شک، از مقررات موجود برای مبادلات تجاری در دنیای واقعی، بسیار متفاوت خواهند بود. بخش عمده‌ای از این تفاوت ناشی از خصوصیتی است که در اینترنت، زمینه حضور راه دور را فراهم می‌آورند و شبکه را به لحاظ فناوری از بُعد مکانی و فیزیکی متمایز می‌کنند (۲۶). موقعیت شبکه آن‌چنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. اطلاع از این موقعیت مکانی برای عملکرد شبکه و ایجادکنندگان آن اهمیتی ندارد، لذا در طراحی یک شبکه امکان تشخیص مکان جغرافیایی در نظر گرفته نشده. در فضا و مکان واقعی، یک شرکت یا طرف تجاری معمولاً می‌تواند مکانی واحد یا شخصی را که با او در تبادل است. شناسایی نماید. چرا که این کار به شناسایی طرفین و اعتبار و مشروعیت مبادلات کمک می‌کند، ولی انجام این کار در محیط مجازی رایانه‌ای بسیار دشوار است، زیرا در اینجا

صورت تعدد محل‌های ارتکاب، محلی که در آن نتیجه حاصل شده است، با توجه به ماهیت جرائم اینترنتی همواره به سهولت انجام نمی‌پذیرد. بر فرض تشخیص محل وقوع جرم یا محل حصول نتیجه نیز، یافتن حوزه صالح به رسیدگی مطرح است. خصوصاً اگر دایره گستردگی مکان‌ها به خارج از کشور نیز برسد و چند کشور درگیر چنین جرائمی شده باشند، اینکه کدام یک از آن‌ها و کدام یک از حوزه‌های قضایی داخلی‌شان دارای صلاحیت قضایی است، مورد بحث است (۲۸).

راهکارهای پیشگیری در جرائم سایبری

۱- بروز کردن قوانین و دادرسی‌های کیفری

در برخورد با جرائم اینترنتی باید ابتدا اطمینان حاصل نمود که آیا جرم‌ها و قوانین موجود از نظر پذیرش در دادرسی‌های قضایی اعمال شدنی می‌باشند یا خیر؟ پس از آن به فراهم ساختن قوانین مناسب و فراهم نمودن امکان ضبط یا استرداد وجوه به دست آمده از طریق جرائم رایانه‌ای همت گمارد. در این راستا لازم است ضوابط پیشگیرانه و امنیتی رایانه با توجه به حریم خصوصی ارتقا یابد. جهت رسیدن به اهداف متعالی در این زمینه باید آموزش عامه مردم در اهمیت پیشگیری از ارتکاب جرائم رایانه‌ای را ایجاد نمود و از طرف دیگر، به صورت کامل و کافی در جرائم رایانه‌ای عوامل قضایی را آموزش داد.

۲- استفاده از فناوری‌های رایانه‌ای و فضای مجازی

جهت حمایت از دیگر فعالیت‌های مجرمانه

دغدغه اصلی عرصه حقوق امروز بیشتر حول مفاهیم و مباحث قوانین شکلی می‌چرخد. حفظ حقوق متهم از یک طرف و مقابله کارآمد با جرائم سازمان‌یافته از طرف دیگر، از دلایلی هستند که لزوم توجه به این حوزه را بیش از پیش آشکار می‌سازند. در حوزه قوانین شکلی بحث صلاحیت قضایی از مباحث چالشی است. همچنین هر مرجع قضایی و ضابطین آن نخست باید احراز صلاحیت ذاتی و محلی نمایند. ارائه نشدن رهنمود و راهکار مناسبی در خصوص بحث صلاحیت و تعارض در آن به لحاظ طبع جرم در مقررات بین‌المللی در حوزه حقوق بین‌الملل نیز دلیلی دیگر بر دشواری این ماجرا است.

طرفین یک مبادله ممکن است در دو اتاق همجوار یا در دو سوی جهان باشند دارند، ولی این آدرس اینترنتی جایگاه و مکان آنها را در دنیای واقعی نشان نخواهد داد و شبکه هم راهی برای تشخیص تفاوت آدرس واقعی و آدرس اینترنتی تبیین نمی‌کند. هیچ هماهنگی و هم‌سویی میان مکان‌های واقعی و فضای مجازی وجود ندارد، هرچند که آدرس‌های اینترنتی گاهی دارای اطلاعاتی از موقعیت مکانی هستند، مثلاً مشخص‌کننده جغرافیایی یا مشخص‌کننده‌هایی که از نظر جغرافیایی قابل تعیین هستند. مانند اینکه آدرس‌های اینترنتی در بریتانیای کبیر پسوند (UK) دارند، اما این مشخص‌کننده‌ها به ندرت در آدرس‌های اینترنتی یافت می‌شوند. ضمن اینکه آدرس‌های اینترنتی، آدرس‌هایی قراردادی در شبکه هستند و به راحتی انتقال پیدا می‌کنند (۲۷).

۲- صلاحیت قضایی در قبال مجرمین

بر اساس قواعد صلاحیت قضایی شروع و یا کامل شدن عنصر مادی جرم در یک حوزه قضایی آن حوزه را صالح به رسیدگی به جرم خواهد نمود. محل ارتکاب جرم اکثراً معیاری است که در مباحث مربوط به صلاحیت قضایی مورد توجه قرار می‌گیرد، زیرا که صلاحیت قضایی جنایی در مقابل میز محاکمه و بر مبنای حضور فیزیکی و واقعی مجرم در یک حوزه استحضاطی مشخص می‌شود. در مواردی که جرائم چند صلاحیتی مانند آدم‌ربایی مطرح باشد، برای صالح شناخته شدن یک حوزه قضایی، کفایت که یک عنصر مادی از جرم در آن حوزه در حال انجام باشد.

اما در رابطه با مبحث صلاحیت در جرائم اینترنتی چند مسئله مطرح است. نخست آنکه ممکن است کاربر اینترنتی در هر حوزه ذی‌صلاحی که با اینترنت در ارتباط است مجرم شناخته شود. دیگر آنکه بر مبنای ماهیت اینترنت، امکان ارتباط متقابل بین چندین حوزه قضایی وجود دارد. در تشخیص مکان وقوع یک جرم اینترنتی ممکن است علاوه بر مکانی که متهم در آن حضور فیزیکی دارد و عناصر یک جرم در آن مکان شروع شده و یا به نتیجه رسیده‌اند، بحث وقوع جرم در حوزه‌های دیگری که در اثر عمل مجرم به صورت الکترونیکی درگیر شده‌اند نیز مطرح باشد. تشخیص محل وقوع جرم یا در

قواعدی که در بحث صلاحیت وجود دارند، امره هستند. اراده و توافقات فردی در موضوعات کیفری که برای برپایی و حفظ نظم عمومی مقرر شده‌اند، مؤثر نخواهد بود، برخلاف دعاوی حقوقی که در اکثر موارد توافق طرفین بر قوانین ماهوی امکان پذیر است (۲۹). در مبحث صلاحیت قضایی اصل جاری در قانون آیین دادرسی کیفری، صلاحیت مرجع قضایی محلی است که جرم در آنجا به وقوع پیوسته است. بنابراین مراجع قضایی ایران صالح به رسیدگی به هر جرمی هستند که در قلمرو حاکمیتی ایران اتفاق می‌افتد. گاهی این اصل کنار رفته و صلاحیت قضایی طور دیگری شناسایی می‌شود، در بعضی موارد بر مبنای تابعیت فعال تعیین شده و در موارد خاصی که منافع ملی مطرح است و یا جرم‌انگاری توسط قوانین خاص یا عام بین‌المللی انجام شده است، رویه دیگری در پیش گرفته خواهد شد.

اصل سرزمینی بودن جرائم و مجازات‌ها، در تمام حوزه‌هایی که مسئله حاکمیت نظام حاکم مطرح است، مانند دریا و فضا و ... جاری است. جواز یا عدم جواز بسط دادن این اصل به فضای سایبری محل تفکر و سؤال است. تعیین مرز و قلمرو به این خاطر صورت گرفته است که کشورها در برابر یکدیگر قائل به احترام متقابل بوده و به قلمروی دیگری تعرض نکنند، اما فضای سایبری این موضوع را نقض می‌کند. سابقاً به این موضوع پرداختیم که فضای سایبر فقط به شبکه جهانی اینترنت اختصاص ندارد، اما به هر صورت نمی‌توان حکمرانی کیفری را در این قضیه به طور کلی کنار گذاشت، مراکز داده‌ها که خدمات شبکه‌ای ارائه می‌دهند، می‌توانند به برپایی و انجام این قضیه کمک کنند (۳۰).

نتیجه‌گیری

هرجا که دریچه‌ای تازه گشوده شود، در مقابل استفاده درست و بهینه، همواره استفاده نابهنجار نیز پا به پیش خواهد گذاشت. با پیشرفت‌های هر روزه دنیای تکنولوژی و اطلاعات قطع به یقین افرادی قانون گریز، فرصت طلب و سودجو با یادگیری دانش این حوزه به سوءاستفاده از این دنیا خواهند پرداخت و باعث ایجاد شبهه و تردید برای استفاده

صحیح از این امکانات و تکنولوژی شده اند تا جایی که امروزه توجه دولتمردان، متخصصین تکنولوژی و حقوق‌دانان را به خود جلب کرده است. باید توجه داشت که هرچه دنیای تکنولوژی گسترده‌تر شود، جرائم مربوط به آن نیز گسترده‌تر شده و توسعه خواهند یافت. در ادامه به تبع قوانینی که بتوانند با این جرائم به طور مناسب برخورد کنند وجود نخواهند داشت. دولت‌ها باید تنظیم قوانین متناسب با این جرائم را در دستور کار خود قرار دهند.

جرائم رایانه‌ای یکی از پدیده‌های نوظهوری است که گرچه برخی از جرائم آن شباهت‌هایی با جرائم سنتی دارد، اما تفاوت‌هایی در روش و ماهیت و نوع جرم دارد که از لحاظ جرم‌شناسی و کیفرشناسی و حقوق کیفری پژوهش‌های نوی را می‌طلبد. جرائم رایانه‌ای به دلیل تأثیرات ناگواری که بر جامعه اطلاعاتی و کاربران دارد، برخورد جدی‌تری را از سوی دولتمردان سیاسی و قضایی می‌طلبد. نظارت و فیلتر کردن دقیق‌تر و جدی‌تری، چه برای جلوگیری از آسیب‌های امنیتی و چه آسیب‌های فرهنگی را می‌طلبد.

برای تبیین نوع جرم رایانه‌ای همیشه یک مرجع تعقیب‌کننده تخصصی در سیستم قضایی هر کشور وجود دارد. در کشور ایران و انگلستان نیز قضات خاصی که تخصص لازم را در جرائم سایبری دارند وجود دارد. در سیستم حقوقی ایران مسئولیت رسیدگی به جرائم در مرحله مقدماتی بر عهد پلیس سایبری است. در مرحله دوم به وسیله دادگاه و سیستم قضایی انجام می‌شود. صدور حکم قضایی بر عهده قضات قضایی است.

پس از وقوع جرم، سیستم قضایی ایران و نظام عدالت کیفری موجود در آن با نهادها و ارکان مختلف خود جهت مقابله با جرم آماده می‌شود. نخستین نهاد قضایی‌ای که در این موقعیت دست به کار می‌شود، یعنی دادسرا و دادستان، پررنگ‌ترین نقش را در تشکیل، پیش‌برد و به نتیجه رسیدن دعوی کیفری داراست. عملکرد نهاد دادسرا و دادستان تا حدود زیادی تعیین‌کننده موفقیت یا عدم موفقیت سیاست کیفری است. در حقوق ایران کلیه نیروها از پلیس، دادستان، شورای حل اختلاف و در نهایت دادگاه دادسرا در کلیه فرآیند جرائم سایبری نقش دارند.

اینترنتی از سوی اشخاص صاحب نفوذ در فضای سایبری متناسب با میزان جرمی که اتفاق افتاده بین ۶ ماه تا ۳ سال حبس و جریمه نقدی تعیین کرده است. نوع جرائم و میزان مجازات‌های تعیین شده در فضای سایبری به طور عام متفاوت است. قانونگذار بر اساس جرائمی که در محیط اینترنتی اتفاق افتاده مجازاتی تعیین کرده است، البته میزان کمیت و کیفیت این مجازات‌ها بر اساس نوع جرمی که اتفاق افتاده توسط قاضی تعیین می‌شود در سیستم حقوقی انگلستان مجازات‌های سنگینی برای جرائم علیه کودکان در فضای سایبری در تعیین کردند. از حبس گرفته تا پرداخت جریمه نقدی تا محروم از حقوق شهروندی است. بیشترین رنج سنی که اطفال در کشور انگلستان مرتکب جرائم فضای سایبری می‌شوند بین ۱۸-۱۲ سال است.

در سیستم حقوقی انگلستان جرائم خاص مانند سوء استفاده از هویت افراد، هک کردن اطلاعات و داده‌های شخصی افراد، و جرائم عام مانند کلاهبرداری، سرقت از افراد در محیط سایبری، میزان مجازات‌های آنها در دادگاه تعیین شده است. و متناسب با این میزان افراد مجازات می‌شود و حکم دادگاه در مورد آنها اجرا می‌شود. به طور مثال جرم کلاهبرداری اینترنتی در دادگاه انگلستان با توجه به کیفیت جرم بین ۱ تا ۲ سال حبس در نظر گرفته‌اند.

حقوق ایران در زمینه جرائم رایانه‌ای گرچه تلاش‌های مفیدی داشته، ولی همچنان نیاز به کار و پژوهش در زمینه ابعاد مختلف آن دارد. ضمن اینکه در عرصه قانونگذاری کاستی‌هایی نیز وجود دارد که امید است با تصویب قانون مجازات جرائم رایانه‌ای که سال‌هاست در فراموش‌خانه مجلس مورد بی‌مهری است، گامی در این راه برداشته شود. متخصصان معتقدند جرم جاسوسی رایانه‌ای، با شدت و پیچیدگی بیشتری در سطح وسیع جهانی ادامه پیدا خواهد کرد و یکی از مواردی است که نیاز مبرم به تصویب قوانین به روز را می‌طلبد.

در نظام حقوقی انگلستان، که متفاوت از دیگر نظام‌های اروپایی است، دادستانی در پروسه‌های تحقیق و بازرسی دخیل نیست و رسیدگی به اکثر جرائم خرد و کلان بر عهده نیروی پلیس منطقه‌ای است، البته از این وجه که در این مرحله نیز قاضی تحقیق وجود ندارد، مشابه با حقوق فرانسه است. در ساختار پلیس نیز این‌گونه نیست که هر پلیسی صلاحیت پرداختن به تمام مراحل رسیدگی و تحقیق را داشته باشد، بلکه امور با تقسیم وظایف صورت می‌گیرد؛ مثلاً یک گروه، فقط مسئول تحقیقات هستند. همچنین پلیس انگلستان دارای واحد تحقیق و کشف جرم است که افسران این واحد، به جرائم مهمی همچون قتل عمد می‌پردازند؛ نام دیگر آن اداره تحقیقات کیفری است. این اداره همچنین واحدهایی نیز مختص رسیدگی به جرائمی همچون سرقت دارد (۱۶).

در حقوق ایران برای زنان و کودکان قربانی فضای سایبری مجازات‌های سنگینی تعیین کرده‌اند. برای حمایت از زنان و کودکان دادگاه قضایی مجازات‌های نظیر زندانی و جریمه‌های شخصی تعیین کرده است.

در حقوق انگلیس زنان و اطفال از حقوق ویژه‌ای برخوردارند. به طوری که دچار سوء قصد شوند و شاکي خصوصی هم نداشته باشند، دادگاه با مصوبات تأیید شده از شورای قضاوتی می‌تواند اقدام کند. در حقوق انگلیس شرکت‌ها و مؤسساتی هستند که با کلاهبرداری اینترنتی زنان و اطفال را قربانی می‌کنند. در این خصوص قضات ویژه‌ای برای جرائم آنها در نظر گرفته‌اند. زنان در حقوق انگلستان می‌توانند مشغول هر نوع فعالیتی شوند و هیچ‌گونه منع قانونی ندارند. در مقام تعقیب توجه به مصالح بزه‌دیدگان باید به یاد داشت که بزه‌دیدگان دارای طیف گسترده‌ای هستند. گروههایی مانند زنان، کودکان، سالمندان، ناتوانان ذهنی و جسمی هر کدام با توجه به نوع جرمی که علیه آنها ارتکاب می‌یابد باید به گونه خاصی حمایت شوند

در سیستم حقوقی ایران جرائم عام سایبری مانند کلاهبرداری، سرقت و جعل است که با استفاده از رایانه انجام می‌شود. قانونگذار در این دسته از جرائم میزان مجازات آنها را تعیین کرده است. به طور مثال قانونگذار جرائم کلاهبرداری

References

1. Sharifi M. Jarayeme Rayane'i Dar Hoghoughge Engelestan Ba Negahi Be Hoghoughge Iran. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2010. p. 34.
2. Sadeghpour N. Naghshe Polis Dar Farayande Dadsie Keyfari Dar Hoghoughge Engelestan Ba Negahi Be Hoghoughge Iran. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2001. p. 50.
3. Ghajar S. Tejarate Elektoronik Va Jarayeme Mortabete An. Majmou'e Maghalate Avalin Hamayeshe Takhasosiye Barasiye Jarayem Rayane'I 2001; 1: 18.
4. Zar Rokh E. Jormshenasiye Fazaye Majazi. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2010. p. 42.
5. Abas Zade M. Taghrirate Darsiye A'ine Dadrasiye Keyfari. 1th. Tehran: University of Tehran Publication; 2013. p. 77.
6. Khaleghi A. A'ine Dadrasiye Keyfari. 1th. Tehran: Shahre Danesh Publication; 2013. p. 112. 220. 228.
7. August R. International Cyber-Jurisdiction: A Comparative Analysis. American Business Law Journal 2002; 1: 33.
8. Zera'at A. A'ine Dadrasiye Keyfariye Iran Ba Tekye Bar Osoul va Ghava'ed. 1th. Tehran: Delpazir Publication; 2009. p. 137.
9. Emm D. Cybercrime and the law. a review of UK computer crime legislation. London: Rutledge Publication; 2009. p. 24.
10. Safariye Kakroudi A. Mas'ouliyate Ma'mour Dar Ejraye Amre 'Amere Ghanouni. Faslnameye Daneshe Entezami 2007; 4: 42.
11. Parvizi Fard P. A'ine Dadrasiye Keyfariye Tatbighiye Salbe Azadi Az Motaham Dar Hoghoughge Iran Va Engelestan. 1th. Tehran: Jangale Javdane Publication; 2001. p. 31.
12. Ford H. criminal procedure and sentencing. 7th. London: Cavendish Publication; 2009. p. 28.
13. Reilly D. Wren C & Berry T. Cloud computing: forensic challenges for law enforcement. Paper presented at the International Conference for Internet Technology and Secured Transactions in London UK; 2010. p. 45.
14. Mosadegh M. A'ine Dadrasiye Keyfari. 1th. Tehran: Jangal Publication; 2014. p. 49.
15. Pad E. Hoghoughge Keyfariye Ekhtesasi. 2th. Tehran: Shahre Danesh Publication; 2008. p. 89.
16. Mehra N. Edalate Keyfariye Koudakan. 1th. Tehran: Mizan Publication; 2011. p. 44.
17. Hindelang M. Victims of personal crime: An empirical foundation for a theory of personal victimization. Cambridge: Cambridge Publication; 2005. p. 52.
18. Karengi M. Hodoude Ekhtiyarate Polis Dar Iran Va Engelestan. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2010. p. 60.
19. Kashfi S. Barasiye Tatbighiye Ekhtiyarate Polis Dar Farayande Keyfari Dar Hoghoughge Iran, Engelestan Vs Velz. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2013. p. 78.
21. Dezyani MH. Ab'ade Jaza'ie Karborde Computer Va Jarayeme Computeri. 1th. Tehran: Amniyate Fazaye Majazi Publication.: p. 157, 158.
22. Hoseyni B. Jarayeme Interneti A'layhe Atfal Va Zaminehaye Jormshenasiye An. Payanameye Karshenasiye Arshad. 2017; 1th: p. 66.
23. Mehra N. Jozveye Motoune Hoghoughi. Daneshgahe Shahid Beheshti. 2010; 1th: p. 48.
24. Jalali A. Konvansiyone Jarayeme Sayber va Porotokole Elhaghiye An. 1th. Tehran: Khorsandi Publication; 2010. p. 34, 48.
25. Sadeghian D. Kalbod Shenasi Jara'eme Sayberi Dar Iran. Majaleh Dadrasi 2011; 88: 44.
26. Mahdi Pour Kh. Tejarate Elektoroniki. 3th. Tehran: Dibagaran Publication; 2010. p. 36.
27. A'bdolahi M. Dalile Elektoroniki Dar Da'aviye Hoghoughi. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2008. p. 53.
28. Dolatshahi Sh. Salahiyate Ghaza'i Dar Mohite Majazi. Paygahe Etel'a Resaniye Vekalat Online ; 2011. p. 3.
29. Oudi S. Naghshe Asnade Elektoroniki Dar Nezame Adeleye Esbate Da'vi Dar Iran. MA Dissertation. Tehran Iran: Islamic Azad University: Tehran Markaz; 2011. p. 33.
30. Zarkalam S. Emzaye Elektoronik Va Jaygahe An Dar Nezame Adeleye Esbate Da'vi. 1th. Tehran: Modares Publication. 2010. p. 40.