گونه‌شناسی سیاست کیفری فنی در قبال جرم رمزنگاری اطلاعات

از منظر آزادی‌گرایی و امنیت‌گرایی*

□ محمدعلی حاجی ده‌آبادی[۱]
□ مهدی خاقانی اصفهانی[۲]

چکیده

نئولیبرالیسم، پس از برچیدن مرزهای تجارت و جداسازی فضای اقتصادی از قلمرو حاکمیت سیاسی، از راهبردهای جرم‌شناسی بازپرورانه و تساهل‌گرا عدول کرد و با رفتن به سوی ابزارهای سرکوبی جرم‌شناسی کیفرگرا نگرانی‌های حقوق بشری را اوج بخشید. بنابراین طراحی راهبردی میان‌رشته‌ای و سنجیده، از رهگذر تعامل آموزه‌های حقوق کیفری با جرم‌شناسی، حقوق بشر، اقتصاد سیاسی و بسیاری از دیگر علوم معین، ضرورت دارد.

این جستار، پس از آسیب‌شناسی تقابل گفتمان آزادی‌گرا و امنیت‌گرا در حقوق غرب و نقض حقوق بشر در پی تسری این تقابل به عرصهٔ محرمانگی تجارت الکترونیکی (به ویژه در حوزهٔ رمزنگاری اطلاعات)، توضیح می‌دهد که در فرایند نواندیشی دینی در اقتصاد ایران، «مدل زرد: مدل احتیاطی» در

* تاریخ دریافت: ۱۳۹۱/۶/۱ ـ تاریخ پذیرش: ۱۳۹۲/۲/۲۶.

۱. استادیار دانشگاه قم (dr_hajidehabadi@yahoo.com).
۲. دانشجوی دکتری حقوق کیفری و جرم‌شناسی (نویسندهٔ مسئول) (mr.khaqani@gmail.com).

عرصهٔ پیشگیری و کیفررسانی جرایم رمزنگاری اطلاعات سایبری را می‌توان یکی از زمینه‌های همگرایی حقوق ایران با حقوق اروپایی دانست و با بومی‌سازی این مدل، گام‌هایی اساسی در مسیر تدوین راهبرد کیفری و جرم‌شناختی کشور برداشت. مدل‌های قرمز (امنیت‌گرای مطلق) و سبز (آزادی‌گرای مطلق) را متقابلاً باید در زمرهٔ زمینه‌های واگرایی نظام‌های حقوقی مذکور برشمرد.

واژگان کلیدی: جرم‌شناسی غربی، مدرنیتهٔ حقوقی، رمزنگاری مجرمانه، سیاست کیفری اسلامی.

مقدمه

ترجیح نظم عمومی و امنیت ملی بر حریم خصوصی افراد، از سپتامبر ۲۰۰۱ تشدید شد. دولت‌های مدعی بزه‌دیدگی با تأکید بر اینکه حملات تروریستی به مراکز تجاری و دفاعی ایالات متحده، ممکن است از طریق اختلال در شبکه‌های اطلاعاتی سایبری رخ دهند، بر آن شدند تا حقوقِ ناظر بر حفظ حریم خصوصی شهروندانِ مظنون و غیر مظنون را زیر پرچم پیشگیری وضعی از وقوع جرم و نظریهٔ جرم‌شناختی فرصت[1] به شدت کم‌رنگ کنند. چیرگی پارادایم امنیت‌گرا و رویکرد ریسک‌مدار به عدالت کیفری، موجب شد گفتمان غالب در سیاست جنایی جهانی در دههٔ اخیر بر گرانیگاه «امنیت‌محوری» و نه «حقوق بشرمحوری» استوار شود.

بروز جلوه‌هایی از جنبش سرکوبگریِ کیفری[2] در قلمرو جرایم علیه امنیت ـو به ویژه علیه امنیت تجارت الکترونیکی‌ـ را نباید در تعارض با اندیشه‌های مبنایی نظام‌های لیبرال ارزیابی کرد. در حقیقت، اگرچه لیبرالیسم به حسب ماهیت وجودی و اصول نظری خود، اعتقادی به جرم‌انگاری حداکثری ندارد، واقعیت‌های عملی

1. Theory of opportunity.

۲. نهضت کیفرشناسی نوین، از یک سو نظارت بر شهروندان را فوق‌العاده تشدید و فنی می‌کند و از سوی دیگر، راهبرد بازپروری و پیشگیری را نفی می‌نماید و با گسترش شبکهٔ کنترل اجتماعی و دولتی و یا محدودسازی و گاه حذف حقوق و آزادی‌های فردی، به شکل سیاست کیفری تسامح صفر در چارچوب راهبرد امنیت‌مداری جلوه‌گر می‌شود (برای مطالعهٔ بیشتر ر.ک: نجفی ابرندآبادی، ۱۳۸۸؛ کاشفی اسماعیل‌زاده، ۱۳۸۴: ش۱۵و۱۶).

جامعه، ضرورت ایجاد دولتی با کارکردهای امنیتی را در این زمینه منطقی و عقلانی جلوه داده است (مجیدی، ۱۳۸۸: ش۳۲۹/۲)، هرچند در حقیقت، عقلانیت و روح عدالت، خلاف چنین راهبردی را اقتضا دارد. دموکراسی‌های لیبرال اروپایی ـ به رغم تصور رایج ـ و نیز بسیاری از دیگر کشورها با محدودسازیِ استفاده از تجهیزات رمزنگاری و پنهان‌نگاریِ کاربران عمومی اینترنت ـ به ویژه کاربران تجارت الکترونیکی ـ استفاده از آن را ویژهٔ خود ساخته‌اند و با این کار، ضمن تضعیف زیرساخت‌های امنیت تجارت سالم الکترونیکی، به بهانهٔ پیشگیری از تروریسم سایبری، به رمزگشایی اطلاعات و پنهان‌شکنی ارتباطات کاربران اینترنت اقدام کرده‌اند.

از حیث ضرورت و اهمیت تحقیق، پژوهشگران ایرانیِ عرصهٔ حقوق کیفری تجارت الکترونیکی، متذکر شده‌اند که با توجه به نوپایی مفهوم امنیت فضای تولید و تبادل اطلاعات، و امکان‌پذیر بودن دستیابی به دانش و فناوری‌های مرتبط و ضرورت بومی‌سازی این حوزه‌ها با توجه به میزان تأثیر آن بر امنیت ملی کشور، پرداختن به امنیت فضای تولید و تبادل اطلاعات، از اولویت‌های کشور تلقی می‌شود (برای مطالعه دربارهٔ سیاست‌گذاری جنایی و کیفری در حوزهٔ امنیت تجارت الکترونیکی ر.ک: قناد، ۱۳۸۶؛ حسن‌بیگی، ۱۳۸۳: ش۹).

رعایت سیاست‌های امنیتی، باعث اطمینان از ایجاد فضای قابل نظارت و پایش و نظام‌مند در انجام معاملات الکترونیکی است. فناوری‌های پیشرفته مانند فناوری رمزنگاری با استفاده از زیرساخت کلید عمومی یا فناوری بایومتریک در تولید امضای رقمی یا بایومتریک، بخشی مستنبط از مجموع دغدغه‌های متنوع و پرچالشی است که قانون‌گذار برای ساماندهی یک استراتژی سنجیده در قبال آن‌ها، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور» را در تاریخ ۱۳۸۷/۱۲/۷ در هیئت وزیران به تصویب رساند و آن را به دیگر موازین حقوق موضوعهٔ کشور در این حوزه، نظیر قانون جرایم رایانه‌ای و قانون تجارت الکترونیکی افزود.

آنچه زمینه را برای سوءاستفادهٔ مجرمان هوشمند و سازمان‌یافتهٔ رایانه‌ای از دو

فناوری هوشمند رمزنگاری[1] و پنهان‌نگاری[2] فراهم آورده است، جدال گفتمان‌های جرم‌شناختی است. این مناقشه، عامل اصلی سرگردانی سیاست جنایی ملی، منطقه‌ای و جهانی در طراحی و کاربرد راهبردهای واکنش جزایی به رفتارهای ناقض امنیت اطلاعات، از جمله رمزنگاری‌ها و پنهان‌نگاری‌های ناقض حریم خصوصی شهروندان است. البته رمزنگاری‌ها و پنهان‌نگاری‌هایی که با هدف ارتقای ضریب امنیت اطلاعات تجاری الکترونیکی سالم انجام می‌گیرد، از این مقوله جداست.

پیامد سردرگمی سیاست جنایی در این قلمرو از حقوق فنّاوری اطلاعات، تشدید ناتوانی حقوق کیفری در مجازات مجرمان رایانه‌ای است؛ چه امروز، از مهم‌ترین مشکلات حقوق کیفری «محدودیت‌های کارکردی» آن است (Rudolph, 2005: 84). به دیگر سخن، اگرچه وجود قانون کیفری برای تمیز هنجارها و ناهنجاری‌ها و تعیین الگوی رفتار قانونی شهروندان برای هر جامعه‌ای ضروری است، در ایجاد جامعه‌ای سالم و قانونمند و تأمین و تضمین حقوق و آزادی اساسی شهروندان تنها از سازوکار جرم‌انگاری نمی‌توان بهره برد و از پیامدهای آن و هزینه‌های جبران‌ناپذیرش غفلت کرد. امکانات دستگاه عدالت کیفری، پرهیز از ایجاد قلمروهای تبعیض‌آمیز و امکان سوءاستفاده در اجرای قانون، احتمال تضعیف قدرت اخلاقی حقوق کیفری، احتمال کاهش کارایی کیفرها، جرم‌زاییِ بالقوهٔ حقوق کیفری در پرتو فرایند برچسب‌زنی و ایجاد شرایط مجرمانه به واسطهٔ جرم‌انگاری برخی رفتارها و تطابق قانون کیفری با انتظارات عمومی و خواست اکثریت مردم، از جمله محدودیت‌های عملیِ توسعهٔ قلمرو حقوق کیفری‌اند که در جرم دانستن یک رفتار باید آن‌ها را مد نظر قرار داد. بی‌توجهی به این محدودیت‌ها و تکیهٔ صرف به توجیهات نظری و فلسفی در توسل به سازوکار جرم‌انگاری، می‌تواند حقوق کیفری را با چالش‌های جدی روبه‌رو سازد و مشروعیت، جایگاه و نقش آن را به پرسش بکشاند (حبیب‌زاده و زینالی، ۱۳۸۴: ش۳/۴۹). با این توصیف، اهمیت این حقیقت مشخص می‌گردد که خطرهای جدید ناشی از تحولات فناوری، اقتصادی و سیاسی، گونه‌هایی بسیار پیچیده‌تر از جرایم را رقم

1. Cryptography.
2. Steganography.

می‌زند و کارکرد حقوق کیفری را در صیانت از منافعِ حمایتی خود، دچار مشکل می‌سازد.

امنیت اطلاعات، یکی از دغدغه‌های مشترک شخصیت‌های حقیقی و حقوقیِ کاربر فضای سایبری است. کاربران اینترنت در هنگام استفاده از شبکه، اطلاعاتی حساس و مهم را بارها ارسال و دریافت می‌کنند. اطمینان از دسترسی نداشتن افراد غیر مجاز به اطلاعات حساس از جمله داده‌پیام‌های خصوصی، اطلاعات مربوط به اسرار امنیتی و مالی و پزشکی و... از مهم‌ترین چالش‌های امنیتی دربارهٔ حق محرمانگی اشخاص است (رضایی‌زاده و احمدی، ۱۳۸۸: ش۵۲/۴). متداول‌ترین و البته متحول‌ترین روش حفاظت اطلاعات، رمزکردن و پنهان‌نگاری آن‌هاست. پرسش اصلی این است که مرز «حق شهروندان برای دسترسی به اطلاعات» با «حق و تکلیف حکومت برای پیشگیری از انتقال اطلاعات مجرمانه»، به ویژه جرایم جاسوسی تجاری و افشای اسرار و اسناد مالی از طریق نقض حق محرمانگی شهروندان مظنون به ارتکاب جرایم مذکور، چگونه ترسیم‌پذیر است؟ در کنار این چالش‌ها به مجموعه‌ای دیگر از مباحث و چالش‌ها ـ به شرح آتی ـ نیز باید توجه داشته باشیم تا بتوانیم راهبردی مرجح را پیش نهیم.

سوی دیگر ماجرا، نسبتِ فهمِ از دین با دستاوردهای علوم مدرن است. آموزه‌های سنتیِ تفسیر از شریعت، در اغلب نظام‌های حقوقی دینی به دلیل ناتوانی در پاسخ‌گویی به نیازهای تازه، ناهمساز با دنیای مدرن تلقی شدند (El-Ansari, 2003: 507). این ناسازگاری، روشنفکران دینی را به تفسیرهایی جدید و منطبق با دنیای مدرن، سوق داده است. از سوی دیگر، اگرچه مدرنیته نافی هرگونه آموزهٔ متافیزیکی تلقی می‌شود، نمی‌توان منکر حضور دین و آموزه‌های دینی در جوامع مدرن و به ویژه در نظام حقوقی معاصر شد. در کشمکش میان سنت و مدرنیته در کشورهای در حال گذار همچون ایران، سنت‌گرایان کسانی‌اند که می‌کوشند دنیای مدرن را در قالب قواعد و منابع سنتی هضم کنند. نوگرایان نیز روشنفکرانی هستند که با پذیرش مبادی مدرنیته، پروژهٔ انتقال و بسط آن را در جوامع پیرامونی پی می‌گیرند.

با وجود این، هم جریان روشنفکری غرب‌گرا و هم روشنفکری سنت‌گرا، هر دو

افراطی و منحرف از مسیر صحیح برای بومی‌سازی الگوهای اجتماعی و حقوقی مدرنیته در کشورهای رو به مدرن شدن، مانند ایران، هستند (Quraishi, 2005: 49). به نظر می‌رسد آنچه را که مسیر صحیح برای ایجاد تحول در آموزه‌های اسلامی است، باید «احیاگرایی دینی» نامید. احیاگرایی مخالف متحول‌سازی نیست، بلکه جریان معقولِ برآمده از دل سنت است که با درک دنیای مدرن، به ویژه مدرنیسم حقوقی، در دفاع عقلانی از دین، سنت را در مدرنیته بازتولید می‌کند. نظام حقوقی ایران که در قلمرو مبانی، منابع و جلوه‌ها هم از شرع اسلام نشئت می‌گیرد و هم از منابع غربی و ملی، در اتخاذ راهبرد نسبت به موضوعات جدیدِ حقوق، نظیر حقوق کیفری فناوری اطلاعات که با وجود غربی بودنش، خاستگاه‌ها و مشرب‌های اسلامی در خصوص حریم خصوصی و جرایم مالی نیز دارد، ناگزیر از مدرنیزاسیون الگوی سنتی سیاست جنایی اسلامی است؛ چرا که بدون بازخوانیِ روزآمدِ نگرش فقهی در پرتو هنجارهای حقوق بین‌الملل و عرصهٔ عمومی بین‌المللی، هرگز نمی‌توان در پیشگیری و مجازات گونه‌های پیچیدهٔ جرایم نوظهور، به ویژه جرایم علیه محرمانگی تجارت الکترونیکی، موفق بود.

به موازات چالش مذکور در تفسیر روزآمدِ فقه جزایی و مشکلات ناشی از آن در ارتباط با مقولهٔ حمایت کیفری از حریم خصوصی، مشکلاتی نیز گریبان‌گیر حقوق و رویه‌های غربی در همین مقوله است. اگرچه نئولیبرالیسم به اقتضای ماهیت وجودی و اصول نظری‌اش، اعتقادی به جرم‌انگاری حداکثری ندارد (El-Gamal, 2006: 62)، اعتراضات ملت‌های غربی علیه دولت‌هایشان همراه با بحران‌های مالی و توسل به نظریه‌های ارعابی و سرکوبی حقوق کیفری در ادبیات معاصر دانش جرم‌شناسی، دولت‌های غربی را به ورطهٔ تضعیف آزادی و تقویتِ امنیت کشانده و نگرانی‌های مذکور را افزایش داده است. رویکرد نوین سیاست جنایی کشورهای غربی به «امنیت‌گرایی» و بالتبع، تشدید مداخلهٔ حقوق کیفری و مجریان قانون در زندگی خصوصی شهروندان، موجب ابهام در تفاوت‌های سیاسی و حقوقی میان امنیت داخلی و خارجی، جرم و جنگ، پیشگیری و سرکوب، و پلیس و سرویس‌های اطلاعاتی شده است.

پرسش اصلی این است که عوامل جدال میان آزادی‌گرایی، به مثابهٔ مهم‌ترین دستاورد مدرنیته که حقوق مدرن از آن حمایت می‌کند و امنیت‌گرایی، به مثابهٔ چالش بزرگ دولت‌ها و ملت‌های کنونی جهان، در پی شیوع تروریسم و دیگر بحران‌های جهانی ناقض صلح و امنیت بشری، چه پیامدهایی را بر تحول حقوق مدرن غربی و حقوقِ در حال تحول ایران دارد؟ به طور خاص، سیاست جنایی ایران و غرب چگونه می‌تواند میان «حق شهروندان به آزادی و محرمانگی اطلاعات» با «حق و تکلیفِ توأمانِ دولت‌ها به محدودسازی حق مذکور شهروندان، با هدف مبارزه با جرایم علیه امنیت (به ویژه امنیت سیاسی و مالی)» تعادلی حقوقی برقرار کند؟

این جستار با تحلیل دو مدل سیاست جنایی در قبال جرایم علیه محرمانگی تجارت الکترونیکی، به ویژه رمزنگاری و پنهان‌نگاری مجرمانه (مدل‌های جرم‌انگاری حداقلی [مدل سبز ـ آزادی‌گرا] و مدل جرم‌انگاری حداکثری [مدل قرمز ـ امنیت‌گرا]) توضیح می‌دهد که چگونه چالش‌های ناشی از تقابل بازخوانی تحول‌گرایانهٔ حقوق کیفری اسلامی با مدرنیتهٔ حقوق کیفری غربی، عامل سردرگمی سیاست جنایی ایران در پیشگیری و مجازاتِ جرایم مالی سنتی و جرایم مالی مدرن شده است. در این جستار می‌کوشیم امکان همگرایی و تعامل حقوقِ کیفری اسلامی و حقوق کیفری غربی را بررسی کنیم تا به برایندی برسیم که مزایای هر دو نظام حقوقی مذکور را در بر داشته باشد.

۱. دایرهٔ حمایت کیفری از رمزنگاری و پنهان‌نگاری اطلاعات در حقوق داخلی و نسبتِ آن با حمایت فقه جزایی از حریم خصوصی

رمزنگاری، دانش تغییر دادن متن پیام به کمک کلید دیجیتال و الگوریتم است. بنابراین تنها شخصی که از کلید و الگوریتم آگاه است، قادر به استخراج متن اصلی از متن رمزشده خواهد بود. در رمزنگاری، امنیت اطلاعات حفظ می‌شود، حتی اگر کانال‌های ارتباطی ناامن باشند.

پنهان‌نگاری، شاخه‌ای از علم مخفی‌سازی اطلاعات است. مخفی‌سازی اطلاعات، چندین شاخه از جمله رمزنگاری و ته‌نقش‌نگاری[1] دارد. به بیان دیگر، در رمزنگاری، خودِ پیام مهم است. در پنهان‌نگاری، خودِ ارتباط است که باید پنهان شود. به همین دلیل است که در رمزشکنی،[2] زمانی حمله موفقیت‌آمیز است که بتوان به تمام یا بخشی از محتوای پیام پی برد، ولی در پنهان‌شکنی،[3] زمانی حمله‌کننده موفق به اجرای حمله می‌شود که بتواند به وجود ارتباط یا پیام مخفی پی ببرد و یا به صورتی احتمالی، آن را آشکار سازد.

در این حوزه، به موارد زیر توجه می‌شود: وضع قوانین لازم برای حفظ امنیت جامعه؛ طراحی و به کارگیری سازوکارهای امنیتی و حفاظتی در فضای الکترونیکی؛ آموزش شهروندان برای مشارکت در ایجاد چنین امنیتی؛ استفادهٔ گسترده از دانش رمز، با هدف پاسداری از حقوق شهروندان. بدیهی است که استفادهٔ گسترده از دانش رمز، مستلزم وجود قوانین مدون در این باره است. در ضمن، با توجه به سند راهبردی نظام جامع فناوری اطلاعات و برنامهٔ راهبردی امنیت فضای تبادل اطلاعات، ضرورت حفظ امنیت ارتباطات و تبادل اطلاعات (الکترونیکی)، یکی از راهبردهای اساسی وزارت ارتباطات و فناوری اطلاعات به شمار می‌رود. بر این اساس، مواجههٔ نظام‌مند و برخورداری از توان بازدارندگی در مقابل تهدیدات فضای تبادل اطلاعات در کشور، نیازمند تبعیت از دستورالعمل‌های فنی و قوانین و مقررات حقوقی در این حوزه و همچنین ایجاد نظام‌های امنیت‌بخشی در سطح بالای مدیریتی کشور است. همچنین سند چشم‌انداز ۱۴۰۴، جایگاه جمهوری اسلامی ایران را جایگاه اول اقتصادی، علمی و فناوری در سطح منطقه معرفی می‌کند. بدیهی است دستیابی به این جایگاه (با توجه به شاخص جدید مطرح در توسعه‌یافتگی جوامع که همانا رشد فناوری اطلاعات است) مستلزم رشد سریع زیرساخت‌ها و در پی آن، ملزومات و خدمات در حوزهٔ فناوری اطلاعات است.

1. Watermarking.
2. Cryptanalysis.
3. Steganalysis.

همچنین باید توجه داشت که رعایت حقوق اجتماعی و حفظ صیانت فرهنگی و فنی کشور در قلمرو ارتباطات و کار با شبکه‌های اطلاع‌رسانی رایانه‌ای، وظیفهٔ نهاد یا سازمانی است که به طور قانونی مسئول ارائه، گسترش و پشتیبانی از این شبکه است. این وظیفهٔ مهم، ذیل عنوان «آیین‌نامهٔ نحوهٔ اخذ مجوز و ضوابط فنی تماس بین‌المللی» در انحصار دولت است. در واقع، شورای عالی اطلاع‌رسانی، وزارت اطلاعات و در مواردی بسیار خاص و محدود، سازمان صدا و سیما بخش‌هایی از نظام دولتی‌اند که در این باره، مسئولیت تجویز، راه‌اندازی و پشتیبانی این بستر ارتباطی را دارند.

گرچه در ایران با تصویب «قانون انتشار و دسترسی آزاد به اطلاعات» (مصوب ۶ بهمن ۱۳۸۷) بنیان‌های قانونی بهره‌مندی از این حق بنا نهاده شده است، اجرای آن با چالش‌هایی روبه‌رو گردیده است که ناشی از عدم شفافیت اداری و ناآگاهی است. علاوه بر این، قانون مزبور با تغییرات بسیار نسبت به لایحهٔ «آزادی اطلاعات» به تصویب رسیده است که اکثر این تغییرات در جهت عکس رویکردهای لازم، به عدم شفافیت قانون و تحدید اصل «دقیق بودن استثنائات» (انصاری، ۱۳۸۷: ۵۰) و سلیقه‌ای و بی‌روش شدن اجرای قانون انجامیده است. از جمله ابهامات مواد ۱۳ تا ۱۷ قانون و حذف مواد مرتبط با هزینه‌های اجرایی، روش‌های دسترسی، فقدان اطلاعات، تکرار درخواست، تعیین واحد اطلاع‌رسانی و آموزش در لایحهٔ دولت، عملاً قانون مزبور را بی‌اثر نموده است.

روش بحث در تحلیل حقوق کیفری اسلامی، اقتصاد اسلامی و دیگر علوم اسلامی، همان روش بحث علمی اسلامی است که عبارت است از روش ملاحظهٔ توافق و تکامل میان تمامی منابع معرفت. این شیوه برعکس روش تحول علم در غرب است و نشان از غنای علوم اسلامی و محدود نبودن آن‌ها به علوم عقلی دارد (Bantekas, 2009: 662). حقوق کیفری اسلامی، پشتوانه و تضمینِ هنجارهای اقتصاد اسلامی است؛ اقتصادی که محدود به عقلانیت ابزاری نیست و محور اصلی آن، همان اندیشه‌ای است که هابرماس، بزرگ‌ترین فیلسوف و جامعه‌شناس معاصر آلمانی، آن را «نظریهٔ عقل ارتباطی» می‌نامد (c.f: Habermas: 2004). عقلانیت در

مفاد اقتصاد اسلامی جنبهٔ غیر ابزارگرا (تعاملی انسان‌مدار) دارد، در حالی که در مبنای اندیشهٔ ارتدوکس، فایده‌گرایی که نتیجهٔ عقلانیت ابزاری است، کارسازترین پیش‌فرض اقتصادی است.

بدون تمسک به متافیزیکِ اسلامی، چیزی به نام علم اقتصاد اسلامی تصورشدنی نخواهد بود. متأسفانه برخی روشنفکران دینی به دلیل بی‌توجهی به مبانی ایدئولوژیک جهان‌بینیِ حاکم بر نظریهٔ اقتصادی نئوکلاسیکی، چارچوب مکتب نئوکلاسیک را وام گرفته و باعث افول نظریهٔ اقتصاد اسلامی شده‌اند (El-Ansari, 2003: 504). اقتصاد پوزیتیویستی آن‌ها از «آنچه هست» صحبت می‌کند و وارد اظهارنظرهای اخلاقی و ارزشی نمی‌شود، ولی روشن است که هیچ نظریهٔ علمی، بدون ارزش‌گذاری ممکن نیست و خودِ بی‌طرفی اخلاقی هم حقیقتاً مؤید موضع اخلاقی سکولار است (امیرارجمند و همتی، ۱۳۸۶: ش۳۹/۲۳). این نقص را طیف دیگری از متفکران فلسفهٔ اقتصاد اسلامی تا حدودی جبران کرده‌اند؛ از این طریق، تبیینی پساپوزیتیویستی از اقتصاد اسلامی ارائه می‌دهند. بروز این نوع پساپوزیتیویسم در عرصهٔ حقوق کیفری اقتصادی، به شکل پیروی از رئالیسم انتقادی و انفسی‌گرایی تعدیل یافته است که بر چندجانبه‌گراییِ انتقادی استوار است (Saleem, 2010: 290).

بدین‌سان به نظر می‌رسد نه این صحیح است که ماهیت دستاوردهای علمی غربی را فقط پوزیتیویستی بدانیم و نه اینکه علوم اسلامی بالفعل در جهان را نهایتِ آنچه اسلام می‌تواند به بشر عرضه کند، بدانیم. قوی‌ترین نقدها به غرب، برخاسته از جریان‌های فلسفی غربی، نظیر نظریهٔ انتقادی مکتب فرانکفورت در آثار هابرماس، مارکوزه و گادامر است. همچنان که نظریه‌های کنونی اقتصاد اسلامی و حقوق کیفری اسلامی نیز تنها بخشی کوچک از پتانسیل بالقوهٔ حقوق اسلام است. مطلوب، آن است که با تلفیق عناصر مثبتِ حقوق مدرن غربی و عناصر قابل به‌روزرسانی حقوق کیفری اسلامی بتوان راهبردی جامع طراحی کرد که دستاورد آن، تقویت عقل‌گراییِ شیعی در تفسیر نصوص فقه جزایی و کاربرد این عقلانیتِ دینی در نظام حقوقی ایران با توجه به اقتضائات جامعه‌شناسی جنایی ایرانی (گونه‌شناسی جرایم و مجرمان در ایران یا بوم‌شناسی جنایی ملی) است.

۲. رمزنگاری اطلاعات، آزادی‌گرایی یا امنیت‌گرایی کیفری؟ چالش سیاست جنایی ایران اسلامی و غربِ در حال گذار از دموکراسی لیبرال به دموکراسی توتالیتر

سیاست جنایی، علاوه بر قواعد حقوقی، عملکرد نهادهایی مختلف را نیز در بر می‌گیرد که اجرای قواعد مزبور را به عهده دارند. این نهادها عبارتند از: پلیس، دادسراها، دادگاه‌ها، ادارهٔ زندان‌ها، ادارهٔ آموزش و تربیت مراقبتی مجرمان، نهادهای پیشگیری از جرم و ادارات خدمات اجتماعی. بنابراین، مجموعه‌ای از فعالیت‌های نهادی (رسمی) وجود دارد که شناخت آن‌ها از طریق جامعه‌شناسی کیفری امکان‌پذیر است و همچون خودِ قانون جزء سیاست جنایی قرار می‌گیرند. شیوهٔ عملکرد نهادها وقواعد حقوقی، نظام عدالت جنایی و نظام کیفری با هم ترکیب می‌شوند و ساختاری به نام «نظام سیاست جنایی» شکل می‌گیرد.

دلماس مارتی، نظریه‌پرداز شهیر فرانسوی در عرصهٔ سیاست جنایی، معتقد است که مهم‌ترین ابهام، به موجّه ساختن اِعمال مجازات کیفری از رهگذر جدال میان رویکرد امنیت‌گرا و رویکرد حقوق‌بشری مربوط است، به نحوی که کارکرد «ابزاری» حقوق کیفری (ضعف همکاری بین‌المللی و مبارزه با بی‌کیفرمانی) را با کارکرد «نمادین» آن (تمایل به تحکیم و حمایت از ارزش‌های بنیادیِ حقوق بشری) در هم می‌آمیزد (دلماس مارتی، ۱۳۸۵: ۸۵).

از این رو باید به نگرانی‌های جامعهٔ بشری در قبال گذار از دموکراسی لیبرال به دموکراسی توتالیتر، خصوصاً در غرب توجه نمود. گرچه روند همگانی شدن دموکراسی راه را برای دموکراسی‌های لیبرال معاصر هموار کرد، موقعیت‌های مورد نیاز برای ظهور و رشد توتالیتاریسم را نیز در اختیار نهاد (Prajer, 1985: 49). شرایط حیات سیاسی در دموکراسی‌های غربی نه تنها نامساعد است که ناخرسندی‌هایی فزاینده و نشانه‌هایی آشکار از زوال خطرناک ارزش‌های دموکراتیک نیز در آن دیده می‌شود. با آنکه اروپا بر قدرت نرم یا مزیت هنجاری، و آمریکا بر قدرت سخت یا مزیت نظامی تکیه می‌کند (سعیدی، ۱۳۹۱: ش۱۶۴/۲۸۷)، جامعهٔ دموکراتیک نقطهٔ اتکایی

ندارد تا بتواند اصول و شاخص‌های نظم اجتماعیِ به نظر تغییرناپذیر را ترسیم کند. از این رو، مشروعیت نظم اجتماع مورد سؤال است. علت‌های اجتماعی به خود اجتماع احاله می‌شوند، لذا جامعه در افق عالم بشریت فهمیده می‌شود. این چنین است که به مدد دموکراسی، جامعه‌ای بر پایهٔ «اصل بلاتکلیفی» ایجاد می‌شود و از این رو دائماً مفهوم دموکراسی زیر سؤال می‌رود و کوشش می‌شود از نو و بهتر فهمیده شود. در نهایت، دموکراسی در جامعه‌ای مطرح می‌شود که در آن قدرت، قانون و معرفت، همواره در معرض آزمون ناشی از تردید و «بلاتکلیفیِ ریشه‌ای» هستند.

در چنین وضعیت گریزناپذیری، دموکراسی، توتالیتاریسم را جواب ممکن به این شرایط استثنایی می‌داند؛ جامعهٔ مدرن به تحجری توتالیتاریسم تن می‌دهد که از طریق آن بتواند برای حذف این تردیدها و بلاتکلیفی‌ها و تقسیم‌بندی جامعه، راه حل تخیلی بیابد. توتالیتاریسم پس از آنکه جامعهٔ مرجعِ یک نظمِ برین را حذف کرد، سعی می‌کند بنیاد بی‌قید و شرط جدیدی را ایجاد کند که نتیجهٔ قطعی آن، بستن راه اجتماع بر روی خود است. توتالیتاریسم می‌کوشد قدرت و جامعه را با حذف تمام نشانه‌های تقسیم‌بندی‌های درونی و با محو تردید و بلاتکلیفی‌ای که تجربهٔ تحجر دموکراتیک را عذاب می‌دهد، به هم جوش دهد (پیرلوگوف، ۱۳۸۶: ۹۵). پس نمی‌توان مدرنیزاسیون را صرفاً مرحلهٔ تکاملی ایدئولوژی بورژوازی دانست. ویژگی مدرنیزاسیون، به افراط کشیدن خصلت‌های مفهوم دموکراسی است، نه نگریستن با عینک توتالیتر و با هدف پوشاندن تردید و بلاتکلیفی از طریق بیان قاطع؛ بلکه برعکس، با تأکید گذاشتن بر بلاتکلیفی تا نقطه‌ای که معنادار بودن دموکراسی از بین برود (همان: ۹۷).

پیش‌شرط ضروری انجام معاملات الکترونیکی، حفظ امنیت اطلاعات مربوط به حساب‌ها و رمزهای عبور اشخاص به منظور جلوگیری از سوءاستفادهٔ نفوذگران است. امنیت اطلاعات به معنای همهٔ ابزارها و عملکردهایی است که «دسترس‌پذیری دائمی»، «محرمانگی» و «تمامیت اطلاعات» یا ارتباطات را تضمین می‌کند و با روش‌ها و عملکردهایی که کارکرد صحیح اطلاعات را تضمین می‌کنند، متفاوت است. این امنیت، روش‌های رمزنگاری و رمزگشایی و پنهان‌نگاری و پنهان‌شکنی را در بر می‌گیرد

و دسترسی به اطلاعات صحیح و نفوذناپذیر را ممکن می‌سازد (Smith, 2002: 619).

بی‌شک حق محرمانگی اطلاعات، حفاظت از اطلاعات را می‌طلبد. پیوند میان حق بر افشا نشدن اطلاعات شخصی ـ از جمله، داده‌پیام‌های تجاری الکترونیکی ـ با حفاظت اطلاعات، در گرو شناخت مبانی این حق است. اولین مبنای حق دسترسی به اطلاعات تجاری الکترونیکی، حق آزادی اطلاعات و آزادی بیان است (انصاری، ۱۳۸۷: ۱۸). گونه‌های غیر مجازِ رمزنگاری و پنهان‌نگاری، ناقضِ حق دسترسی به اطلاعات است. آزادی اطلاعات دیگر آزادی منفی نیست، بلکه دولت‌ها موظفند استفاده از رسانه‌های گروهی و ابزارهای تضمین روایی محتویات نوشتاری، صوتی و تصویری این رسانه‌ها را برای ملت فراهم آورند. رمزنگاری و پنهان‌نگاری از جملهٔ این ابزارهاست که منع دولتی آن مصداق بارز نقض حق حفاظت اطلاعات، حق محرمانگی، حق بر اصالت اطلاعات و حق دسترسی به اطلاعات است. سیاست جنایی قرمز (منع کامل رمزنگاری و پنهان‌نگاری و ورود به داده‌پیام‌های ترافیک‌شدهٔ رمزشده و پنهان‌شدهٔ تجار کاربر اینترنت) که شرح آن می‌آید، تجلی نقض حقوق بشر در این زمینه است.

فهم نحوهٔ تمشیت و تحول سیاست جنایی در ایران همانند دیگر کشورها، در چارچوب تحولات جهانی سیاست جنایی درک‌شدنی است. از این رو، نقد سیاست جنایی ایران در قبال تعیین حدود قانون‌مندیِ رمزنگاری و پنهان‌نگاری، ضرورتی است که پس از بررسی از توصیف و تحلیل گفتمان‌های سیاست جنایی معاصر باید به عمل آید. شناخت دو گفتمان امنیت‌محور و حقوق بشرمدار، از این حیث ضروری است.

در حالی که ایدئولوژی بازپروری از راه آمیختن نظام پیشگیری و نظام پاسخ‌دهی به جرایم و انحرافات خطیر، بر آن است تا راه‌ها و نهادهای مبارزه با بزه و انحراف را مدیریت کند و الگویی مشارکتی از سیاست جنایی به دست بدهد، ایدئولوژی امنیت‌گرا با تکیه بر فرمول سنّتی «جرم، دولت و سرکوب» و بزرگ‌نمایی احساس عدم امنیت، به شدّتِ عملِ[1] کیفری روی آورده است و به

1. Punitivity.

اذهان شهروندان چنین القا می‌کند که بزهکاران در کمین نشسته‌اند و در صورت سرکوب نشدن، نسل شهروندان را تباه خواهند کرد.

گرایش شدیدتر به «امنیت» و «پیشگیری» و بالتبع، مداخله‌های حقوق کیفری پیش از تحقق جرم را می‌توان یکی از ویژگی‌های سیاست جنایی در عصر «دولت مدرن» دانست؛ به گونه‌ای که از میان رفتن تفاوت‌های سیاسی و حقوقی میان امنیت داخلی و امنیت خارجی، جرم و جنگ، پیشگیری و سرکوب، پلیس و سرویس‌های اطلاعاتی و نیز سرویس‌های اطلاعاتی و نیروهای نظامی، به تازگی رشتهٔ پیچیده و چندسطحی «حقوق امنیت» را تأسیس کرده است که بیش از هر چیز، خطرزدایی را هدف قرار می‌دهد و حقوق کیفری سنتی در آن، فقط نقشی محدود و فرعی را عهده‌دار است (صدر توحیدخانه، ۱۳۸۸: ۴۶۶).

تأکید بر پیش‌بینی جرم و تکرار جرم بر پایهٔ مدل آماری و مدل بالینی پیش‌بینی و نیز دغدغهٔ کنترل و مراقبت اجتماعی ـ قضایی ـ پلیسی نامحدود (به ویژه نسبت به بزهکاران خطرناک)، نگهداری و نظارت الکترونیکی سیار آن‌ها و اقدام‌های نظارتی پساکیفری موجب شده است تا مدلِ دولتِ اقتدارگرای فراگیر از میان انواع مدل‌های سیاست جنایی (مدل جامعهٔ لیبرال، مدل جامعهٔ آنارشیست و...)، مالکِ گفتمانِ معاصر جرم‌شناسی در سراسر جهان شود و رفته رفته، هژمونی و برتریِ زورمندانهٔ پارادایم امنیت‌گرا را بر پارادایم آزادی‌گرا که طرف‌دار جرم‌انگاریِ حداقلی است، شکل دهد.

۳. آثار سیاست جنایی جرم‌انگارِ حداکثری و حداقلی در قبال جرایم رمزنگاری و پنهان‌نگاری

مرتکبان جرایم هوشمند در حوزه‌های مختلف و به روش‌های گوناگون می‌توانند از رمزنگاری استفاده کنند؛ برای مثال، در جرایم سازمان‌یافته، از آنجا که اجزای مختلف این سازمان‌ها نیاز به تبادل وسیع اطلاعات (از نوع داده، مکالمات تلفنی و...) برای هماهنگی در برنامه‌های خود دارند، معمولاً ارتباطاتشان در بستر

شبکه‌های ارتباطی عمومی ولی به شکل محرمانه رمز شده است. همچنین این افراد اسناد و مدارک خود را به صورت رمزشده نگهداری می‌کنند تا در صورت دستگیری و یا بازپرسی، این اطلاعات به راحتی در دسترس نباشند. در حوزهٔ جرایم هوشمند اقتصادی و مالیاتی هم چنین است. در این حوزه، مجرمانی که برای رهایی از مالیات و... حساب دومی دارند که از آن اصطلاحاً به حساب سیاه[1] یاد می‌شود و باید مخفی بماند، لازم است از ابزارهایی مفید و مؤثر برای مخفی کردن عملیات این حساب استفاده کنند. این ابزارها در واقع الگوریتم‌های رمزنگاری هستند (بوخمان، ۱۳۸۲: ۸۳). به این ترتیب، اکثر مجرمان در حوزهٔ جرایم رایانه‌ای هوشمند به کمک دانشی که در حوزهٔ فناوری‌های مدرن دارند، معمولاً از رمزنگاری برای پنهان کردن فعالیت‌های خود بهره می‌جویند. کلاهبرداری‌های رایانه‌ای معمولاً در فایل‌های رمزشده مخفی می‌شوند و سازندگان ویروس‌ها معمولاً برای پایدارسازی و ایجاد ابهام در ویروس‌هایشان از روش‌های رمزنگاری استفاده می‌کنند.

به این ترتیب در بسیاری مواقع، در جریان تجسس و یا رسیدگی به جرایم و اتهامات، دسترسی به اطلاعات الکترونیکی دیجیتال یا آنالوگ مورد نیاز است. این اطلاعات که یا در یک حافظه ذخیره شده‌اند و یا در حال تبادل در یک بستر ارتباطی‌اند، در هر دو حالت می‌توانند رمزشده باشند. برای تحلیل اطلاعات رمزشده و کشف آن‌ها (در هر یک از دو حالت یادشده) روش‌هایی وجود دارد؛ برای مثال، در خصوص دسترسی به اطلاعات در حال تبادل، روش‌های شنود[2] و تحلیل ترافیک[3] پیشنهاد می‌گردد که اولی برای دسترسی به خود اطلاعات و دومی برای تحلیل روی کیفیت و رفتار اطلاعات (و نه خود اطلاعات) در جهت استحصال نتایج مورد نظر به کار گرفته می‌شود. بر اساس قوانین بسیاری از کشورها، کاربران موظفند شبکهٔ خود را قابل شنود کنند تا در موارد قانونی این کار انجام شود. همچنین، در خصوص روش‌های مفید برای دسترسی به اطلاعات ذخیره‌شده روی

1. Black account.
2. Tapping.
3. Traffic analysis.

حافظه، به روش جستجو و توقیف[1] می‌توان اشاره کرد.

به هر حال اگرچه استفاده از روش‌های مختلف رمزنگاری در کاربردهای مختلفِ مجرمان، روند رسیدگی و تجسس را با تأخیر یا سردرگمی روبه‌رو می‌کند، معمولاً در کنار استفاده از رمزنگاری توسط مجرمان، شواهد دیگری نیز مبنی بر وقوع جرم و یا آغاز اقدامی مجرمانه وجود دارد که از این شواهد می‌توان به استفاده از رمزنگاری جهت مقاصد مجرمانه پی برد و ابهام‌ها و یا تأخیرهای مذکور را تا حد زیادی بی‌اثر کرد. در این حالت، با توجه به شواهد و پی بردن به مجرمیت افراد، باید آن‌ها را مجبور به دادن اطلاعات دربارهٔ تجهیزات استفاده‌شدهٔ رمزنگاری کرد تا با رمزگشایی این اطلاعات، جوانب نهان جرم نیز مشخص گردد. البته در اینجا باید اشاره کرد که اگر مجرمی با الگوریتم OTP[2] آشنا باشد، به راحتی می‌تواند هر متن اصلی دلخواهی را به مستندات رمزشده‌اش نسبت دهد و ادعای خود را برای مراجع ذی‌صلاح به اثبات برساند.

از آنجا که معمولاً اعمال مجرمانه نیازمند تمهیدات و مرور زمان هستند، می‌توان با روش‌های یادشدهٔ بالا و در یک بازهٔ زمانی، اهتمام به جمع‌آوری اطلاعات مختلف (و از جمله رمزشده) نمود. این امر در مواردی رمزگشایی اطلاعات را آسان‌تر می‌کند. همچنین از آنجا که اجرای این روش‌ها (خصوصاً روش تحلیل ترافیک) نیاز به برخورداری از مرکز جمع‌آوری اطلاعات دارد، ایجاد مراکز قوی جمع‌آوری اطلاعات به شدت توصیه می‌گردد. علاوه بر آن، توسعه و بازنگری روش‌های شنود نیز بسیار مؤثر است.

به این ترتیب روشن است که معمولاً جرایم رمزنگاری تنها بخشی از حوزهٔ جرایم رایانه‌ای محسوب می‌شوند. در بخش قابل توجهی از مستنداتِ مطالعه‌شده در این پروژه هم تعریف دقیقی برای جرایم رمزنگاری یافت نشد، اما با در نظر گرفتن تعریفی که معمولاً برای جرایم رایانه‌ای یا هوشمند ارائه می‌شود، می‌توان اصطلاح جرایم رمزنگاری را به هرگونه استفادهٔ مجرمانه از تجهیزات رمزنگاری اطلاق کرد.

1. Search & seizure.
2. One time pad.

برخی موارد از این‌گونه جرایم عبارتند از: ۱. استفاده از رمزنگاری برای مخفی کردن اطلاعاتی از یک عمل و یا نقشهٔ مجرمانه؛ ۲. استفاده از روش‌های غیر استاندارد رمزنگاری در شرایطی که قانون‌گذار روش‌های استاندارد و مشخصی را بدین منظور پیش‌بینی کرده است.

حقوق اروپایی در سیاست‌گذاری جنایی در قبال رمزنگاری اطلاعات، دستاوردهای قابل توجهی دارد؛ برای مثال، بخش قابل توجهی از «قانون اعتمادسازی در اقتصاد دیجیتالی» مصوب سال ۲۰۰۴ فرانسه تحت عنوان «ابزارهای خدمات رمزنگاری» به ابعاد تأمین و ارتقای امنیت در اقتصاد دیجیتالی در مواد ۲۹ به بعد اختصاص دارد و در ادامهٔ گرایش مقنّن به آزادسازی عملیات رمزنگاریِ آغازشده با قانون مورخ ۲۹ دسامبر ۱۹۹۰ تلقی می‌شود. پس از آنکه حقوق فرانسه در اعطای تسهیلات دسترسی اشخاص حقوقی خصوصی به فناوری رمزنگاری، نمونه شد، قانون ۲۹ دسامبر ۱۹۹۰ به شکل پیچیده‌ای خدمات و ابزارهای رمزنگاری را از هم تفکیک کرد. مادهٔ ۳۰ قانون اعتمادسازی در اقتصاد دیجیتالی فرانسه بدون هیچ ابهامی اعلام داشت: «استفاده از ابزارهای رمزنگاری آزاد است». همین آزادی در عرصهٔ انتقال، صادرات و واردات ابزارهای رمزنگاری که فقط کارکردهای تأیید اصالت و کنترل تمامیت را تأمین می‌کند، اعطا شده است. به علاوه، مجازات‌هایی در قبال رعایت نکردن قواعد اداریِ ساخت و استفاده از سخت‌افزارها و نرم‌افزارهای رمزکننده نیز در قانون مذکور مقرر شد که حداکثر دو سال حبس و سی هزار یورو جزای نقدی، از آن جمله است (دُبِلفون، ۱۳۸۸: ۱۷۵).

در اتخاذ سیاست جنایی سنجیده در قبال رمزنگاری باید به اهمیت مسئلهٔ برقراری تعادل میان منافع متعارض، توجه وافری داشت. با توجه به آنچه دربارهٔ ابعاد امنیتی و حقوقیِ رمزنگاریِ اطلاعات بیان شد، می‌توان گفت که افراد، سازمان‌ها و دولت هر کدام در حوزهٔ رمزنگاری، نیازها، منافع و علاقه‌مندی‌های خاص خود را دارند؛ برای مثال، مهم‌ترین نیاز افراد حفظ حریم خصوصی آن‌ها و از نیازهای مهم دولت‌ها دسترسی قانونی به کلیدهای رمزنگاری در مواقع لزوم است (پژوهشکدهٔ امنیت اطلاعات و ارتباطات، ۱۳۸۷: ۲۲). از میان این نیازمندی‌ها و منافع، برخی به نظر متضاد و

متناقض می‌نُمایند. در ادامه، به برخی از این منافع متعارض اشاره می‌شود:

۱. کاربران در رمز نمودن اطلاعات شخصی خود آزادند تا از آن‌ها در برابر دسترسی‌های غیر قانونی و فعالیت‌های مجرمانه‌ای که می‌تواند به آن‌ها ضرری برساند، محافظت کنند. کاربران همچنین توقع دارند در صورت مواجهه با فعالیت‌های مجرمانه، پلیس، قدرت و ابزار کافی برای رمزگشایی اطلاعات را داشته باشد تا بتواند مدارک و اطلاعاتی کافی علیه مجرمان جمع‌آوری کند.

۲. کاربران می‌خواهند اطلاعات رمزشده‌شان به اندازهٔ کافی امن و دور از دسترس باشد. همچنین آن‌ها می‌خواهند در صورت گم شدن کلید رمزگشایی این اطلاعات، بتوانند به کمک مرجع قابل اعتمادی، اطلاعات خود را بازیابی کنند. بنابراین کلیدها باید در جایی امن مثلاً TTP نگهداری شوند. نهادهای اجرای قانون نیز می‌خواهند به این مراجع قابل اعتمادِ ذخیرهٔ کلیدها دسترسی داشته باشند تا بتوانند در صورت لزوم، مکالمات افراد را شنود نمایند.

۳. کاربران نیاز دارند هنگامی که کلیدهای خصوصی‌شان را در جایی به امانت می‌سپارند، حتی‌الامکان امن و کنترل‌شدنی باشند. در صورتی که این امر از کنترل آن‌ها خارج شود، اعتماد کاربران به مخابرهٔ اطلاعات در چنین محیطی به شدت کاهش می‌یابد.

۴. استفادهٔ همگانی از رمزنگاری اطلاعات و گسترش روزافزون آن به منظور حفظ محرمانگی اطلاعات و پیام‌ها باعث شده است تا جلوگیری و کاهش برخی اعمال مجرمانه، همانند کلاهبرداری‌های اقتصادی و مالیاتی نیز بسیار مشکل‌تر شود.

۵. یکی از علاقه‌مندی‌های نهادهای اجرای قانون این است که کاربران بتوانند از روش‌های رمزنگاری قوی استفاده نمایند. در این صورت، از بسیاری از اعمال مجرمانه، خودبه‌خود جلوگیری می‌شود. ولی از طرف دیگر، یکی دیگر از علاقه‌مندی‌های نهادهای اجرای قانون در اختیار داشتن مجوزِ دسترسی به کلیدهای خصوصی افراد جهت بازرسی و نظارت بر اعمال مجرمانهٔ احتمالی است.

۶. رمزنگاری از نظر کاربران یک فناوری همانند فناوری‌های دیگر است. بنابراین، کاربران اعمال هیچ‌گونه محدودیتی را در استفاده از این فناوری

برنمی‌تابند. اما از نظر دولت، محصولات رمزنگاری، کالاهایی دو وجهی[1] هستند که می‌توانند علاوه بر کاربردهای معمول، کاربرد نظامی نیز داشته باشند. بنابراین به منظور مقابله با تروریسم و تهدیدات امنیت ملی باید تحت کنترل و اعمال محدودیت قرار گیرند.

همان‌طور که مشاهده می‌شود، تعارض‌های زیادی بین نیازها و علاقه‌مندی‌های کاربران شخصی و نیازها و علاقه‌مندی دولت‌ها به منظور اجرای قانون و جلوگیری از اعمال مجرمانه وجود دارد. در صورتی که تنها علاقه‌مندی‌های کاربران در نظر گرفته شود، مسلماً همانند هر فناوری دیگر، رمزنگاری نیز می‌تواند در معرض سوءاستفادهٔ مجرمان قرار گیرد و حتی باعث تهدید امنیت ملی کشور شود. همچنین اگر هدف، تنها حفظ حقوق دولت‌ها باشد، ساده‌ترین راه تسلط و دسترسی کامل دولت به جزئی‌ترین اطلاعات شخصی کاربران است که این امر یکی از مهم‌ترین و مقدماتی‌ترین حقوق انسانی یعنی حفظ حریم خصوصی را زیر پا می‌نهد و چه بسا در صورت صلاحیت نداشتن عوامل دولتی، زمینه برای سوءاستفاده از این اطلاعات شخصی فراهم گردد. بنابراین واضح است که برقراری تعادل مناسب بین دو مقولهٔ فوق، بهترین راه حل مسئله است. در برقراری این تعادل، باید حد و مرز اختیارات و وظایف دولت‌ها در دسترسی به اطلاعات شخصی کاربران از یک سو و میزان و نحوهٔ استفادهٔ مجاز افراد از فناوری رمزنگاری از سوی دیگر، کاملاً مشخص شود. این مهم، از طریق تدوین سیاست‌ها، وضع قوانین و ضوابطِ استفاده از رمزنگاری در کشور محقق خواهد شد.

بررسی‌ها حول حقوق موضوعهٔ کشورهای شاخص از دو جهت قدرت و ضعف زیرساخت‌های فنی مخابراتی، و پیشرفتگی حقوقی نشان می‌دهد که کشورها بر اساس میزان محدودیت و نظارتی که قوانین مربوط به تولید، توزیع، توسعه، استفاده و صادرات و واردات انواع محصولات رمزنگاری و پنهان‌نگاری در آن‌ها اِعمال می‌کنند، به سه گروه اصلی سبز، زرد و قرمز تقسیم می‌شوند:

---

1. Dual-use goods.

مدل سبز: شامل کشورهایی که سیاست کاملاً آزادانه‌ای را در تولید، توزیع، توسعه، استفاده، صادرات و واردات محصولات رمزنگاری و پنهان‌نگاری در پیش گرفته‌اند و ممنوعیت و محدودیت خاصی در هیچ یک از این زمینه‌ها ندارند (سویس و فرانسه).

مدل زرد: شامل کشورهایی که قوانین آن‌ها نظارت خاصی در یک یا چند زمینه از امور مذکور نسبت به محصولات رمزنگاری اعمال می‌کنند و خود را ملزم به پیروی از برخی قوانین سخت‌گیرانه می‌دانند (مانند آفریقای جنوبی).

مدل قرمز: شامل کشورهایی که نظارت‌های همه‌جانبه بر امور مذکور دارند (مانند چین و رژیم صهیونیستی).

برای برقراری موازنه میان رعایت و تضمین رعایت حقوق شهروندی کاربران سامانه‌های الکترونیکی (با تأکید بر سیاست جنایی حداقلی و آزادی‌گرا) و امنیت‌گرایی (مبارزه با تروریسم سایبری اعم از حمله‌های خُرد و کلان به امنیت تجارت الکترونیکی) و نهایتاً پیشنهاد راهکارهای جامع و منطبق با الگوی هزینه ـ فایده در زمینهٔ میزان محدودیت و نظارت بر تولید، توزیع، توسعه، استفاده، صادرات و واردات محصولات رمزنگاری و پنهان‌نگاری، ابتدا باید مزایا، معایب، ملزومات فنی و مدیریتی و دستاوردهای حاصل از قرارگیری در هر یک از گروه کشورهای سبز و قرمز را درک کرد. نتایج می‌تواند به طراحی و اصلاح سیاست جنایی مبارزه با جرایم سایبر توسط تصمیم‌سازان در کشورهایی که رویکرد تیمی و بین رشته‌ای دارند، کمک کند. بحث بر رمزنگاری و پنهان‌نگاری غیر قانونی متمرکز است.

پیامدهای مخابراتی، جرم‌شناختی و حقوق بشری مدل قرمز (جرم‌انگاری حداکثری)

در کشورهای پیرو سیاست جنایی قرمز، هر شهروند برای استفاده از سرویس‌های امنیتی مذکور در حالت‌های غیر استاندارد، باید مجوز قانونی بگیرد. از یک طرف، اخذ این مجوز منوط به افشای جزئیات و ویژگی‌های دقیق الگوریتم‌های استفاده‌شده در کاربرد مورد نظر آن شهروند و گاه حتی تشریح علل و انگیزه‌های

به کارگیری این سرویس‌هاست. روشن است که این سیاست به شدت با حفظ حریم خصوصی شهروندان در تعارض است.

تلقی منفی عموم شهروندان از قانون‌گرایی، ایراد دیگر این رویکرد است. اتخاذ سیاست‌های تقنینیِ سخت‌گیرانه و انقباضی بر هر یک از امور اجتماعی، شکاف میان ملت و حاکمیت را عمیق می‌کند. تلقی شهروندان از نگاه سخت‌گیرانه به استفاده از سرویس‌های رمزنگاری و پنهان‌نگاری، بیش از هر چیز این خواهد بود که در وهلهٔ اول، مجرمان سایبری از این سرویس‌های امنیتی استفاده می‌کنند (Higgins, 2005: 178). به همین دلیل قانون‌گذاران به خود حق می‌دهند ضوابط سخت‌گیرانه‌ای را در ارائهٔ این سرویس‌ها در نظر بگیرند. این در حالی است که مجرمان سازمان‌یافته هرگز در به کارگیری محصولات رمزنگاری و پنهان‌نگاری، دغدغهٔ رعایت قوانینِ موجود را ندارند؛ خواه این قوانین سبز باشند و خواه قرمز.

ایراد سوم، منع استفادهٔ کاربران از برخی سرویس‌های ضروری است که باعث ناخشنودیِ آنان می‌گردد. تجربه نشان داده است که کاربران همیشه گرایشی ناخودآگاه به سوی استفاده از محصولات و سرویس‌های ممنوع و غیر مجاز دارند. این حساسیت، به ویژه دربارهٔ سرویس‌ها و محصولاتی اهمیت می‌یابد که نیاز به استفاده از آن‌ها بیشتر احساس می‌شود (Kennedy, 2002: 277). با توجه به لزوم استفادهٔ شهروندان از رمزنگاری برای حفظ حریم خصوصی و اطلاعات شخصی آن‌ها، این تهدید جدی کاملاً احساس می‌شود که در صورت تحمیل هرگونه محدودیت غیر ضروری بر چنین استفاده‌ای، کاربران رو به استفادهٔ غیر مجاز از چنین سرویس‌هایی بیاورند و توان کنترلی نهادهای رسمی و غیر رسمی در وقوع جرم و پیشگیری از جرایم سایبری مرتبط، بسیار کاهش یابد؛ زیرا به دلیل استقبال گسترده از چنین سرویس‌هایی، طیف وسیعی از کاربران را باید مجرم محسوب کرد. چنین عملکردی سیاست کیفری امنیت‌گرا به شمار می‌رود که هم مغایر اصل برائت و هم اجرانشدنی است؛ زیرا سخت‌افزار و زیرساخت فنی و نیروی انسانی کافی برای انجام نظارت الکترونیکی با این حجم وسیع وجود ندارد.

همچنین باید در نظر داشت که رویکرد قرمز توان بازدارندگی مجرمان

سازمان‌یافته را ندارد که می‌توان آن را ایراد چهارم بر رویکرد قرمز دانست. یکی از اهداف اصلی موافقانِ رویکرد قرمز در تدوین ضوابط صادرات و واردات محصولات رمزنگاری و نهان‌نگاری، تصویب قوانین مبارزه با جرایم علیه امنیت الکترونیکی و پیشگیری از سوءاستفادهٔ آن‌ها از ابزارهای رمزنگاری و پنهان‌نگاری و نیز کاهش فرصت‌های مجرمانه است؛ امری که در چارچوب نظریهٔ جرم‌شناختیِ فرصت، درک می‌شود. با وجود این، این‌گونه مجرمان با دور زدن محدودیت‌های شبکه‌ای کنترل‌کننده، از روزنه‌های گریزناپذیر اجرای این گونه مقررات می‌گریزند. آن‌ها با طراحی زیرزمینی الگوریتم‌های مورد نیاز خود و یا قاچاق غیر قانونی و غیر قابل ردگیری این محصولات، به اهداف خود می‌رسند، در حالی که نهادهای متولی تأمین امنیت الکترونیکی، ابزاری برای مقابله و پیشگیری ندارند. بدین ترتیب، به رغم تحمیل محدودیت‌های غیر ضروری فراوان بر بسیاری از شهروندان عادی که هرگز قصد سوءاستفاده از ابزارهای رمزنگاری و نهان‌نگاری را ندارند و با وجود صرف هزینه‌های فراوان در فراهم کردن شرایط لازم برای اجرای قوانین سخت‌گیرانه، هدف قانون‌گذاران مذکور در پیشگیری از جرایم ارتکابی مجرمان یقه‌سفید[1] علیه محصولات رمزنگاری و نهان‌نگاری، به هیچ وجه محقق نخواهد شد.

پنجمین ایراد رویکرد قرمز، کارکرد جرم‌زا و نه چندان پیشگیرانه از جرم است. اتخاذ رویکرد قرمز، نه تنها از میزان جرایم مذکور نمی‌کاهد، بلکه جرم‌زا نیز هست. با توجه به ایرادهای پیشین، بدیهی است با وضع مقررات سخت‌گیرانه (امنیت‌گرا ـ ناقض حقوق بشر) کاربران عادی این شبکه‌ها و نیز مجرمان حرفه‌ای و سازمان‌یافته جرایمی جدید را مرتکب خواهند شد. نظام عدالت کیفری هر کشور (پلیس ویژهٔ مبارزه با جرایم الکترونیکی، دادگاه‌های کیفری، زندان، مراکز تعلیق مراقبتی) باید بهره‌مند از فن‌های پیشگیری، کشف، محاکمه، اثبات و مجازات مرتکبان این گونه جرایم باشد (Khaghani, 2012: 8).

البته رویکرد قرمز، ابعادی مثبت نیز دارد؛ برای مثال سبب بازدارندگی سطحی

1. White-color offence.

(ظاهری) مجرمان رایانه‌ای آماتور می‌شود و از بروز شبه جرم‌های فاقد سوء نیت ـ فاقد سبق تصمیم از حیث رکن روانی جرم ـ پیشگیری می‌کند (Lim & Others, 2003: 124). طبعاً شهروندان عادی و افرادی که هدف مجرمانه‌ای از استفاده‌های روزمره از محصولات رمزنگاری و پنهان‌نگاری ندارند، در صورت حاکمیت رویکرد قرمز، هم بر قوانین امنیت الکترونیکی و هم بر راهبردهای جرم‌شناختیِ حاکم بر الگوهای رفتاری پلیس (دایرهٔ ویژهٔ مبارزه با جرایم رایانه‌ای)، از سوءاستفاده‌های احتمالی از این محصولات بازداشته می‌شوند (نظریهٔ جرم‌شناختی انتخاب عقلانی). اتخاذ این رویکرد نمی‌تواند مجرمان حرفه‌ای و سازمان‌یافته را از ارتکاب اعمال مجرمانه و تهدیدهای بزرگ علیه امنیت ملی یک کشور باز دارد.

بند ۱ مادهٔ ۱۵ «کنوانسیون جرایم سایبری» بر لزوم انطباق قوانین داخلی کشورهای عضو با «میثاق بین‌المللی حقوق مدنی و سیاسی» سازمان ملل متحد و دیگر اسناد بین‌المللی حامی حقوق بشر تأکید دارد. بند ۱ مادهٔ ۲۱ روش‌های محدود کردن اختیارات مأموران نظام عدالت کیفری را در مبارزه با جرایم سایبر و با هدف جلوگیری از امنیت‌گرایی پلیسی، پیشنهاد کرده است. مجموعهٔ این مواد قانونی نشانگر مخالفت تصمیم‌گیرندگان در عرصهٔ سیاست جنایی مشترک اروپایی با حاکم شدن پارادایم امنیت‌گرایی (رویکرد قرمز) در این قارّه است؛ قاره‌ای که بیشتر کشورهای آن، فناوری لازم را برای اجرای مدل قرمز دارند، اما به دو دلیل از این مدل بیزارند؛ نخست، تعارض آن با حقوق بشر؛ دوم، تشدید بحران استغراق سیاست جنایی غربی از حیث تورم قوانین و رویه‌های جزایی که با گرفتگی و کندی نهادهای سرکوبگرِ نظام عدالت کیفری غربیِ جمهوری‌خواه (دموکراتیکِ اتوریته یا گاه دموکراتیک توتالیتر) توأم است.

پیامدهای مخابراتی، جرم‌شناختی و حقوق بشری مدل سبز (جرم‌انگاری حداقلی)

این رویکرد، طرف‌دار سیاست آزادانه و مخالفِ ممنوعیت و محدودیتِ قوانین تجاری و کیفری مربوط به صادرات و واردات محصولات رمزنگاری و پنهان‌نگاری

است. مزایای این رویکرد بشردوستانه و غیر امنیت‌گرا که گاه منطبق بر معایب رویکرد قرمز است، عبارتند از:

الف) برنینگیختن حساسیت‌های منفی در کاربران و گرایش کنجکاوانهٔ بی‌هدف آن‌ها به سمت سرویس‌های رمزنگاری و پنهان‌نگاری.

ب) پیشگیری از بروز جلوه‌های نوین بزهکاری و در نتیجه، صرفه‌جویی در هزینه‌های مالی و منابع انسانی در حوزهٔ ساختارهای نظارتی برای کشف جرایم الکترونیکی و سیاست‌گذاری جهت پیشگیری از آن‌ها.

ج) کاهش امنیت حریم خصوصی شهروندان: به دلیل امکان استفادهٔ آزادانهٔ افراد از محصولات متنوع رمزنگاری و پنهان‌نگاری و نبود هرگونه محدودیت، ممنوعیت و شروط استفاده از چنین محصولاتی، شهروندان می‌کوشند از قوی‌ترین ابزارهای رمزنگاری برای محافظت از اطلاعات شخصی خود استفاده کنند و هنگام ارسال چنین اطلاعاتی از طریق شبکه‌های ارتباطی عمومی، حداکثر امنیتِ ممکن را برای داده‌های مبادله‌شدهٔ خود فراهم آورند. بدین ترتیب امکان سوءاستفادهٔ مجرمان از اطلاعات شخصی افراد از قبیل مدارک و مشخصات شناسایی، اطلاعات مالی و تجاری، پزشکی و تحصیلی آنان از بین خواهد رفت و به طور غیر مستقیم، از حریم خصوصی افراد که دربرگیرندهٔ تمامی اطلاعات الکترونیکی مربوط به آن‌هاست، محافظت بیشتر می‌شود (Zhang, 2004: 76).

د) کاهش انگیزهٔ ارتکاب برخی جرایم خاص رایانه‌ای: روشن است که به دلیل الکترونیکی شدن بیشتر تراکنش‌های تجاری شهروندان در عصر حاضر، مجرمان رایانه‌ای با تسلط بر دانشِ پروتکل‌های پیاده‌کنندهٔ چنین تراکنش‌هایی به راحتی می‌توانند با نفوذ به این پروتکل‌ها و جعل، تغییر، تحریف و تکرار اطلاعاتِ در حال مبادله، از کاربران چنین سرویس‌هایی سوءاستفاده کنند (Kahf, 2003: 36). دسترسی آسان و بدون محدودیت به ابزارهای رمزنگاری، شهروندان و کاربران این گونه شبکه‌ها و نیز سرویس‌دهندگان و اپراتورهای این سرویس‌ها را می‌تواند به ابزارهایی قدرتمندتر مجهز سازد تا با به کارگیری آن‌ها، مجرمان را از سوءاستفاده از این تراکنش‌های الکترونیکی باز دارند.

ح) امکان تعقیب مجرمان حرفه‌ای و سازمان‌یافته: هدف سیاست جنایی قرمز از تصویب قوانین سخت‌گیرانه و اعمال محدودیت شدید بر استفاده از محصولات رمزنگاری و پنهان‌نگاری، افزایش احتمال شناسایی مجرمان و سوءاستفاده‌کنندگان از این محصولات، تعقیب کیفری، محاکمه و مجازات آن‌هاست. در این صورت، اصل بر عدم برائت همهٔ کاربران شبکه‌های ارتباطی عمومی است و نهادهای نظارتی تلاش می‌کنند با نظارت کامل و ذخیره و پردازش گستردهٔ اطلاعات و ارتباطاتِ در حال مخابره از طریق بستر شبکه‌های ارتباطی، از نرخ سیاه بزهکاری بکاهند و به نرخ قرمز بیفزایند. به دلیل گستردگی حجم این گونه ارتباطات و مشکلات فنی و مدیریتی اجرای چنین مقرراتی، دستیابی به این هدف، دور از تصور به نظر می‌رسد و هدفی خیال‌پردازانه می‌نُماید (Bernstein, 2009: 175). در مقابل، هدف «مدل سیاست جنایی سبز: جرم‌انگاری حداقلی»، شناسایی مجرمان سایبری از طریق روش‌های غیر معمول (تاکتیک غافلگیری در قلمرو استراتژی‌های پلیسی) و سپس نظارت و ذخیرهٔ تمامی ارتباطات و اطلاعات در حال مخابرهٔ آن‌ها از طریق شبکه‌های ارتباط عمومی و نهایتاً پردازش آن‌هاست. این راهبرد، ادلهٔ کافی را برای تعقیب کیفری مظنونان فراهم می‌آورد. لذا در کشورهای سبز، اصل برائت کاملاً رعایت می‌شود و نهادهای نظارتی تلاش می‌کنند تنها به کنترل و ذخیره و پردازش کامل اطلاعات و ارتباطاتِ در حال مخابره از طریق بستر شبکه‌های ارتباط عمومیِ مربوط به تعدادی از مجرمان بالقوه بپردازند و در صورت تشخیص رمز بودن این گونه ارتباطات، تلاش می‌کنند با رمزگشایی آن‌ها به دلایل و شواهد جرایمشان پی ببرند.

واضح است که به دلیل تمرکز کامل توانمندی‌های نهادهای نظارتی در ذخیره، پردازش، تشخیص رمز بودن یا نبودن و نیز شکستن داده‌های رمزشده یا استخراج کلید رمزنگاری مورد استفاده (مثلاً از طریق الزام فرد مجرم به افشای کلید مورد استفاده در رمزگذاری داده‌ها با حکم دادگاه صالح)، تعقیب مجرمان حرفه‌ای و سازمان‌یافته در چنین کشورهایی ممکن است و انتظارات از نهاد نظارتی، کاملاً واقع‌گرایانه و متناسب با توانمندی‌های آن‌ها خواهد بود.

با این همه، برخی معایب رویکرد سبز بدین شرح است: قدرت بازدارندگی

واکنش‌های قانونی در نظام عدالت کیفری رسمی سبز ضعیف است و تنها مجرمان غیر حرفه‌ای را می‌ترساند. این مجرمان به دلیل نبود منع قانونی در چنین سیستمی، عموماً مرتکب برخی شبه جرم‌ها یا حداکثر، تخلفات خرد می‌شوند. با این حال، با توجه به دو نکتهٔ مهم، می‌توان از این عیوب چشم پوشید: اولاً، مجرمان غیرحرفه‌ای، بر خلاف مجرمان حرفه‌ای و سازمان‌یافته، از ابزارها و محصولات رمزنگاری و نهان‌نگاری موجود در بازار استفاده می‌کنند که به خوبی برای نهادهای نظارتی شناخته‌شده‌اند و امکان سوءاستفاده از آن‌ها بسیار محدود است. ثانیاً، با تمهیداتی فرهنگی و افزایش آگاهی شهروندان عادی، می‌توان تا حدی پذیرفتنی، زمینهٔ ارتکاب چنین شبه جرم‌هایی را در بین آن‌ها از بین برد.

نتیجه‌گیری

مبارزهٔ شایسته با جرایم علیه تجارت الکترونیکی، مدیریت بحران در افقی وسیع با بازهٔ زمانی بلندمدت محسوب می‌شود. تنظیم سیاست جنایی بر پایهٔ مدل امنیت‌گرا، با قوانین بین‌المللی و فلسفهٔ تصویب آن‌ها سازگاری ندارد؛ البته مبارزه با جرایم سازمان‌یافتهٔ خشونت‌بار مانند قتل عمد، تجاوز خشن جنسی، بمب‌گذاری و گروگان‌گیری را باید استثنا دانست. این ناسازگاری، آنجا که بحث از مدیریت راهبردیِ عقلانی و منطبق با الگوی هزینه ـ فایده، جهت مقابله با جرایم علیه تجارت الکترونیکی است، مشهودتر است؛ چرا که نظریه‌های ارعاب‌گرای کلاسیک و استحقاقی نئوکلاسیک، نه توان بازدارنگی از این جرایم را دارند و نه قابلیت پیشگیری از آن‌ها را. همچنین امکان نظارت، ذخیره و پردازش همهٔ اطلاعات در حال مبادله در بستر الکترونیکی جهت کشف جرایم احتمالی (به ویژه رمزنگاری و پنهان‌نگاری غیر قانونی) وجود ندارد. محدودیت زیرساخت‌های سخت‌افزاری، تنوع و روزآمدیِ نرم‌افزاری تجارت الکترونیک بین‌المللی در عصر حاضر، لزوم رعایت کنوانسیون‌های بین‌المللی حامی و ترویج‌کنندهٔ نسل سوم حقوق بشر[1]

1. Promoter of human rights third generation.

(حقوق همبستگی) و اثبات ناکارامدی نظریه‌های جرم‌شناختی قرون وسطایی سزادِه، همه و همه به جامعهٔ جهانی این هشدار را می‌دهند که تلاش‌ها باید به سمت و سوی تضعیفِ ـتا حدّ ممکنِـ برتری پارادایم امنیت‌گرا بر پارادایم آزادی‌گرا معطوف گردد. بی‌شک، عملکرد پلیس فتا و دادسراهای ویژهٔ رسیدگی به جرایم رایانه‌ای، در اتخاذ رویکرد قرمز و یا حتی زرد، به شکوفایی و افزایش اقتدار این نهادهای متکفل مبارزه با رمزنگاری و پنهان‌نگاری‌های مجرمانه و نیز رمزگشایی و پنهان‌شکنیِ اطلاعات و ارتباطات مشکوک می‌انجامد.

جدال دو گفتمان اصلی سیاست جنایی (گفتمان امنیت‌گرا و گفتمان آزادی‌گرا) موجب سردرگمی و ناتوانی سیاست‌گذاران جنایی اغلب کشورها در مدیریتِ مبارزه با جرایم علیه امنیت اطلاعات، به ویژه جرایم علیه تجارت الکترونیکی شده است. به نظر می‌رسد در چنین شرایطی، هدفمند کردن راهبرد بایسته در قبال موارد مجرمانهٔ رمزنگاری و پنهان‌نگاری، رویه‌ای منطقی را در مسیر عقلانیت حقوق کیفری کاربردی فراروی تصمیم‌گیران نظام‌های حقوقی کشورها قرار دهد؛ به ویژه کشورهای درگیر با چالش توسعه‌نیافتگی تجارت الکترونیکی و کشورهای آماج تروریسم سایبری و نفوذ به شبکه‌های اطلاعاتی.

در مقابل این مزایا، این خلأ بزرگ نیز وجود دارد که هنوز اقتصاد اسلامی نظریه‌پردازی و اجرایی نشده است و حداکثر، حاوی نقدها و آموزه‌هایی کلی است؛ مانند تأیید کاربرد بیمه و بیع دِین و شمول نظریهٔ زکات بر بیش از نه کالا ـآن هم طبق برخی فتاوا ـ و مواردی محدود از این قبیل. کشورهایی با نظام حقوقی اسلامی، همچنان در تلاش برای کاربردی کردن آیات و روایاتند؛ متونی که روزآمد ساختن آن‌ها نیازمند نظریه‌پردازی‌های بسیار قوی و حل «چالشی بزرگ» است که آن را «ناتوانی فعلی در رویارویی با اقتصاد لیبرال و نئوکلاسیکِ جهانی‌شدهٔ معاصر» می‌نامیم. این مسئله، از آن رو «چالشی بزرگ» است که علی‌رغم وارد دانستن همهٔ ایراداتِ بر اومانیسم و پروژهٔ نافرجام مدرنیته، بر اقتصاد غربی نمی‌توان از موفقیت این اَبَرنظریه در چرخاندن ارابهٔ الگوی جهانی‌شدهٔ زندگی بشر معاصر چشم پوشید.

کتاب‌شناسی

۱. امیرارجمند، اردشیر و مجتبی همتی، «بررسی و تحلیل تضمینات حقوق اقتصادی و اجتماعی بین‌الملل (حقوق رفاهی) در نظام‌های داخلی»، ***الهیات و حقوق***، مجلهٔ تخصصی دانشگاه علوم اسلامی رضوی، دورهٔ هفتم، شمارهٔ ۲۳، ۱۳۸۶ ش.

۲. انصاری، باقر، ***حقوق ارتباط جمعی***، چاپ دوم، تهران، سمت، ۱۳۸۷ ش.

۳. بوخمان، یوهانز، ***مقدمه‌ای بر رمزنگاری***، ترجمهٔ مرتضی اسماعیلی، اصفهان، دانشگاه صنعتی اصفهان، ۱۳۸۲ ش.

۴. پژوهشکدهٔ امنیت اطلاعات و ارتباطات، ***گزارش فنی فاز اول طرح ملی «تدوین ضوابط و مقررات فنی استفاده از رمزنگاری و نهان‌نگاری اطلاعات توسط کاربران شبکه‌های ارتباطی عمومی کشور»***، تهران، شرکت پیام‌پرداز، ۱۳۸۷ ش.

۵. پیرلوگوف، ژان، ***دموکراسی پساتوتالیتر***، ترجمهٔ کاظم ایزدی، تهران، چشمه، ۱۳۸۶ ش.

۶. حبیب‌زاده، محمدجعفر و امیرحمزه زینالی، «درآمدی بر برخی محدودیت‌های عملی جرم‌انگاری (ضرورت ارزیابی منافع و مضار یک جرم)»، ***نامهٔ مفید***، شمارهٔ ۴۹، ۱۳۸۴ ش.

۷. حسن‌بیگی، ابراهیم، «توسعهٔ شبکهٔ ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملی»، ***اندیشهٔ انقلاب اسلامی***، شمارهٔ ۹، ۱۳۸۳ ش.

۸. دبلفون، زویه دینان، ***حقوق تجارت الکترونیک***، ترجمهٔ ستار زرکلام، تهران، مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش، ۱۳۸۸ ش.

۹. دلماس مارتی، می‌ری، ***نظام‌های بزرگ سیاست جنایی***، ترجمهٔ علی‌حسین نجفی ابرندآبادی، تهران، میزان، ۱۳۸۱ ش.

۱۰. رضایی‌زاده، محمدجواد و یحیی احمدی، «مبانی حق دسترسی شهروندان به اطلاعات و اسناد دولتی»، ***فصلنامهٔ حقوق***، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، دورهٔ سی‌ونهم، شمارهٔ ۴، ۱۳۸۸ش.

۱۱. سعیدی، سیاوش، «استراتژی امنیتی آمریکا و قدرت نرم اروپا»، ***اطلاعات سیاسی و اقتصادی***، شمارهٔ ۲۸۷، ۱۳۹۱ ش.

۱۲. صدر توحیدخانه، محمد، «حقوق در چنبرهٔ دشمن؛ از سیاست آمریکایی «جنگ با ترور» تا نظریهٔ آلمانی «حقوق کیفری دشمنان»»، ***تازه‌های علوم جنایی*** (مجموعه مقالات)، تهران، میزان، ۱۳۸۸ ش.

۱۳. قناد، فاطمه، ***ابعاد کیفری حقوق تجارت الکترونیکی***، رسالهٔ دکتری حقوق جزا و جرم‌شناسی، دانشگاه شهید بهشتی، ۱۳۸۶ ش.

۱۴. کاشفی اسماعیل‌زاده، حسن، «جنبش‌های بازگشت به کیفر»، ***آموزه‌های حقوق کیفری***، مشهد، دانشگاه علوم اسلامی رضوی، شماره‌های ۱۵و۱۶، ۱۳۸۴ ش.

۱۵. مجیدی، سیدمحمود، «جلوه‌های ظهور حقوق کیفری امنیت‌مدار در فرانسه»، ***فصلنامهٔ حقوق***، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، دورهٔ سی و نهم، شمارهٔ ۲، ۱۳۸۸ ش.

۱۶. نجفی ابرندآبادی، علی‌حسین، «کیفرشناسی نو ـ جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار»، ***تازه‌های علوم جنایی*** (مجموعه مقالات)، تهران، میزان، ۱۳۸۸ ش.

17. Bantekas, I., "The Disunity of Islamic Criminal Law and the Modern Role of Ijtihād", ***International Criminal Law Review***, Vol. 9, 2009.

18. Bernstein, D., ***Introduction to Post-quantum Cryptography***, Chicago, University of

Illinois Press, 2009.

19. El-Ansari, W., "Islamic Economics and the Sciences of Nature: The Contribution of Seyyed Hossein Nasr", in Mohammad Faghfoory (ed.) ***Becaon Quantum Enigma and Islamic Sciences of Nature 171 of Knowledge: Essays in Honor of Seyyed Hossein Nasr***, Louisville, Kentucky, Fons Vitae, 2003.
20. El-Gamal, M., ***Islamic Finance law, Economics, and Practice***, New York, Cambridge University Press, 2006.
21. Habermas, J., ***Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*** (Studies in Contemporary German Social Thought), Cambridge, Polity Press, 2004.
22. Higgins, E., "An Application of Deterrence Theory to Software Piracy", ***Journal of Criminal Justice and Popular Culture***, Vol. 3, 2005.
23. Kahf, M., "Islamic Economics: Notes on Definition and Methodology, ***Review of Islamic Economics***, Vol. 13, 2003.
24. Kennedy, S., "Computer Crimes", ***American Criminal Law Review***, Vol. 39, 2002.
25. Khaghani, M., "Challenges Confronting the Modernization of Islam and Iran's Criminal Law in regard to Crimes against Security of e-Commerce, ***6th International Conference on e-Commerce in Developing Contries: With Focus on Islamic Banking***, ISC indexed, Shiraz, Iran, 2012.
26. Lim, S. & Others, "Modeling of Multiple Agent based Cryptographic Key Recovery Protocol", ***Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003)***, Las Vegas, 2003.
27. Prajer, J., "Totalitarian and Liberal Democracy: Two Types of Modern Political Orders", in Jeffrey, C. Alexander (eds), ***Neo-Functionalism***, Publications Beverly Hills London New Delhi, 1985.
28. Quraishi, M., ***Muslims and Crime: A Comparative Study***, Aldershot, UK, Ashgate, 2005.
29. Rudolph, P., ***Crime and Punishment in Islamic Law***, Cambridge University Press, 2005.
30. Saleem, M., "Methods and Methodologies in Fiqh and Islamic Economics", ***Review of Islamic Economics***, Vol. 14, 2010.
31. Smith, G., et al, ***Law of Intectronic Commerce, Aspan Law & Business***, 4th Edition, 2002.
32. Zhang, W., "Security Measurements of Steganographic Systems", in Jakobsson, M. & Others (Eds), ***Applied Cryptography and Network Security***, Berlin Heidelberg, Springer 2004.