Criminal law doctrines of Islamic countries

https://diplic.qom.ac

The Capacity of the Malaysian Legal System to Commit Digital Crimes

Peyman Namamian[1]

Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Iran, Arak

Abstract

Developments in information and communication technology have had a significant impact on individuals and society as a whole. Digitalization has changed the way of action and interaction in social contexts. Information communication infrastructure as well as digital devices have now become an integral part of today's reality. Digitalization has a huge impact on the development and observance of human rights, as well as the individual's own situation. Therefore, digital crime is an activity that has become more popular in different countries today. Today, this crime is taken seriously by all countries because it has negative impacts on society. In Malaysia, the types of digital crime we face are hacking, money laundering, phishing and digital fraud. Digital crime can be defined as any form of criminal behavior that uses any type of electronic device through an Internet connection and includes individual or group behavior. Of course, digital crimes usually occur during online money transactions, ordering food through apps like e-orders, online money transfer and company registration, and more. However, considering the speed of Internet use that has a positive effect on society, it cannot be denied that there are also negative effects that need to be considered.

Keywords: information and communication technology, digital space, digital crimes, digital security, Malaysian government.

Received: 11/08/2024 **Accepted**: 12/11/202

How To Cite: Namamian, P., (2024). The Capacity of the Malaysian Legal System to Commit Digital Crimes, *Criminal law doctrines of Islamic countries*, 1(4), 113-133 .

doi.org/ 10.22091/dclic.2024.10996.1016

Published by: University of Qom **Article type**: Research

آموزه‌های حقوق کیفری کشورهای اسلامی
https://diplic.qom.ac.ir

ظرفیت نظام حقوقی مالزی در قبال ارتکاب جرائم دیجیتالی

پیمان نمامیان[1]

دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد دانشگاه اراک، ایران، اراک، رایانامه:
p_namamian1512@yahoo. com

چکیده

تحولات در فناوری اطلاعات و ارتباطات تأثیر قابل توجهی بر افراد و جامعه به‌عنوان یک کل داشته است. دیجیتالی شدن شیوه عمل و تعامل را درزمینه‌های اجتماعی تغییر داده است. زیرساخت‌های ارتباطی اطلاعات و همچنین دستگاه‌های دیجیتال در حال حاضر به بخشی جدایی‌ناپذیر از واقعیت امروز تبدیل شده‌اند. دیجیتالی شدن تأثیر بسیار زیادی بر توسعه و رعایت حقوق بشر و همچنین بر وضعیت خود فرد دارد. ازاین‌رو، جرائم دیجیتالی فعالیتی است که امروزه در کشورهای مختلف رواج بیشتری یافته است. امروزه این جرائم توسط همه کشورها جدی گرفته می‌شود؛ زیرا تأثیرات منفی بر جامعه گذاشته است. در مالزی، انواع جرائم دیجیتالی که ما با آن مواجه هستیم، هک، پول‌شویی، فیشینگ و کلاهبرداری دیجیتالی است. جرائم دیجیتالی را می‌توان هر شکلی از رفتار مجرمانه تعریف کرد که از هر نوع وسیله الکترونیکی از طریق اتصال اینترنتی استفاده می‌کند و رفتار فردی یا گروهی را در برمی‌گیرد. البته جرائم دیجیتالی معمولاً در حین تراکنش‌های پول برخط، سفارش غذا از طریق برنامه‌هایی مانند سفارش‌های الکترونیکی، انتقال پول برخط و ثبت شرکت و موارد دیگر رخ می‌دهد. با این حال، با توجه به سرعت استفاده از اینترنت که تأثیر مثبتی بر جامعه دارد، نمی‌توان انکار کرد که تأثیرات منفی نیز وجود دارد که باید مورد توجه قرار گیرد.

کلیدواژه‌ها: فناوری اطلاعات و ارتباطات، فضای دیجیتال، جرائم دیجیتال، امنیت دیجیتال، دولت مالزی.

تاریخ دریافت: ۱۴۰۳/۰۵/۲۱ **تاریخ پذیرش:** ۱۴۰۳/۰۸/۲۲

استناد: نمامیان، پیمان، (۱۴۰۳). ظرفیت نظام حقوقی مالزی در قبال ارتکاب جرائم دیجیتالی، آموزه‌های حقوق کیفری کشورهای اسلامی، ۱(۴)، ۱۳۳-۱۱۳.
doi.org/ 10.22091/dclic.2024.10996.1016

ناشر: دانشگاه قم **نوع مقاله:** پژوهشی

مقدمه

بشر به‌عنوان یک پدیده اجتماعی در حال ظهور در عصر اطلاعات، جرائم دیجیتال به دلیل تخریب زیاد و تأثیر گسترده، نگرانی‌های فزاینده‌ای را در سراسر جهان برانگیخته است. در کنار توسعه سریع فناوری اطلاعات و ارتباطات و شیوع فزاینده اینترنت، این فعالیت‌های جنایی به‌طور قابل توجهی اقتصاد جهانی، امنیت ملی، ثبات اجتماعی و علایق فردی را مختل می‌کند؛ اگرچه تخمین هزینه دقیق مالی جرائم دیجیتال دشوار است. شواهد آماری از دولت‌ها و صنایع نشان می‌دهد که خسارات اقتصادی ناشی از جرائم دیجیتال بسیار عظیم بوده و در حال حاضر به سرعت در حال افزایش است (McAfee, 2021).

درزمینهٔ زیرساخت‌های فنی، اینترنت ثابت کرده است که سریع‌ترین حوزه توسعه در حال رشد است. گرایش به سمت دیجیتالی شدن با گذشت زمان در حال افزایش است در حالی که تقاضا برای رایانه و اتصال به اینترنت، فناوری رایانه‌ها را به سطوح بالاتری سوق داده است (Prasad, Ibrahim, Abdul Manaf, F, 2014: 112). بنابراین، توسعه اینترنت و فناور ی‌های دیجیتال، فرصتی بزرگ برای بشریت در تبدیل کسب‌وکارها و ارائه ابزارهای جدید برای ارتباطات روزمره است. کاربران اینترنت زمان فزاینده‌ای را به صورت آنلاین سپری می‌کنند و دامنه وسیع‌تری از فعالیت‌های آنلاین و شبکه‌های اجتماعی را انجام می‌دهند.[۱]

در عصر دیجیتال نوین، اطلاعات می‌توانند در کسری از ثانیه در سراسر جهان به صورت ویروسی انتشار یابند. جرائم دیجیتال اغلب به‌عنوان جرائم رایانه‌ای یا جرائم با فناوری پیشرفته تعریف می‌شوند. آن‌ها به قصد آسیب رساندن به اموال دیگران، تمامیت شخصی، جان دیگران و سرقت اقلام و اطلاعات ارزشمند از افراد دیگر متعهد شده‌اند. نمونه‌هایی از جرائم دیجیتال شامل ویروس‌های رایانه‌ای، توزیع محتوای غیرقانونی و غیراخلاقی، هک یا دسترسی غیرمجاز، تغییر غیرمجاز داده‌های رایانه‌ای، مخدوش کردن گسترده برخط،

---

۱. توسعه و تکامل فضای دیجیتال سبب ایجاد اشکال مختلفی از جرائم دیجیتال شده است. از اینرو در دهه‌های اخیر کشورها در قبال جرائم دیجیتال در جهت تدوین معاهدات بین‌المللی گام برداشته‌اند. یکی از این معاهدات بین‌المللی، معاهده جرائم دیجیتال شورای اروپا (کنوانسیون بوداپست) در سال ۲۰۰۱ بوده که به‌عنوان نخستین معاهده در این زمینه نگاشته شده است. این معاهده شامل اصول سیاست نمادین از جمله اطمینان بخشیدن به مردم در جهت خنثی کردن سلاح‌های جاسوسی دیجیتال، آموزش عمومی درباره جرائم دیجیتال و بازدارندگی ارتکاب فعالیت‌های مجرمانه در فضای دیجیتالی، است (کتانچی و پورقهرمانی، ۱۳۹۸: ۳۱).

سرقت هویت[1] یا فیشینگ، اسکوات دیجیتال، تعقیب دیجیتال و بسیاری موارد دیگر است (Mohamed, 2012).

فناور ی‌های دیجیتال ابزار جدیدی برای دفاع و اجرای حقوق بشر فراهم می کنند. استفاده از فناور ی‌های جدید اطلاعات و ارتباطات حتی توسط افراد و نهادهای غیردولتی ممکن است تهدیدی برای صلح و امنیت بین‌المللی باشد. دیجیتالی شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشیده‌اند. در حال حاضر هیچ ابزار هنجاری خاصی وجود ندارد که به‌طور جامع حقوق بشر قابل اجرا در عصر دیجیتال را تعیین کند. در مقابل، پیشرفت‌های فناوری اطلاعات و ارتباطات برای رژیم‌های مختلف بین‌المللی و محلی موجود که به دنبال حمایت از حقوق بشر هستند، پیامدهایی دارد. توسعه فناور ی‌های دیجیتال همه جنبه‌های زندگی بشر و حقوق بین‌الملل ازجمله دامنه، موضوعات، ابزار و روش‌های تحریم‌های بین‌المللی و یک‌جانبه را تغییر داده و همچنان در حال تغییر است.

جرائم دیجیتال[2] هیچ مرز جغرافیایی ندارد و کل جهان تحت تأثیر قرار خواهد گرفت. این در حالی است که با رشد فناور ی‌های دیجیتالی، جرائم دیجیتالی در فضای مجازی هم گسترش یافت و فرصت‌های زیادی را برای مرتکبان جرائم دیجیتالی فراهم کرد تا اقدام‌هایی را جهت ورود آسیب جدی به زیرساخت‌ها و بسترهای اجتماعی، سیاسی و حتی امنیتی فراهم نماید. همچنین کارهای مشترکی بین کشورها (به‌عنوان مثال ایالات متحده و اتحادیه اروپا در سال ۲۰۱۰) و گروه‌های کاری از مؤسسات برای مبارزه با جرائم دیجیتال و

---

۱. جرائم هویتی یکی از آن جرایمی است که می‌تواند نهادهای مالی، افراد و یا حتی کل جامعه را تحت تأثیر قرار دهد. تأثیرات جرم هویتی، از جمله، تأثیرات عاطفی و روانی، مالی و امنیتی است. جرم هویتی در معنای اصلی خود اصطلاحی است که برای اشاره به انواع فعالیت‌های غیرقانونی (سرقت، استفاده متقلبانه، تغییر و...) که تحت هویت افراد (نام، گذرنامه، حساب‌های بانکی و...) انجام می‌شود، به کار می‌رود. اصطلاح «هویت» شامل کلیه اطلاعات مربوط به اشخاص (حقیقی یا حقوقی) از قبیل نام، آدرس، ایمیل، شماره تلفن، حساب بانکی، لباس فرم و مواردی از این قبیل است .این نوع جرائم جدید نیستند، اما شکی نیست که در دسترس بودن اطلاعات و داده‌ها در دنیای مجازی، جرائم هویتی را شکوفا می‌کند و ارتکاب آنها را آسان می‌کند؛ مانند سایر کشورهای جهان، مالزی مقررات کلی و اختصاصی برای مبارزه با جرائم هویتی و محاکمه مجرمان دارند (Sidi Ahmed, 2019: 154).

۲. جرائم دیجیتال را می‌توان معاصر مقررات کیفری کلی دانست. استفاده از بیان معاصر نشان می‌دهد که جرائم دیجیتال به عنوان بخشی از مقررات کیفری کلی رشد سریعی داشته است که از سال ۱۹۷۰ شروع شد و تاکنون ایجاد شده است (Srivastava, 2023: 193).

بحث در مورد مسائل امنیتی و قانونی وجود دارد (به‌عنوان مثال گروه کاری حقوقی جرائم دیجیتال که توسط مؤسسه شرق غرب[1] در سال ۲۰۱۰ تأسیس شد).[2]

افزایش بسیار قابل توجهی در استفاده از اینترنت در سال ۲۰۲۰ مشاهده می‌شود به علت همه‌گیری کووید-۱۹ که کشور را تحت تأثیر قرار داد و اولین مورد در مالزی در ۲۵ ژانویه ۲۰۲۰ شامل شهروندان چینی که در ۲۳ ژانویه ۲۰۲۰ به مالزی آمدند گزارش شد (See: Zakon, 2003). لازم به ذکر است مطابق گزارش سال ۲۰۲۳، امنیت دیجیتال مالزی در سال ۲۰۲۲، ۴۷۴۱ مورد تهدید دیجیتال بوده است، در حالی که تا فوریه ۲۰۲۳، موارد گزارش شده ۴۵۶[3] مورد کلاهبرداری بود.[4] برای پیشگیری از گسترش همه‌گیری از جدی‌تر شدن، دولت اولین فرمان کنترل حرکت[5] را در ۱۸ مارس ۲۰۲۰ اجرا کرد و پس از آن مرحله دوم فرمان کنترل حرکت، دستور کنترل حرکت مشروط،[6] فرمان کنترل جنبش توان‌بخشی را اجرا کرد.

مرتکبان جرائم دیجیتال در مالزی به‌طور فزاینده‌ای در سوءاستفاده از بزه‌دیدگان بی‌احتیاط از طریق انواع فعالیت‌های مخرب مهارت یافته‌اند. یکی از رایج‌ترین آن‌ها فیشینگ است که در آن مجرمان از شرکت‌های معتبر تقلید می‌کنند تا مردم را برای افشای اطلاعات مهم فریب دهند. کلاهبرداری‌های برخط، مانند سایت‌های جعلی تجارت الکترونیک و برنامه‌های سرمایه‌گذاری جعلی نیز در حال افزایش هستند. متأسفانه، حملات باج‌افزار که در آن داده‌ها تا زمان پرداخت باج گروگان نگه داشته می‌شوند و سرقت هویت که در آن اطلاعات شخصی برای مقاصد بدخواهانه به سرقت می‌رود، رویدادهای گسترده‌ای هستند.[7] در هر حال، محقق سعی دارد تا با استفاده از منابع کتابخانه‌ای و اینترنتی ضمن پردازشی اولیه به مختصات و ساختار امنیت در فضای دیجیتال مالزی، نسبت به شناسایی مفاهیم جرائم دیجیتال و رویکردها و سیاست‌های تقنینی مالزی را در قبال این پدیده مورد مطالعه قرار دهد. البته این مقاله برای پاسخ به این پرسش که «در چارچوب فضای

1. The East West Institute.
2. Judge Stein Schjolberg, (Dec.2011), Global Phenomenon and its Challenges Courmayeur. ISPAC.
3 . International Conference on Cybercrime, Italy.
4. https://www.nst.com.my/.
5. Movement Control Order (MCO).
6. Conditional Movement Control Order (CMCO).
7. https://condition-zebra.com/blog/the-rise-of-cybercrime-in-malaysia-what-you-need-to-avoid/.

دیجیتال دولت مالزی به چه نحوی با جرائم ارتکابی مقابله می‌کند؟» از روش توصیفی تحلیلی، استفاده می‌کند.

۱. شناسایی و ادراک مفهوم

امروزه فناور ی‌ها امکان افزایش جرائم به‌ویژه جرائم دیجیتال را فراهم می‌کنند. جرائم در فضای دیجیتال، جرائمی هستند که با استفاده از دستگاه‌های دیجیتال، رایانه، تلفن همراه و موارد دیگر مرتبط هستند. جرم دیجیتال به‌عنوان جرمی تعریف می‌شود که داده‌های رایانه‌ای و سیستم‌های دیجیتال مرتبط با آن را هدف قرار می‌دهد که در آن دسترسی، سرقت، تغییر، فساد یا اختلال غیرمجاز انجام می‌شود. با این حال، یک جرم دیجیتال تنها زمانی رخ می‌دهد که یک آسیب‌پذیری در سیستم یا برنامه مورد نظر شناسایی و مورد سوءاستفاده قرار گیرد (ملکوتی و خلیل‌زاده، ۱۴۰۱: ۸۳-۸۱). آسیب‌پذیری به‌عنوان ضعفی تعریف می‌شود که در دستگاه‌ها یا گروهی از دستگاه‌ها (منابع) وجود دارد که می‌تواند توسط یک تهدید مورد سوءاستفاده قرار گیرد. بنابراین، آسیب‌پذیری‌ها منابع را در معرض خطر بزرگی قرار می‌دهند. خطر به‌عنوان امکانی برای داده‌ها یا یک سیستم تعریف می‌شود که دچار فساد، از دست دادن، سرقت، آسیب، اختلال یا تخریب شود. البته این دسته از جرائم در گونه‌ها و اَشکالی نظیر کلاهبرداری و سرقت هویت، جنگ اطلاعاتی، کلاهبرداری‌های فیشینگ و هرزنامه قابل ملاحظه است.

جرائم دیجیتال از نظر ماهیت پیچیده است و شامل رشته‌های بسیاری ازجمله جرم‌شناسی، علوم رایانه، روان‌شناسی، جامعه‌شناسی، اقتصاد، جغرافیا، علوم سیاسی و حقوق است (Dupont and Holt, 2022). بنابراین، جرائم دیجیتال جرائمی است که مولود جامعه فناور و مدرن بوده و به همین دلیل، ابهامات زیادی در باب ماهیّت و پیشینه این‌گونه جرائم از یک سو و ویژگی‌های این جرائم و مرتکبان آن‌ها از سوی دیگر وجود دارد. با عنایت به این ابهامات و نیز تفاوت‌های موجود بین جرائم دیجیتال و سایر جرائم، پیشگیری و مقابله با جرائم دیجیتال اقدامات تهاجمی خاصی را می‌طلبد (موسوی و دیگران، ۱۴۰۱: ۳۲۳).

فناوری دیجیتال به‌عنوان ابزاری بسیار پویا برای ارتباطات دارای کاربرد قابل ملاحظه‌ای است. به‌نحوی‌که این فناوری هم‌چنین نیروی محرکه‌ای برای بازیگران غیردولتی و حامیان آن‌ها برای طیف وسیعی از اهداف

است. اینترنت به دلیل مزایای بسیاری که ارائه می‌کند، به ابزار مورد علاقه مرتکبان جرائم دیجیتالی تبدیل شده است ازجمله دسترسی آسان، مقررات اندک یا بدون محدودیت، سانسور ضعیف یا بدون آن یا سایر اشکال کنترل دولتی، مخاطبان بالقوه عظیمی که در سراسر جهان منتشر می‌شوند (Sander, 2022: 295). ناشناس بودن ارتباطات، جریان سریع اطلاعات، تعامل، توسعه و نگهداری ارزان یک حضور وب، یک محیط چندرسانه‌ای و توانایی تأثیرگذاری بر پوشش در رسانه‌های جمعی سنتی. بنابراین، عصر دیجیتال و گسترش پلتفرم‌های موجود در فضای مجازی، ظهور جرائم دیجیتالی را تسهیل کرد (Odhiambo, Ochara and Kadymatimba, 2018: 149-151). با این همه، ارتکاب جرائم دیجیتالی در مقیاس بزرگ با سرعت هشداردهنده‌ای در سراسر جهان در حال افزایش است.

این حمله‌ها اغلب با تهدیدهای ناشی از جرائم دیجیتالی که به‌طور گسترده تبلیغ و عمومی شده است، مرتبط هستند. با این حال، «جرائم دیجیتالی» یک زمینه تحقیقاتی نسبتاً جوان است و اصطلاحات آن، نظیر اصطلاح اصلی آن، تاکنون به نحو قابل پذیرشی مورد تعریف قرار نگرفته است (Taylor, 2014: 48-50). البته تعریف جدید از تجزیه‌وتحلیل دقیق تعاریف موجود در ادبیات قابل دسترس عموم قابل ملاحظه است که مشتمل بر کلیه اشتراکات کلیدی شناسایی شده وفق طبقه‌بندی جدید پیشنهادی (یعنی بازیگر، انگیزه، قصد، وسیله، اثر و هدف) است. این رویکرد نوین برای تعریف جرائم دیجیتالی درک مشترکی از تهدید گسترده‌تر برای استانداردسازی سیاست، همکاری جهانی و تحقیقات ارائه می‌کند، در حالی که اجازه می‌دهد، زیرمجموعه‌های منحصربه‌فردی از این شاخه از جرائم دیجیتالی برای کاربردهای قانونی یا تخصصی خاص تعریف شود (Plotnek and Slay, 2021: 136-137). با این همه، پرسشی که به ذهن متبادر می‌شود این است که آیا جرائم دیجیتال وجود دارد؟ مادامی‌که پرسش‌هایی راجع به وجود یک مفهوم مطرح می‌شود، پاسخ به تعریف آن بستگی دارد. با توجه به تعاریف موجود در خصوص جرائم دیجیتالی، هدف از آن ایجاد ارعاب و هراس افراد یک سازمان یا یک دولت از طریق ایجاد اختلال در فرآیندهایی است که در آن سازمان یا دولت عمل می‌کند یا از طریق کشتن یا معلول کردن آن افراد. ازاین‌رو، نقطه مشترک بین تعریف جرائم دیجیتالی متعارف و تعریف جرائم دیجیتال این است که هر دو جرم سعی در ایجاد اختلال در فرآیندهای

یک سازمان یا دولت دارند. تفاوت در این دو تعریف به این بستگی دارد که آیا قتل و معلول کردن افراد برای معنای جرائم دیجیتال حیاتی است یا خیر؟

اگر کشتار و معلول کردن افراد یکی از ویژگی‌های ذاتی جرائم دیجیتال باشد، به ظاهر تفاوتی بین هیچ‌یک قابل ملاحظه نیست. در جرائم دیجیتال، ابزار ارتکاب حمله از یک حمله جنبشی مستقیم به یک حمله دیجیتالی تغییر کرده است، جایی که اثرات جنبشی پیامد حمله دیجیتالی است. یک تفاوت قابل توجه بین جرائم متعارف و جرائم دیجیتال این است که فراوانی حملات ناشی از جرائم دیجیتالی از میزان حملات دیجیتالی سنتی کمتر است (Buresh, 2020: 71-72). با این همه، امنیت سایبری مالزی برای این نوع از جرائم سه دسته طبقه‌بندی ارائه کرده است؛ اولین دسته، جایی است که سیستم‌های فناوری اطلاعات و مالکیت معنوی برای بهره‌برداری یا سرقت و نفوذ هدف قرار می‌گیرند؛ دوم، اینکه از تجهیزات فناوری اطلاعات و ارتباطات برای ارتکاب جرم استفاده می‌شود، به‌عنوان نمونه، تجهیزات رایانه خانگی برای اجرای یک برنامه مخرب برای نفوذ به رایانه‌های دیگر استفاده می‌شود؛ دسته سوم، مربوط به بخشی است که از تجهیزات فناوری اطلاعات و ارتباطات به‌عنوان ابزاری برای ارتکاب جرم مورد استفاده قرار می‌گیرد که در این رابطه می‌توان به مثال، تحریک، انتقاد، تحریک ناهماهنگی، قلدری و جاسوسی اشاره داشت (CyberSecurity Malaysia, 2020). به‌طور کلی، جرائم دیجیتالی شامل فعالیت‌های غیرقانونی است که در «فضای دیجیتال» ارتکاب می‌یابند و رایانه به‌عنوان رسانه یا ابزاری برای ارتکاب آن جرائم استفاده می‌شود؛ این اعمال گاهی اوقات به‌عنوان «جرائم قدیمی، ابزارهای جدید» شناخته می‌شوند؛ زیرا جرائم ارتکابی در اصل از نوع قدیمی (از دنیای غیر برخط) یا انواع سنتی جرائم هستند، اما فنون ارتکاب چنین جرمی در محیط دیجیتال تغییر کرده است.[1]

۱. یکی از نمونه‌های جرم دیجیتالی، کلاهبرداری در فضای دیجیتال بوده که با دستکاری داده‌های رایانه‌ای متعلق به دیگران به منظور به تصاحب یا اختلاس غیرصادقانه پول یا دارایی و ایجاد ضرر ارتکاب می‌یابد. البته انواع دیگر کلاهبرداری شامل، «سوءاستفاده از کارت‌های ماشین باجه خودکار»، «سوءاستفاده از کارت‌های اعتباری و انتقال الکترونیکی وجوه» است. در ضمن، نوع دیگری از جرائم دیجیتالی به «جنایت جدید، ابزارهای جدید» موسوم است؛ زیرا جرائم شامل موقعیتی است که مظنون از سیستم رایانه‌ای برای تغییر یا اصلاح داده‌های خاص در آن سیستم استفاده می‌کند که شامل، خرابکاری، خرابکاری و استراق سمع الکترونیکی یا به دست آوردن دسترسی غیرقانونی با جعل هویت یک کاربر مجاز یا تجاوز از اختیارات یک فرد، انتشار ویروس‌های رایانه‌ای، جنگ دیجیتالی، جرم تروریستی دیجیتالی، هرزنگاری دیجیتالی، تجاوز به حریم خصوصی نظیر دسترسی به اطلاعات شخصی، سرقت دریایی نرم افزاری هم‌چون تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای، هک، فیشینگ یا سرقت هویت، تعقیب دیجیتالی، تخریب انبوه وب‌گاه همگی به‌عنوان جرائم دیجیتالی طبقه‌بندی می‌شوند.

۲. اقسام جرائم دیجیتالی

همان‌گونه که توسط نظام امنیت دیجیتالی مالزی گزارش شده است، آمارها نشان می‌دهد که در مجموع ۸۲۲۶ پرونده مربوط به جرائم دیجیتالی از ژانویه ۲۰۲۱ تا سپتامبر ۲۰۲۱ رخ داده است. ازاین‌رو، موارد زیر برخی از رایج‌ترین انواع جرائم دیجیتالی در مالزی است:

الف. «فیشینگ» نوعی حمله دیجیتالی است که در آن وب‌سایتی ایجاد می‌کند که قانونی و قانع‌کننده به نظر می‌رسد، اما سعی می‌کند داده‌های شخصی و حساس را سرقت نماید (Paraschiv et al, 2021). نوع از این وب‌سایت‌های فیشینگ وجود دارد، اول، برای سرقت مالی و دوم، جعل، یعنی تقلید از وب‌سایت‌های قانونی برای سرقت هویت و انتشار بدافزار (Chen et al, 2020). در بیشتر موارد، بزه‌دیده ایمیل یا پیامی را دریافت می‌کند که قانع کننده به نظر می‌رسد از بانک یا ارائه دهنده خدمات. بزه‌دیدگان فریب خورده اطلاعات محرمانه‌ای مانند افشای رمز عبور یا اطلاعات شخصی را برای مجرمان وارد می‌کنند.

ب. «هک» به معنای هرگونه فعالیت یا دسترسی است که در یک سیستم رایانه‌ای بدون اجازه یا اطلاع صاحب رایانه رخ می‌دهد. هکر کامپیوتر معمولاً کسی است که کامپیوتر و برنامه‌نویسی کامپیوتر را می‌شناسد. هکرها معمولاً با تلاش برای سرقت یا کپی اطلاعات موجود در رایانه، تغییر یا آسیب رساندن به سیستم رایانه، سیستم امنیتی رایانه را تغییر می‌دهند. گذشته از این، برخی از هکرها فقط برای سرگرمی و نشان دادن مهارت‌های خود هک می‌کنند (Redzuan Mohamad, et al, 2024: 168).

ج. «کلاهبرداری عشقی یا توطئه عشقی» نوعی جرم دیجیتالی است. این با هدف قرار دادن زنان به‌ویژه زنان حرفه‌ای با داشتن رابطه عاشقانه اتفاق می‌افتد. این جرم زمانی حادث می‌شود که مرتکب وانمود می‌کند که رابطه عاشقانه با بزه‌دیده را آغاز می‌کند و سپس بزه‌دیده را فریب می‌دهد تا مبلغی پول به او بدهد (Whitty & Buchanan, 2012). برابر اذعان پلیس سلطنتی مالزی، شیوه کار این سندیکا تلاش برای آشنایی با بزه‌دیده از طریق ایمیل و شبکه‌های اجتماعی برای فریب بزه‌دیده است. به‌طور معمول بزه‌دیدگانی که تنها هستند و شریک زندگی ندارند به راحتی فریب می‌خورند (Ismail, 2023).

د. «هرزنامه‌ها» مدتی است که یک نگرانی بوده است. ارسال هرزنامه عمل ارسال کپی‌های متعدد از نامه‌های ناخواسته یا ایمیل‌های انبوه برای گیرندگان متعدد، مانند نامه‌های زنجیره‌ای است. مؤثرترین سازوکار در رفع این چالش، بر دسته‌بندی و فیلتر کردن ایمیل‌های هرزنامه تکیه دارد (Selamat, et al, 2013).

هـ. «سرقت هویت» رفتاری است که فردی از اطلاعات حساس و محرمانه شخص دیگری برای ارتکاب جرم استفاده کند. اطلاعات محرمانه ممکن است حاوی نام، تاریخ تولد، آدرس و اطلاعات مالی فرد باشد. سهولت دسترسی به فناوری اینترنت اکنون فرصتی برای مجرمان است تا به راحتی اطلاعات محرمانه دیگران را به دست آورند. بزه‌دیدگان معمولاً از اینکه هویت آن‌ها برای ارتکاب جرائم غیرقانونی استفاده می‌شود، بی‌اطلاع هستند. کاربران باید هنگام پر کردن و ارائه اطلاعات محرمانه به وب‌سایت‌های غیرقابل اعتماد مراقب باشند (Redzuan Mohamad, et al, 2024).

آزار و اذیت یا آزار دیجیتالی زمانی حادث می‌شود که گروهی از افراد با استفاده از اطلاعات الکترونیکی و ابزارهای ارتباطی مانند ایمیل، وبلاگ‌ها و تلفن‌های همراه با استفاده از اینترنت، سعی در تهدید، شرمساری و ارتکاب حملات افتراآمیز یا شخصی به سایر افراد دارند. انواع مزاحمت‌های دیجیتالی که اغلب رخ می‌دهند عبارت‌اند از ارسال پیام‌های آزاردهنده و تهدیدآمیز، سوءاستفاده از نام‌های صفحه نمایش یا جعل هویت دیگران، گسترش و انتشار عکس‌ها و نظرات نامناسب برای دیگران (Farhana, 2016). بزه‌دیدگان قلدری دیجیتالی می‌توانند تا حد خودکشی افسرده شوند. بنابراین زورگویی دیجیتالی به‌عنوان یک عمل مجرمانه طبقه‌بندی می‌شود و قابل پیگرد قانونی است. پنج نوع جرائم دیجیتالی در مالزی وجود دارد. فیشینگ، هک، کلاهبرداری، سرقت هویت و آزار و اذیت یا قلدری دیجیتالی است. جرائم دیجیتالی حتی با وجود نظام عدالت کیفری ملی به یک معضل فزاینده در جامعه ما تبدیل شده است. تمامی این جرائم دیجیتالی بر اساس موارد خاص و طبقه‌بندی بر اساس قوانین ملی طبقه‌بندی شده‌اند.

انتشار ویروس‌ها فرآیندی است که طی آن نرم‌افزارهای مضر خود را به برنامه‌های دیگر متصل می‌کنند و نظام بزه‌دیده را از بین می‌برند. آن‌ها رایانه‌ها را مختل می‌کنند و داده‌ها را تغییر می‌دهند یا حذف می‌کنند که بر ذخیره‌سازی داده‌ها تأثیر می‌گذارد (Syamsiar Binti Muharram, et al, 2022). کرم‌ها و

ویروس‌ها هر دو دسته‌ای از نرم‌افزارهای مضر هستند، بنابراین تقریباً معادل هستند. هنگامی‌که یک ویروس یک برنامه را آلوده می‌کند، به‌طور خودکار به سایر برنامه‌ها سرایت می‌کند. ویروس‌ها و کرم‌ها هر دو بدون اطلاع کاربر کار می‌کنند (Khan, 2012).

۳. تهدیدها و چالش‌های پیش‌روی

جرائم دیجیتالی همچنان روبه افزایش است و به یکی از معضلات مدرنی تبدیل شده است که امنیت عمومی و اقتصاد کشور را تهدید می‌کند. اگر تلاشی برای کاهش یا پیشگیری از آن‌ها صورت نگیرد، این فعالیت‌ها همچنان افزایش خواهند یافت. بسیاری از کشورها برای پیشگیری از گسترش این «بیماری‌ها» تلاش کرده‌اند، اما به نظر می‌رسد پیشگیری کامل غیرممکن باشد. با این وجود، این امر دولت‌ها و سایر سازمان‌ها را از ادامه تلاش‌های خود برای کاهش چنین جنایاتی از گسترش به سطوح وسیع‌تر جامعه منصرف نمی‌کند. یکی از تلاش‌های دولت مالزی ارائه قوانین و مقررات دیجیتالی بوده است.

فضای بی‌مرز دیجیتال، جهانی موازی با جهان فیزیکی را به وجود آورده است که درواقع کنترل و ادارهٔ حقوقی آن از حیطهٔ اعمال قدرت یک حاکمیت برنمی‌آید. بنابراین، برای حاکمیت بر این فضا و مقابله با جرائم روزافزون و پیچیدهٔ ارتکابی در فضای دیجیتال همکاری و معاضدت جامعهٔ بین‌المللی برای قاعده‌مندی نیاز است، به‌گونه‌ای که هیچ مجرمی بدون مجازات نماند و این مهم به دست نمی‌آید، مگر با تدوین مقررات هماهنگ و متحدالشکل؛ زیرا جرائم ارتکابی در فضای دیجیتال مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند و به سبب ویژگی‌هایی که دارند، می‌توان برخی از این‌گونه جرائم را در زمرهٔ آن دسته جرائمی به شمار آورد که برای مقابله با آن‌ها اعمال صلاحیت جهانی ضرورت دارد (جلالی و توسلی‌اردکانی، ۱۳۹۸: ۱۳۵۱).

نظیر سایر کشورها، مالزی نیز در رسیدگی به پرونده‌های جرائم دیجیتالی با مشکلاتی مواجه است. شناسایی و ردیابی مرتکبین جرائم دیجیتالی برخلاف سایر جرائم سنتی بسیار دشوار است؛ زیرا جرائم ارتکابی به صورت برخط بوده و به‌طور صریح به هیچ موقعیت جغرافیایی مربوط نمی‌شود (Jahankhani et al,

2014). البته راهبرد امنیت دیجیتالی مالزی[1] با ابزارهایی برای ایجاد اعتماد در محیط دیجیتالی ما نه‌تنها برای امنیت ملی، بلکه برای حمایت از دستور کار دولت در اقتصاد دیجیتال، طراحی شده است. به هر روی، اقداماتی که دولت برای مقابله با تهدیدات امنیتی و جرائم دیجیتالی در مالزی انجام داده است به شرح زیر است:

الف. کمپین‌های آگاهی بخشی و تبلیغات: برای مقابله با جرائم دیجیتالی، اولین اقدامی که باید انجام شود، آگاهی‌رسانی به جامعه در مورد اینکه چگونه جرائم دیجیتالی می‌تواند جان بزه‌دیدگان را تهدید کند، است. کمپین‌های مختلف از طریق رسانه‌های چاپی و دیجیتال باید با جدیت بیشتری انجام شود تا مصرف‌کنندگان آگاهی بیشتری داشته باشند و نگرش آگاهانه‌ای در رابطه با جرائم دیجیتالی اتخاذ کنند. در این رابطه می‌توان اظهار داشت که طی سال ۲۰۱۹، یک کمپین آگاه‌سازی پیشگیری از جرائم دیجیتالی توسط وزارت ارتباطات و چندرسانه‌ای سازماندهی شد. هدف این کمپین ارائه آموزش و افزایش آگاهی عمومی در رابطه با جرائم مخابراتی است. کمپین آگاه‌سازی پیشگیری از جرائم دیجیتالی همچنین بازنشستگان، طبقه متوسط، زنان شغلی، دانش آموزان دبیرستانی و همچنین تحصیلات عالی و دانشجویان را هدف قرار می‌دهد. جدای از آن، وزارت ارتباطات و چندرسانه‌ای با رسانه‌ها، پلیس سلطنتی مالزی، آژانس‌ها و بخش‌های زیرمجموعه وزارت ارتباطات و چندرسانه‌ای مانند بخش اطلاعات، وزارت ارتباطات و پخش چندرسانه‌ای نیز همکاری می‌کند. لازم به ذکر است «برنامه آگاهی دیجیتالی برای همه»، ابتکاری از امنیت دیجیتالی مالزی است که هدف آن پرورش دانش عمومی مرتبط با امنیت دیجیتالی و آگاهی از امنیت اینترنت برای ایجاد فرهنگ استفاده مثبت از اینترنت در بین ملت مالزی است. واژه آگاهی امنیت دیجیتالی برای همه شکل کوتاهی از آگاهی امنیت دیجیتالی برای همه است که مأموریت آن ارائه دانش و اطلاعات مختلف در مورد آگاهی دیجیتالی به جامعه است (Redzuan Mohamad, et al, 2024).

1. Malaysia Cyber Security Strategy (MCSS).

ب. ایجاد سازمان‌های مرتبط با امنیت دیجیتالی؛ دولت مالزی در مورد مهار و پیشگیری از هرگونه جرم مرتبط با جرائم دیجیتالی بسیار جدی است. بنابراین، دولت امنیت دیجیتالی مالزی را تحت نمایندگی وزارت علوم و فناور ی[1] ایجاد کرده است (Jayabalan et al, 2014).

۴. ظرفیت‌ها؛ از رویکردهای قانونی تا راهبردهای اجرایی

۴-۱. رویکردهای حقوقی

با این همه، با توجه به تهدیدات مختلف مربوط به جرائم دیجیتالی به دلیل رشد سریع فناوری اطلاعات، مالزی در وضع قوانین و مقررات در حوزه دیجیتالی برای حفاظت و حفاظت از حاکمیت و هماهنگی کشور مستثنا نیست؛ ازجمله اقدامات مربوطه ایجاد شده که عبارت است از:

الف. قانون جرائم رایانه‌ای ۱۹۹۷ در مارس ۱۹۹۷ در مجلس تصویب شد و در ۳۰ ژوئن ۲۰۰۰ لازم‌الاجرا شد.[2] هدف اصلی آن مربوط به جرائم و جرم سوءاستفاده از رایانه برای ارتکاب جرم است. این قانون هرگونه دسترسی غیرمجاز یا تغییر برنامه‌ها و داده‌های موجود در رایانه را بدون اجازه توصیف می‌کند که می‌تواند اشتباه و قابل مجازات باشد. بخش‌هایی از این قانون به جرائمی می‌پردازد که شامل دسترسی غیرمجاز یا غیرقانونی به داده‌های رایانه‌ای و سوءاستفاده از آن است. این قانون همچنین در مورد جرائم خاصی مانند فیشینگ و سرقت هویت اعمال می‌شود. با این حال، این قانون هیچ ماده‌ای در مورد جاسوسی دیجیتالی ارائه نمی‌کند (Bidin et al, 2015; Jayabalan et al, 2014).

ب. قانون ارتباطات و چندرسانه‌ای (۱۹۹۸) برای نظارت بر کلیه فعالیت‌ها و محتوای ارائه دهندگان خدمات ارتباطی و چندرسانه‌ای در مالزی و ایجاد تمرکز روان در صنعت ارتباطات و چندرسانه‌ای طراحی شده است.[3] ازجمله فعالیت‌ها و خدمات تنظیم شده در این قانون می‌توان به پخش سنتی، مخابرات و خدمات برخط اشاره کرد. قانون همچنین مقرر می‌دارد که هیچ ماده‌ای برای سانسور اینترنت وجود ندارد.

---

1. Ministry of Science and Technology (MOSTI).
2. Computer Crimes Act 1997; Date of Royal Assent 18 June 1997 Date of publication in the Gazette 30 June 1997 PREVIOUS REPRINT, http://www.commonlii.org/my/legis/consol_act/cca1997185/.
3. Communications and Multimedia Act 1998; date of Royal assent 3 september 1998 date of publication in the Gazette 5 october 1998.

ج. قانون امضای دیجیتال در ۱ اکتبر ۱۹۹۸ تصویب شد که هدف آن تنظیم استفاده از امضای دیجیتال در مالزی است.[1] این امر برای اطمینان از امنیت در مورد مسائل حقوقی مربوط به تراکنش‌های الکترونیکی و تأیید استفاده از امضای دیجیتال[۲] از طریق گواهی‌های صادر شده توسط مقامات محلی مجاز است. همچنین قوانینی را در مورد واسطه‌هایی که به‌عنوان مقامات صدور گواهینامه و شناسایی امضای دیجیتال عمل می‌کنند ارائه می‌کند (Redzuan Mohamad, et al, 2024).

د. با تصویب قانون تجارت الکترونیک در سال ۲۰۰۶ برای شناسایی قانونی پیام‌های الکترونیکی در معاملات تجاری، استفاده از پیام‌های الکترونیکی برای تحقق الزامات قانونی و امکان و تسهیل معاملات تجاری از طریق استفاده از وسایل الکترونیکی و سایر موارد مرتبط با آن اقدامات مؤثری صورت پذیرفت.[۳] این در حالی است که یک سال بعد در راستای تکمیل فرایند مزبور در سال ۲۰۰۷ قانون فعالیت‌های دولت الکترونیک برای شناسایی قانونی پیام‌های الکترونیکی در معاملات بین دولت و مردم، استفاده از پیام‌های الکترونیکی برای تحقق الزامات قانونی و امکان و تسهیل معاملات از طریق استفاده از وسایل الکترونیکی و سایر موارد مرتبط با آن از سوی دولت مالزی به منصه ظهور رسید.

لازم به ذکر است پس از اجرایی شدن این اساسنامه، تجارت الکترونیکی که شامل تراکنش‌های الکترونیکی می‌شود از نظر قانونی معتبر می‌شود. این اساسنامه همچنین دارای استانداردهای امنیت اطلاعات خاص خود است که باید به‌منظور اطمینان از روان و ایمن بودن فعالیت‌های تجارت الکترونیکی، به‌ویژه زمانی که شامل پیام‌های الکترونیکی باشد و برای اثبات اصالت یک سند رعایت شود.[۴]

---

https://www.vertic.org/media/National%20Legislation/Malaysia/MY_Communications_and_Multimedia_Act.pdf

1. Digital Signature Act 1997; Date of Royal Assent 18 June 1997 Date of publication in the Gazette 30 June 1997 PREVIOUS REPRINT

۲. امضای دیجیتال، نوع خاصی از امضای الکترونیکی است که از فنون رمزنگاری برای اطمینان از صحت و یکپارچگی سند امضا شده استفاده می‌کند. این شامل استفاده از یک گواهی دیجیتال صادر شده توسط یک مرجع گواهی معتبر و استفاده از رمزنگاری کلید عمومی برای امضا و تأیید اسناد است؛ https://www.cleartax.com/my/en/digital-signature-in-malaysia

3. Electronic Commerce Act 2006; Date of Royal Assent 30 August 2006, Date of publication in the Gazette 31 August 2006, Date of coming into operation 19 October 2006 [P.U. (B) 280/2006], http://www.commonlii.org/my/legis/consol_act/eca2006182/.

4. https://www.azamlaw.com/publications/?a=45.

هـ. قانون حفاظت از داده‌های شخصی ۲۰۱۰[۱] قانونی است که پردازش داده‌های شخصی در رابطه با معاملات تجاری را تنظیم می‌کند.[۲] هفت اصل اساسی در این قانون به‌منظور حفاظت از داده‌های شخصی تعیین شده است. اصل امنیت بر اساس این قانون حیاتی‌ترین نقش را ایفا می‌کند؛ زیرا کاربر داده را ملزم می‌کند هنگام پردازش داده‌های شخصی، اقدامات عملی را برای اطمینان از انتقال امن داده‌های شخصی از هرگونه از دست دادن، سوءاستفاده، تغییر، دسترسی یا افشای غیرمجاز یا تصادفی انجام دهد.[۳] لازم به ذکر است اداره حفاظت از داده‌های شخصی[4] یک آژانس زیرمجموعه وزارت ارتباطات و کمیسیون چندرسانه‌ای است که در ۱۶ مه ۲۰۱۱ پس از تصویب قانون حفاظت از داده‌های شخصی ۲۰۱۰ توسط پارلمان تأسیس شد.[۵] مسئولیت اصلی این بخش نظارت بر پردازش داده‌های شخصی افراد درگیر در معاملات تجاری توسط داده‌های کاربر است که توسط طرف‌های ذینفع مورد سوءاستفاده و استفاده نادرست قرار نگیرد.[۶]

ر. قانون ضد اخبار جعلی ۲۰۱۸،[۷] فقدان ظرافت عنوان خبرگزاری قانون ضد اخبار جعلی،[۸] بی‌محتوا بودن متن آن را پیش‌بینی می‌کند.[۹] هدف اولیه قانون ضد اخبار جعلی، قانونی برای مقابله با اخبار جعلی و موضوعات مرتبط است. بند دوم قانون «اخبار جعلی» را این‌گونه تعریف می‌کند: «هر خبر، اطلاعات، داده و گزارشی که کاملاً یا تا حدی نادرست است، اعم از اینکه به صورت ویژگی‌ها، تصاویر، ضبط‌های صوتی یا به هر شکل دیگری که بتواند پیشنهاد کلمات یا ایده‌ها. »[۱۰] البته در این قانون، اخبار جعلی به‌طور کلی

1. Personal Data Protection Act 2010; https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en.
2. https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf.
3. https://www.azamlaw.com/publications/?a=45.
4. Personal Data Protection Department (PDPD).
5. https://opengovasia.com/2024/02/07/malaysia-explores-new-cybersecurity-legislation/.
6. https://www.malaysia.gov.my/portal/content/654.
7. Anti-Fake News Act 2018; The Act was passed by the Malaysian Parliament on April 4 and received Royal Assent on April 9, https://www.loc.gov/item/global-legal-monitor/2018-04-19/malaysia-anti-fake-news-act-comes-into-force/.
8. AFNA's.
9 https://upload.wikimedia.org/wikipedia/commons/2/2c/Anti-Fake_News_%28Repeal%29_Act_2020.pdf
۱۰ . لازم به‌ذکر است، توسعه فناوری دیجیتال مزایای استفاده از رسانه‌های دیجیتال به مثابه منبع اصلی اطلاعات را تشویق می‌کند. با این حال، چنین توسعه‌ای نیز توسط افراد یا نهادهای خاص برای گمراهی مردم با تولید اخبار جعلی مورد سوءاستفاده قرار گرفته است. در اینترنت، اطلاعات نادرست سریع‌تر از حقیقت حرکت می‌کنند و برای پیشگیری از آن تلاش زیادی می‌شود (Sukumaran, Herng Chin, Rahman, Kadhim, 2023: 79).

به‌عنوان هر خبر، اطلاعات، داده و گزارشی است که کاملاً یا تا حدودی نادرست است، خواه به صورت ویژگی‌ها، تصاویر تصویری یا ضبط‌های صوتی یا به هر شکل دیگری که بتواند کلمات یا ایده‌هایی را پیشنهاد کند، تعریف می‌شود (Ren Kok, 2020).

ز. قانون امنیت سایبری ۲۰۲۴ به‌طور رسمی توسط دادستان کل در ۲۶ ژوئن ۲۰۲۴ به تصویب رسیده است.[۱] این قانون نقطه عطفی در تقویت دفاع دیجیتالی مالزی و افزایش انعطاف‌پذیری ما در برابر تهدیدات نوظهور است. هدف از تصویب این قانون بهبود و حفاظت از محیط امنیت دیجیتالی در مالزی است و الزاماتی را برای نهادهای تعیین‌شده در بخش‌های زیرساخت اطلاعات حیاتی ملی معرفی می‌کند تا در آیین‌نامه عملکرد، استانداردها، اقدامات و فرآیندهای خاص را رعایت کنند.[۲]

۴-۲. سیاست‌های قضایی؛ تشکیل دادگاه ویژه دیجیتالی

توسعه سریع فناوری اطلاعات کاربردهای نوینی همچون تجارت الکترونیک و تجارت جهانی را با خود به همراه داشته است. ازاین‌رو، طی سال‌های اخیر مالزی در عرصه قانون‌گذاری، مقرراتی را در مقابله با جرائم دیجیتالی مصوب نمود که با توجه به شکاف‌های ناشی از رسیدگی تخصصی به این‌گونه جرائم، ضرورت حاکم در نظام قانون‌گذاری موجب شد تا در چارچوب سیاست قضایی، مبادرت به تأسیس دادگاهی برای رسیدگی به جرائم دیجیتالی شود. بر این اساس، با توجه به افزایش تهدید در جرائم دیجیتالی و لزوم رسیدگی مؤثر به پرونده‌های جرائم دیجیتالی، دولت مالزی تشکیل «دادگاه ویژه دیجیتالی»[۳] را اعلام کرد.[4] اولین دادگاه دیجیتالی ویژه، مستقر در مجتمع دادگاه کوالالامپور در اول سپتامبر سال ۲۰۱۶ به بهره‌برداری

1. The Cyber Security Act 2024; https://www.rajahtannasia.com/media/7831/2024_03_2024-dr-8-bi.pdf.
2. https://www.ey.com/en_my/take-5-business-alert/malaysia-cyber-security-bill-2024-enhancing-and-safeguarding-malaysias-cybersecurity-landscape.
3. Malaysian Special Cyber Court; https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/
4. لازم به‌ذکر است دسترسی به اطلاعات مربوط به پرونده‌های جرائم دیجیتالی در مالزی برای عموم مردم بسیار دشوار است؛ زیرا این پرونده‌ها به‌طور عمده در دادگاه‌های پایین‌تر مورد رسیدگی قرار می‌گیرند و در رسانه‌های قانونی گزارش نمی‌شوند؛
https://www.researchgate.net/publication/335867251_CYBERCRIME_CASES_IN_A_DECADE_The_Malaysian_Experience

رسید.[۱] هدف از تشکیل این دادگاه ارائه ابزارهای مکفی و اثرگذار برای نظام قضایی جهت رسیدگی به جرائم دیجیتالی نظیر هک، کلاهبرداری برخط، سرقت اطلاعات برخط و غیره است.[۲]

دادگاه ویژه در حال حاضر فعال بوده و در حال حاضر به پرونده‌های مربوط به جرائم سایبری رسیدگی می‌کند. بر اساس دستورالعمل شماره ۵ در سال ۲۰۱۶ که توسط رئیس ثبت دادگاه فدرال مالزی صادر شده است، گستره صلاحیت قضایی دادگاه به امور مدنی و تخلفات هم در ارتباط است. مزایای این دادگاه سرعت‌بخشی به فرایند رسیدگی به پرونده‌های جرائم دیجیتالی، تقویت نهادهای قانونی در مالزی و نیز کاهش چنین جرائم در فضای دیجیتال است. این دادگاه به ابزار و تجهیزات مناسب برای رسیدگی به مدارک جمع‌آوری شده در پرونده‌های مفتوحه مجهز است.[۳] البته به قضات، دادستان‌ها و سایر ذینفعان مربوطه آموزش داده می‌شود تا اطمینان حاصل شود که آن‌ها به دانش و مهارت‌های لازم فناوری اطلاعات مجهز هستند که به آن‌ها در درک موضوع پیچیده جرائم دیجیتال کمک می‌کند.[۴]

۴-۳. راهبردهای اجرایی

در ۱۲ اکتبر ۲۰۲۰، دولت مالزی «راهبرد امنیت سایبری مالزی ۲۰۲۴-۲۰۲۰»[۵] را تدوین و تصویب کرد. اهداف اساسی در پنج رکن راهبردی طبقه‌بندی شده است که بر کلیه ابعاد برنامه‌ریزی و اجرای امنیت سایبری در مالزی تا سال ۲۰۲۴ حاکم خواهند بود.[۶] ارکان مزبور مشتمل بر مراتب ذیل است:

---

۱. اولین دادگاه دیجیتالی مالزی نشانه تعمیق اقتصاد دیجیتال است. از اینرو، مفهوم دادگاه دیجیتالی، مفهوم جدیدی نیست؛ چرا که جرائم دیجیتالی تا مادامی که اینترنت وجود داشته است، وجود دارند. امری که به‌طور فزاینده‌ای در کل جهان در حال فراگیری است؛
-https://www.digitalnewsasia.com/digital-economy/malaysia%E2%80%99s-first-cyber-court-signals-deepening-digital-economy

۲. در حالی که دادگاه ویژه دیجیتالی مادام یک مفهوم بسیار جدید است، مالزی دادگاه الکترونیکی را معرفی کرده‌اند؛ اساساً، این دادگاه از فناوری حمایتی برای تسهیل امور روزمره دادگاه استفاده می‌کند وهدف این نظام تسریع کارآمد در دفع موارد با استفاده از فناوری است. در واقع، هدف سیستم دادگاه الکترونیکی به عنوان یک کل، استفاده از فناوری برای رسیدگی به مسائل و پرونده‌هایی است که سال‌ها نظام قضایی را درگیر خود کرده است. لازم به‌ذکر آیت که این نوع از دادگاه در ژانویه سال ۲۰۱۶ تأسیس شد؛ https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/

3. https://ir.uitm.edu.my/id/eprint/32203/1/32203.pdf

4. https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/

5. Malaysia Cyber Security Strategy (MCSS); https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

6. https://www.coe.int/en/web/octopus/-/malaysia

الف. حکمرانی و مدیریت مؤثر؛ پرداختن به ارتقای مدیریت حاکمیت ملی و امنیت سایبری از طریق بهبود زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات کشور[1] و نیز ارتقای توانایی مقابله مؤثر با مسائل امنیت سایبری؛

ب. تقویت چارچوب قانونی و اجرای آن: تقویت اجرای سیاست‌ها و استانداردهای امنیت سایبری موجود با بررسی مقررات دیجیتال و نیز تدوین قوانین خاص برای مقابله با امنیت سایبری؛

ج. کاتالیزور نوآوری، فناوری، تحقیق و توسعه و صنعت در سطح جهانی؛ توانمندسازی نوآوری و فناوری در سطح جهانی برای اتخاذ ابزارها و فنون امنیت سایبری؛

د. افزایش ظرفیت و ظرفیت‌سازی، آگاهی و آموزش؛ بهبود ظرفیت توسعه و نیز مهارت‌ها و قابلیت‌های امنیت سایبری برای حفاظت از منافع مالزی؛

ر. تقویت همکاری جهانی؛ تقویت همکاری‌های بین‌المللی از طریق فعال‌سازی همکاری‌های منطقه‌ای و بین‌المللی برای حفاظت از منافع و دارایی‌های دیجیتال ملی.

بنابراین، راهبرد امنیت سایبری مالزی شامل ۱۲ راهبرد، ۳۵ طرح اقدام و ۱۱۳ برنامه است که شامل ابتکارات گوناگون برای حفاظت از فضای سایبری کشور است. وزارت ارتباطات و چندرسانه‌ای[2] و آژانس امنیت سایبری ملی[3] وظیفه تدوین، اجرا، نظارت و هماهنگی برنامه اقدام میان‌مدت را بر عهده دارند. مالزی یکی از اولین کشورهای آسیای جنوب شرقی بود که سیاست امنیت سایبری ملی[4] را اتخاذ کرد. سیاست امنیت سایبری ملی که در سال ۲۰۰۶ تدوین شد، تأسیس آژانس دولتی مربوطه را ایجاد کرد و پایه محکمی برای راهبرد امنیت سایبری مالزی ۲۰۲۴-۲۰۲۰ فراهم کرد. [5] به‌هر روی، تردیدی وجود ندارد که مقررات و راهبردهای مصوب در چارچوب نظام حقوقی مالزی با هدف تنظیم فعالیت‌های دیجیتالی و کنترل جرائم در فضای دیجیتالی ابلاغ شده است، اما به نظر می‌رسد که در برخی موارد مرتبط با فضای دیجیتالی، مقررات

1. Information and Communication Technology (ICT).
2. Communications and Multimedia Ministry (KKMM).
3. National Cyber Security Agency (NACSA).
4. National Cyber Security Policy (NCSP).
5. https://www.coe.int/en/web/octopus/-/malaysia.

سنتی همچنان حاکم بوده و ضرورت شناخت بیشتر نسبت به مقررات دیجیتالی در قلمرو حاکمیت قانون مالزی امری انکارناپذیر است.

نتیجه‌گیری

جرائم دیجیتالی یک جرم هزارساله جدید است که چالش‌های جدیدی را به‌ویژه برای نیروی کار در محکومیت جرائم دیجیتالی ایجاد می‌کند. همه طرف‌ها باید نقش‌های مربوطه خود را ایفا کنند و با یکدیگر برای مهار گسترش این جرائم دیجیتالی و تهدید دیجیتالی همکاری کنند.

جرائم دیجیتال و جرائم سنتی تسهیل شده توسط اینترنت یک پدیده مجرمانه جهانی است که تمایز متعارف بین تهدیدات امنیت داخلی و خارجی نظیر جرائم، فعالیت‌های نظامی و تروریستی را مخدوش می‌کند. مسئولیت‌پذیری شبکه‌های برخط برای فعالیت برای اهداف مختلف و توانایی انتقال افراد از یک نوع فعالیت غیرقانونی به نوع دیگر، نشان می‌دهد که سرزمین‌گرایی مانع از تلاش‌ها برای مبارزه مؤثر با استفاده نادرست از فناوری می‌شود. در حال حاضر، مقامات ملی در مالزی با سازماندهی با آژانس‌هایی که توانایی پاسخگویی بهتر و درک جرائم تسهیل شده از طریق اینترنت را دارند، بر محدودیت‌های قضایی غلبه کرده‌اند.

مالزی مقررات مختلفی دارد که اطلاعات پاسخگو را ایمن می‌کند که شامل مقررات حریم خصوصی بانکی و قوانینی است که از سایر گزارش‌های محرمانه محافظت می‌کند. با این حال، پس از افزایش چشمگیر گزارش‌های جرائم دیجیتال، امنیت در این فضا همچنان یکی از نگرانی‌های اصلی مالزی است. همه‌گیری کووید-۱۹ استفاده از فناوری دیجیتال را در مالزی افزایش داده است که منجر به افزایش جرم و افزایش نگرانی‌های امنیتی شده است. همه در معرض خطر هستند، حتی اگر همه بزه‌دیده جرائم دیجیتالی نباشند. رایانه‌ها برای ارتکاب انواع مختلفی از جنایات، ازجمله مواردی که همیشه در مقابل رایانه رخ نمی‌دهند، استفاده می‌شود. به هر روی، افزون بر وضع قوانین و اقدامات مربوطه، دولت همچنین باید روابط چندجانبه با سایر کشورها را برای مقابله با تهدید جرائم دیجیتالی تقویت کند و در هنگام گشت‌وگذار در اینترنت در برابر هرگونه تهدید جرائم دیجیتالی، احساس امنیت و مصونیت به مصرف‌کنندگان بدهد.

فهرست منابع

جلالی، محمود؛ سعیده توسلی اردکانی (۱۳۹۸)، «ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرائم در فضای مجازی»، مطالعات حقوق عمومی، شماره ۴.

کتانچی، الناز؛ بابک پور قهرمانی (۱۳۹۸)، «سیاست‌های نمادین معاهده جرائم سایبری شورای اروپا»، مطالعات بین‌المللی، شماره ۲.

موسوی، سیدجمال؛ محمد روحانی‌مقدم؛ مریم آقائی بجستانی (۱۴۰۱)، «تدابیر پیشگیری از جرائم سایبری با تأکید بر اقدامات پلیسی با رویکردی فقهی»، مطالعات فقه و حقوق اسلامی، شماره ۲۶.

ملکوتی، رسول؛ مونا خلیل‌زاده (۱۴۰۱)، :راهکار حقوقی تأمین امنیت سایبری»، رسانه، شماره ۱.

References

Barrie, Sander (2022), International Law in the Age of Digital Media: Reflections on History, the Neoliberal Communication Sphere, and Race, London Review of International Law, (10)2, 295.

Bidin, A. B, et al. (2015). Intipan Siber: Jenayah Baru dalam Masyarakat Kontemporari. Jurnal Islam dan Masyarakat Kontemporari, 11, 12-25.

Buresh, Donald L (2020), "Does Digital Terrorism Really Exist?", Journal of Advanced Forensic Sciences, 1(1): 18-29.

Cyber Security Malaysia (2020). Cybersecurity Incidents and Trends in Malaysia. Vol. 1. https://www. cybersecurity. my/data/content_files/46/2222. pdf

Chen, W. L, Guo, X. F, et al. (2020). Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem. Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20), Yokohama, 7 January 2021, 4506. https://www. ijcai. org/proceedings/2020/0621. pdf

Ismail, A. I. (2023, February 24). Love Scam sasar mangsa kesunyian. Sinar Harian. https://www. sinarharian. com. my/article/246957/berita/semasa/love-scam-sasar-mangs a-kesunyian

Farhana (2016, April 1). Cyberbullying. PORTAL MyHEALTH. http://www. myhealth. gov. my/en/cyberbullying-2/

Odhiambo, N. A, Ochara, N. M, and Kadymatimba, A. (2018), "Structuring of the Terrorism Problem in the Digital Age: a Systems Perspective", in: 2018 Open Innovations Conference, OI 2018 (Johannesburg: IEEE), pp. 148-154.

Jahankhani, H, Al-Nemrat, A, & Hosseinian-Far, A. (2014). Cybercrime Classification and Characteristics. In: B. Akhgar, A. Staniforth, & F. Bosco, Eds, Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164), Syngress.

Dupont B, Holt T (2022) The human factor of cybercrime. Soc Sci Comput Rev 40(4):860–864.

Jayabalan, P, Ibrahim, R, & Abdul Manaf, A. (2014). Understanding Cybercrime in Malaysia: An Overview. Sains Humanika, 2, 109-115.

Khan, I. (2012). An introduction to computer viruses: problems and solutions. Library Hi Tech News, 29 (7): 8 – 12.

Plotnek, Jordan J and Jill Slay (2021), "Cyber Terrorism: A Homogenized Taxonomy and Definition", Computers & Security, 102: 102-145.

McAfee (2021) McAfee and the Center for Strategic and International Studies (CSIS). The Hidden Costs of Cybercrime. https://www. csis. org/analysis/hidden-costs-cybercrime

Mohamed, D. (2012). Investigating Cybercrimes Under the Malaysian Cyberlaws and the Criminal Procedure Code: Issues and Challenges. Malaysian Law Journal, 6: 1–10.

Prasad, J. Ibrahim, R. and Abdul Manaf, F (2014), Understanding Cybercrime in Malaysia: An Overview. Sains Humanika. 2(2), 109-115.

Paraschiv, D, Toade, L, et al. (2021). Internet Fraud and Phishing Attacks—A European Perspective. 7th BASIQ International Conference on New Trends in Sustainable Business and Consumption, Foggia, 3-5 June 2021, 394-400.

Redzuan Mohamad, Ahmad, et al. (2024), The Efficacy of the Malaysian Government's Response towards Cybercrime, Open Journal of Political Science, 14, 166-176.

Whitty, M. T. and Buchanan, T. (2012). The Online Romance Scam: A Serious Cybercrime. Cyberpsychology, Behavior, and Social Networking, 15, 181-183.

Ren Kok, Raphael Chi (2020), Suppressing Fake News or Chilling Free Speech Are the Regulatory Regimes of Malaysia and Singapore Compatible With International Law, Journal of Malaysian and Comparative Law, 47(1): 25-69.

Sidi Ahmed, Sidi Mohamed (2019), Identity Crime in the Digital Age: Malaysian and Mauritanian Legal Frameworks. International Journal of Law, Government, and Communication, 4(15): 154-165.

Selamat, A, Nguyen, N. T, & Haron, H. (2013). Intelligent Information and Database Systems (Vol. 7802). Springer Publishing.

Srivastava, Vishal (2023), Law Relating to Cyber Crimes: International Perspective, International Journal of Innovative Research in Engineering and Managemen, 10(3): 193-198.

Sukumaran, Sajanee, Yuh Herng Chin, Rizal Rahman, Ammar Abbas Kadhim (2023), Jurisprudence Concerning 'Fake News' and Related Concepts in Malaysia, International Geopolitical Quarterly, 19: 79-99,

Taylor, Robert W, Eric J. Fritsch, John Liederbach (2014), Digital Crime and Digital Terrorism, Prentice Hall Press.

Syamsiar Binti Muharram, Sitti, et al. (2022), cybercrimes in malaysia, Journal of Education and Social Sciences, (22)1: 34-38.

Zakon, R. H. (2003). Hobbes' Internet Timeline: The Definitive ARPAnet & Internet History. https://www. zakon. org/robert/internet/timeline/