فصلنامه علمی
سیاست پژوهی تحول در علوم انسانی

سیاست جنایی تقنینی ایران، ترکیه و مالزی در قبال جرایم سایبری ناقض کیان خانواده

مرضیه عیوضی[۱]، مهدی خاقانی‌اصفهانی[۲]، منصوره زارعان[۳]، معصومه زارعی[۴]

۱۵
دوره ٤، شماره ۳، پیاپی ۱۵
پاییز ۱٤۰٤
مقاله پژوهشی
تاریخ دریافت:
۱٤۰٤-۰۱-۲۵
تاریخ پذیرش:
۱٤۰٤-۰۹-۱۷
صص: ۳۰-۱
شاپا چاپی: ۵۵۹۹-۲۳۲۲
رتبه علمی
ب
بررسی صحت گواهی در :
JOURNALS.MSRT.IR

چکیده

تحولات شـــتابان فناوری‌های اطلاعات و ارتباطات، در کنار فرصـــت‌های نوین ارتباطی، زمینه بروز گونه‌های نوینی از جرایم سایبری شده‌اند که امنیت حریم خصو صی و کارکردهای بنیادین نهاد خانواده را با چالش مواجه کرده است. هدف این پژوهش تحلیل تطبیقی سیاست کیفری ایران، ترکیه و مالزی در پیشگیری و واکنش به جرایم سایبری مخل کیان خانواده و ارزیابی میزان بازدارندگی و کار آمدی این سیا ست‌ها ست. اهمیت پژوهش در آن است که خانواده، به‌عنوان رکن اجتماعی و فرهنگی جوامع اسلامی، در فضای سایبری با تهدیدهایی مواجه شـده که پاسـخ‌های صـرفاً کیفری یا کنترلی برای مواجهه با آن‌ها کفایت نمی‌کند. روش تحقیق تو صیفی–تحلیلی و مبتنی بر مطالعه ا سنادی قوانین، ا سناد ر سمی و گزارش‌های نهادی و منابع علمی معتبر است. یافته‌ها نشان می‌دهد که سیاست‌های کیفری ایران بیشتر ماهیت کنترل محور و امنیت مدار دارد و حمایت نهادی و اجتماعی از بزه‌دیدگان خانوادگی در آن محدود اســـت. ترکیه با بهره‌گیری از تنظیم‌گری پلتفرمی، واکنش قضـــایی ســـریع و همکاری‌های بین‌المللی، از کارآمدی بیشـــتری در مرحله مداخله اولیه برخوردار اســـت، هرچند با چالش‌هایی در حوزه آزادی بیان مواجه اســـت. مالزی با اتخاذ رویکردی تلفیقی و حمایت‌محور، از طریق پیوند میان جرم‌انگاری، نهادهای حمایتی، آموزش اجتماعی و همکاری‌های منطقه‌ای، الگوی متوازن‌تری در حمایت از خانواده دیجیتال ارائه می‌دهد. نتایج کلی پژوهش نشـــان می‌دهد که گذار از ســـیاســـت کیفری صـــرفاً مجازات محور به ســـیاســـتی خانواده‌محور و حمایت‌مدار، شـــرط اســـاســـی ارتقای بازدارندگی و اعتماد اجتماعی در مواجهه با جرایم سایبری خانوادگی است.

کلیدواژه‌ها:

سیاست کیفری، خانواده، جرایم سایبری، حقوق تطبیقی، حمایت از بزه‌دیدگان، تحول، علوم انسانی

۱ . دانشجوی دکتری مطالعات زنان، گرایش حقوق زن در اسلام، دانشگاه ادیان و مذاهب، قم، ایران
(نویسنده مسئول) meyvazi1349@gmail.com
۲ . استادیار، حقوق جزا و جرم‌شناسی پژوهشکده تحقیق و توسعه علوم انسانی (سمت)، تهران، ایران.
۳ . دانشیار، گروه مطالعات علوم اجتماعی و جمعیت، پژوهشکده زنان دانشگاه الزهراء، تهران، ایران.
۴. استادیار گروه روان‌شناسی و مطالعات خانواده، دانشگاه کوثر بجنورد، بجنورد، ایران.

مقدمه و بیان مسأله

در دهه‌های اخیر، تحولات فناورانه و ظهور «جامعه شبکه‌ای» (کاستلز، ۱۳۹۶: ۲۹) به تعبیر مانوئل کاستلز، ساختار سنتی خانواده را در معرض چالش‌های پیچیده‌ای قرار داده است. گسترش فناوری‌های دیجیتال، شبکه‌های اجتماعی و فضای سایبر، ضمن ایجاد فرصت‌های جدید ارتباطی، بسترهای نوینی از جرم، انحراف و خشونت را نیز فراهم ساخته است که مستقیماً «کیان خانواده» را به‌عنوان یکی از بنیادی‌ترین نهادهای اجتماعی و حقوقی تهدید می‌کند. در این میان، مفهوم «جرایم سایبری علیه خانواده» شامل مجموعه‌ای از کنش‌های مجرمانه نظیر بهره‌کشی جنسی آنلاین از کودکان، باج‌گیری اینترنتی، افشای تصاویر خصوصی، خیانت دیجیتال، خشونت روانی مجازی و استثمار عاطفی از طریق رسانه‌های ارتباطی است که به حقوق بنیادین خانواده از جمله حق بر صیانت حیثیت، حق بر امنیت روانی، حق بر حریم خصوصی، حق بر تربیت سالم فرزندان و حق بر کرامت زن آسیب می‌رساند. (معصومی، گودرزی، ۱۴۰۰: ۴).

جرایم سایبری علیه خانواده، صرفاً امتداد الکترونیکی جرایم سنتی نیستند، بلکه به دلیل ویژگی‌هایی همچون فرامکانی بودن، گمنامی مرتکب، سرعت انتشار محتوا و ماندگاری آثار دیجیتال، الگوهای جدیدی از بزهکاری و بزه‌دیدگی خانوادگی را شکل داده‌اند که واکنش‌های کیفری کلاسیک توان پاسخ‌گویی مؤثر به آن‌ها را ندارند.(Weulen Kranenbarg, et al, 2018:347)

جرایم سایبری پدیده‌ای منحصر به فرد در عصر دیجیتال به شمار می‌روند که پاسخ به آن‌ها نیازمند رویکردی دقیق، علمی و نوآورانه است. ویژگی‌های خاص فضای سایبری ایجاب می‌کند تا قانون‌گذار با نگاهی به‌روز و همه‌جانبه، نسبت به اتخاذ تدابیر کیفری و غیرکیفری برای پیشگیری و مقابله با این جرایم اقدام نماید. به‌ویژه با توجه به شیوه‌های نوین ارتکاب جرم از طریق فناوری‌هایی مانند متاورس و هوش مصنوعی، لازم است راهبردها و سیاست‌های کیفری با بهره‌گیری از علوم میان‌رشته‌ای نظیر جرم‌شناسی، روان‌شناسی، فناوری اطلاعات و سیاست‌گذاری کیفری به‌روزرسانی شود.(Efremova, Russkevich,2025)

در حوزه خانواده، جرایم سایبری می‌توانند پیامدهای مخرب و ماندگاری بر روابط اعضا و امنیت روانی خانواده‌ها بر جا گذارند. بنابراین حمایت قانون‌گذار در شناسایی این معضلات و ارائه راهکارهای مؤثر، نقشی اساسی در حفظ انسجام خانواده و پیشگیری از آسیب‌های ناشی از فضای مجازی دارد. از دهه ۷۰ میلادی تاکنون، بسیاری از دولت‌ها و سازمان‌های بین‌المللی با هدف حمایت از نهاد خانواده، اقدام به تدوین قوانین خاص برای پیشگیری از جرایم کرده‌اند که این روند، گامی مهم در جهت حمایت کیفری از بنیان خانواده محسوب می‌شود. (خاقانی و رایجیان اصلی، ۱۴۰۰: ۵).

جرایم سایبری به جهت خسارت‌های گسترده، تحقق آسان، تعدد جرم، تحقق در مکان‌های مختلف و ایجاد دشواری در کشف، تعقیب و جمع‌آوری ادله، مستحق نگاه سخت‌گیرانه قضایی هستند (میرعربی، ۱۳۹۸: ۱۴). بررسی کیفیت و کارآمدی

این قوانین، تحلیل سیاست‌های تقنینی و پیش‌بینی تدابیر پیشگیرانه غیرکیفری، همراه با آموزش و آگاهی‌بخشی عمومی، ضرورتی انکارناپذیر است.

با وجود این، مسئله اساسی آن است که آیا سیاست کیفری ایران در حوزه جرایم سایبری علیه خانواده، از کارآمدی لازم برای حمایت مؤثر از امنیت اخلاقی، روانی و حیثیتی خانواده برخوردار است یا خیر، و در مقایسه با برخی کشورهای اسلامی و آسیایی، در چه جایگاهی قرار می‌گیرد.

بدین منظور، در این مقاله جلوه‌های عینی نارسایی‌های حقوق کیفری ایران در حمایت از کیان خانواده در برابر جرایم سایبری، مورد نقد و تحلیل قرار می‌گیرد و دستاوردهای قابل اقتباس کشورهای منتخب بررسی می شود. کشور ترکیه به دلیل قرابت فرهنگی و دینی و جایگاه فناورانه و حقوقی در منطقه غرب آسیا (لطیفی، ۱۳۹۸: ۶) و کشور مالزی به‌عنوان الگویی موفق در میان کشورهای مسلمان در حال توسعه با ساختار حقوقی تلفیقی و سیاست‌های حمایتی فعال در حوزه خانواده دیجیتال (قنبری باغستانی، ۱۳۹۸: ۵)، به‌عنوان نمونه‌های تطبیقی انتخاب شده‌اند.

در این چارچوب، پژوهش حاضر در پی پاسخ به این پرسش اصلی است که سیاست جنایی تقنینی ایران، ترکیه و مالزی در قبال «جرایم سایبری ناقض کیان خانواده» از حیث سه ضلعِ مدل «مثلث حکمرانی سایبری خانوادگی (ضلع قانونی–نهادی، ضلع حمایتی–اجتماعی، ضلع پیشگیرانه–توانمندساز) چه تفاوت‌ها و شباهت‌هایی دارد و هر نظام حقوقی در کدام الگوی مسلط (کنترل‌محور، تنظیمی–حقوق‌محور، حمایت‌محور–اجتماعی) قابل طبقه‌بندی است؟ همچنین دومین پرسش این مقاله تفاوت‌های تقنینی و نهادی در سه کشور تا چه حد بر بازدارندگی عملی (قطعیت اجرا، سرعت مداخله، دسترسی بزه‌دیدگان به حمایت، و قابلیت تعقیب فراملی/ادله‌یابی دیجیتال) اثر می‌گذارد و کدام ترکیب از ابزارها می‌تواند به کاهش بزه‌دیدگی پنهان، کاهش بزه‌دیدگی ثانویه و افزایش اعتماد اجتماعی در جرایم سایبری خانوادگی منجر شود؟

فرضیه اصلی این پژوهش این است که سیاست جنایی تقنینی ایران در مواجهه با جرایم سایبری ناقض کیان خانواده، غالباً کنترل‌محور و مجازات‌گرایانه است و به‌دلیل فقدان مفهوم‌پردازی مستقل از «کیان خانواده دیجیتال»، ضعف پیوند میان نهادهای قضایی–اجتماعی، و کم‌رنگ بودن پیشگیری و توانمند سازی، در مقایسه با ترکیه و به‌ویژه مالزی، از کارآمدی و بازدارندگی عملی پایین‌تری برخوردار است. وانگهی، فرضیه دوم مقاله این است که نظام‌های حقوقی‌ای که میان جرم‌انگاری هدفمند، و تنظیم‌گری پلتفرمی و حمایت نهادی از بزه‌دیدگان و آموزش/سواد دیجیتال و والدگری دیجیتال و همکاری‌های منطقه‌ای/بین‌المللی توازن ایجاد می‌کنند، نسبت به نظام‌های صرفاً کیفرمدار یا کنترل‌مدار، بازدارندگی مؤثرتر، نرخ گزارش‌دهی بالاتر، بزه‌دیدگی ثانویه کمتر و اعتماد اجتماعی بیشتر در مواجهه با جرایم سایبری خانوادگی خواهند داشت.

نوآوری این پژوهش در سه سطح قابل صورت‌بندی است: نخست، تعریف مسئله «جرایم سایبری ناقض کیان خانواده» به‌عنوان یک مقوله مستقل سیاست‌گذاری جنایی (نه صرفاً امتداد جرایم حیثیتی/عفت عمومی یا نقض حریم خصوصی) و انتقال کانون تحلیل از فرد به «خانواده به مثابه واحد اجتماعی». دوم، ارائه و به‌کاربست مدل تحلیلی بومی‌سازی‌شده «مثلث حکمرانی سایبری خانوادگی «برای سنجش نظام‌مند کارآمدی سیاست‌های تقنینی در سه ضلع قانونی–نهادی، حمایتی–اجتماعی و پیشگیرانه–توانمندساز، به‌گونه‌ای که امکان مقایسه ساختاری و نه صرفاً توصیفی فراهم شود. سوم، تولید نتیجه سیاستیِ قابل اقتباس از مقایسه سه الگو (کنترل‌محور ایران، تنظیمی–حقوق‌محور ترکیه، حمایت‌محور–اجتماعی مالزی) نشان می‌دهد ارتقای بازدارندگی در جرایم سایبری خانوادگی، بیش از تشدید کیفر، به ترکیب هوشمند جرم‌انگاری با حمایت نهادی، مداخله زودهنگام، آموزش خانواده‌محور و حکمرانی شبکه‌ای با مشارکت پلتفرم‌ها و جامعه مدنی وابسته است.

۱. چارچوب نظری و مدل تحلیلی پژوهش

تبیین جرایم سایبری علیه خانواده و ارزیابی پاسخ‌های تقنینی به آن، مستلزم عبور از تحلیل تک‌بعدی حقوقی و اتخاذ رهیافتی میان‌رشته‌ای است. این پژوهش با ادغام سه رهیافت کلان جرم‌شناسی، جامعه‌شناسی و حقوق کیفری، چارچوبی نظری می‌سازد که هم به علل ساختاری این جرایم و هم به معیارهای ارزیابی پاسخ‌های دولتی می‌پردازد.

۱-۱. مبانی نظری: یک تلفیق سه‌لایه‌ای

الف) لایه علت‌شناختی: نظریه بی‌سازمانی اجتماعی و شکاف دیجیتال در خانواده

در سطح کلان، نظریه بی‌سازمانی اجتماعی شاو و مک‌کی (Shaw & McKay, 1942) توضیح می‌دهد که چگونه ضعف پیوندهای اجتماعی همسایگی و محلی به افزایش جرم می‌انجامد. در عصر دیجیتال، این مفهوم به درون خانواده تسری می‌یابد و به شکل «بی‌سازمانی دیجیتال خانوادگی» ظهور می‌کند. شکاف نسلی در سواد دیجیتال، غیبت والدین از فضای برخط فرزندان، و فقدان قواعد مشترک اخلاقی در استفاده از فناوری، همگی نشانگر تضعیف «کنترل اجتماعی غیررسمی» درون خانواده هستند که مطابق نظریه تراویس هرشی (Hirschi, 1969, pp. 25–27)، مهم‌ترین مانع رفتار انحرافی است. این خلأ کنترل، خانواده را در برابر تهدیدات خارجی و داخلی (مانند بهره‌کشی توسط غریبه‌ها یا خشونت بین اعضا) آسیب‌پذیر می‌سازد.

ب) لایه پاسخ‌شناختی: از بزه‌دیده‌شناسی انتقادی تا حکمرانی شبکه‌ای

در سطح واکنش، دو مکتب فکری راهنمای تحلیل هستند. نخست، بزه‌دیده‌شناسی انتقادی(Walklate, 1989:34-36) استدلال می‌کند که سیستم‌های عدالت کیفری سنتی، با بی‌اعتنایی به نیازهای عاطفی و روانی قربانی و متمرکز شدن بر مجازات مجرم، خود می‌توانند منجر به «بزه‌دیدگی ثانویه» شوند. این دیدگاه برای تحلیل سیاست‌هایی حیاتی است که صرفاً

بر تعقیب و مجازات تأکید دارند. دوم، نظریه حکمرانی شبکه‌ای(Rhodes, 1997) در تو ضیح پا سخ به جرایم سایبری کاربرد دارد. این نظریه نشـــان می‌دهد که حکمرانی مؤثر در جهان پیچیده امروز، نه از عهده دولت به تنهایی، بلکه از طریق شبکه‌ای از کنشگران (دولت، پلتفرم‌های خصوصی، نهادهای مدنی، خانواده‌ها) ممکن است. موفقیت سیاست جنایی در گرو توانایی هماهنگی و تقسیم مسئولیت در چنین شبکه‌ای است.

ج) لایه حقوقی–سیاستی: پیوستار سیاست جنایی از کنترل تا توانمندسازی

در سطح سیا ست‌گذاری، می‌توان پا سخ‌های دولتی را بر روی یک پیو ستار از تمرکز بر دولت تا تمرکز بر جامعه قرار داد. در یک سر این پیو ستار، الگوی سیا ست جنایی کنترلی قرار دارد که بر حاکمیت مطلق دولت، جرم‌انگاری گ سترده، نظارت و فیلترینگ تأکید دارد. در سوی دیگر، الگوی سیاست جنایی توانمندساز واقع شده است که اولویت را بر حمایت از بزه‌دیدگان، آموزش ســـواد دیجیتال به شـــهروندان، تنظیم‌گری هوشـــمند پلتفرم‌ها و تقویت ســـرمایه اجتماعی خانواده می گذارد. یک موقعیت میانی نیز تحت عنوان الگوی تنظیمی–حقوقی قابل تصـــور اســـت که در آن دو لت از طریق چارچوب‌های حقوقی شـــفاف (مانند قوانین حفاظت از داده) به تنظیم فضـــای مجازی می‌پردازد، بی آنکه لزوماً بر حمایت اجتماعی مستقیم تأکید کند.

مدل تحلیلی یکپارچه پژوهش بر اساس تلفیق سه‌لایه نظری فوق، با عنوان «مثلث حکمرانی سایبری خانوادگی» پیشنهاد می‌دهد. کارآمدی سیاست جنایی هر کشور در حمایت از کیان خانواده، تابعی از تعادل و قدرت سه ضلع این مثلث است:

(الف) ضلع قانونی–نهادی

سنجه‌ها: دقت و جامعیت جرم‌انگاری، وجود نهادهای تخصصی (پلیس سایبر خانواده‌محور، دادگاه‌های ویژه)، شفافیت رویه‌های قضایی، سرعت دسترسی به عدالت.

نظریه پشتیبان: حقوق کیفری و نظریه حکمرانی شبکه‌ای (تمرکز بر نقش دولت و قانون).

(ب) ضلع حمایتی–اجتماعی

ســـنجه ها: وجود خد مات مشـــاوره و بحران مداخلی برای بزه‌د ید گان، هم‌کاری بین‌نهادی (پلیس، بهزیســـتی، آموزش‌وپرورش)، مکانیسم‌های جبران خسارت، تلاش برای کاهش انگ اجتماعی.

نظریه پشتیبان: بزه‌دیده‌شناسی انتقادی و نظریه حکمرانی شبکه‌ای (تمرکز بر نقش نهادهای مدنی و حمایتی).

(ج) ضـلع پیشـگیرانه–توانمندسـاز سـنجه‌ها: گسـتردگی برنامه‌های آموزش سـواد دیجیتال و رسـانه‌ای برای والدین و کودکان، ترویج «والدگری دیجیتال»، شفاف‌سازی و مسئولیت‌پذیری پلتفرم‌ها.

نظریه پشتیبان: نظریه کنترل اجتماعی و نظریه حکمرانی شبکه‌ای (تمرکز بر نقش خانواده و بخش خصوصی).

فرض مدل: سیاست جنایی بهینه (کارآمد) سیاستی است که تعادل پویایی میان این سه ضلع برقرار کند. تأکید افراطی بر یک ضلع (مثلاً فقط ضلع قانونی، منجر به کنترل‌محوری خالص) یا ضعف شدید در یک ضلع (مثلاً ضعف در ضلع حمایتی)، کارآمدی کل نظام را کاهش می‌دهد.

۲-۱.کاربست مدل در پژوهش تطبیقی

در بخش‌های بعدی، سیاست جنایی تقنینی هر یک از سه کشور ایران، ترکیه و مالزی با استفاده از مدل و سنجه‌های سه‌گانه آن تحلیل خواهد شد. این تحلیل به ما اجازه می‌دهد نه تنها کشورها را در قالب الگوهای کلی (کنترلی، تنظیمی، حمایتی) طبقه‌بندی کنیم، بلکه درجات مختلف تعادل یا عدم تعادل در سیستم هر کشور و تأثیر آن بر کارآمدی را به صورت عینی‌تر نشان دهیم. این رویکرد، فراتر از یک توصیف ساده، به یک ارزیابی ساختاریافته از نظام‌های حقوقی می‌پردازد.

۲. پیشینه پژوهش

پژوهش درباره جرایم سایبری هم‌زمان با گسترش فناوری‌های اطلاعات و ارتباطات از دهه ۱۹۹۰ میلادی در ادبیات حقوقی و جرم‌شناختی شکل گرفت. مطالعات اولیه عمدتاً ناظر بر ابعاد فنی و امنیتی فضای مجازی بودند، اما به‌تدریج با آشکار شدن پیامدهای اجتماعی و فرهنگی این فضا، توجه پژوهشگران به آثار آن بر نهادهای اجتماعی، از جمله خانواده، معطوف شد. در سطح بین‌المللی، اسناد و گزارش‌های نهادهایی مانند سازمان ملل متحد، سازمان توسعه و همکاری اقتصادی و انجمن بین‌الملل حقوق جزا، بر ضرورت پاسخ‌های تقنینی نوین و هماهنگ در برابر جرایم سایبری تأکید داشته‌اند؛ امری که در نهایت به تدوین کنوانسیون بوداپست (۲۰۰۱) و اسناد تکمیلی در حوزه حمایت از کودکان و خانواده انجامید.

در حوزه مطالعات تطبیقی، پژوهش‌های متعددی به بررسی سیاست‌های کیفری دولت‌ها در قبال جرایم سایبری پرداخته‌اند، اما تمرکز این مطالعات غالباً بر امنیت اطلاعات، جرایم اقتصادی یا آزادی‌های دیجیتال بوده و خانواده به‌عنوان بزه‌دیده اصلی، کمتر به‌صورت مستقل و نظام‌مند مورد توجه قرار گرفته است. در این میان، برخی تحقیقات خارجی به افزایش آزار جنسی آنلاین کودکان، طعمه‌گذاری اینترنتی و تأثیر خرده‌فرهنگ‌های برخط بر روابط خانوادگی اشاره کرده‌اند، بی‌آنکه تحلیل جامعی از واکنش‌های تقنینی در نظام‌های حقوقی مختلف ارائه دهند.

در ایران، مطالعات انجام شده درباره جرایم سایبری عمدتاً ماهیتی کلی داشته و بر موضوعاتی چون هرزه‌نگاری، نقض حریم خصوصی، جرایم علیه عفت عمومی و چالش‌های قانون جرایم رایانه‌ای متمرکز بوده‌اند. مرور ادبیات داخلی نشان می‌دهد پژوهش‌هایی از جمله آثار عبدالمناب (۱۳۹۰)، نگهی (۱۳۹۱)، صبح‌خیز (۱۳۹۴)، بخارایی و کریمی (۱۳۹۵)، تقی‌پور و زرینه (۱۳۹۶)، فرجی‌ها و علمداری (۱۳۹۶)، سوریان (۱۳۹۷)، شفیعی سرو ستانی و علوی (۱۳۹۷)، گرگین و

باقری (۱۳۹۹)، خلیل‌پور چالکیا سری (۱۳۹۹) و احمدی‌مقدم و همکاران (۱۴۰۰)، به ضعف قانون‌گذاری در حوزه جرایم سایبری، ابهام در مفاهیم کلیدی نظیر «مستهجن» و «مبتذل»، فقدان تفکیک میان اطفال و بزرگسالان در جرایم جنسی و ناکارآمدی سیاست‌های پیشگیرانه اشاره کرده‌اند. با این حال، این مطالعات غالباً به خانواده به‌عنوان یک کل اجتماعی توجه مستقلی نداشته و تحلیل سیاست جنایی در این حوزه را به‌صورت پراکنده و غیرتطبیقی دنبال کرده‌اند.

در خصوص کشورهای ترکیه و مالزی نیز، بیشتر نوشته‌های موجود بر تحولات تقنینی، ساختارهای تنظیم‌گری فضای مجازی و نسبت این سیاست‌ها با آزادی‌های دیجیتال تمرکز دارند. در ترکیه، مطالعات عمدتاً قانون اینترنت شماره ۵۶۵۱ و پیامدهای آن را بررسی کرده‌اند و در مالزی، پژوهش‌ها بیشتر ناظر بر سیاست‌های کلان امنیت سایبری و نقش نهادهای اجرایی بوده است. با این حال، بررسی تطبیقی این دو نظام حقوقی با ایران، آن هم از منظر حمایت از کیان خانواده در برابر جرایم سایبری، کمتر مورد توجه پژوهشگران قرار گرفته است.

جمع‌بندی پیشینه پژوهش نشان می‌دهد که علی‌رغم گسترش مطالعات درباره جرایم سایبری، خلأ جدی در زمینه تحلیل تطبیقی سیاست جنایی تقنینی در قبال جرایم سایبری ناقض کیان خانواده وجود دارد.

۳. روش پژوهش

این پژوهش از نظر هدف کاربردی و از نظر طرح تحقیق، یک مطالعه توصیفی-تحلیلی با رویکرد تطبیقی است. طرح توصیفی-تحلیلی به این معناست که در مرحله نخست، سیاست‌های تقنینی هر کشور به صورت نظام‌مند توصیف می‌شود و در مرحله بعد، این توصیف‌ها در قالب یک تحلیل مقایسه‌ای، مورد تبیین و تفسیر قرار می‌گیرند تا الگوهای حاکم و عوامل مؤثر استخراج شوند.

روش گردآوری داده‌ها در این پژوهش، مطالعه اسنادی است. داده‌های مورد نیاز از طریق بررسی عمیق و انتقادی منابع زیر گردآوری شدند: متون قانونی اولیه(قوانین مصوب، آیین‌نامه‌ها و تصویب‌نامه‌های رسمی)؛ اسناد سیاستی و گزارش‌های رسمی(استراتژی‌های کلان، گزارش‌های عملکرد نهادهای مسئول، و اسناد منتشر شده توسط مراجع نظارتی)؛ منابع ثانویه معتبر: مقالات علمی منتشرشده در مجلات معتبر، کتب تخصصی و گزارش‌های تحلیلی نهادهای بین‌المللی (مانند یونیسف، شورای اروپا، آسه‌آن).

ابزار اصلی گردآوری داده، فیش‌برداری نظام‌مند بر اساس یک برگه کدگذاری اولیه بود که محورهای کلیدی تحقیق (مانند مفاد قانونی، نهادهای اجرایی، سازوکارهای حمایتی) را پوشش می‌داد.

جامعه آماری، نمونه‌گیری و واحد تحلیل کلیه اسناد و متون مرتبط با سیاست جنایی تقنینی در حوزه جرایم سایبری علیه خانواده در سه کشور ایران، ترکیه و مالزی و از روش نمونه‌گیری هدفمند معیارمحور استفاده شد. معیارهای انتخاب

ا سناد عبارت بودند از: ۱) ارتباط م ستقیم با مو ضوع تحقیق، ۲) اعتبار منبع (ر سمی بودن یا انت شار در مجلات معتبر)، ۳) جدید بودن اسناد.

واحد تحلیل سیاست جنایی تقنینی هر کشور به عنوان یک کل واحد در نظر گرفته شد. سپس برای توصیف هر واحد، خرده واحدهایی مانند «قوانین»، «ساختار نهادی» و «برنامه‌های حمایتی» مورد تحلیل قرار گرفتند.

تحلیل داده‌ها در دو مرحله اصلی و منطبق بر طرح «توصیفی-تحلیلی» انجام پذیرفت:

مرحله اول: تو صیف نظام‌مند در این مرحله، داده‌های گردآوری شده از هر ک شور، در چارچوب مقوله‌های تو صیفی از پیش تعیین‌شده سازماندهی شدند. این مقوله‌ها که از اهداف تحقیق و سؤالات فرعی استخراج شده بودند، عبارتند از:

۱ .دامنه و محتوای جرم‌انگاری‌ها

۲ .ساختار و صلاحیت نهادهای مسئول

۳ .سازوکارهای حمایت از بزه‌دیدگان

۴ .برنامه‌های پیشگیری و آموزش عمومی

خروجی این مرحله، ارائه یک توصیف منسجم و قابل اعتماد از وضعیت هر کشور بود.

مرحله دوم: تحلیل تطبیقی و تبیینی در این مرحله، توصیف‌های به‌دست‌آمده از سه کشور وارد فرآیند تحلیل مقایسه‌ای کیفی شدند. این تحلیل بر اساس روش تطبیق کارکردی انجام شد. بدین صورت که نهادها و قوانین کشورها نه بر اساس شباهت ظاهری، بلکه بر ا ساس کارکرد اجتماعی آنها (یعنی «حمایت از کیان خانواده») با یکدیگر سنجیده شدند .در این مرحله از چارچوب نظری پژوهش (بخش ۲) برای تبیین علل تفاوت‌ها و ارزیابی کارآمدی نسبی الگوها استفاده شد. خروجی این مرحله، استخراج الگو های مسلط (کنترل‌محور، تنظیمی، حمایت‌محور) و ارائه تحلیل تبیینی از دلا یل شکل‌گیری این الگوها و نتایج آنها بود.

برای افزایش اعتبار (صحت) درونی یافته‌های توصیفی، از مثلث‌سازی منابع داده استفاده شد؛ بدین معنا که اطلاعات هر کشور از طریق چندین سند (قانون، گزارش، مقاله) برر سی و بازبینی گردید. برای افزایش پایایی (ثبات فرآیند)، چارچوب مقوله‌بندی و معیارهای تحلیل به وضوح تعریف و در تمام مراحل رعایت شد.

۴. حمایت از کیان خانواده در قبال جرایم سایبری: مبانی بین‌المللی و جرم‌شناختی-جامعه‌شناختی

خانواده در ا سناد بنیادین بین‌المللی حقوق ب شر، به‌عنوان واحد طبیعی و ا سا سی جامعه شناخته شده ا ست. ماده ۱۶ اعلامیه جهانی حقوق بشر (۱۹۴۸)، ماده ۲۳ میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) و ماده ۱۰ اعلامیه حقوق بشر ا سلامی (قاهره، ۱۹۹۰) بر ضرورت حمایت دولت‌ها از نهاد خانواده تأکید دارند. این رویکرد در ا سناد و قوانین ا سا سی کشورهای مورد مطالعه نیز بازتاب یافته ا ست؛ به‌گونه‌ای که ا صل دهم قانون ا سا سی ایران، ماده ۴۱ قانون ا سا سی ترکیه و

اصل ۱۲ قانون اساسی فدرال مالزی، خانواده را موضوع حمایت ویژه قانونی دانسته‌اند. بر این اساس، تهدیدهای ناشی از فضای سایبر علیه خانواده را می‌توان در زمره نقض حقوق بنیادین و تعهدات حمایتی دولت‌ها تحلیل کرد.

در حقوق کیفری معاصر، حمایت از خانواده در برابر جرایم سایبری صرفاً به واکنش کیفری محدود نمی‌شود، بلکه در چارچوب سیاست‌های پیشگیرانه نیز مورد توجه قرار می‌گیرد. نظریه‌های پیشگیری اجتماعی، به‌ویژه الگوی سه سطحی پیشگیری، بر مداخلات اولیه (آموزش و آگاهی‌بخشی)، ثانویه (حمایت از گروه‌های در معرض خطر) و ثالثیه (حمایت از بزه‌دیدگان و بازپروری) تأکید دارند. (رایجیان اصلی، ۱۳۸۳: ۱۴۹) در همین راستا، بسیاری از کشورها با ایجاد سازوکارهای نهادی چندلایه، از جمله واحدهای تخصصی پلیس، برنامه‌های آموزشی خانواده‌محور و همکاری‌های فراملی، تلاش کرده‌اند به جرایم سایبری ناقض کیان خانواده پاسخ دهند.

از منظر جامعه‌شناسی حقوق، تفاوت سیاست‌های جنایی کشورها را می‌توان در چارچوب نظم هنجاری تحلیل کرد. به تعبیر دورکیم، کارآمدی نظم حقوقی در گرو هماهنگی آن با ارزش‌های اخلاقی مسلط در جامعه است (Durkheim, 1957: 7). در این چارچوب، نظام‌هایی که میان قواعد حقوقی، آموزش اجتماعی و هنجارهای فرهنگی پیوند برقرار کرده‌اند، در مدیریت آسیب‌های اجتماعی فضای مجازی موفق‌تر ارزیابی می‌شوند. بررسی تطبیقی نشان می‌دهد که برخی کشورها، به‌ویژه در جنوب شرق آسیا، بیش از تمرکز صرف بر کنترل کیفری، به آموزش و تقویت تاب‌آوری اجتماعی خانواده‌ها توجه داشته‌اند.(UNICEF Malaysia,2025)

در نظام حقوقی ایران، مبانی فقهی نقش مهمی در تعریف سیاست‌های حمایتی از خانواده ایفا می‌کند. اصولی همچون کرامت انسانی، صیانت از عفت عمومی و حفظ بنیان خانواده، که در آیات قرآن و فقه اسلامی مورد تأکید قرار گرفته‌اند، مبنای جرم‌انگاری و مداخله دولت در برابر رفتارهای تهدیدکننده خانواده محسوب می‌شوند (منیری، ۱۳۹۷). این مبانی، در کنار ملاحظات حقوقی و اجتماعی، چارچوبی ارزشی برای سیاست جنایی در فضای سایبر فراهم می‌آورند.

از منظر جامعه شناسی خانواده و فرهنگ دیجیتال، پژوهش‌ها نشان می‌دهد که سطح سواد دیجیتال و الگوهای تعامل والدین و فرزندان، نقش تعیین‌کننده‌ای در پیشگیری از بزه‌دیدگی سایبری دارد. (Castells, 2000: 22–29) مطالعات تطبیقی حاکی از آن است که رویکردهای مبتنی بر آموزش، گفت‌وگو و اعتماد متقابل، در مقایسه با راهبردهای صرفاً محدودکننده، اثربخشی بیشتری در کاهش آسیب‌های سایبری دارند.(Hirschi, 1969: 26–31) تجربه کشورهایی مانند مالزی نیز نشان می‌دهد که تقویت والدگری دیجیتال و مشارکت فعال خانواده‌ها، می‌تواند به ارتقای امنیت کودکان و نوجوانان در فضای مجازی کمک کند .(Idris & Yusof, 2021: 77؛ ECPAT et al, 2022: 5)

برآیند این مبانی نظری و ا سنادی ن شان می‌دهد که تحلیل سیا ست‌های تقنینی در حوزه جرایم سایبری علیه خانواده، مستلزم توجه هم‌زمان به تعهدات بین‌المللی، زمینه‌های فرهنگی و اجتماعی و رویکردهای جرم‌شناختی است. این چارچوب تحلیلی، مبنای بررسی قوانین و ساختارهای حمایتی ایران، ترکیه و مالزی در بخش‌های بعدی پژوهش قرار می‌گیرد.

۵.چارچوب کلی سیاست جنایی سایبری در نظام حقوقی سه کشور ایران، ترکیه و مالزی

۵-۱. چارچوب کلی سیاست جنایی سایبری در نظام حقوقی ایران

سیا ست جنایی جمهوری ا سلامی ایران در حوزه جرایم سایبری، به‌طور عمده در قالب قانون جرایم رایانه‌ای م صوب ۱۳۸۸ و برخی مقررات پراکنده در قوانین کیفری و آیین دادرسی کیفری تبلور یافته است. این سیاست جنایی در بستر گفتمان حفظ نظم عمومی، صیانت از اخلاق عمومی و حمایت از ارزش‌های بنیادین اجتماعی شکل گرفته و کمتر مبتنی بر یک رویکرد خانواده‌محور یا بزه‌دیده‌مدار است.

در این چارچوب، فضای مجازی عمدتاً به‌مثابه «قلمرو تهدید» تلقی می‌شود و واکنش تقنینی بیشتر بر کنترل، محدود سازی و جرم‌انگاری متمرکز ا ست تا بر توانمند سازی خانواده‌ها و حمایت از قربانیان. این تلقی، به‌طور م ستقیم بر نحوه مواجهه قانون‌گذار با جرایم سایبری ناقض کیان خانواده اثر گذاشته است. قانون جرایم رایانه‌ای به صورت مستقیم از کیان خانواده نام نمی‌برد، اما برخی از مواد آن به طور غیر مستقیم ناظر به حمایت از اعضای خانواده و روابط خانوادگی است. از جمله مهم‌ترین این مواد می توان به جرم‌انگاری دسترسی و شنود غیرمجاز به داده خصوصی (مواد ۱ و ۲)، انتشار محتواهای مستهجن(مواد ۱۴ و ۱۵)، تغییر یا انتشار تصویر و صوت دیگران، تعرض به حریم خصوصی (ماده ۱۶ و ۱۷) و نشر اکاذیب (ماده ۱۸) و نیز جرایم علیه عفت عمومی (مواد ۱۴ و ۱۵) و در کنار آن قوانین سنتیِ کیفری (ماده ۶۴۰ و ۶۴۱ مجازات اسلامی؛ ماده ۷۰۵ و پس از اصلاح شامل قمار در فضای مجازی) و مقررات تجارت الکترونیک برخی ضمانت‌های جزایی اشاره کرد. در مقررات جدید نیز حوزه کودکان و نوجوانان با تصویب «قانون حمایت از کودکان و نوجوانان» (۱۳۹۹) و سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) نیز حمایتهای پیش‌بینی شده است.

با این حال، تحلیل محتوایی این قانون نشان می‌دهد که قانون‌گذار بیشتر بر رفتار مجرمانه فردی تمرکز کرده و پیامدهای اجتماعی و خانوادگی جرم را به‌عنوان یک متغیر مستقل در نظر نگرفته است. به بیان دیگر، اگرچه انتشار تصاویر خصوصی یک فرد ممکن است منجر به فروپاشی خانواده، طلاق یا طرد اجتماعی شود، اما قانون تنها به حیثیت فردی توجه دارد و از کیان خانواده به‌عنوان یک ارزش مستقل حمایت نمی‌کند. این خلأ مفهومی سبب شده است که بسیاری از آسیب‌های سایبری خانوادگی، از جمله آزار آنلاین همسران، تهدیدهای عاطفی در روابط خانوادگی یا فشارهای دیجیتال منجر به خشونت خانگی، در نظام تقنینی ایران فاقد عنوان مجرمانه خاص باشند و ذیل عناوین کلی و پراکنده رسیدگی شوند.

در ایران همچنین برای مبارزه با جرایم سایبری نهاد اجرایی ایجاد شده است مانند نیروی انتظامی- پلیس فضای تولید و تبادل اطلاعات (پلیس «فتا»)[1] و نقش آن کشف، تحقیق و تعقیب مقدماتی جرایم سایبری (هک، کلاهبرداری آنلاین، نفوذ، فیشینگ، جعل دیجیتال و موارد مشابه) و دریافت شکایات مردمی در سطح کشور است. قوه قضائیه - دادستانی کل، دادسراها و «دادسرای ویژه جرایم رایانه‌ای» دادگاه‌های تخصصی نقش نظارت قضایی، تشکیل و ریاست دبیرخانه «کارگروه تعیین مصادیق محتوای مجرمانه»[2]، رسیدگی قضایی به پرونده‌های سایبری و صدور اوامر قضایی (حفظ داده، توقیف، دستورات حمایتی و کیفری) را بر عهده دارند. کارگروه نیز نقش مرجع رسمی تعیین و پالایش «مصادیق محتوای مجرمانه» (فیلترینگ،حذف محتوا) و دریافت و پیگیری شکایات محتوای را بر عهده دارند.

وزارت ارتباطات و سازمان‌های تابعه (از جمله سازمان فناوری اطلاعات ایران) و «مرکز مدیریت امداد و هماهنگی رخدادهای رایانه‌ای) «مرکز ماهر[3] نقش‌ها سیاست‌گذاری، اداره و تنظیم‌گری زیرساخت‌های ارتباطی، مدیریت فنی رخدادهای امنیتی ملی (تشخیص، هشدار و امداد در حملات سایبری)، نگهداری سازوکارهای فنی برای حفظ لاگ‌ها و تعامل با دستگاه‌ها و نهادها را عهده دارند. شورای‌عالی فضای مجازی[4] دبیرخانه یا مرکز ملی فضای مجازی نقش تنظیم راهبرد کلان فضای مجازی، تعیین سیاست‌های امنیتی و محتوایی و هماهنگی بین‌دستگاهی در سطوح استراتژیک ایفاد می کند. نهادهای اطلاعاتی و امنیتی (وزارت اطلاعات، سازمان اطلاعات سپاه و واحدهای مرتبط) نقش مقابله با تهدیدهای امنیتی- سایبری ساخت‌یافته، جرایم سازمان‌یافته فرامرزی، حفاظت اطلاعات کلان و عملیات اطلاعاتی مرتبط با تهدیدات ملی است.نهادهای بخش فرهنگی-محتوایی و حمایتی (وزارت فرهنگ و ارشاد اسلامی، دادگستری در بخش آیین‌دادرسی، و نهادهای حمایتی مرتبط با کودک و خانواده) نقش همکاری در تعیین مصادیق محتوایی، مشارکت در فرآیند فیلترینگ، حذف محتوا و هماهنگی حمایت‌های اجتماعی و قضایی از قربانیان (مخصوصاً کودکان) را دارد. این نهادها عضو یا همکار کارگروه‌ها و فرآیندهای ذی‌ربط هستند.

ویژگی‌های بارز سیاست جنایی ایران در قبال جرایم سایبری، غلبه رویکرد کنترل‌محور است. این رویکرد خود را در سه سطح نشان می‌دهد:

نخست، گسترش دامنه جرم‌انگاری بدون تفکیک دقیق میان رفتارهای واقعاً مخرب و رفتارهای پرخطر اما قابل مدیریت اجتماعی. دوم، تکیه بر ابزارهای فنی نظیر فیلترینگ و مسدودسازی به‌عنوان راهکار اصلی پیشگیری. سوم، اولویت دادن به تعقیب و مجازات بزهکار به‌جای حمایت نهادمند از بزه‌دیدگان. (فتح‌الهی، همکاران، ۱۴۰۳: ۲۷۱)

---

1 . fata.gov.ir

۲. در سال ۱۳۸۷ در پی تصویب قانون جرایم رایانه ای در مجلس شورای اسلامی تصویب شد.

3 . https://cert.ir

٤ . اسفند ۱۳۹۰ این شورا به فرمان مقام معظم رهبری ایجاد شد.

در این چارچوب، خانواده بیشتر به‌عنوان نهادی نیازمند حفاظت انفعالی دیده می‌شود، نه کنشگری که باید از طریق آموزش، آگاهی‌بخشی و حمایت حقوقی توانمند گردد. چنین رویکردی با نظریه‌های نوین سیاست جنایی که بر پیشگیری اجتماعی و کاهش آسیب تأکید دارند، هم‌خوانی محدودی دارد.

یکی از نقاط ضعف اساسی سیاست جنایی ایران، فقدان توجه نظام‌مند به بزه‌دیدگان جرایم سایبری خانوادگی است. در قوانین موجود، حمایت از بزه‌دیده عمدتاً به امکان شکایت کیفری و مطالبه مجازات محدود می‌شود و سازوکارهای حمایتی غیرکیفری نظیر مشاوره روانی، حمایت اجتماعی یا تدابیر حفاظتی فوری پیش‌بینی نشده است.

این وضعیت به‌ویژه در مورد زنان و کودکان به‌عنوان آسیب‌پذیرترین اعضای خانواده تشدید می‌شود. بسیاری از قربانیان جرایم سایبری خانوادگی به دلیل ترس از بی‌آبرویی، تشدید تعارضات خانوادگی یا ناکارآمدی نظام حمایتی، از مراجعه به مراجع قضایی خودداری می‌کنند. نتیجه این وضعیت، شکل‌گیری پدیده «بزه‌دیدگی پنهان» و تداوم چرخه آسیب در درون خانواده است.

از منظر بزه‌دیده‌شناسی، سیاست جنایی ایران بیشتر بزه‌مدار است تا بزه‌دیده‌مدار و این امر کارآمدی آن را در حمایت واقعی از کیان خانواده کاهش می‌دهد. (داودی دهاقانی، رضایی، ۱۴۰۱: ۱۰-۱۱)

تحلیل سیاست تقنینی ایران نشان می‌دهد که پیشگیری اجتماعی جایگاه محدودی در مواجهه با جرایم سایبری دارد. قانون‌گذار کمتر به نقش آموزش سواد دیجیتال، توانمندسازی والدین، یا مشارکت نهادهای مدنی در کاهش آسیب‌های سایبری توجه کرده است. در حالی که بسیاری از جرایم سایبری ناقض کیان خانواده ریشه در ناآگاهی کاربران، شکاف نسلی دیجیتال و فقدان مهارت‌های ارتباطی در فضای مجازی دارند، سیاست جنایی ایران همچنان به واکنش پسینی و کیفری متکی است. این امر موجب شده است که هزینه‌های اجتماعی جرم افزایش یابد و مداخلات قانونی غالباً دیرهنگام و ناکارآمد باشند.

بر اساس مدل تحلیلی ارائه‌شده در این پژوهش، سیاست جنایی تقنینی ایران را می‌توان به‌طور غالب در زمره سیاست‌های کنترل‌محور طبقه‌بندی کرد. ویژگی‌های اصلی این الگو در ایران عبارت‌اند از:

- تأکید بر جرم‌انگاری و مجازات
- نگاه تهدیدمحور به فضای مجازی
- فقدان مفهوم‌پردازی مستقل از کیان خانواده دیجیتال
- ضعف حمایت نهادمند از بزه‌دیدگان
- کم‌رنگ بودن پیشگیری اجتماعی و آموزشی

اگرچه این سیاست در مهار برخی جلوه‌های آشکار جرایم سایبری مؤثر بوده است، اما در مواجهه با آسیب‌های پیچیده و پنهان خانوادگی، کارآمدی محدودیت دارد و نیازمند بازنگری اساسی است.

۲-۵.تحلیل سیاست جنایی تقنینی ترکیه در قبال جرایم سایبری ناقض کیان خانواده

سیاست جنایی ترکیه در حوزه جرایم سایبری در بستر پیوستن تدریجی این کشور به ساختارهای حقوقی اروپایی و تلاش برای هم‌سویی با استانداردهای اتحادیه اروپا شکل گرفته است.[۱] ترکیه از اوایل دهه ۲۰۰۰ میلادی، هم‌زمان با گسترش اینترنت و رسانه‌های دیجیتال، به تدوین مقررات خاص در حوزه جرایم سایبری و حفاظت از داده‌های شخصی روی آورد و به‌تدریج سیاستی فراتر از جرم‌انگاری صرف اتخاذ کرد.[۲]

در این چارچوب، خانواده نه‌تنها به‌عنوان یک نهاد اخلاقی، بلکه به‌مثابه واحدی اجتماعی با حقوق قابل حمایت در فضای دیجیتال مورد توجه قانونگذار قرار گرفت. با این حال، این توجه بیشتر به صورت غیرمستقیم و از طریق حمایت از حریم خصوصی، کرامت انسانی و داده‌های شخصی اعضای خانواده اعمال شد.(لطیفی، ۱۳۹۸: ۱۲)

نظام حقوقی ترکیه در مواجهه با جرایم سایبری ناقض کیان خانواده، مجموعه‌ای از قوانین عام و خاص را به‌کار گرفته است. قانون جزای ترکیه، قانون تنظیم اینترنت و مبارزه با جرایم ارتکابی از طریق رسانه، و قانون حفاظت از داده‌های شخصی، هسته اصلی سیاست تقنینی این کشور را تشکیل می‌دهند.

در قانون شماره ۵۲۳۷ انواع جرایم مرتبط با حریم خصوصی و حیثیت، ضبط و انتشار غیرقانونی داده‌ها، توهین و تهدید در فضای دیجیتال، و بهره‌کشی جنسی از کودکان جرم‌انگاری شده است. در قانون جزا تشویق خودکشی (ماده ۸۴)، آزار و اذیت (ماده ۹۶)، آزار جنسی کودکان (ماده ۱۰۳)، تهدید به قتل (ماده ۱۰۶)، نقض محرمانگی ارتباطات (ماده ۱۳۲)، تجاوز به حریم خصوصی و افشای اسرار خصوصی (مواد ۱۳۴ و ۱۳۵)، تسهیل مواد مخدر (ماده ۱۹۰)، تولید یا عرضه مواد خطرناک (ماده ۱۹۴)، فحاشی (ماده ۲۲۶)، روسپیگری (ماده ۲۲۷) و قمار (ماده ۲۲۸). همچنین هرزه‌نگاری کودکان صراحتاً جرم‌انگاری شده است و تولید، توزیع و نگهداری این نوع محتوا در همه رسانه‌ها از جمله دیجیتال جرم است.

اهمیت این مقررات در آن است که برخلاف رویکرد سنتی کیفری، تمرکز قانون‌گذار ترکیه بیشتر بر حقوق بنیادین افراد است که به‌طور طبیعی از کیان خانواده نیز حمایت می‌کند. با این حال، همچون ایران، در قوانین ترکیه نیز مفهوم «جرایم سایبری ناقض کیان خانواده» به‌صورت مستقل صورت‌بندی نشده و حمایت از خانواده بیشتر نتیجه تبعی حمایت از حقوق فردی اعضای آن است. برخلاف ایران که سیاست کنترل‌محور بر آن غالب است، سیاست جنایی ترکیه را می‌توان در زمره

---

۱ . سایت سی‌اوئی. آی‌ان‌تی.

2. The Law on Regulation of Broadcasts VIA Internet and Combating Crimes Committed by the Means of Such Publications: P. 21

رویکردهای تنظیمی–حقوق‌محور طبقه‌بندی کرد. در این الگو، قانون‌گذار می‌کوشد میان آزادی‌های دیجیتال، نظم عمومی و حمایت از حقوق افراد تعادل برقرار کند.

این رویکرد در چند محور نشان داده می‌شود: نخست، تنظیم فعالیت ارائه‌دهندگان خدمات اینترنتی و الزام آن‌ها به حذف یا مسدودسازی محتوای مجرمانه با دستور قضایی.[1] دوم، تأکید بر حفاظت از داده‌های شخصی (PDPL) به‌عنوان ابزار اصلی صیانت از حریم خانواده در فضای مجازی. سوم، پرهیز نسبی از جرم‌انگاری افراطی و استفاده از سازوکارهای اداری و حقوقی در کنار ضمانت اجراهای کیفری.

در این چارچوب، خانواده نه صرفاً موضوع مداخله کیفری، بلکه ذی‌نفع سیاست‌های تنظیم‌گرایانه تلقی می‌شود.

یکی از نقاط قوت سیاست جنایی ترکیه نسبت به ایران، توجه بیشتر به حمایت از بزه‌دیدگان، به‌ویژه کودکان و نوجوانان، در جرایم سایبری است. قانون‌گذار ترکیه سازوکارهایی برای حذف سریع محتوای آسیب‌زا، حمایت قضایی از قربانیان و همکاری با نهادهای بین‌المللی پیش‌بینی کرده است.

با این حال، این حمایت‌ها عمدتاً فردمحور باقی مانده و کمتر به سطح خانواده به‌عنوان یک واحد اجتماعی گسترش یافته است. به‌عبارت دیگر، اگرچه از کودک یا فرد بزه‌دیده حمایت می شود، اما پیامدهای خانوادگی جرم، مانند فروپاشی روابط یا فشارهای روانی بر سایر اعضا، کمتر در سیاست تقنینی بازتاب یافته است.

در مجموع، تحول حقوقی ترکیه از ۲۰۰۷ به بعد حکمرانی پلتفرم‌محور، تمرکز بر حفاظت از اطفال و خانواده (فیلترینگ، حذف سریع محتوا، الزام به نگهداری داده‌ها و محلی‌سازی مسئولیت پلتفرم‌ها) و تقویت ابزارهای واکنش سریع را به‌همراه آورد؛[2] اما همزمان ریسک‌های مهمی نیز پدید آمد. افزایش قدرت دولت در اعمال سانسور و مسدودسازی، احتمال خطا و هدف‌گیری نادرست محتوا، تهدید آزادی بیان و تداخل دولت در منازعات خصوصی (حریم خصوصی و هتک حیثیت). بنابراین، تجربه ترکیه نشان می‌دهد که دستیابی به محافظت کارآمد از خانواده و صغار در فضای مجازی نیازمند ترکیب ابزارهای فنی و حقوقی سریع‌الواکنش است، اما محافظت از آزادی‌های بنیادی و تضمین رویه‌های قضایی مستقل و شفاف نیز باید همزمان مدنظر قرار گیرد.

نهاد نظارتی بر فضای مجازی اداره کل جرایم سایبری[3]، نهاد حفاظت داده‌ها[4] و سازمان فناوری ارتباطات[5] ساختار اصلی را تشکیل می‌دهند.[6]

---

2 . Erdem & Erdem Law Firm. (2020, August 4). Regulations on social media and internet contents through Law No. 7253.

۲ . مواد ۸،۹ و ۹ الف قانون ۵۶۵۱.

3 . Siber Suçlar Dairesi
4 . KVKK Kurumu
5 . BTK
6 . https://www.edpb.europa.eu/system/files/2024-04/edpb_annual_report_2023_en.pdf

سازمان فناوری و ارتباطات ترکیه[1] نهاد مرکزی نظارت بر محتوای دیجیتال است. بر اساس ماده ۶ قانون ۵۶۵۱، این سازمان صلاحیت دارد تا محتوای مخل اخلاق عمومی یا تهدیدکننده بنیان خانواده را به درخواست دادگاه یا مستقیماً با دستور ریاست جمهوری مسدود کند. گزارش سالانه سازمان فناوری و ارتباطات (2022) نشان می‌دهد که از میان ۵۷۳ هزار درخواست حذف محتوا، حدود ۱۸٪ مربوط به شکایات خانوادگی (انتشار عکس خصوصی یا تهدید عاطفی) بوده است.

نهاد حفاظت از داده‌های شخصی سال ۲۰۱۶ تشکیل شد و از قدرت الزام‌آور برخوردار است. بر اساس ماده ۲۲ قانون ۶۶۹۸، هر شهروند می‌تواند در صورت نقض داده‌های خانوادگی (مانند تصاویر کودکان یا مکاتبات خصوصی)، شکایت خود را به این نهاد ارسال کند. گزارش سال ۲۰۲۳ این نهاد حاکی است که ۱۲٪ از پرونده‌ها مربوط به انتشار غیرمجاز تصاویر خانوادگی در شبکه‌های اجتماعی بوده است.

اداره کل جرایم سایبری[2] در وزارت کشور ترکیه، نقش محوری در کشف و تعقیب جرایم خانوادگی آنلاین دارد. این اداره از سال ۲۰۱۱ به بعد در تمام استان‌ها واحدهای تخصصی ایجاد کرده است. طبق گزارش رسمی این اداره (۲۰۲۲)، در سال ۲۰۲۱ حدود ۳۷۵۰ پرونده تهدید و اخاذی خانوادگی در بستر دیجیتال به ثبت رسیده است، که ۶۵٪ آن علیه زنان بوده است (Siber Suçlar Dairesi, 2022: 9).

جامعه ترکیه دارای ساختاری دوگانه است: از یک سو تأثیرپذیرفته از فرهنگ اسلامی–محافظه‌کار و از سوی دیگر در معرض مدرنیته اروپایی و رسانه‌های آزاد. این دوگانگی فرهنگی سبب شده است که نگرش‌ها نسبت به «اخلاق دیجیتال» ناپایدار باشد. پژوهش (Demir & Kaya, 2021: 135) نشان می‌دهد که در خانواده‌های شهری، ۵۲٪ والدین از فعالیت فرزندان در شبکه‌های اجتماعی بی‌اطلاع‌اند، اما ۷۸٪ آنان نگران تأثیرات اخلاقی آن هستند؛ در مقابل، در خانواده‌های روستایی میزان دسترسی کمتر اما نظارت خانوادگی قوی‌تر است.

در حوزه آموزش، وزارت ملی آموزش ترکیه از سال ۲۰۱۷ برنامه‌ای با عنوان «اینترنت امن برای خانواده»[3] راه‌اندازی کرده است که شامل کارگاه‌های آگاهی‌بخشی به والدین و دانش‌آموزان درباره خطرات آنلاین است. بر اساس گزارش این وزارتخانه(MEB, 2022: 33) ، تا سال ۲۰۲۲ بیش از ۴۵۰ هزار خانواده در این برنامه شرکت کرده‌اند.

با این حال، کارشناسان جرم‌شناسی مانند (Karagül 2021: 58) هشدار داده‌اند که «سیاست‌های ترکیه بیش از آنکه بر پیشگیری اجتماعی متمرکز باشند، بر کنترل فنی و فیلترینگ تأکید دارند»؛ این امر مشابه وضعیت ایران است و می‌تواند به شکل‌گیری «نظارت دولتی بیش از حد» بینجامد.

1 . Information and Communication Technologies Authority – BTK
2 . Siber Suçlar Dairesi Başkanlığı
3 . Safe Internet for Family

در ترکیه تنظیم‌گر فضای مجازی، حفاظت داده و پلیس سایبری تقسیم‌کار روشنی دارند؛ هرچند گزارش‌های مستقل به «تمرکزگرایی در مسدودسازی» و «ناهماهنگی موردی» اشاره کرده‌اند. با این حال، مکانیسم قضایی سریع برای حذف محتوا و اختیار انتظامی–تنظیمی KVKK در رسیدگی به نقض داده‌های خانوادگی، از نقاط قوت است.

در مقایسه با ایران، ترکیه توجه بیشتری به پیشگیری غیرکیفری و آموزش دیجیتال نشان داده است. برنامه‌های آموزشی در مدارس، همکاری با سازمان‌های غیردولتی و مشارکت در طرح‌های بین‌المللی مقابله با جرایم سایبری، بخشی از سیاست پیشگیرانه این کشور را تشکیل می‌دهد. با این حال، این اقدامات عمدتاً پراکنده بوده و در قالب یک سیاست جامع حمایت از خانواده دیجیتال نهادینه نشده‌اند. نبود پیوند منسجم میان سیاست‌های آموزشی، حمایتی و کیفری موجب شده است که تأثیر پیشگیری اجتماعی در کاهش آسیب‌های سایبری خانوادگی محدود باقی بماند.

بر اساس مدل تحلیلی پژوهش، سیاست جنایی تقنینی ترکیه را می‌توان در قالب سیاست تنظیمی–حقوق‌محور طبقه‌بندی کرد. مهم‌ترین ویژگی‌های این الگو عبارت‌اند از:

- تمرکز بر حقوق بنیادین و حفاظت از داده‌های شخصی
- استفاده از تنظیم‌گری حقوقی در کنار ضمانت اجراهای کیفری
- توجه نسبی به حمایت از بزه‌دیدگان، به‌ویژه کودکان
- ضعف در مفهوم‌پردازی مستقل از کیان خانواده دیجیتال
- فقدان انسجام کامل میان پیشگیری، حمایت و جرم‌انگاری

این سیاست در مقایسه با ایران پیشرفته‌تر و متوازن‌تر است، اما هنوز به سطح یک سیاست جنایی خانواده‌محور کامل نرسیده و در عمل، خانواده بیشتر بهره‌مند غیرمستقیم حمایت‌های فردی است تا موضوع حمایت مستقل تقنینی.

۳-۵. تحلیل سیاست جنایی تقنینی مالزی در قبال جرایم سایبری ناقض کیان خانواده

سیاست جنایی مالزی در قبال جرایم سایبری در بستری چندلایه شکل گرفته است که در آن، ملاحظات دینی، فرهنگی، توسعه اقتصادی و الزامات بین‌المللی به‌طور هم‌زمان نقش‌آفرینی می‌کنند. مالزی به‌عنوان کشوری با اکثریت مسلمان و نظام حقوقی مختلط (حقوق عرفی، شریعت اسلامی و حقوق مدرن)، از آغاز توسعه فضای دیجیتال، نگاه پیشگیرانه‌تری به پیامدهای اجتماعی و خانوادگی فناوری‌های نوین داشته است.

در این چارچوب، خانواده نه‌تنها به‌عنوان نهادی اخلاقی، بلکه به‌مثابه واحد بنیادین توسعه اجتماعی و سرمایه انسانی تلقی می شود. همین نگرش موجب شده است که قانون‌گذار مالزی، جرایم سایبری ناقض کیان خانواده را صرفاً به‌عنوان انحرافات فردی در نظر نگیرد، بلکه آن‌ها را تهدیدی علیه انسجام اجتماعی و ثبات ارزشی جامعه ارزیابی کند.

– نخستین قانون جرایم رایانه‌ای در مالزی؛[1] سال ۱۹۹۷ شکل گرفت (اجرایی از ژوئن ۲۰۰۰)، که هسته جرم‌انگاری سایبری را از طریق سه محور اصلی — دسترسی غیرمجاز (ماده ۳)، دسترسی با قصد ارتکاب جرم (ماده ۴) و تغییر غیرمجاز محتوا، داده (ماده ۵) — تبیین کرد و برای آنها مجازات مالی و حبس تعیین نمود.(زندی، مشتاقی، ۱۳۹۴: ۱۱۷)

قوانین کیفری عام و موضوعی مالزی ـ از قبیل قانون مجازات و مواد مرتبط با افترا، تقلب، سرقت و تجاوز جنسی ـ به فضای آنلاین تسری یافته و مواردی چون کلاهبرداری سایبری، سرقت داده، افشای اسرار خصوصی و استثمار جنسی کودکان تحت شمول چندین متن قانونی قرار گرفته‌اند. قانون ویژه مقابله با آزار و بهره‌کشی جنسی کودکان، از جمله در فضای آنلاین؛[2] و قانون کودک و مقررات حمایتی[3] (مطابق استانداردهای بین‌المللی) حریم حمایتی ویژه‌ای برای افراد زیر ۱۸ سال فراهم می‌آورند و قوانین جداگانه‌ای برای مبارزه با قاچاق انسان و استثمار جنسی وجود دارد که مصادیق جدید ـ از جمله قاچاق جنسی دیجیتال و پخش زنده اعمال جنسی اجباری ـ را تحت پوشش کیفری قرار می‌دهند. همچنین قانون امضای دیجیتال (۱۹۹۷)، قانون تجارت الکترونیک (۲۰۰۶) و اصلاحات اخیرِ قانون جرایم رایانه‌ای، مبانی حقوقی لازم برای صحت معاملات الکترونیکی و مقابله با کلاهبرداری دیجیتال را فراهم کرده‌اند.

در مالزی D11/RMP و زیروا حد MICAC در خط مقدم OCSEA قرار دارند؛ MCMC نیز در حذف، مسدودسازی محتوا نقش مکمل دارد. در سطح سیاست‌گذاری، وزارت زنان و خانواده، طرح ملی را اجرا کرده و با یونیسف ماژول‌های «والدگری دیجیتال» را گسترش داده است. گزارش ملی مالزی ضمن تأیید این ظرفیت‌ها، به کمبود نیروی انسانی تخصصی، محدودیت پهنای باند برای اتصال به پایگاه‌های بین‌المللی ادله، و وقفه در کارگروه بین‌وزارتی پس از ۲۰۲۰ اشاره می‌کند.

در عمل، رویکرد مالزی ترکیبی از «ایجابی‌سازی» فناوری (ترویج نوآوری و بهره‌برداری از ظرفیت‌های دیجیتال برای توسعه) و «تنظیم‌گری‌کنترل‌محور» است.(پژوهشگاه فضای مجازی، ۱۳۹۹) از یک سو چارچوب قانونی نسبتاً جامع و نهادهای اختصاصی برای حمایت از کودکان، حفاظت داده و مقابله با جرایم سایبری وجود دارد؛ از سوی دیگر، در دهه‌های اخیر پنل اصلاحات و لوایحی جهت جرم‌انگاری تهدیدات نوظهور (بدافزار، جعل هویتی، کلاهبرداری دیجیتال، تصاویر صمیمی بدون رضایت و موارد مرتبط) و تقویت مجازات‌ها مطرح و تصویب شده‌اند. راهکارهای اجرایی — از جمله ایجاد دادگاه‌های تخصصی سایبری (از سپتامبر ۲۰۱۶ در کوالالامپور) و رویکردهای سامانه‌ای به جمع‌آوری و نگهداری شواهد دیجیتال ـ ظرفیت واکنش را افزایش داده‌اند.[4]

1 . Computer Crimes Act 1997(CCA)
2 . Sexual Offences Against Children Act 2017 (Act 792)
3 . Child Act 2001 (as amended 2017)
۴ .https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/?utm_source=chatgpt.com

نظام تقنینی مالزی در حوزه جرایم سایبری، مجموعه‌ای نسبتاً منسجم از قوانین را دربرمی‌گیرد که به‌طور مستقیم یا غیرمستقیم از کیان خانواده حمایت می‌کنند. این قوانین حوزه‌هایی چون سوءاستفاده جنسی از کودکان در فضای مجازی، تولید و انتشار محتوای مضر، نقض حریم خصوصی دیجیتال، آزار آنلاین و سوءاستفاده از داده‌های شخصی را پوشش می‌دهند.(محمدی،۱۴۰۰ :۶)

ویژگی متمایز سیاست مالزی آن است که قانون‌گذار، به‌ویژه در حوزه کودکان و نوجوانان،[1] به‌صورت صریح به پیامدهای خانوادگی جرم توجه نشان داده و حمایت از خانواده را بخشی از هدف قانون‌گذاری معرفی کرده است. در این چارچوب، کودک نه صرفاً یک بزه‌دیده فردی، بلکه عضوی از یک ساختار خانوادگی آسیب‌پذیر تلقی می شود که نیازمند حمایت چندسطحی است.

قانون ارتباطات و چندرسانه‌ای سازوکارهای مجوزدهی، ممنوعیت و مسؤولیت ارائه‌دهندگان محتوا و خدمات را پیش‌بینی کرده است: از جمله جرم‌شناسیِ ارائه محتوای بدون مجوز (ماده ۲۰۵)، ممنوعیت ارائه محتوای «مبتذل، زشت یا توهین‌آمیز» (ماده۲۱۱)، مجازات ارسال پیام‌های موهن و تهدیدآمیز (ماده ۲۳۳)، رهگیری و افشای غیرمجاز ارتباطات (ماده ۲۳۴) و برخورد با اظهارات گمراه‌کننده (ماده۲۴۱). در کنار این، مواد دیگری (مثل ماده ۷۵) انتشار اطلاعات و مدارک نادرست را نیز جرم‌انگاری کرده‌اند و احکام حمایت از مصرف‌کننده اینترنتی (بخش هشتم؛ ماده ۱۸۷) تکالیف نظارتی برای ارائه‌دهندگان خدمات وضع می‌کنند. کمیسیون ارتباطات و چندرسانه‌ای مالزی نهادی تنظیم‌گر در حوزه‌ی محتواست و با همکاری پلیس، مسئول مسدودسازی سایت‌های دارای محتوای مستهجن یا سوءاستفاده از کودکان است. طبق بند ۲۱۱ قانون ۱۹۹۸، این کمیسیون می‌تواند هرگونه محتوای «خلاف عفت عمومی» را حذف کند. گزارش سالانه این نهاد (۲۰۲۱) نشان می‌دهد که طی سال ۲۰۲۰ بیش از ۱۲٬۰۰۰ سایت غیراخلاقی و ۴۲ مورد مرتبط با آزار کودکان مسدود شده‌اند.

پلیس سلطنتی مالزی[2] و واحد ویژه بخش تحقیقات زنان و کودکان[3] در پلیس سلطنتی مالزی، مسئولیت مستقیم رسیدگی به جرایم جنسی آنلاین علیه کودکان را بر عهده دارد. زیرمجموعه‌ی این واحد جرایم اینترنتی علیه کودکان،[4] است که از سال ۲۰۱۶ فعالیت دارد. طبق گزارش رسمی (ECPAT, et al. 2022: 3)، تنها در بازه ۲۰۱۷ تا ۲۰۱۹، ۳۵ پرونده‌ی رسمی بهره‌کشی و سوء استفاده جنسی از کودکان (آنلاین)[5] در این واحد ثبت شده که البته به‌دلیل عدم گزارش‌دهی عمومی، رقم واقعی بسیار بالاتر برآورد می‌شود.

1. Child Act 2001 (Act 611)
2 . Royal Malaysia Police – RMP
3 .D11
4 . Malaysia Internet Crimes Against Children (MICAC)
5 . OCSEA (Online Child Sexual Exploitation and Abuse)

واحد ویژه تحقیقات زنان و کودکان و بخش جرایم اینترنتی علیه کودکان از فناوری‌های دیجیتال پلیس بین‌الملل[1] برای ردیابی تصاویر سوءاستفاده از کودکان استفاده می‌کنند. با این حال، به گفته گزارش (ECPAT, et al., 2022: 4)، محدودیت نیروی انسانی، کمبود تجهیزات و ضعف اتصال اینترنت پرسرعت از موانع اصلی عملکرد آن‌هاست.

در سیاست جنایی مالزی، پیشگیری اجتماعی جایگاهی محوری دارد. آموزش سواد دیجیتال در مدارس، برنامه‌های آگاهی‌بخشی والدین، همکاری با سازمان‌های مردم‌نهاد و مشارکت فعال در ابتکارات منطقه‌ای و بین‌المللی مقابله با جرایم سایبری، بخشی جدایی‌ناپذیر از این سیاست است.[2]

نکته قابل توجه آن است که این اقدامات پیشگیرانه به‌صورت پراکنده یا نمادین اجرا نمی‌شوند، بلکه در چارچوب یک راهبرد ملی حفاظت از کودکان و خانواده در فضای دیجیتال قرار دارند. همین انسجام سیاستی، اثربخشی مداخلات غیرکیفری را به‌طور محسوسی افزایش داده است.[3]

وزارت زنان، خانواده و توسعه اجتماعی این وزارتخانه متولی اصلی سیاست‌گذاری در حوزه‌ی خانواده است و «طرح اقدام برای حفاظت از کودکان در فضای آنلاین»[4](۲۰۱۵–۲۰۲۰) را با همکاری یونیسف و امنیت سایبری مالزی اجرا کرده است. این طرح شامل آموزش دیجیتال خانواده‌ها، ایجاد خطوط تماس فوری و گسترش سواد رسانه‌ای است (ECPAT, et al., 2022: 5).

نهادهای حمایتی غیردولتی سازمان‌هایی مانند محافظت از کودکان و نجات آنها[5] و سازمان حمایت زنان[6] در فرآیند قضایی از کودکان و خانواده‌های آسیب‌دیده حمایت می‌کنند. طبق گزارش این سازمان تنها در سال ۲۰۱۹ بیش از ۳۵۰ مورد مشاوره به قربانیان سوءاستفاده آنلاین ارائه داده است. (ECPAT, et al, 2022: 5)

با این حال، چارچوب حقوقی مالزی بیشتر بر گونه‌ای محافظت جمعیِ نظم و توسعه و حمایت از گروه‌های آسیب‌پذیر تمرکز دا شته تا بر تعریف‌زدایی مطلق و تفکیک سازی ویژه «خانواده» به‌عنوان شاکیِ جداگانه؛ بنابراین خانواده‌ها عمدتاً از طریق شمول جرایم علیه حیثیت، حریم خصوصی، استثمار جنسی کودکان، قمار و تقلبِ دیجیتال مورد حمایت قرار می‌گیرند. در مجموع می‌توان گفت مالزی الگوی «تنظیم توسعه‌محورِ همراه با نظارت» را اتخاذ کرده است.توانمندسازی فناوری و هم‌زمان ایجاد ابزارهای قانونی و نهادی برای مهار آثار زیان‌بار، با این نکته که پوشش کامل تهدیدات نوظهور نیازمند تکمیل لوایح و تقویت سازوکارهای اجرایی و حمایت مدنی متناسب باقی می‌ماند.

1 . INTERPOL’s ICSE database
2 . The Law of Marriage and Divorce with Special Reference to Malaysia.
۳ . سایت ای‌تیسز. وایت‌رُز. ای‌سی.یو کی
4 . Plan of Action on Child Online Protection
5 . Protect and Save the Children (P.S. the Children
6 . Women’s Aid Organisation

سیاست جنایی تقنینی مالزی را می‌توان نمونه‌ای برجسته از رویکرد حمایت‌محور–اجتماعی دانست. در این الگو، جرم‌انگاری تنها یکی از ابزارهای مداخله است و در کنار آن، حمایت اجتماعی، آموزش دیجیتال و مشارکت نهادی نقش اساسی ایفا می‌کنند.

در این چارچوب، قانون‌گذار مالزی تلاش کرده است تا میان واکنش کیفری و سیاست‌های پیشگیرانه توازن برقرار کند. مجازات‌ها به‌گونه‌ای طراحی شده‌اند که بازدارندگی مؤثر ایجاد کنند، اما هم‌زمان سازوکارهایی برای مداخله زودهنگام، حذف سریع محتوای آسیب‌زا و حمایت از بزه‌دیدگان و خانواده‌های آنان پیش‌بینی شده است Communications . (and Computer Crimes Act 1997 Multimedia Act 1998)

این رویکرد نشان‌دهنده عبور سیاست جنایی مالزی از منطق سرکوب کیفری صرف و حرکت به سوی یک سیاست چندبعدی و انسان‌محور است. در این نظام، حمایت از بزه‌دیدگان به اقدامات کیفری محدود نمی‌شود، بلکه شامل حمایت‌های روانی، اجتماعی و حتی اقتصادی نیز می‌گردد. به‌ویژه در مورد کودکان، قانون‌گذار مالزی سازوکارهایی را پیش‌بینی کرده است که مداخله خانواده، نهادهای حمایتی و دستگاه قضایی را به‌صورت هماهنگ ممکن می‌سازد. این هماهنگی نهادی، از بزه‌دیدگی ثانویه جلوگیری کرده و امکان بازسازی روابط خانوادگی آسیب‌دیده را فراهم می‌آورد.

از منظر بزه‌دیده شناسی، سیاست مالزی نمونه‌ای موفق از گذار از بزه‌مداری به بزه‌دیده‌محوری و حتی خانواده‌محوری محسوب می‌شود.(Wemmers, 1996: 7-12)

بر اساس مدل تحلیلی ارائه‌شده در این پژوهش، سیاست جنایی تقنینی مالزی به‌وضوح در دسته سیاست‌های حمایت‌محور–اجتماعی قرار می‌گیرد. ویژگی‌های شاخص این الگو عبارت‌اند از:

- توجه صریح به کیان خانواده دیجیتال
- تلفیق جرم‌انگاری با حمایت اجتماعی و نهادی
- بزه‌دیده‌محوری و خانواده‌محوری در سیاست تقنینی
- نقش محوری پیشگیری اجتماعی و آموزش دیجیتال
- هماهنگی میان نهادهای تقنینی، قضایی و اجتماعی

در مقایسه تطبیقی، می‌توان گفت که سیاست مالزی، در میان سه کشور مورد مطالعه، بیشترین انطباق را با نظریه‌های نوین سیاست جنایی و الزامات اجتماعی عصر دیجیتال دارد و می‌تواند به‌عنوان الگویی قابل اقتباس برای اصلاح سیاست جنایی ایران و ترکیه مورد توجه قرار گیرد.

۶. تحلیل تطبیقی نهایی سیاست جنایی تقنینی در قبال جرایم سایبری ناقض کیان خانواده سه کشور مورد مطالعه

مقایسه سیاست‌های جنایی تقنینی ایران، ترکیه و مالزی نشان می‌دهد که این کشورها نه‌تنها از حیث ابزارهای حقوقی، بلکه از نظر منطق‌های بنیادین سیا ست‌گذاری جنایی نیز تفاوت‌های معناداری دارند. این تفاوت‌ها را می‌توان در قالب سه منطق مسلط تحلیل کرد: کنترل‌محور، تنظیمی–حقوق‌محور و حمایت‌محور–اجتماعی.

در ایران، سیاست جنایی سایبری عمدتاً بر منطق کنترل استوار است.(Vatani,, & Asadi, 2016) فضای مجازی به‌عنوان قلمرو تهدید تلقی می شود و واکنش تقنینی بیش از هر چیز بر محدود سازی، جرم‌انگاری و مداخله پلیسی متمرکز است. در چنین الگویی، خانواده موضوعی ثانویه تلقی می‌شود و حمایت از آن، نتیجه تبعی کنترل رفتارهای مجرمانه است.

در مقابل، ترکیه سیاستی میانه منطق تنظیمی–حقوق‌محور اتخاذ کرده است.(Law No. 5651) این کشور تلاش می‌کند تعادلی میان آزادی‌های دیجیتال، نظم عمومی و حمایت از حقوق بنیادین برقرار کند. خانواده در این چارچوب نه به‌عنوان هدف مستقل سیاست جنایی، بلکه به مثابه ذی‌نفع حقوق فردی اعضای خود مورد حمایت قرار می‌گیرد.

مالزی اما رویکردی متفاوت برگزیده است. منطق حمایت‌محور–اجتماعی در سیاست جنایی این کشور، خانواده را واحد اصلی مداخله می‌داند و جرم‌انگاری را در کنار حمایت اجتماعی، آموزش دیجیتال و هماهنگی نهادی به‌کار می‌گیرد. این تفاوت در منطق سیاست‌گذاری، تأثیر مستقیمی بر کارآمدی حمایت از کیان خانواده داشته است.

در سطح نهادی، پلیس فتا در ایران، BTK و KVKK در ترکیه، و D11/MCMC در مالزی محور اصلی‌اند، اما تنها در مالزی پیوند میان پلیس و نهادهای اجتماعی فعال است.از منظر فرهنگی، هر سه کشور با تابوی گزارش آزار جنسی و شرم فرهنگی مواجه‌اند. برنامه‌های آموز شی و والدگری دیجیتال در مالزی موفق‌تر بوده‌اند (Idris & Yusof, 2021: 77)

از منظر جرم‌انگاری، ایران گسترده‌ترین دامنه مداخلات کیفری را دارا ست، اما این گ ستردگی الزاماً به معنای اثربخ شی بیشتر نیست. جرم‌انگاری‌های کلی و فاقد تفکیک دقیق در قانون جرایم رایانه‌ای، موجب شده است که بسیاری از آسیب‌های خاص خانوادگی در قالب عناوین عام و غیرتخصصی پیگیری شوند. «قانون جرایم رایانه‌ای مصوب ۱۳۸۸» ا ست. مواد ۱۶ و ۱۷، انت شار محتوای م ستهجن و اف شای ت صاویر خ صو صی را جرم‌انگاری می‌کنند؛ اما طبقه‌بندی م ستقلِ «خ شونت و جرم خانوادگیِ دیجیتال» وجود ندارد و ب سیاری از م صادیق (اخاذی عاطفی آنلاین، تهدید به انت شار ت صاویر خصوصی، استاکینگِ خانوادگی) با تفسیر موسع در ذیل عناوین عام قرار می‌گیرند. عدم الحاق به کنوانسیون‌های همکاری فراملی (بوداپست) باعث دشواری در گردآوری ادله و معاضدت قضایی می‌شود.

ترکیه در این زمینه رویکردی محدودتر اما هدفمندتر اتخاذ کرده است. تمرکز بر نقض حریم خصوصی، حفاظت از داده‌ها و بهره‌کشی جنسی از کودکان، نشان‌دهنده تلاش برای جرم‌انگاری متناسب با مخاطرات واقعی فضای دیجیتال است. دو قانون کلیدی ۵۶۵۱ (اینترنت) و ۶۶۹۸ (حمایت از داده‌های شخصی KVKK) شبکه‌ای نسبتاً روزآمد برای حراست از حریم خصوصی و واکنش سریع قضایی ایجاد کرده‌اند. امکان مسدودسازی فوری محتوای ناقض حریم خصوصی ظرف ۲۴

ساعت (به‌استناد ماده ۹ قانون ۵۶۵۱) و صلاحیت مستقل نهاد حفاظت از داده‌ها در KVKK، ترکیه را از حیث «کارآمدیِ واکنش اولیه» در جایگاهی بالاتر از ایران قرار می‌دهد. افزوده بر این، الحاق به کنوانسیون بوداپست (۲۰۱۴) ماده ۳۵ ظرفیت نقطه‌تماس ۲۴ساعته و تبادل الکترونیک ادله را فعال کرده است. با این حال، نبود عنوان مجرمانه مستقل برای جرایم سایبری خانوادگی همچنان یک خلأ محسوب می‌شود.

مالزی در مقایسه، سیاست جرم‌انگاری خود را به‌گونه‌ای طراحی کرده است که پیوند روشنی میان رفتار مجرمانه و پیامدهای خانوادگی آن برقرار شود. این امر موجب شده است که جرم‌انگاری‌ها نه‌تنها بازدارنده، بلکه معطوف به حمایت عملی از خانواده باشند. مجموعه‌ای از قوانین پیشرفته، از جمله قانون جرایم رایانه ۱۹۹۷، قانون فناوری و ارتباطات ۱۹۹۸ و جرایم جنسی علیه کودکان ۲۰۱۷ منظومه‌ای تلفیقی از جرم‌انگاری و حمایت را ساخته است. قانون جرایم جنسی علیه کودکان، رفتارهایی چون ارتباط جنسیِ دیجیتال با کودک، درخواست،تهدید برای ارسال تصاویر جنسی، و پخش زنده سوءاستفاده را صراحتاً در بر می‌گیرد و از دادگاه‌ها و مراکز مصاحبه با کودکان برای رسیدگی کودک‌محور بهره می‌برد.

یکی از مهم‌ترین محورهای تطبیق، جایگاه بزه‌دیدگان جرایم سایبری خانوادگی در سیاست جنایی است. در ایران، بزه‌دیدگان عمدتاً در نقش شاکی کیفری تعریف می‌شوند و حمایت از آنان به فرایند دادرسی محدود می‌گردد. (نجفی ابرندآبادی، ۱۳۹۳: ۲۳۱-۲۳۵) فقدان سازوکارهای حمایتی غیرکیفری، موجب تشدید بزه‌دیدگی ثانویه و کاهش تمایل به گزارش جرم شده است. در ترکیه، اگرچه حمایت از بزه‌دیدگان در قالب حذف محتوا و حمایت قضایی پیش‌بینی شده است، اما این حمایت‌ها بیشتر فردمحور باقی مانده و کمتر به سطح خانواده گسترش یافته‌اند. Akdeniz, 2008: 128–(137) خانواده در این چارچوب، بستر وقوع جرم است، نه موضوع حمایت مستقل. مالزی در این زمینه رویکردی متمایز دارد. حمایت از بزه‌دیدگان به‌صورت نهادمند و چندسطحی طراحی شده و خانواده به‌عنوان واحدی نیازمند بازسازی و حمایت در نظر گرفته می‌شود.[1] این رویکرد، امکان ترمیم آسیب‌های اجتماعی و کاهش آثار بلندمدت جرم را فراهم می‌سازد.

ایران به عضویت کنوانسیون بوداپست نپوسته، همکاری‌ها موردی و از مسیر مکاتبات دوجانبه و نمایندگی‌ها دنبال می‌کند؛ این امر در پرونده‌هایی که سرورها خارج از کشورند، گردآوری ادله را دشوار و زمان‌بر می‌کند.

ترکیه از سال ۲۰۱۴ به‌طور رسمی عضو کنوانسیون بوداپست شد (Council of Europe, 2014: 2) .الحاق به این کنوانسیون باعث شد چارچوب همکاری بین‌المللی در زمینه تبادل داده‌های الکترونیکی میان ترکیه و سایر کشورها ایجاد شود. بر اساس ماده ۳۵ کنوانسیون، کشورهای عضو متعهد به ایجاد «نقطه تماس ۲۴ ساعته» برای همکاری قضایی هستند؛ ترکیه این سازوکار را در اداره پلیس سایبری خود ایجاد کرده است.

1. https://www.unicef.org/malaysia/press-releases/asean-unites-build-safer-digital-spaces-every-child

ترکیه همچنین در سال ۲۰۱۲ به کنوانسیون پالرمو ملحق شد که در مبارزه با قاچاق انسان و جرایم سازمان‌یافته، از جمله سوءاستفاده جنسی از کودکان، کاربرد دارد .(UNODC, 2019: 14) این عضویت به ترکیه امکان می‌دهد تا در پرونده‌های فراملی (مانند شبکه‌های پورنوگرافی کودک) همکاری مؤثری با پلیس بین‌الملل داشته باشد.

در سطح منطقه‌ای، ترکیه در چارچوب شورای همکاری کشورهای ترک‌زبان نیز تفاهم‌نامه‌ای برای تبادل اطلاعات در حوزه امنیت خانواده دیجیتال امضا کرده است. (TÜRKSOY, 2021: 6)

مالزی با تکیه بر چارچوب‌های آسه‌آن (اعلامیه ۲۰۱۹ و اقدامات منطقه‌ای ۲۰۲۱) و شبکه‌های بین‌المللی چارچوب‌های برای آموزش، گردآوری داده، و هم‌افزایی بین‌نهادی نقشه‌راه مشخص ارائه می‌کنند. مالزی یکی از کشورهای فعال در حوزه همکاری‌های منطقه‌ای آسه‌آن است. این کشور در سال ۲۰۱۹ به اعلامیه آسه‌آن[1] درباره حمایت از کودکان در برابر بهره‌کشی آنلاین پیوست و در سال ۲۰۲۱ نیز در تدوین «طرح اقدام منطقه‌ای برای حفاظت از کودکان در برابر انواع استثمار و سوءاستفاده آنلاین»[2] مشارکت داشت. این سند منطقه‌ای، مالزی را موظف می‌کند تا تا سال ۲۰۲۵ ظرفیت پلیس، دادگستری و آموزش عمومی در حوزه حمایت از کودکان آنلاین را ارتقا دهد (ASEAN Secretariat, 2021: 7).

علاوه بر آن، مالزی عضو رسمی اتحادیه جهانی[3] است که با هدف توسعه الگوی پاسخگو ملی[4] برای مقابله با آزار آنلاین کودکان فعالیت می‌کند. (WePROTECT, 2021: 9) این مدل، ۲۱ قابلیت ملی از جمله قانون‌گذاری، نهادهای حمایت از قربانیان و آموزش بین‌نهادی را مشخص می‌کند.

ترکیه و مالزی به‌واسطه الحاق وهمکاری ساختاری در سطح منطقه‌ای–بین‌المللی، در کشف، ادله‌یابی و تعقیب برون‌مرزی مزیت آشکار دارند.

در حوزه پیشگیری، تفاوت سیاست‌ها به‌وضوح نمایان است. ایران کمترین توجه را به پیشگیری اجتماعی و آموزش دیجیتال نشان داده و عمدتاً به پیشگیری کیفری و فنی متکی بوده است. این امر موجب شده است که ریشه‌های اجتماعی و فرهنگی جرایم سایبری خانوادگی نادیده گرفته شوند.

ترکیه گام‌هایی در جهت آموزش و آگاهی‌بخشی برداشته است، اما این اقدامات فاقد انسجام راهبردی بوده و به‌صورت پروژه‌ای اجرا می‌شوند. پیشگیری اجتماعی در سیاست جنایی ترکیه هنوز جایگاه نهادمند نیافته است.

مالزی اما پیشگیری اجتماعی را به‌عنوان رکن اصلی سیاست جنایی سایبری خود تلقی کرده و آن را در قالب برنامه‌های ملی، آموزشی و مشارکتی نهادینه ساخته است. این تفاوت، نقش تعیین‌کننده‌ای در کاهش آسیب‌های سایبری خانوادگی ایفا کرده است.

1. ASEAN, 2019
2 . Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse
3 . WePROTECT Global Alliance
4 . Model National Response

با ارجاع به چارچوب نظری پژوهش، می‌توان گفت که سیاست جنایی ایران بیشترین فاصله را با نظریه‌های کنترل اجتماعی و بزه‌دیده‌شناسی حمایتی دارد. تأکید یک‌جانبه بر کنترل کیفری، کارآمدی این سیاست را در حمایت از کیان خانواده کاهش داده است. سیاست جنایی ترکیه تا حدی با نظریه‌های تنظیم‌گری حقوقی هم‌خوانی دارد، اما در گذار به سیاست خانواده‌محور ناکام مانده است. در مقابل، سیاست مالزی بیشترین انطباق را با نظریه جامعه شبکه‌ای و بزه‌دیده‌شناسی نوین نشان می‌دهد و توانسته است به مدلی متوازن و کارآمد دست یابد.

مقایسه بازدارندگی حقوق کیفری سه کشور

بعد بازدارندگی	وضعیت ضعیف‌تر	وضعیت میانه	بهترین وضعیت
شدت مجازات برای جرایم مهم سایبری	مجازات‌های مالزی در موارد جدی و کافی نیست و قانون نیاز به اصلاحات دارد	ایران با بعضی جرایم شدید، مخصوصاً در حوزه امنیت ملی و محتوای حساس درقانون تعریف و استفاده گسترده با ابهامات همراه است	ترکیه دارای قوانین جدید و مجازات‌های تشدیدشده برای حملات بزرگ و زیرساختی است
قطعیت اجرا (احساس اینکه مرتکب در نهایت شناسایی و مجازات می‌شود)	ایران مشکلات جدی در اثبات جرم، وجود فعالیت‌های پنهان، قضایی شدن موارد سیاسی، و تطبیق با استانداردهای بین‌المللی حقوق بشر دارد	مالزی در مواردی خوب است ولی ظرفیت فنی و همکاری بین‌المللی و جمع‌آوری شواهد گاهی چالش دارد	ترکیه به دلیل نهادهای نظارتی جدید و قانون امنیت سایبری جدید، قطعیت بیشتر دارد
سرعت و شفافیت اجرای قانون	ایران نگرانی‌هایی درباره فرایند قانونی، شفافیت، دسترسی به دادگاه مستقل، و امکان تأخیر یا استفاده از قوانین به نحو سرکوبگرانه وجود دارد	مالزی سابقه قانونی و تجربه، اما نیاز به ارتقاء ظرفیت و فرایندهای قضایی سریع‌تر دارد	ترکیه به دلیل قانون جدید، مقررات روشن‌تر، الزامات اداری جدید سرعت بیشتری دارد
محافظت حقوق بشر ، آزادی بیان	ایران بالاترین میزان نگرانی در این زمینه؛ قوانین محتوا معمولاً گسترده و امکان سرکوب انتقاد بالا است.	ترکیه به دلیل نگرانی‌ها، به ویژه در تعریف «اطلاعات نادرست»، قوانینی که ممکن است به سرکوب بیان منجر شوند، دارد. اما با اصلاحات جدید ممکن است تعادل بهتری برقرار شود	مالزی تا حدی بهتر است؛ نسبتاً قوانین روشن‌تر در زمینه محتوا و آزادی بیان دارد، نگرانی‌ها اما هنوز هستند

نتیجه‌گیری

پژوهش حاضر با هدف تحلیل حقوقی و جامعه‌شناختی واکنش به جرایم سایبری علیه خانواده در سه کشور ایران، ترکیه و مالزی سامان یافته است. مطالعه تطبیقی نشان داد که این سه کشور، علی‌رغم اشتراک در بنیان‌های فرهنگی اسلامی و دغدغه‌های اخلاقی مشابه، در نحوه مواجهه با تهدیدهای سایبری خانوادگی از الگوهای متفاوتی پیروی می‌کنند. در ایران، تمرکز سیاست جنایی عمدتاً بر جنبه‌های صیانتی، انتظامی و کنترلی است و قانون‌گذار کوشیده است از رهگذر جرم‌انگاری و نظارت فناورانه، امنیت اخلاقی خانواده را حفظ کند. در ترکیه، پیوند میان الزامات بین‌المللی و ساختار سکولار نظام حقوقی، سبب ایجاد چارچوبی دوگانه و درعین‌حال منسجم در اجرای قوانین مرتبط با جرایم اینترنتی شده است. در مالزی، الگوی چندسطحی و جامعه‌محور با مشارکت نهادهای مدنی، پلیس تخصصی و نهادهای آموزشی، بیش از دو کشور دیگر توانسته است جنبه‌های حمایتی و پیشگیرانه را با سیاست کیفری تلفیق کند.

نتایج تحلیل تطبیقی نشان می‌دهد که کارآمدی سیاست جنایی تقنینی در قبال جرایم سایبری ناقض کیان خانواده، نه به شدت جرم‌انگاری، بلکه به میزان توجه به خانواده به‌عنوان واحد اجتماعی مستقل وابسته است و همچنین «تعادل سه‌گانه» میان قانون، فرهنگ و فناوری نهفته است. هرگاه یکی از این سه ضلع مغفول بماند، نظام حقوقی به جای پیشگیری از آسیب، در بازتولید ناامنی و بی‌اعتمادی ظهور می‌یابد.

در این میان، نهاد خانواده که در فقه اسلامی و حقوق تطبیقی به‌عنوان رکن طبیعی جامعه تلقی می شود، امروز در بستر فضای سایبری با نوعی «فقدان مرز» مواجه است. پدیده‌هایی چون افشای داده‌های خصوصی، باج‌گیری جنسی دیجیتال، تهاجم به حریم عاطفی از طریق شبکه‌های اجتماعی، و استثمار عاطفی یا اقتصادی کودکان، مفهوم «امنیت خانوادگی» را از سطح فیزیکی به سطح دیجیتال متحول کرده است. یافته‌های این پژوهش نشان داد که اگرچه ساختارهای قانونی در سه کشور مورد مطالعه در پی پاسخگویی به این تحولات‌اند، اما شکاف میان رشد فناوری و واکنش حقوقی همچنان عمیق است. تحلیل تطبیقی سیاست‌های جنایی ایران، ترکیه و مالزی نشان می‌دهد که کارآمدی سیاست تقنینی در قبال جرایم سایبری ناقض کیان خانواده، بیش از آن‌که به شدت واکنش کیفری وابسته باشد، به چگونگی صورت‌بندی مسئله خانواده در سیاست‌گذاری جنایی بستگی دارد. در این چارچوب، سیاست‌هایی که خانواده را صرفاً بستر وقوع جرم یا مجموعه‌ای از افراد مستقل تلقی می‌کنند، در مواجهه با آسیب‌های پیچیده فضای مجازی ناکام می‌مانند.

سیاست جنایی ایران نمونه بارز این ناکامی است. تمرکز بر کنترل، جرم‌انگاری گسترده و مداخله پسینی، بدون توجه کافی به زمینه‌های اجتماعی، موجب شده است که بسیاری از جرایم سایبری خانوادگی یا گزارش نشوند یا پس از وقوع، آثار جبران‌ناپذیری بر ساختار خانواده بر جای گذارند. از منظر جامعه شناسی حقوق، این سیاست نه‌تنها پیشگیرانه نیست، بلکه در برخی موارد به بازتولید آسیب منجر می‌شود.

در ترکیه، هرچند سیاست تقنینی از افراط در کنترل کیفری فاصله گرفته، اما فقدان نگاه خانواده‌محور سبب شده است که حمایت‌های حقوقی عمدتاً به سطح فرد محدود بماند. این وضعیت، شکافی میان حمایت قانونی و واقعیت‌های اجتماعی خانواده ایجاد کرده و مانع از تحقق حمایت جامع از کیان خانواده دیجیتال شده است.

در مقابل، تجربه مالزی نشان می‌دهد که سیاست جنایی زمانی کارآمد است که جرم‌انگاری، حمایت اجتماعی و آموزش دیجیتال در قالب یک راهبرد منسجم به‌کار گرفته شوند. این انسجام، امکان مداخله زودهنگام، کاهش بزه‌دیدگی پنهان و ترمیم آسیب‌های خانوادگی را فراهم می‌سازد.

از منظر نظری، پژوهش حاضر نشان داد که جرایم سایبری علیه خانواده صرفاً در چهارچوب مفاهیم کلاسیک جرم و مجازات قابل تحلیل نیست، بلکه نیازمند نگرشی چندبُعدی است که عناصر فرهنگی، روان‌شناختی و فناورانه را نیز در برگیرد. بر اساس تحلیل‌های انجام‌شده، چند نتیجه نظری اساسی قابل استخراج است:

نخست، فضای مجازی موجب تحول در الگوی بزهکاری و بزه‌دیدگی خانوادگی شده است. در این فضا، مرز میان عامل و قربانی سیال است؛ گاه همان عضوی که تهدید می شود، در موقعیتی دیگر عامل آسیب به دیگر اعضای خانواده می‌گردد. بنابراین، نظریه‌های کلاسیکی مانند کنترل اجتماعی تنها در صورتی کارآمدند که با تحلیل روان شناسی دیجیتال و ساختارهای فرهنگی همراه شوند. در حالیکه بر اساس نظریه کنترل اجتماعی، تضعیف پیوندهای خانوادگی یکی از عوامل اصلی افزایش آسیب‌های سایبری است. و در ایران با نادیده گرفتن این پیوندها و تمرکز صرف بر ابزارهای کنترلی، عملاً از تقویت سرمایه اجتماعی خانواده غفلت کرده است. این امر با مبانی نظری کنترل اجتماعی در تعارض آشکار قرار دارد. از طرف دیگر از منظر بزه‌دیده‌شناسی حمایتی نیز، سیاست‌های ایران و تا حدی ترکیه فاقد سازوکارهای مؤثر حمایت از بزه‌دیدگان خانوادگی هستند. در این نظام‌ها، بزه‌دیده اغلب پس از ورود به فرایند کیفری با فشارهای اجتماعی، روانی و خانوادگی مضاعف مواجه می شود؛ امری که به بزه‌دیدگی ثانویه دامن می‌زند. در مقابل، سیاست جنایی مالزی با رویکرد خانواده‌محور خود، انطباق بیشتری با نظریه جامعه شبکه‌ای دارد. این سیاست، خانواده را به‌عنوان کنشگری فعال در شبکه‌های اجتماعی–دیجیتال تلقی کرده و می‌کوشد از طریق آموزش، حمایت نهادی و تنظیم‌گری حقوقی، قدرت خانواده را در این شبکه‌ها افزایش دهد.

دوم، مفهوم «حق بر امنیت خانوادگی» به‌عنوان یکی از مصادیق نوپدید حقوق بشر و حقوق اسلامی باید در سیاست جنایی سایبری بازتعریف گردد. امنیت خانواده صرفاً به معنای مصونیت از خشونت فیزیکی نیست، بلکه شامل امنیت داده‌ها، امنیت روانی، کرامت جنسی و حریم ارتباطی اعضای خانواده نیز هست. به‌ویژه در جوامع اسلامی، حفظ حرمت، عفاف و اسرار خانوادگی، وجهی الهی و اجتماعی دارد که قانون‌گذار موظف است آن را از تعرض فناوری مصون دارد.

سوم، جرم‌شناسی واکنشی در حوزه جرایم سایبری خانوادگی باید از سطح «مجازات‌محوری» به سطح «حمایت‌محوری» تغییر یابد. یافته‌ها نشان دادند که سیاست‌های صرفاً تنبیهی، نه‌تنها مانع تکرار جرم نیستند، بلکه در مواردی موجب اختفای بزه‌دیدگی، افزایش احساس شرم و کاهش اعتماد اجتماعی می شوند. سیاست مؤثر، سیاستی است که بر محور آموزش، آگاهی، بازپروری و تقویت سرمایه اجتماعی خانواده استوار باشد.

چهارم، از منظر جامعه‌شناختی، خانواده در عصر دیجیتال از وضعیت نهادی بسته به شبکه‌ای باز بدل شده است. تعاملات اعضای خانواده دیگر صرفاً در فضای حقیقی صورت نمی‌گیرد، بلکه در محیط‌های مجازی شکل می‌پذیرد و ارزش‌ها، نقش‌ها و حدود اخلاقی را بازتعریف می‌کند. بدین ترتیب، هرگونه جرم در این فضا مستقیماً بر ساخت قدرت و نظم درونی خانواده اثرگذار است. بی‌توجهی به این واقعیت، منجر به گسست نسلی و بحران اعتماد بین والدین و فرزندان می‌شود.

پنجم، در تحلیل تطبیقی سه کشور روشن گردید که سیاست‌های موفق، آن‌هایی هستند که میان شریعت و قانون عرفی، و میان آموزش رسمی و کنترل اجتماعی، هم‌افزایی ایجاد کرده‌اند. در ترکیه، رویکرد نظام‌مند به آموزش سواد دیجیتال در مدارس و تربیت قضات متخصص، اثربخشی واکنش قضایی را افزایش داده است. در مالزی، تلفیق ارزش‌های اسلامی با برنامه‌های آموزش جنسی سالم در فضای مجازی، به تقویت ایمنی کودکان انجامیده است. در مقابل، در ایران، غلبه رویکرد امنیتی بر فرهنگ ، مانع از شکل‌گیری نهادهای حمایتی مستقل شده است. این امر ضرورت بازنگری در نگاه کیفری حاکم بر سیاست‌های خانواده‌محور در فضای سایبر را آشکار می‌کند.

تحلیل حاضر نشان می‌دهد که نوآوری نه در تصویب قوانین جدید، بلکه در تغییر پارادایم سیاست جنایی نهفته است. در این چارچوب، سیاست‌های ایران و ترکیه را نمی‌توان نوآورانه تلقی کرد؛ زیرا همچنان در چارچوب‌های سنتی جرم‌انگاری یا تنظیم‌گری فردمحور باقی مانده‌اند. در مقابل، سیاست مالزی از حیث تلفیق حمایت اجتماعی، آموزش دیجیتال و مداخله کیفری هدفمند، واجد نوآوری ساختاری است. این نوآوری نه صرفاً تقنینی، بلکه سیاستی و نهادی است و می‌تواند الهام‌بخش اصلاح سیاست جنایی در سایر کشورها باشد.

پژوهش حاضر نشان داد که جرایم سایبری ناقض کیان خانواده، پدیده‌ای چندبعدی هستند که مواجهه مؤثر با آن‌ها مستلزم فراتر رفتن از سیاست جنایی سنتی و سرکوب‌محور است. تحلیل تطبیقی ایران، ترکیه و مالزی آشکار ساخت که کارآمدترین سیاست جنایی، سیاستی است که خانواده را واحد اصلی حمایت و مداخله تلقی کند. در این میان، سیاست جنایی ایران به دلیل غلبه رویکرد کنترل‌محور، فاقد توان لازم برای حمایت مؤثر از کیان خانواده دیجیتال است. سیاست ترکیه اگرچه متوازن‌تر است، اما به دلیل فردمحوری، از تحقق حمایت جامع خانوادگی بازمانده است. در مقابل، سیاست مالزی با اتخاذ رویکرد حمایت‌محور–اجتماعی، توانسته است الگویی نسبتاً موفق در این حوزه ارائه دهد.

بر اساس یافته‌های پژوهش، پیشنهادهای زیر قابل ارائه است:

۱. بازتعریف مفهومی کیان خانواده دیجیتال در قوانین کیفری و شناسایی آن به‌عنوان ارزش مستقل قابل حمایت.

۲. تدوین مقررات خاص درباره جرایم سایبری خانوادگی با تفکیک از جرایم سایبری عام.

۳. تقویت حمایت‌های غیرکیفری از بزه‌دیدگان خانوادگی شامل مشاوره، حمایت روانی و تدابیر حفاظتی فوری.

۴. نهادینه‌سازی آموزش سواد دیجیتال خانواده‌محور به‌عنوان رکن پیشگیری اجتماعی.

۵. حرکت از سیاست کنترل‌محور به سیاست حمایت‌محور–اجتماعی با الگوگیری انتقادی از تجربه مالزی.

نوآوری اصلی این مقاله در ارائه مدل تحلیلی سه‌گانه سیاست جنایی سایبری خانواده و اثبات برتری رویکرد حمایت‌محور–اجتماعی در مواجهه با جرایم سایبری ناقض کیان خانواده است. این مدل می‌تواند مبنای پژوهش‌های آتی و اصلاح سیاست‌گذاری جنایی در جوامع مشابه قرار گیرد.

منابع

۱. اساسنامه پلیس فتا(۱۳۹۱)

۲. اعلامیه آسه آن(۲۰۱۹)

۳. خاقانی ا صفهانی، مهدی و مهرداد رایجیان ا صلی، (۱۴۰۰)، سیا ست جنایی ایران در حمایت از خانواده در آینهٔ « سند تحول ق ضایی» و دستورالعمل نحوه مشارکت و تعامل نهادهای مردمی با قوه قضاییه، دانشگاه سیستان و بلوچستان، مجموعه مقالات نخستین همایش ملی چالش‌ها و راهکارهای تعالی نهاد خانواده در مذاهب اسلامی با محوریت آسیب‌های اجتماعی.

۴. پژوهشگاه فضای مجازی (۱۳۹۹)، سلسله گزارش‌های بررسی وضعیت حکمرانی ۱۱ کشور توسعه یافته و در حال توسعه در فضای مجازی

۵. داودی دهاقانی، ابراهیم، رضایی، نورمحمد، (۱۴۰۱)، پیشگیری از بزه دیدگی زنان در فضای سایبر، تهران: دانشگاه علوم انتظامی امین.

۶. رایجیان اصلی، (۱۳۸۳) ، رهیافتی نو به بنیانهای نظری پیشگیری از جرم، مجله حقوقی دادگستری شماره ۴۸-۴۹.

۷. زندی، محمدرضا، مشتاقی، مریم،(۱۳۹۴)، شنود غیر مجاز (و رویه قضایی جرایم رایانه‌ای)، تهران: انتشارات مجد.

۸. فتح الهی، نوید، رستمی فر، علی، سراجی، مصطفی، (۱۴۰۳) اعمال حاکمیت بر فضای مجازی از منظر مداخلات سلبی در حقوق ایران با تأکید بر مسئله فیلترینگ، نشریه حقوق و مطالعات سیاسی، دوره۴ شماره ۲.

۹. قنبری باغستانی، عباس، (۱۳۹۸)، حکمرانی فضای مجازی در کشورهای جهان مالزی، پژوهشگاه فضای مجازی، گروه مطالعات فرهنگی و اجتماعی.

۱۰. کنوانسیون بوداپست(۲۰۰۱)

۱۱. کاستلز، مانوئل، (۱۳۹۶)، قدرت ارتباطات، ترجمه: حسین بصیریان جهرمی، تهران: انتشارات علمی و فرهنگی.

۱۲. لطیفی، محمدرضا، (۱۳۹۸)، حکمرانی فضای مجازی در کشورهای جهان ترکیه، تهران: پژوهشگاه فضای مجازی گروه مطالعات فرهنگی و اجتماعی.

۱۳. محمدی، حافظ،(۱۴۰۰) مطالعه تطبیقی شاخص‌های حکمرانی سایبری در کشورهای جهان. دومین همایش ملی حکمرانی اسلامی.

۱۴. معصومی گودرزی، شیما، (۱۴۰۰)، تحلیل بزه‌دیدگی قاچاق زنان و دختران از طریق فضای مجازی، مجله دستاوردهای نوین در مطالعات علوم انسانی، (۳۸) ۴

۱۵. منیری، حمیدرضا، (۱۳۹۷)،تحلیل و بررسی فقهی اجرای فیلترینگ در فضای مجازی، فصلنامه حکومت اسلامی، ۸۴.

۱۶. میرعربی، علی ا صغر، (۱۳۹۸)، جرایم سایبری علیه حیثیت معنوی و کیان خانواده در حقوق کیفری ایران، دو فصلنامه علمی مطالعات فقه و حقوق رسانه دانشکده رفاه، (۱)۱

۱۷. نجفی ابرندآبادی، علی‌حسین) ۱۳۹۳ .*بزه‌دیده‌شناسی* (چاپ سوم). تهران: میزان، **صص. ۲۳۱–۲۳۵.**

1. Akdeniz, Y. (2008). *nternet child pornography and the law: National and international responses.* Farnham: Ashgate Publishin.
2. ASEAN Secretariat. (2021). Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN. Jakarta: ASEAN Secretariat.
3. Castells, M. (2000). The Rise of the Network Society (2nd ed.). Oxford: Blackwell.
4. Council of Europe. (2014). Budapest Convention: Country Profile – Türkiye. Strasbourg: COE.
5. Demir, M., & Kaya, A. (2021). Family values and digital interactions in conservative societies: The Turkish case,Journal of Family Studies, 27,(2), 130–138.

6. Durkheim, É. (1893/2014). *The Division of Labor in Society* (W. D. Halls, Trans.; First ed., pp. 29–31, 87–90). Free Press. (Original work published 1893)
7. ECPAT, INTERPOL, & UNICEF. (2022). Disrupting Harm in Malaysia: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence Against Children.
8. Efremova, M. A., & Russkevich, E. A. (2025). Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development. Journal of Digital Technologies and Law, 3(2), 187–202
9. Hirschi, T. (1969),Causes of Delinquency. Berkeley: University of California Press.
10. Law No. 5651 on Regulation of Publications in the Internet and Fighting Against Crimes Committed by Means .
11. Idris, F., & Yusof, M. (2021). Parental mediation and online safety in Malaysian families. Asian Journal of Communication, 31 (1), 72–82.
12. Karagül, M. (2021). Cybercrime policies and family safety in Turkey,Turkish Journal of Criminology, 4.(1), 55–62.
13. MEB (Ministry of National Education). (2022), Safe Internet for Family Program Evaluation Report. Ankara: MEB.
14. Rhodes, R. A. W. (1997). Understanding governance: Policy networks, governance, reflexivity and accountability. Buckingham: Open University Press.
15. Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas*. University of Chicago Press.
16. UNODC. (2019) ,Country Review Report: Turkey – UNTOC Implementation, Vienna: UNODC
17. Vatani, A., & Asadi, H. (2016). *Criminal policy of the Islamic Republic of Iran in dealing with cyber crimes Pazhuheshnameh-ye Ḥoqūq-e Eslāmī*, 17(2), 99–126. https://doi.org/10.30497/law.2016.1959.
18. Venice Commission. (2016). Opinion on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication.
19. UNICEF Malaysia. (2025, November 18). *ASEAN unites to build safer digital spaces for every child*. UNICEF Retrieved from https://www.unicef.org/malaysia/press-releases/asean-unites-build-safer-digital-spaces every - child.
20. Walklate, S. (1989). *Victimology: The victim and the criminal justice process* , London: Unwin Hyman
21. **Wemmers, J.-A. (1996).** *Victims in the criminal justice system*. Amsterdam: Kugler Publications
22. WePROTECT Global Alliance. (2021),Model National Response to Preventing and Tackling Child Sexual Exploitation and Abusem, London: WGA.