پژوهش حقوق کیفری، سال پنجم، شماره هجدهم ، بهار ۱۳۹۶، ص ۱۴۱ - ۱۰۱

دکترین شخص ثالث در تحقیقات کیفری سایبری

محمد جواد فتحی* سید وحید ابولمعالی‌الحسینی**

(تاریخ دریافت : ۹۴/۸/۴ تاریخ پذیرش : ۹۵/۸/۲۴)

چکیده؛

یکی از مواردی که ممکن است تفتیش و توقیف یک مکان و یا دسترسی به ادله، بدون صدور قرار قضایی مجاز شمرده شود، موقعیت‌هایی است که ذیل دکترین «رضایت شخص ثالث» مطرح می‌گردد. بر اساس یک قاعده کلی، در نظام حقوقی آمریکا، «مأموران می‌توانند از هر مکان یا شیئی، بدون داشتن قرار یا حتی سبب محتمل تفتیش به عمل آورند و ادله‌ی موجود در آن گستره را توقیف نمایند، به شرطی که شخصی که صلاحیت ابراز رضایت دارد، داوطلبانه با آن موافقت کند». دکترین شخص ثالث همواره با دو مسئله تبیین «قلمرو رضایت ثالث» و «هویت اشخاصی که برای اعلام رضایت دارای صلاحیت هستند» درگیر بوده است، اما مشکل اصلی زمانی بروز پیدا کرد که شبهات مطرح‌شده، زیربنای فلسفی و بنیادهای این دکترین را زیر سؤال برد و چنین ادعا شد که این دکترین قابلیت ادامه حیات در وضعیت فعلی و مطابق با خوانش قدیمی خود را ندارد. توضیح آن‌که دکترین شخص ثالث با ورود فن‌آوری‌های نوین در عصر ارتباطات و در قلمرو سایبر، به دلیل تغییر در موضوعات و تحول مفهومی دکترین در عرصه فن‌آوری‌ها با چالش‌های فراوانی روبرو گردید و تردیدها نسبت به کارآیی دکترین زمانی آشکارتر شد که ملاحظه گردید تقریباً تمام خدمات ارائه‌شده در عصر حاضر توسط ثالث ارائه می‌شود و بدین ترتیب، خوانش سنتی و مرسوم دکترین شخص ثالث، عملاً هیچ اثری از حریم خصوصی به‌جای نخواهد گذاشت. در این نوشتار، محور اصلی بحث، محیط سایبر است و در این راستا، به‌صورت محوری، به تبیین دکترین رضایت شخص ثالث در محیط سایبر خواهیم پرداخت.

واژگان کلیدی: **تفتیش، توقیف، حریم خصوصی، دکترین شخص ثالث.**

---

* دانشیار حقوق جزا و جرم‌شناسی دانشگاه تهران، پردیس فارابی

** دانشجوی دکتری رشته حقوق جزا و جرم‌شناسی دانشگاه تهران پردیس فارابی (نویسنده مسئول):

Vahid.ab@live.com

مقدمه:

در قوانین مربوط به تحقیقات کیفری جمهوری اسلامی ایران، خصوصیتی برای ارتباط بین مکان مورد بازرسی با شخص متهم و یا نوع ارتباط متهم با مکان یا شیء مورد تفتیش، مانند مالکانه بودن یا وجود تصرفات مشروع و یا نوع ارتباط متصرف مکانی که موضوع مورد تفتیش در آن واقع است با متهم، یا اتهام مقرر نشده است و به‌جز در موارد معدود، موضوع منصرف از این است که ادله‌ی مجرمانه در اختیار چه شخصی قرار دارد و این موضوع که شخص مورد تفتیش و یا مکان مورد تفتیش، چه ارتباطی با شخص متهم دارد، مورد توجه ویژه قرار نگرفته است (انصاری، ۱۳۸۳: ۲۰- ۲۵). در مقابل، در برخی نظام‌های حقوقی، برای تشخیص مشروعیت دسترسی اشخاص ثالث به اطلاعات افراد و جواز افشای آن‌ها، به ارتباط شخص با محل نگهداری اطلاعات و یا با شخص نگهدارنده یا دارای دسترسی توجه شده است. به‌عنوان‌مثال، در زمینه‌ی نظارت بر محل‌های کار، دیوان کشور فرانسه در سال ۲۰۰۱، در پرونده «نیکون» علیه «اونوف»[1] اعلام کرد که کارگران حتی در محل کار و در ساعات کار از حق حریم خصوصی[2] برخوردار بوده و لذا مستحق رعایت محرمانه بودن مکاتبات و مکالمات خود با کارفرمایان هستند (Sánchez Abril, Levin & Del Riego, 2012: 78).

در قانون آئین دادرسی کیفری ایران اصولاً برای صدور مجوز تفتیش و بازرسی و ورود به حریم خصوصی اشخاص، صرف این‌که مکان موردنظر از نظر مقام قضایی حاوی ادله‌ی مجرمانه تشخیص داده شود و یا مواردی ازاین‌دست که مثلاً حضور متهم فراری در آن مکان پیش‌بینی شده باشد، کافی به‌نظر می‌رسد (ورواییی و دیگران، ۱۳۸۹: ۴۹) ولو این‌که مکان موردنظر، به شخص دیگری تعلق داشته و وی هیچ رضایتی مبنی بر تفتیش[3] نداشته باشد و تنها

1. Nikon v. Onof, Decision No 4164 (2 October 2001).
2. Privacy
3. Search

محدودیت‌های وارده، برخی مسائل شکلی،[1] مانند نحوه یا زمان ورود و یا مواردی مانند سرّی یا محرمانه بودن اطلاعات موردنظر یا تعلق اطلاعات به اشخاص ویژه، یا منافی عفت بودن جرم واقعه، همانند موضوع تبصره ماده ۴۳ قانون آئین دادرسی کیفری مصوب ۱۳۹۲ و یا تشریفات لازم‌الرعایه مربوط به مصونیت‌های سیاسی می‌باشد. در ایران، مشروعیت تحصیل دلیل و حریم خصوصی به‌جز موارد استثنایی مانند بی‌اعتباری اقرار تحصیل‌شده از طریق شکنجه، مورد اشاره در اصل ۳۸ قانون اساسی و ماده ۵۷۸ ق. م. ا.، کتاب پنجم، هرگز مورد توجه جدی قرار نگرفته و حتی به نظر می‌رسد که در قانون آئین دادرسی کیفری، تئوری «فاسد بودنِ میوه‌ی درخت فاسد» مورد تبعیت قرار نگرفته و باید جرم مکشوفِ (متعاقب تفتیش نامشروع) را قابل تعقیب دانست (رحمدل، ۱۳۹۳: ۵۷). لذا شاید به این دلیل بوده است که در قانون آئین دادرسی کیفری ایران، گستره‌ی ورودِ قانونی به حریم خصوصی، در مقام کشف و تعقیب جرم، تنها بسته به پاسخ به این پرسش که جرم مشهود است یا خیر، کاهش و یا توسعه پیدا خواهد کرد. در حقیقت، ظاهراً مبنای اولیه‌ی تقسیم‌بندی جرائم به مشهود و غیرمشهود، کوشش برای «تعیین مرزهای دقیق موارد استثناییِ تفتیش و توقیفِ قانونی، بدون دستور مقام قضایی» با تفتیش‌های غیرمجاز بوده است. درعین‌حال، مشخص است که برخی نیازهای اجرای قانون، مانند موارد اضطراری و یا ویژه‌ای که ممکن است «انتظار برای صدور دستور قضایی» موجب دفع‌الوقت و از بین رفتن ادله‌ی جرم و یا فرار متهم شود و مصالحی مانند رعایت امنیت مأمورین در قالب برخی مواد قانونی و ذیل بهانه‌ی کلی ضرورت «حفظ مصالح عامه» (مؤذن‌زادگان، ۱۳۷۲: ۸۸) مورد توجه قرار گرفته است. درحالی‌که در حقیقت، این تقسیم‌بندی، ابتدا یک روش توصیفی برای تقسیم‌بندی جرائم است که از آن برای پاسخ به این پرسش کارکردگرایانه استفاده شده است که «در چه مواردی، تفتیش ضابط که بدون مجوز مقام قضایی صورت می‌گیرد، جایز تلقی می‌شود؟». بدین ترتیب، ابتدا این ذهنیت ایجاد شده است که «اگر جرم و ادله‌ی آن در

---

۱. برای آشنایی با محدودیت ها و ضوابط شکلی، ر.ک: (وروایی، جهانگیرپور، جربانی و هاشمی، ۱۳۸۹: ۵۹–۵۰)

مرئی و منظر ضابطین باشد، آن‌ها حق مداخله، به معنای بازرسی، تفتیش و توقیف[1]، بدون صدور قرار خواهند داشت» و لذا جرائم به دو دسته‌ی مشهود و غیرمشهود تقسیم گردیدند، اما درنهایت، آنچه در نص قانون‌گذار راه یافت، توسعه‌ی مفهوم جرم مشهود به مواردی بود که به‌سختی می‌توانیم ماهیت آن‌ها را مشهود بدانیم و در واقع، تنها وجه اشتراک آن با جرائم مشهود، نیاز به دخالت ضابط قضایی برای حفظ ادله یا جلوگیری از فرار مجرم و یا انجام تفتیش بدون قرار در آن موارد خاص است. «در این راستا، لازم است به حکم بی‌سابقه‌ی آئین دادرسی کیفری ایران در مورد جرائم مشهود اشاره نمود که در تبصره ۱ ماده ۴۵ آمده است» (خالقی، ۱۳۹۴: ۷۹ و ۸۰) و در آن، در ادامه‌ی توسعه وضعیت‌های مشمول جرائم مشهود و اختیارات کنشگران آن، اختیاراتی در زمینه‌ی حفظ صحنه جرم به شهروندان عادی اعطا شده است که می‌تواند تهدیدی جدی برای نظم عمومی و حریم خصوصی اشخاص باشد. این توسعه به موارد و موقعیت‌های جدید، در حالی بوده است که اغلب آن موقعیت‌ها ذیل عنوان «جرائم مشهود» جای نمی‌گیرند و با توجه به این که «در جرائم مشهود، ... اختیارات بیشتری به آنان (ضابطین دادگستری) واگذار گردیده است» (آشوری، ۱۳۸۸: ۱۴۵)، نگاه یکپارچه به‌تمامی آن جرائم ذیل جرم مشهود محل تأمل به‌نظر می‌رسد. این شیوه؛ یعنی شیوه‌ای که قانون‌گذار ایرانی در روند تغییرات قانون آیین دادرسی کیفری و نهایتاً در ماده ۴۵ قانون حاکم در نظر گرفته، با تفاوت سال‌های تصویب، دقیقاً منطبق با تغییرات تدریجی رویه‌ی قضایی و قانون آئین دادرسی کیفری فرانسه است که در آن، بر اساس رویه‌های قضایی کیفری، در ۸ اکتبر ۱۹۸۵، ۲۳ اکتبر ۱۹۹۱، ۲۲ آوریل ۱۹۹۲، ۸ آوریل ۱۹۹۸، مواردی به مصادیق جرم مشهود اضافه شد و در قانون ۹ مارس ۲۰۰۴، قانون ۱۸ مارس ۲۰۰۳ و قانون ۲۳ ژوئن ۱۹۹۹ نیز مواردی تحت عنوان جرائم در حکم مشهود معرفی گردید.[2] در مقابل، در برخی نظام‌های حقوقی مانند نظام حقوقی

1. Seizure

۲. برای توضیح بیشتر در این رابطه و آشنایی با مصادیق، ر.ک: (بوریکان و سیمون، ۱۳۸۹: ۱۲۹–۱۳۱)

ایالات‌متحده آمریکا که از آن به‌عنوان حقوقی متناسب با انتظارات اجتماعی زمان یا حقوق تجربی یاد می‌شود (یوسفی، ۱۳۹۲: ۱۷۵ و۱۷۶)، به‌عنوان یکی از منعطف‌ترین مدل‌ها در میان مدل‌های دادرسی کیفری، راه‌حل دیگری در پیش گرفته شده است. به‌نظر می‌رسد آن‌ها مستقیماً به دنبال پاسخ برای این پرسش رفته‌اند که چه مواقعی تفتیش، بازرسی و توقیف می‌تواند بدون صدور قرار و یا دستور قضایی، صحیح باشد و در چه مواقعی حتماً نیازمند صدور قرار و جواز مقام قضایی هستیم.[۱] از سال ۱۹۶۷ و قضیه‌ی «کاتز» علیه «ایالات‌متحده امریکا»[۲] دیوان عالی کشور این کشور، از حریم خصوصی اطلاعاتی افراد، به شرطی حمایت می‌نماید که در رابطه با آن‌ها یک انتظار متعارف برای رعایت حریم خصوصی وجود داشته باشد (Issacharoff & Wirsha, 2016: 987). لیکن یکی از مسائل به‌شدت مورد مناقشه و چالش-برانگیز در این حوزه، «دکترین شخص ثالث»[۳] است که به دولت اجازه می‌دهد هر اطلاعاتی راجع به یک متهم کیفری که توسط وی نزد شخص ثالث سپرده شده است را جمع‌آوری نماید؛ بدون این‌که انتظار متعارف رعایت حریم خصوصی و در ایالات‌متحده آمریکا، اصلاحیه چهارم قانون اساسی را نقض کرده باشد. اساس این قاعده بسیار ساده و صریح است: وقتی

---

۱. به عنوان مثال، کتابچه‌ی راهنمای «تفتیش و توقیف رایانه‌ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری» یا:
Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,
که توسط بخشِ جرایم رایانه‌ای و مالکیت معنوی (Computer Crime and Intellectual Property Section (CCIPS)) از بخش کیفری وزارت دادگستری ایالات متحده آمریکا تنظیم شده و دائما به روزرسانی می‌شود، به موضوع تفتیش و توقیف رایانه‌ها بدون صدور قرار و به موجب قرار و سپس شرح قانون حریم ارتباطات الکترونیکی در این رابطه، تشریح نظارت الکترونیکی بر شبکه‌ای ارتباطی بر اساس مقررات موجود، ادله اثبات دعوا و نمونه‌های اوراق قانونی و انجام تشریفات مربوطه می‌پردازد. آخرین نسخه این سند، در قالب فایل pdf، در ۲۹۹ صفحه، در آدرس اینترنتی زیر قابل دسترس است:

*https://www.justice.gov/**criminal**/cyber**crime**/docs/ssmanual2009.pdf*

2. *Katz v. United States*, 1967
3. Third - Party Consent Doctrine

اطلاعات در اختیار دیگری قرار می‌گیرد، مالک اصلی اطلاعات، حق حریم خصوصی خود را که قبلاً بر آن اطلاعات ممکن است داشته باشد، از دست می‌دهد (Kerr, 2009: 561–563). در حقیقت، یکی از مواردی که ممکن است تفتیش و توقیف یک مکان و یا دسترسی به ادله، بدون صدور قرار قضایی مجاز شمرده شود، موقعیت‌هایی است که ذیل دکترین «شخص ثالث» مطرح می‌گردد. «هر یک از افراد جامعه (امروزه) خواسته یا ناخواسته، داده‌های زیادی را در اختیار دولت و برخی از مؤسسات بخش خصوصیِ (ارائه‌دهندگان خدمات که در نگاه ما شخص ثالث خوانده می‌شوند) قرار می‌دهند.» (انصاری، ۱۳۸۷: ۲۰۲) و عمده‌ی این خدمات، امروزه به کمک فن‌آوری‌های نوین سایبری در حال ارائه هستند و فن‌آوری‌های اطلاعاتی و ارتباطی تبدیل به ابزاری شده‌اند که کنار گذاشتن آن غیرممکن است (یزدان‌پور ، ۱۳۸۴: ۲۳). ویژگی‌ای که دکترین شخص ثالث دارد این است که هم ساده است و هم به نحو جامعی قابلیت اعمال دارد. این ویژگی‌ها، موجب شده است که در دهه‌های گذشته، تئوری مزبور به‌شدت مورد استقبال سیستم پلیسی، قضایی و به‌ویژه نهادهای امنیتی در کشورهای مختلف قرار گیرد و دولت‌ها در گسترش کاربرد این دکترین زیاده‌روی نمایند. در مقابل، در نظر برخی قضات و حقوقدانان، این مفهوم همواره درگیر و در ارتباط با مفاهیم حریم خصوصی و انتظار برای رعایت حق حفظ محرمانگی و رازداری در زندگی اجتماعی هر شهروند بوده و لذا چنین تأکیداتی در رویه‌ی قضایی نیز راه یافته است (*Couch v. United States*, 1973; *Smith v. Maryland*, 1979). پدیده‌ی سایبر، روزافزونی آن و تقریباً ناممکن بودن قیاس موضوعات، احکام و تشریفاتِ قانونی مرتبط و حاکم بر فضای سایبر با وضعیت‌های مشابه قبل از ورود فن‌آوری‌ها، مسئله دکترین شخص ثالث را با چالش‌های فراوانی روبرو کرده است. فی‌المثل، آیا ارائه‌کنندگان خدمات دسترسی به وب یا ارائه‌کنندگان خدمات میزبانی در فضای سایبر که طبیعتاً به فضاها و اطلاعات وابسته به حریم خصوصی اشخاص دسترسی دارند، مجاز و یا حتی

موظف به افشای اطلاعات در اختیار خود هستند؟ و این «افشا»؛ امری اختیاری است یا تحمیلی؟ و گستره‌ی هر یک تا کجاست؟

در این نوشتار، شخص ثالث، در ذیل عنوان تفتیش و توقیف، دقیقاً به کسانی گفته می‌شود که به‌هردلیل به اطلاعات یا گستره‌ای خاص دسترسی مجاز دارند، اما مظنون اصلی در تعقیب کیفری محسوب نمی‌شوند. همچنین پیش از ورود به بحث خاطرنشان می‌شود که «دو خطر و تهدید جدی در جمع‌آوری و استفاده از این داده‌ها (داده‌های در اختیار شخص ثالث) وجود دارد: از یک‌سو، ممکن است داده‌هایی که ملازمه‌ای بین آن‌ها و ارائه‌ی خدمات عمومی وجود ندارد جمع‌آوری شود و از سوی دیگر، داده‌هایی که با وجود ملازمه‌ی منطقی جمع‌آوری شده‌اند، برای اهداف دیگری غیر از ارائه‌ی خدمات عمومی به کار روند و درنهایت، از امور مادی یا معنوی شخصی که داده‌ها به او مربوط است سوءاستفاده شود.» (انصاری، ۱۳۸۷: ۲۰۲ و۲۰۳)؛ خطری که موجب می‌شود، علاوه بر ضرورت توجه به دغدغه‌های کشف جرم، به ملاحظات امنیت داده‌ها، حمایت از آن‌ها و حفظ حریم خصوصی نیز توجه شود؛ کما این‌که اهمیت داده‌های شخصی و ارتباط آن‌ها با آزادی، استقلال و کرامت انسانی، سبب شده است که در برخی از اسناد خارجی، مانند «دستورالعمل شورای اروپا در حمایت از داده‌های شخصی» حق افراد در مصون بودن داده‌های شخصی از تعرض، یکی از حقوق اساسی بشر و حمایت از آن، حمایت از حقوق بنیادین و آزادی‌های اشخاص و به‌ویژه حق حریم خصوصی (Korff, 2002: 6) محسوب و عنوان گردد (انصاری، ۱۳۸۷: ۲۰۳).

۱. تحول مفهومی دکترین شخص؛

طرح دکترین شخص ثالث و ورود جدی آن به‌صورت یک قاعده به منابع حقوقی ایالات‌متحده آمریکا را باید از زمان رأی صادره در دعوای «ایالات‌متحده آمریکا» علیه «متلوک»[1] در سال

1. United States v. Matlock, 1974

۱۹۷۴ میلادی محسوب کرد. اصلاحیه چهارم قانون اساسی ایالات‌متحده آمریکا از حق حریم خصوصی شهروندان، با ممنوع کردن تفتیش و توقیف‌های غیرمعقول و نامتعارف حمایت می‌کند. مأمورین رسمی (ضابطین) باید این ملاحظه را داشته باشند که تمامی تفتیش‌ها و توقیف‌ها باید بر مبنای سبب محتمل[1] توجیه شوند (Amar, 1996: 54).

درعین‌حال، برای الزام پلیس به اخذ چنین قراری، استثنائات متعددی وجود دارد (Abrams, 1984: 963) که یکی از آن‌ها رضایت شخص ثالثی است که به محل مورد تفتیش دسترسی دارد (Fiske, 2006: 721).

در مفهوم سنتی دکترین شخص ثالث، عنوان می‌شود که ممکن است فی‌المثل چند نفر باهم از یک رایانه استفاده کنند یا مالک آن باشند. اگر هر یک از آن‌ها اجازه‌ی تفتیش داده‌ها را بدهد، اصولاً این امکان وجود دارد که مأموران (رسمی) با اتکا به آن رضایت، البته تا جایی که شخص صلاحیت لازم را داشته باشد، عمل کنند. درواقع، مبنایی که در این نظام حقوقی برای این مسئله مطرح می‌شود این است که زمانی که چند کاربر به یک سیستم دسترسی دارند، تمامی آنان قاعدتاً این خطر را پذیرفته‌اند که کاربر دیگر می‌تواند به هر چیز در رایانه دست یابد یا به مجریان قانون اجازه‌ی تفتیش «محیط مشترک»[2] را بدهد (اورین اس. کِر و گروه نویسندگان، : ۳۵ و۳۶) و در حقیقت، تنها شرط وجود صلاحیت برای اعطای مجوز برای تفتیش، این است که شخصی که رضایت برای تفتیش می‌دهد، یکی از اشخاصی باشد که «استفاده‌ی متقابل» از یک گستره یا موضوع می‌نمایند یا «دسترسی مشترک» بدان دارند و طبیعتاً لازم است که این «استفاده» و یا «دسترسی»، برای آن شخص، به‌طورکلی (یا) برای بیشتر مقاصد باشد، به‌نحوی‌که بتوان به آن بر اساس یک معیار متعارف و معقول، «دسترسی مشترک» یا «استفاده متقابل» نام نهاد. در دعوای «ایالات‌متحده» علیه «متلوک»، دیوان عالی کشور اظهار

1. Probable Cause.
2. Common Area.

داشت که باوجود مخالفت احتمالی یا بعدی یک یا چند نفر از کسانی که نسبت به یک محیط مشترک دارای «اختیار مشترک» هستند، وجود تنها رضایت دست‌کم یکی از این اشخاص، برای تفتیش کافی خواهد بود و چنین تفتیشی نیازمند دستور یا مجوز قضایی نخواهد بود.[۱] در تعریف سنتی دکترین شخص ثالث، اطلاعاتی که در اختیار ثالث قرار می‌گیرد از تعریف حریم خصوصی باید خارج شود؛ چراکه دکترین اعلام می‌کرد وقتی اطلاعات با اشخاص ثالث به اشتراک گذاشته می‌شود، دیگر انتظار رعایت حریم خصوصی، متعارف و معقول نخواهد بود (Stern, 2013, p. 389). در حقیقت اگر بخواهیم کماکان و بر اساسِ مبنای این تئوری در نخستین دهه‌ی طرح، به موضوعات جدید نیز نگاه کنیم، در حال حاضر باید حکم کرد که دارندگان یک حساب کاربری و استفاده‌کنندگان از خدمات شبکه‌ای در فضای سایبر، نمی‌توانند انتظار متعارف «رعایت حریم خصوصی اطلاعات» در نزد ارائه‌دهندگان خدمات شبکه‌ای، به‌عنوان شخص ثالث داشته باشند؛ چراکه استفاده از این خدمات، به معنی در دسترس قرار دادن اطلاعات مزبور برای ارائه‌دهندگان خدمات شبکه‌ای هست و علت امر اخیر نیز این است که ازنقطه‌نظر فنی، استفاده از خدمات مزبور و ارائه‌ی مناسب آن، متضمن دراختیارگیری اطلاعات بسیاری از فعالیت‌های کاربر در بستر شبکه، توسط ارائه‌دهندگان خدمات شبکه‌ای خواهد بود. بدین‌ترتیب، صرف استفاده از این خدمات، مطابق رهیافت دعوای «ایالات‌متحده آمریکا» علیه «میلر»[۲]، می‌تواند به معنی افشای اطلاعات نزد ثالث و به معنای از بین رفتن حریم خصوصی مزبور باشد. در این پرونده دادگاه مقرر کرد که سوابق بانکی، اطلاعات افشاشده به شمار می‌آید و لذا تحت حمایت‌های حریم خصوصی مندرج در اصلاحیه چهارم قانون اساسی قرار نمی‌گیرد (Kerr, 2001, p. 8). این رهیافت که به‌تدریج یک منبع قانونی برای قواعد حاکم بر تحقیقات مقدماتی کیفری، تفتیش و توقیف و حریم خصوصی محسوب شد، در

---

۱. برای توضیح بیشتر در خصوص این پرونده، ر.ک: (White، 1974)

2. *United States v. Miller*, 1976

دعوای فراوان دیگری نیز ملاک قرار گرفت. به‌عنوان‌مثال، در دعوای «اسمیت» علیه «مری‌لند»[1] نیز دادگاه اعلام کرد برای شماره‌ی تلفن ضبط‌شده توسط شرکت ارائه‌دهنده‌ی خدمات تلفن (که از مصادیق شخص ثالث شناخته می‌شود)، هیچ‌گونه انتظار متعارف حریم خصوصی‌ای قائل نیست (McLaughlin, 2006: 430). لذا این نگرش، در قرائت اولیه‌اش، موجب شد که اطلاعاتِ نزدِ ثالث، از حمایت‌های قانون اساسی برخوردار نبوده و عملاً افشاشده محسوب گردد و این دقیقاً همان چهارچوبِ نظری‌ای بود که نزدیک به سه دهه‌ی قبل از طرح جدی دکترین، در دهه‌ی ۴۰ میلادی، در دعوای «نیوفیلد» علیه «ریان»[2]، توسط دادگاه در صدور حکم مورد استفاده قرار گرفت. در این دعوا، دادگاه عالی آمریکا، حکم کرد که عملکرد مأمورین رسمی که بدون اخذ قرار و صرفاً با تقدیم درخواست به شرکت تلگراف، کپی‌های تلگراف‌های متهم را در اختیار قرار گرفته بودند و افشای شرکت مزبور متعاقب این درخواست، تجاوز به حریم خصوصی شخص محسوب نمی‌شده است (Fox, 1955: 624). در نظام حقوقی آمریکا، این موضوع بسیار سریع به متن قوانین راه یافت؛ به‌موجب قانون حریم ارتباطات الکترونیکی (ECPA) ایالات‌متحده آمریکا مصوب ۱۹۸۶[3] تا هنگامی‌که موضوعات و

1. *Smith v. Maryland*, 1979
2. *Newfield v. Ryan*, 1937

۳. قانون حریم ارتباطات الکترونیکی (Electronic Communications Privacy Act) یا به اختصار (ECPA) مصوب ۱۹۸۶: این قانون نحوهٔ دستیابی مأموران به اطلاعات ذخیره شده در اعتبار ارائه‌دهندگان خدمات شبکه‌ای (نظیر ISPها) را مشخص می‌کند. قانون حریم ارتباطات الکترونیکی (ECPA)، مصوب ۱۹۸۶ میلادی، به وسیله کنگره ایالات متحده آمریکا تصویب شد تا دایره شمول ممنوعیت شنود تماس های تلفنی را به شنود اطلاعات الکترونیکی در حال انتقال نیز گسترش دهد (ماده ۲۵۱۰ به بعد از عنوان ۱۸ قانون ایالات متحده آمریکا). همچنین مقررات جدیدی تحت عنوان قانون ارتباطات ذخیره شده به عنوان ۱۸ مجموعه قوانین ایالات متحده آمریکا از ماده ۲۷۰۱ به بعد نیز اضافه شد تا دسترسی به ارتباطات الکترونیکی ذخیره شده را نیز ممنوع سازد و همچنین مقرراتی که اصطلاحا «pen trap» به آن گفته میشد از ماده ۳۱۲۱ به بعد اضافه شد که ردیابی ارتباطات الکترونیکی را اجازه می داد. قانون اکپا اصولا برای جلوگیری از دسترسی بدون جواز قانونی دولت به ارتباطات الکترونیی خصوصی طراحی و وضع شده بود؛ اما این قانون در سال ۱۹۹۴، ۲۰۰۶ و ۲۰۰۸ به

اطلاعات مربوط یا متعلق شخص که اصولاً داخل در حریم خصوصی وی شمرده می‌شود، در تصرف شخص ثالث باشد، مأمورین رسمی، بدون نیاز به اخذ دستور مقام قضایی که خود نیازمند اثبات «سبب محتمل، معارف و معقول» برای وجود ادله‌ی مجرمانه است، می‌توانند صرفاً با درخواست رسمی و رعایت تشریفات خاص، آن اطلاعات یا موضوعات را از شخص ثالث درخواست کنند. در رویه قضایی ایالات‌متحده آمریکا، دست‌کم تا سال ۲۰۰۶ میلادی و تا پرونده «جئورجیا» علیه «راندولف»[1]، بر اساس رهیافت «متلوک» و همانند دعوای «ایلینویس» علیه «رودریگز»[2]، رویه قضایی تمایل داشت که حتی اگر شخص ثالث به مأمورین رسمی در خصوص صلاحیت خود در دسترسی به محیط مشترک دروغ گفته باشد، بازهم دلایل تحصیل شده‌ی ناشی از آن تفتیش مورد رد قرار نمی‌گرفتند (Webb, 2008: 3390)؛ مشروط به این‌که «بر اساس شواهد در دسترس، مأمور، در آن زمان و با توجه به درایتی که یک انسان محتاط متعارف دارد، باور یابد رضایت‌دهنده صلاحیت مزبور را داشته است» (Campbell, 1992: 48-482).

مبنای اصلی دکترین شخص ثالث که درواقع، «قاعده‌ی مشروعیت تفتیش بدون قرار پلیس، متعاقب تحصیل رضایت احدی از متصرفین مشترک یک ملک برای تفتیش قلمرو مشترک» بود. بعداً به‌وسیله‌ی رهیافت اتخاذی در پرونده‌ی «ایلینویز» علیه «رودریگز» در سال ۱۹۹۰ شرح و بسط بیشتری یافت و پس‌ازآن در پرونده «جورجیا» علیه «راندولف» در سال ۲۰۰۶ محدود شد. این محدودیت نیز در سال ۲۰۱۴ و در پرونده «فرناندز» علیه «کالیفرنیا»[3]، با اندکی تفاوت نسبت به سابقه این قاعده و یا دکترین، مورد تفصیل قرار گرفت و تعدیل گردید. بدین ترتیب،

ترتیب با قوانین « Communications Assistance for Law Enforcement Act (CALEA)»، قانون میهن پرستی (تصویب مجدد) و «FISA Amendments Act» مورد اصلاح قرار گرفت.

1. Georgia v. Randolph, 2006
2. Illinois v. Rodriguez, 1990
3. Fernandez v. California, 2014

در سیر تطور و تحول این دکترین و برای فهم بهتر آن، لازم است که دعاوی مزبور از «متلوک» تا «فرناندز» و به‌ویژه دو رأی صادره در پرونده‌های «متلوک» در سال ۱۹۷۴ و «راندولف» در سال ۲۰۰۶ مورد توجه قرار گیرد؛ چراکه آخرین گرایش رویه‌ی قضایی به این دکترین، متأثر از رأی سال ۲۰۱۴ پرونده‌ی «فرناندز» علیه «کالیفرنیا» است که خود از دو حکم پرونده‌ی «متلوک» و «راندولف» تبعیت می‌نمود.[1] دیوان عالی ایالات‌متحده آمریکا در پرونده‌ی «ایالات‌متحده آمریکا علیه متلوک»، اصطلاح «قاعده یا دکترین رضایت متصرف مشترک» را تبیین نمود. این قاعده بدین معنی است که زمانی که پلیس برای انجام تفتیش بدون اجازه یا دستور مقام قضایی، از یک ملک، رضایت ارادی یکی از اشخاصی را که با دیگران، برای دسترسی به آن ملک، یک اجازه و اختیار مشترک (با شخص دیگر) دارد، تحصیل می‌نماید، می‌تواند تفتیش خود را بدون این‌که اصلاحیه‌ی چهارم قانون اساسی نقض شود، انجام دهد دیوان عالی کشور آمریکا، اختیار مشترک را به «استفاده متقابل» از اموال به‌وسیله‌ی اشخاصی که «عموماً دسترسی یا کنترل مشترک برای اغلب اهداف دارند» معنی نمود. درواقع در چنین

---

۱. در پرونده فرناندز، وقتی پلیس به آپارتمان والتر فرناندز (Walter Fernandez) رسید، اعتقاد داشت که یک مظنون حمله دسته‌جمعی تبهکارانه که پلیس به دنبال مظنونین آن بود، قبلا به آن منزل وارد شده است. در حین این که آنها به آپارتمان نزدیک می‌شدند، صدای جیغ و دعوا از داخل آپارتمان شنیدند. پلیس درب آپارتمان را زد و دوست غرقه به خون فرناندز، روکسان روجاس (Roxanne Rojas) درب را باز کرد. با این باور که فرناندز احتمال به روجاس حمله کرده بوده است، پلیس تلاش کرد که آنها را از هم دور نگه دارد. فرناندز ضمن این که فریاد می‌زد شما حق ندارید وارد آپارتمان من شوید، متذکر می‌شد که حقوق خود را بلد است و متعاقبا از دستور پلیس مبنی بر این که از روجاس فاصله بگیرد امتناع کرد. خیلی طول نکشید که پلیس متوجه شد فرناندز همان مظنون حمله دسته‌جمعی تبهکاران است و به همین دلیل اصلی وی را بازداشت کرد. حدود یک ساعت بعد پلیس برای این که از روجاس فرناندز برای تفتیش آپارتمان اجازه بگیرد به محل بازگشت و او نیز اجازه داد. فرناندز بعدها قانونی بودن رضایت شخص ثالث را در این پرونده زیر سوال برد. نهایتا در دادگاه، با رای سه در مقابل شش، چنین حکم داده شد که تفتیش انجام شده پس از بازداشت فرناندز نقض اصلاحیه چهارم قانون اساسی نبوده و معتبر است؛ چرا که فرناندز در زمان تفتیش به موجب یک مبنای قانونی بازداشت شده بوده و دیگر حضور در محل نداشته است و زمانی که در محل حضور فیزیکی ندارد، رضایت متصرف ثالث برای تفتیش باید محترم شمرده شود.

وضعیتی است که گفته می‌شود این نتیجه طبیعی خواهد بود که هر یک از ساکنین آن مکان همان‌گونه که حق دسترسی دارند، این حق را نیز دارند که اجازه‌ی تفتیش را به پلیس بدهند و دیگران نیز قاعدتاً این خطر را پذیرفته‌اند یا باید بپذیرند (Matasar, 2015: 203–205) و درواقع، دادگاه در مقام بیان این قاعده بود که چنین مواردی نیاز به اخذ دستور یا مجوز مقام قضایی نخواهد داشت. این قاعده که درواقع، «قاعده‌ی رضایت احدی از متصرفین مشترک یک ملک» بود، بعداً به‌وسیله‌ی رهیافت اتخاذی در پرونده‌ی «ایلینویز علیه رودریگز» در سال ۱۹۹۰ شرح و بسط بیشتری یافت و پس‌ازآن در پرونده‌ی «جورجیا علیه راندولف» در سال ۲۰۰۶ چنین مقرر شد که رضایت شخص ثالث، در هنگام «مخالفت حضوری» شخص دیگری که با وی «اختیار و دسترسی مشترک» دارد، مجوزی برای تفتیش بدون قرار قضایی نخواهد بود و درواقع رهیافت دکترین رضایت شخص ثالث در پرونده‌های «متلوک و رودریگز»، در پرونده‌ی «راندلوف» به‌شرط «اعتبار رضایت ثالث در صورت حضور فیزیکی وی» محدود شد (McNeeley, 2006: 260) و نهایتاً در پرونده‌ی «فرناندز علیه کالیفرنیا» در سال ۲۰۱۴، حکم پرونده‌ی «راندولف» تفصیل داده شد (Voorheis, 2014: 399-401). بر اساس رهیافت جدید مطروحه در پرونده‌ی «فرناندز»، اگر در هنگام تفتیش، یکی از متصرفین مشترک به‌صورت فیزیکی حاضر باشد و مخالفت خود را اعلام کند، پلیس به دلیل اخذ رضایت از متصرف یا متصرفین مشترک دیگر نمی‌تواند به تفتیش بپردازد (Dery, 2014: 1137–1138) و به نظر می‌رسد چنانچه شخص مخالف با تفتیش، بر اساس دلایل قانونی بازداشت شود و از محل برده شود، متصرف مشترک دیگر، حق دارد که به تفتیش بدون قرار پلیس رضایت دهد.

۲. توسعه، تنوع و فراگیری استفاده از خدمات ثالث (متصدیان سیستم‌ها و شبکه-های سایبری)[1] در عصر فن‌آوری‌ها؛

واقعیت این است که حریم خصوصیِ مرتبط با محیط‌های استفاده‌کننده از فن‌آوری‌های نوین، در مقابله با این تئوری تا حد زیادی با محدودیت‌ها و دشواری‌هایی روبرو شده است. از زمانی که جامعه دچار تغییر و تحول شده است، راهکارهای وابسته به استفاده از فن‌آوری‌های ارتباطی متنوع گردیده و در پی آن، قلمرو آنچه تحت شمول دکترین شخص ثالث قرار می‌گیرد نیز گسترش یافته است. امور ارتباطات، تجاری و مالی، به نحو فزاینده‌ای به‌صورت آنلاین گسترش یافته‌اند و از طریق مؤسسات خصوصی فعالیت می‌کنند که در دکترین شخص ثالث، همگی «ثالث» محسوب می‌شوند؛ لذا این دکترین موجب شده است که حجم زیادی از اطلاعات شخصی که می‌توانست تحت عنوان حریم خصوصی مورد حمایت قرار گیرد از این دایره خارج شود (Issacharoff & Wirsha, 2016: 988). شاید به همین دلیل این بود که در سال ۲۰۱۲، پنج قاضی دیوان عالی کشور در ایالات‌متحده آمریکا، در پرونده‌ی ایالات‌متحده علیه جونز[2] اذعان داشتند که دکترین شخص ثالث دیگر نمی‌تواند به شکلی کاملاً مطلق و مطابق با وضعیت اخیرش حفظ شود (Slobogin, 2012: 1–2). امروزه تقریباً تمام خدمات اقتصادی، اجتماعی، فرهنگی و حتی مدنی و سیاسی، بر روی شبکه‌های مبتنی بر وب ارائه می‌شود. هر شبکه رایانه‌ای نیز توسط یک مدیر یا اپراتور سیستم[3] اداره می‌شود. وظیفه‌ی این شخص حفظ کارکرد مداوم سیستم، نظارت بر امنیت و برقراری آن و تعمیر شبکه در زمان بروز مشکل است. بدیهی است که در صورت تعریف مسئولیت برای ارائه‌دهندگان خدمات در فضای سایبر، به‌موجب داده‌های غیرقانونی ارائه‌شده در این فضا توسط کاربرانِ خدمات و تهدیدهای

1. Computer/Internet/Web System Administrators.
2. US v. Jones, 2012 .
3. System Operator.

ارائه‌شده علیه تمامیت و محرمانگی اطلاعات و شبکه‌های رایانه‌ای، باید مقتضیِ مسئولیت برای ارائه‌دهنده‌ی خدمات، یعنی شایستگی برای سرزنش و پاسخگویی بابت قصور یا تقصیر را لحاظ نمود و این شایستگی تنها درزمانی ایجاد می‌شود که توانایی کنترل و نظارت برای آن شخص تعریف شده باشد و چنانچه یک نظام حقوقی، در مبانی فلسفی مسئولیت خود برای این‌گونه اشخاص، دکترینی مانند دکترین تکلیف اشخاصِ محافظ و ناظر بر منبع خطر، به نظارت و امن نگاه‌داشتن آن[۱] را در نظر داشته باشد، باید اختیار بیشتر نظارت و سرکشی به حریم خصوصی را نیز جایز تلقی نماید. درهرصورت، اشخاص ثالث، در دسترسی به سیستم، یک «سطح مبنایی»[۲] را در اختیار دارند که به آن‌ها امکان می‌دهد هر حساب کاربری، یعنی اعتبار مشتری را مشاهده کنند و عموماً هر فایلی را که مربوط به شخص مشترک است را مطالعه نمایند. زمانی که یک مدیر شبکه می‌خواهد به‌صورت اختیاری و رضایت‌مندانه، اطلاعاتی مربوط به اعتبار یک مشتری را برای مأمورین رسمی افشا نماید، دیگر اهمیتی ندارد که این اطلاعات به یک ارائه‌کننده‌ی خدماتی ارتباطی[۳] یا یک تجارت خصوصی[۴] یا یک نهاد دولتی[۵] مربوط است (Kerr, 2001: 25). البته ممکن است بسته به نوع خدماتی که ارائه می‌شود و یا بسته به اطلاعات موردنظر، تشریفات افشا در نظام‌های حقوقی مختلف، متفاوت باشد و برخی اطلاعات از خطر افشای بدون اخذ دستور مقام قضایی برای پلیس، به دور نگه داشته شوند و این چیزی است که نظام حقوقی ایران، به‌طور اساسی و شاید تعمدانه به آن ورودی نداشته است. به‌عنوان‌مثال، در نظام حقوقی آمریکا، برای ارائه‌دهندگان خدمات ارتباطی تجاری عمومی[۶]، مانند گوگل یا یاهو، برای افشای اختیاری و اجباری اطلاعات توسط «ISP»ها، تشریفات ویژه‌ای در قانون

---

۱. برای توضیح بیشتر در این خصوصریال ر.ک: (فضلی، ۱۳۸۹: ۱۱۰)

2. Root Level.
3. Communication Service Provider.
4. Private business.
5. Government entity.
6. Public Commercial Communication Service Provider.

«SCA»[1] پیش‌بینی شده است (Kerr, 2001: 25) و مثلاً ماده ۲۷۰۲ این قانون، ارائه‌دهندگان خدمات را از افشای اختیاری اطلاعاتِ مربوطِ به مشتریان، به دولت، منع می‌کند و افشای اختیاری را تنها در موارد منصوص استثنایی قانون، مقرر در اصلاحیه‌ی چهارم قانون اساسی، جایز می‌داند. درعین‌حال باید پذیرفت که وظیفه‌ی پاسخگویی مدیران شبکه‌ها به مقامات دولتی در پایش فضای سایبری در جمع‌آوری و پردازش برخی اطلاعات مربوط به مشتریان نیز عامل دیگری بوده که موجب شده است ورود به عرصه‌ی پایش و پردازش این اطلاعات و درواقع حریم خصوصی افراد، امری ضروری تلقی شود. در ایالات‌متحده آمریکا، قانون «حریم ارتباطات الکترونیکی»[2]، به چگونگی دستیابی مأموران رسمی، به اطلاعات ذخیره‌شده‌ی مربوط به حساب کاربری اشخاصی که از خدمات شبکه‌ای توسط ارائه‌دهندگان این‌گونه خدمات، نظیر «ISP»ها، می‌پردازد و بر مبنای دکترین رضایت شخص ثالث، ضوابط افشای اطلاعات توسط ارائه‌دهندگان خدمات را تبیین می‌کند. در ایالات‌متحده آمریکا، بااینکه اصلاحیه‌ی چهارم قانون اساسی، اصولاً برای هر تفتیش، صدور مجوز پیشینی قضایی را لازم می‌داند، قانون «حریم ارتباطات الکترونیکی»، عملاً محتوای ذخیره‌شده و برخی اطلاعات دیگر مربوط به‌حساب کاربری اشخاص نزد ارائه‌کنندگان خدمات اینترنتی مأموران را مشمول دکترین رضایت شخص ثالث قرار داده و مأمورین رسمی، اجازه می‌یابند تحت شرایط متنوع و متعددی، حتی بدون اخذ قرار و راساً با صدور و ابلاغ یک احضاریه برای شخص ثالث مزبور، به وی دستور دهند که محتواهای مربوط به حساب کاربری اشخاص را افشا نمایند (Winick, 1994: 75). اگرچه دغدغه‌های حریم خصوصی همواره موجب تغییر در این قوانین می‌شود؛ مانند قانون حریم خصوصی ایمیل‌ها، مصوب ۲۰۱۶ که کنگره ایالات‌متحده تصمیم گرفت با

1. Stored Communications Act (codified at 18 U.S.C. Chapter 121 §§ 2701–2712).
2. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-2522.

تصویب آن، ایرادها و رخنه‌های موجود در قانون ECPA، مصوب ۱۹۸۶ را اصلاح نماید (Brattain, 2016: 188).

۳. فن‌آوری‌های نوین و تحول موضوعات تفتیش؛

در یک رهیافت سنتی از سوی دیوان عالی کشور آمریکا، اشیایی که در محفظه‌های مات قرار دارند، از انتظار متعارف حریم خصوصی برخوردارند، اما آیا ابزارهای ذخیره‌ساز دیجیتالی هم همین‌طور هستند؟ این را باید در نظر داشت که یک هارددرایو، ممکن است کوچک باشد، ولی امکان دارد که جهانی از اطلاعات نامحسوس در آن ذخیره شده باشد (Kerr, 2005: 569). همچنین «با اینکه دادگاه‌ها عموماً پذیرفته‌اند که ابزارهای ذخیره‌ساز الکترونیکی را می‌توان شبیه محفظه‌های بسته دانست، اما دراین‌باره که آیا به هر یک از فایل‌های ذخیره‌شده بر روی رایانه نیز باید به مثابه‌ی دو محفظه‌ی بسته‌ی مجزا نگریسته شود یا خیر، به نتایج متفاوتی رسیده‌اند» (Kerr, 2001: 35). در برخی پرونده‌ها، مانند دعوای «ایالات‌متحده علیه کری»[1]، گرایش بر این بود که بر اساس تفسیر مناسب و مطابق با اهداف اصلاحیه‌ی چهارم، فولدرهای مختلف موجود در یک هارددیسک، همانند محفظه‌های بسته‌ی جداگانه هستند و در برخی دیگر، مانند دعوای «ایالات‌متحده علیه رانیان»[2]، یا دعوای «ایالات‌متحده» علیه «اسلانینا»[3]، کل هارددیسک، منصرف از محتوایش، تنها به‌مثابه‌ی یک محفظه در نظر گرفته شد (Kerr, 2001: 4) و مثلاً در پرونده‌ی «رانیان»، دادگاه اعلام نمود که در شرایطی که یک شخص خصوصی (شخصی به‌غیراز ضابطین)، فایل‌هایی را بر روی کامپیوتر یک متهم دیده است، متهم هیچ انتظار حریم خصوصی‌ای در ارتباط با بقیه فایل‌های روی هارددرایو خود نخواهد داشت (Ziff, 2005: 852). نگاه سنتی اخیر، به تصمیم سال ۱۹۷۹ دیوان عالی کشور آمریکا در پرونده

1. *US v. Carey*, 1999
2. *US v. Runyan*, 2001
3. *US v. Slanina*, 2002

«ایالات‌متحده علیه بوش»[1] بازمی‌گشت که در آن پرونده، گفته شده بود زمانی که یک دفترکل، محتوی ریزدریافت‌ها و پرداخت‌ها، شامل اطلاعاتی است که برای دستیابی به آن یک قرار اخذ می‌شود، ممکن است مأمورین، تفتیش جامع‌تری نسبت به آن دفتر و تفتیشی فراتر از تنها همان صفحات مربوطه انجام دهند (Kerr, 2001: 4). در مقابل، در پرونده‌ی «ایالت متحده علیه والسر»[2]، دادگاه چنین مقرر کرد که «رایانه‌ها، قابلیت نگهداری حجم بسیار زیادی از اطلاعات و انواع مختلف آن را دارند و به‌صورت بالقوه می‌توانند دارای اطلاعات بسیار گسترده‌ای از حریم خصوصی اشخاص باشند که با سایر اطلاعات دیگر درهم‌آمیخته هستند (Kerr, 2001: 5) و لذا زمانی که ضابط در مقام جست‌وجو در رایانه‌ی مزبور است، ممکن است به حریم خصوصی اشخاص تجاوز نماید»[3]. این رهیافت در پرونده «گست» علیه «لیس» (*Guest v. Leis*, 2001) نیز دیده شد و فایل‌های موجود در کامپیوتر به‌عنوان فضاهای مستقل در نظر گرفته شد(Kerr, 2001: 5). درهرصورت، باید قبول کرد که حتی با همین محدودیت-ها، باز هم به نظر می‌رسد در این دیدگاه، پلیس با استفاده از دکترین شخص ثالث، بسیار مقتدر و دارای اختیارات گسترده در سرکشی به قلمرو حریم خصوصی اطلاعات اشخاص و در موقعیت بسیار بهتری نسبت به گذشته خواهد بود، اما به‌عنوان یک نقطه عطف جدی، به دنبال رأی و استدلال قاضی «استومایر» در پرونده «جونز»، عمارت نفوذناپذیر دکترین شخص ثالث دچار فرسایش و سستی شد. درحالی‌که برخی دادگاه‌ها و قضات آن‌ها به سخت‌گیری‌های سابق دکترین شخص ثالث مقید و وفادار باقی مانده بودند(*American Civil Liberties Union v. Clapper*, 2013 (vacated, 785 F.3d 810, 824– 25 (2d Cir. 2015)). *In re US for Historical Cell Site Data*, 2013) ، بقیه قضات، در پرونده‌های دیگر، رهیافت پرونده «جونز» را در دستور کار خود قرار داده بودند و یک انتظار متعارف حریم خصوصی در

1. *United States v. Beusch*, 1979
2. *US v. Walser*, 2001
3. *US v. Walser*, 2001

اطلاعات مربوط به حوزه ارتباطات تلفنی و اطلاعات مربوط و موجود در «Cell-Site»ها[۱] تعریف کرده بودند[۲]. و در یک رأی قابل‌توجه، در پرونده «ریلای» علیه «کالیفرنیا» (*Riley v. California*, 2014)، دیوان از این‌که بخواهد دایره و گستره تفتیش بدنی مشروعِ بدون اخذ متهمی که بازداشت و آن وضعیت، در اصلاحیه چهارم، به‌عنوان یک استثنای قانونی برای تفتیش‌های بدون قرار، به‌صورت سنتی تعریف شده بود، به تفتیش گوشی همراه متهم، متعاقب بازداشت او تسری دهد، امتناع نمود(Issacharoff & Wirsha, 2016: 993). رأی صادره در این پرونده، با اشاره به رأیی که نزدیک به چهار دهه پیش در پرونده «ایالات‌متحده» علیه «رابینسون» (United States v. Robinson, 1973) صادر شده بود، آن را متعادل نمود. در آن پرونده، دادگاه، پذیرفته بود که در تفتیش منجر به بازداشت در موقعیت‌های پذیرفته‌شده در قانون، افسر پلیس اختیار گسترده‌ای برای تفتیش شخص بازداشت‌شده و تمام قلمرو تحت کنترل او در زمان بازداشت داشته باشد (Gillespie, 1999: 11–12). شروع ماجرای پرونده «رابینسون» به سال ۱۹۶۵ بازمی‌گردد. در آن سال، یک افسر پلیس یک ماشین کادیلاک را که «رابینسون» راننده آن بود را بر اساس یک ظن معقول مبنی بر این‌که گواهینامه رانندگی راننده منقضی شده است، متوقف کرد. تمامی سه سرنشین آن ماشین خارج شدند و افسر پلیس راننده را بازداشت کرد. این بازداشت بر اساس مبانی ارائه‌شده به دادگاه صحیح به نظر می‌رسید. افسر پلیس بلافاصله بعد از بازداشت «رابینسون» شروع به تفتیش بدنی او نمود و به پاکت کوچکی برخورد که محتویاتش ابتدا برای افسر نامشخص بود. او پاکت را بیرون آورد. پاکت یک بسته

---

۱. پایگاه سلولی مجموعه آنتن‌ها و تجهیزات ارسال و دریافت رادیویی برای ارتباط بین تلفن‌های همراه سلولی و مرکز راهگزینی تلفن همراه در سیسم تلفن همراه سلولی.

۲. برای مطالعه‌ی پرونده‌هایی که در آنها آرائی موافق با این رهیافت صادر شده است به پرونده‌های ذیل رجوع نماید:

- United States v. Graham, 796 F.3d 332, 344–61 (4th Cir. 2015).
- United States v. Davis, 754 F.3d 1205, 1215 (11th Cir. 2014).
- Klayman v. Obama, 957 F. Supp. 2d 1, 33 (D.D.C. 2013), vacated, 800 F.3d 559 (D.C. Cir. 2015).

سیگار مچاله شده بود. درب آن را باز کرد و داخل آن را نیز تفتیش کرد و متعاقب تفتیش، ۱۴ عدد کپسول هروئین کشف نمود؛ اگرچه نهایتاً دادگاه هروئین کشف‌شده را در آن اوضاع‌واحوال؛ به‌عنوان دلیل کسب‌شده در یک تفتیش بدون قرار، در موقعیتی که شخص برای رانندگی بدون پروانه بازداشت شده بود، نپذیرفت و آن را استنادناپذیر دانست(Aaronson & Wallace, 1975: 67–98). درهرصورت، حتی با صدور این رأی نیز تعرضی به اختیار کامل تفتیش پلیس در این موقعیت‌ها ایجاد نشد و مدتی بعد، با اشاره به این پرونده، دادگاه در پرونده «ریلای» استدلال کرد که ازنظر فیزیکی، تفتیش تلفن همراه ممکن است شبیه به تفتیش کیف پول، کیف‌دستی و دیگر مواردی که در پرونده «رابینسون» مقرر شده بود باشد (Lamparello & MacLean, 2014: 2488) و لذا در یک کاربرد ماشینی، فیزیکی و بدون فکر، می‌توان معیار «رابینسون» را به تمام پرونده‌ای مشابه نیز تسری داد (Ibid :2484)؛ اما دادگاه به استدلال خود مطلبی افزود که بسیار حائز اهمیت بود. دادگاه با استدلالی تمثیلی تأکید کرد که «اگرچه سوار بر زین اسب نشستن و به مسافرت رفتن، مسافرتی مانند سوار موشک شدن و به ماه رفتن و هر دو، یک نوع سوار شدن و مسافرت کردن است، اما حقیقت این است که تفاوت بسیار باهم دارند و درواقع دادگاه با تبیین این مثال، درصدد این بود که بگوید قیاس تفتیش جیب لباس با تفتیش تلفن همراه، شبیه قیاس مسافرت توسط اسب با مسافرت با موشک به ماه است! دادگاه اصرار داشت که تلفن‌های همراه نوین، آن‌چنان سطحی از اطلاعات مربوط به حریم خصوصی ارتباطی یا اطلاعاتی شخص را در خود ذخیره کرده‌اند که هرگز قابل‌مقایسه با حریم خصوصی نیست که ممکن است در تفتیش یک بسته سیگار یا یک کیف یا جیب متهم مورد تعرض قرار گیرد.» (Ibid: 2488–2489). بدین ترتیب می‌توان گفت که: «حافظه‌های مدرن اطلاعاتی یا ابزارهایی که قابلیت ذخیره اطلاعات را دارند، مانند تلفن‌های هوشمند، تنها یک ابزار دیگر برای مقصود اصلی اختراعشان، مانند برقراری ارتباط به‌صورت پیشرفته و فن‌آورانه نیستند. به دلیل تمام چیزهایی که این تلفن‌ها می‌توانند در خود ذخیره کنند و همه‌ی چیزهایی که این

تلفن‌ها می‌توانند افشا نمایند، برای بسیاری از مردم، آن‌ها داخل در قلمرو «حریم خصوصی زندگی‌شان» هستند؛ و این واقعیت که فن‌آوری پیشرفته در حال حاضر اجازه می‌دهد یک شخص چنین حجمی از اطلاعات محرمانه را با خود حمل نماید، باعث نمی‌شود که ارزش حریم خصوصی این اطلاعات از آن چیزی که بنیان‌گذاران دفاع از حریم خصوصی در نظر داشتند و برای آن چندین دهه جنگیده‌اند کمتر قلمداد شود» (Issacharoff & Wirsha, 2016: 994). به تعبیر دیگر، در یک ارتباط مستقیم‌تر با دکترین شخص ثالث، فن‌آوری‌های نوین و همیشه در حال تکامل، مقایسه نمودن موضوعات دیجیتال را با موضوعات سنتی را سخت و در برخی موارد غیرممکن نموده است.

همچنین در تبیین مبانی هنجارین دکترین شخص ثالث، در حقوق کامن‌لا، برخی دادگاه‌ها در ابتدای پیدایش تئوری تا چند دهه به‌صورت عقلی استدلال می‌کردند که در دکترین شخص ثالث، ارائه‌دهندگان خدمات، مانند دوستان دروغین هستند و چنین فرضی موجب می‌شد مفهوم انتظار رعایت حریم خصوصی بر اساس معیار شخصی متزلزل شود و کاهش یابد (Stern, 2013: 379). این تفسیر از دکترین شخص ثالث برای کاهش انتظار حریم خصوصی تا این میزان، مخالفت‌های فراوانی را موجب شد؛ چراکه مشتریانِ استفاده از خدمات عمومی، قدرت انتخاب زیادی برای استفاده از خدمات جایگزین برای آن خدماتی که ارائه‌کننده‌اش، می‌توانست و یا مجاز بود که اطلاعات مشتری را افشا نماید نداشتند و لذا آن‌ها درواقع مجبور و موظف می‌شدند که برای استفاده از خدمات، اطلاعات خود را در اختیار دیگری قرار دهند؛ درحالی‌که آشکار است که ممکن است این اطلاعات زمانی علیه آن‌ها مورداستفاده قرار گیرد (Henderson, 2004: 520).

بااین‌حال تا اخیراً نیز انتقاداتِ گسترده‌ی مطروحه، هیچ توجیه مناسبِ دارایِ جایگزینِ مناسب‌تری برای نظریه کاهش انتظارات حریم خصوصی در موقعیت‌های شخص ثالث مطرح

نکرده است. در مقابل، در مقاله‌ای که در سال ۲۰۰۹ منتشر شد، «اورین کر»[1] از این دکترین چنین دفاع کرد که دکترین بین رفتارهای عمومی و خصوصی تمایز قائل می‌شود و بر همین اساس این امکان را برای خطاکاران از بین می‌برد تا بتوانند فعالیت‌های خود را که در معرض عموم است با استفاده از فرصت دفاع حریم خصوصی به قلمرو مربوطه بکشانند و بدین ترتیب برای خود مصونیت ایجاد نمایند. او می‌گوید دکترین از این‌که مجرمین پشت حصار و سپر حریم خصوصی زمانی که از تلفن، حساب بانکی، ایمیل یا هر نوع خدمات عمومی دیگری استفاده می‌نمایند مخفی شوند؛ ممانعت می‌کند؛ درحالی‌که این توانایی‌ها پس از ظهور فن‌آوری‌های نوین ایجاد شده است و مجرمین به‌جای این‌که مجبور باشند عملکرد مستقیم و درنتیجه ردپای مستقیمی بر جای بگذارند از طریق خدماتی که ثالث ارائه می‌دهد راحت‌تر عمل می‌کنند و آن ادله‌ای که از رفتار آن‌ها در عموم، قبلاً قابل‌مشاهده بود، از بین برده و پشت حصار حریم خصوصی مخفی می‌شوند؛ کاری که تعادل میان مفهوم حریم خصوصی و اختیارات مأمورین رسمی در نظارت، تعقیب و اجرای عدالت را از بین می‌برد(Kerr, 2009: 564). طرفداران این ایده می‌گویند «یک رفتار ذاتاً عمومی نباید با یک نقاب فنّاورانه وصف خصوصی پیدا نماید و این رفتارها، نه به دلیل به اشتراک گذاشته شدن، بلکه به دلیل ماهیت و ذات عمومی آن‌ها برای دسترسی پلیس، آشکار باقی خواهد ماند و این نتیجه خود بدان دلیل است که چنین اطلاعاتی در جهان بدون جایگزین‌های فنّاورانه، عمومی باقی می‌ماندند. لذا اگر شخصی حتی اگر از شخص ثالث بهره نبرد، بلکه صرفاً رفتاری را که سابقاً از خود ردپا باقی می‌گذاشت، به کمک یک فن‌آوری، مخفی نماید، بازهم رفتار عمومی باید عمومی باقی بماند و لذا اگر پلیس به هر شکل بتواند به اطلاعات دسترسی پیدا کند، متهم هیچ حقی برای رد ادله به بهانه‌ی خصوصی بودن آن‌ها ندارد؛ چون آن اطلاعات در اصل و در ذات، عمومی بوده است.» (Stern, 2013: 390) لذا بر این مبنا که چنانچه ابزاری موجب شده باشد که رفتار یا

1. Orin S. Kerr.

اطلاعاتی از قلمرو حریم عمومی، جنبه و ظاهر خصوصی به خود بگیرد، به‌نحوی‌که اگر آن ابراز و یا ترفند وجود نداشت، آن موضوع، قابل‌مشاهده برای عموم و در حوزه حقوق عمومی باقی می‌ماند، هرگز نباید حکم کرد که به قلمرو حریم خصوصی وارد شده است، پست و تلفن که رفتارهای عمومی را ظاهر خصوصی می‌بخشند نیز نباید خصیصه عمومی رفتار متعلق به خود را به خصوصی تغییر دهند چراکه بر اساس این تئوری، زمانی می‌توان گفت که یک رفتار در حوزه قلمرو حریم خصوصی وجود دارد که امکان این‌که جایگزین یک رفتار عمومی شده، به‌هیچ‌وجه وجود نداشته باشد.

دلایل زیادی برای رد این نگرش وجود دارد. یکی از مهم‌ترین ایرادات کاربردی در این حوزه این است که دکترین شخص ثالث تنها به اطلاعاتی محدود نمی‌شود که اگر وسیله جایگزینی اختراع نمی‌شد تا متهم آن را ذخیره نماید و نقاب حریم خصوصی به آن بدهد، قابل‌مشاهده و عمومی باقی می‌ماند. به‌عنوان‌مثال، دکترین شخص ثالث، علاوه بر جواز دسترسی به شماره تلفن‌های مشتریان یک شرکت تلفن، دسترسی به زمان برقراری تماس و مدت‌زمان تماس انجام‌شده را هم جایز می‌داند. درحالی‌که اگر متهم به‌جای آن‌که تماس تلفنی بگیرد، برای دیدن همدستش مسافرت می‌نمود، بسیار بعید بود که اطلاعاتی همانند این‌که در ملاقات انجام‌شده، چه مدت‌زمانی متهم صحبت نموده و در چه زمانی صحبت کرده است، به این دقّت قابل‌تعیین باشد. درحالی‌که در برخی موارد، چنین دقّت و جزئیاتی، برای توجیه وجود سبب محتمل بسیار حیاتی و مؤثر به شمار می‌رود و این جزئیات، در شرایطی که گفتگو در پشت درب‌های بسته صورت پذیرد، با احتمال زیاد غیرقابل‌دسترس باقی خواهند ماند. واقعیت این است که حتی اگر رفتار قابل‌مشاهده متهم در یک‌زمان و به یک‌زمان مشخص هم باشد، بازهم ارائه‌دهندگان خدمات مبتنی بر شبکه، نسبت به آن ردپاهایی که متهم با رفتار سنّتی خود به‌جای می‌گذاشت، جزئیات و وسعت بیشتری از اطلاعات را ذخیره می‌کنند؛ درحالی‌که هنوز هیچ دادگاهی این اعتقاد را ندارد که این جزئیات برای پلیس و نهایتاً دادگاه در دادرسی غیرقابل

استفاده است. همچنین، بدون شک اگر بخواهیم اطلاعات ثبت‌شده در بانک را با اسنادی که در یک فضای باز برای عموم رها شده است را کاملاً شبیه به هم و ذیل یک حکم بدانیم، مبنای چندان درستی برای حکم خود در نظر نگرفته‌ایم. بعلاوه، این تئوری، برای این استدلال خود که «هر چیزی که در دنیای بدون فنّاورانه عمومی تلقی می‌شود و دارای یک جنبه قابل‌مشاهده در آن وضعیت است، پس لزوماً باید خارج از حریم خصوصی محسوب شود»، هیچ مبنایی ارائه نمی‌کند. واقعیت این است که این نگرش که ما رفتاری را که در حال حاضر در پشت درب‌های بسته و به‌دوراز دسترس پلیس صورت می‌گرفت به این دلیل که اگر در زمان گذشته واقع می‌شد به‌ناچار در منظر عمومی واقع می‌گردید و قابل پنهان کردن نبود، باید عمومی تلقی کنیم خیلی منطقی به نظر نمی‌رسد. در حقیقت به نظر می‌رسد که در این نگاه، در اصل، به این دلیل که موازنه سنّتی بین رفتارهای مجرمانه و کنترل پلیس به هم خورده است، ما به دنبال روشی برای برقراری موازنه جدید هستیم؛ درحالی‌که چنین راهکاری، یک روش منطبق بر استانداردهای قانونی مانند احترام به حریم خصوصی تلقی نمی‌شود و ما در این شیوه، تنها به دنبال افزایش نرخ جرائم قابل‌کشف توسط پلیس بوده و یک نتیجه‌ی مطلوب را بدون امعان نظر به مبانی علم حقوق، به‌عنوان یک هدف تلقّی کرده‌ایم و به همین دلیل، احتمال بسیار خواهد داشت که از چهارچوب اهداف عالیه حقوق خارج گردیم. درعین‌حال، حتی ممکن است این تصور که با ورود فن‌آوری‌ها، مجرمین در پشت نقاب فن‌آوری‌ها مخفی شده‌اند و ردپاهای بسیار کمتری از خود به‌جا می‌گذارند نیز نادرست باشد و شاید «پلیس در این وضعیت، در موقعیت بسیار بهتری نسبت به گذشته قرار گرفته باشد» (Stern, 2013: 389).

٤. تردید در کارآیی تئوری دکترین شخص ثالث، در عصر فن‌آوری‌های نوین:

در سال ۲۰۱۲، پنج قاضی دادگاه، در پرونده ایالات‌متحده علیه جونز(US v. Jones, 2012) ، اذعان داشتند که دکترین شخص ثالث دیگر نمی‌تواند به شکلی کاملاً مطلق و مطابق با وضعیت اخیرش حفظ شود، اگرچه این پنج دیوان عالی نتوانستند یک راهکار کنترلی جایگزین نیز

پیشنهاد نمایند(Kerr, 2012: 1,3–4). ضرورت بررسی تئوریک دکترین شخص ثالث با حکم اخیر دادگاه در پرونده‌ی «ریلای» علیه «کالیفرنیا» بیشتر احساس شد. در این پرونده در ارزیابی تفتیش تلفن همراه یک متهم که متعاقب بازداشت وی صورت گرفته بود، دادگاه به‌اتفاق آرا احراز کرد که تغییرات سریع فن‌آوری و انتظارات اجتماعی، از کاربردهای ساده و قدیمی دکترین شخص ثالث در اصلاحیه چهارم فاصله گرفته است و آن کاربردها را بیهوده و کم‌اثر نموده است (Issacharoff & Wirsha, 2016: 988). در این راستا، نظریه‌پردازان، انتقادات تندوتیز مفصلی نسبت به دکترین شخص ثالث داشته‌اند[1]. این ایرادات بر هر دو ضابطه مطروحه در این تئوری وارد می‌شود: الف- نخست: آیا معیار انتظار ذهنی یا شخصی برای رعایت حریم خصوصی در حال حاضر در قیاس با گذشته، قضاوت یکسانی برای موضوعات ارائه می‌دهد؟ ب- دوم: آیا این معیار که شاخص مذکور در بند پیشین، باید ازنظر جامعه متعارف تلقی شود نیز در مواجهه با فن‌آوری‌های نوین نسبت به گذشته، منتج به نتیجه یکسانی می‌شود؟ در پاسخ به سؤال اول، بسیاری، بحث‌وجدل بر سر این باور نمودند که تغییرات فنّاوری، معیار ذهنی یا شخصی انتظار متعارف حریم خصوصی در تئوری دکترین شخص ثالث را تغییر داده است. آن‌ها می‌گفتند ممکن است که سابق بر این، این حرف قابل‌قبول تلقی می‌شد که تصمیم یک شخص برای ارائه اطلاعات به شخص ثالث، می‌توانست نشان از عدم انتظار معقول حفظ حریم خصوصی باشد؛ اما انتظارات اخیر در حال حاضر متفاوت هستند. در جامعه دیجیتال مدرن، افراد به شکل معمول از اینترنت به‌منظور مکاتبه و برقراری ارتباطات و ذخیره اطلاعاتی که به‌عنوان اطلاعاتی کاملاً خصوصی به آن‌ها می‌نگرند، استفاده می‌نمایند (Mulligan, 2004: 1551,1571). برای مثال، رشد استفاده از پدیده‌ی «Cloud Computing» یا « Cloud

---

۱. این موضوع به تفصیل در (Tokson, 2010, p. 581) مورد بررسی قرار گرفته است.

storage»[1] که از آن در متون فارسی، با عنوان «رایانش ابری» نیز یاد شده است تا حد قابل‌توجهی چالش‌هایی را در رابطه باوجود یا عدم وجود یک انتظار معقول برای رعایت حریم خصوصی در خصوص اطلاعاتی که از این طریق در دسترس شخص ثالث قرار می‌گیرد، ایجاد کرده است (Suo, Liu, Wan & Zhou, 2013: 655–659)؛ چراکه اشخاص در هنگام استفاده از این فن‌آوری(برای توضیح بیشتر در این خصوص، ر.ک: «مرکز پژوهش‌ها – رایانش ابری»، بدون تاریخ)، به‌طور کامل انتظار دارند که حریم خصوصی آن‌ها رعایت شود. ذخیره در فضای ابری یکی از ساده‌ترین و کم دردسرترین شیوه‌های موجود است. در حقیقت با این شیوه داده-های خود را روی فضایی متشکل از رایانه‌های مختلف که به‌هم‌پیوسته هستند، قرار می‌دهیم و در صورت نیاز می‌توانیم به آن‌ها دست یابیم. هرروز میلیون‌ها کاربر حجم زیادی از محتوای دیجیتال در دنیا را تولید می‌کنند. فیلم، عکس و فایل‌های متنی بخشی از این محتوای دیجیتال است که بی‌شک باید در جایی ذخیره شوند. در گذشته اگرچه چیزی مانند هارددیسکِ رایانه،

---

۱. مدل Cloud Computing که از آن در برخی متون به رایانش ابری نیز تعبیر شده است، مدلی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی (شامل زیرساخت، نرم‌افزار، بستر و سایر منابع رایانشی) با به کارگیری شبکه ارائه می‌کند. این اصطلاح از ترکیب دو کلمه محاسبه کامپیوتری (رایانش) و ابر ایجاد شده است. ابر در اینجا استعاره از شبکه یا شبکه‌ای از شبکه‌های وسیع مانند اینترنت است که کاربر معمولی از پشت صحنه و آنچه در پی آن اتفاق می‌افتد اطلاع دقیقی ندارد (مانند داخل ابر). در نمودارهای شبکه‌های رایانه‌ای نیز از شکل ابر برای نشان دادن شبکه اینترنت استفاده می‌شود. دلیل تشبیه به ابر در این است که این تکنیک مانند ابر جزئیات فنی‌اش را از دید کاربران پنهان می‌سازد و لایه‌ای از انتزاع را بین این جزئیات فنی و کاربران به وجود می‌آورد. نرم‌افزارهای کاربردی و اطلاعات، روی سرورها ذخیره می‌گردند و بر اساس تقاضا در اختیار کاربران قرار می‌گیرد. جزئیات از دید کاربر مخفی می‌مانند و کاربران نیازی به آشنایی یا کنترل در مورد فناوری زیرساخت ابری که از آن استفاده می‌کنند ندارند. رایانش ابری راهکارهایی برای ارائه خدمات فناوری اطلاعات به شیوه‌های مشابه با صنایع همگانی (آب، برق، تلفن و ...) پیشنهاد می‌کند. ذخیره‌ساز ابری یا «Cloud storage» نیز فضای تعبیه شده بر روی یک سرور به اشتراک گذاشته شده با مالکیتِ شخص ثالثِ ارائه دهنده‌ی خدمات است که عملاً به جای چندین هارددرایو محلی عمل خواهد کرد. برای توضیح بیشتر در این رابطه، ر.ک:
(Aaronson & Wallace, 1975: 2321,2323)

پاسخگوی این تراکنش‌ها بود، اما امروزه این نیاز فراتر رفته و باید به دنبال راه‌های جایگزینی برای این حجم زیاد داده بود. امروزه بسیاری از شرکت‌های بزرگ حوزه دیجیتال، خدمات ذخیره‌سازی در فضای ابری را بر اساس همین تکنیک و فن‌آوری، به کاربران خود در جهان ارائه می‌کنند. «مایکروسافت» با سرویس «وان‌درایو»[1]، «گوگل» با سرویس «گوگل‌درایو»[2]، «اپل» با «آی‌کلاود»[3] و «آمازون» با «کلاوددرایو»[4] و «دراپ‌باکس»[5] و بسیاری دیگر از ارائه-کنندگان این نوع خدمات، در این زمینه، حضوری رقابتی دارند. همه این سرویس‌ها حجم قابل‌توجهی را بر روی سرورهای خود به کاربران خود، رایگان یا درازای مبلغ ناچیزی ارائه می‌دهند. به‌عنوان‌مثال، در «آی‌کلود»، کمپانی «اپل»، اطلاعات دستگاه‌های اپل شما را در خود ذخیره می‌کند و به‌طور بیسیم و از طریق شبکه، آن را به تمام دستگاه‌هایتان می‌فرستد و همه‌چیز به‌صورت خودکار انجام می‌شود. ادعای آن‌ها این است که این روش آسان‌ترین روش برای مدیریت، ذخیره و بازیابی فایل‌ها روی دستگاه‌های مختلف است. آن‌ها تمامی اطلاعات تماس، موسیقی‌ها، تصاویر، برنامه‌ها، تقویم‌ها و تمامی اسناد و اطلاعات فراوان دیگری را ذخیره می-کنند و شما از طریق دستگاه‌های دیگران به آن‌ها دسترسی خواهید داشت(Gold, 2014: 2321,2323). بدین ترتیب، حتی ما دیگر با یک کامپیوتر یا یک هارددیسک ساده هم روبرو نیستیم. در حال حاضر، این خطر وجود دارد که با قرائت سنتی از دکترین شخص ثالث، اطلاعات موجود در فضاهای رایانش ابری، تحت نظارت چشمان نظارت‌گر مأمورین قانون قرار گیرند و بسیاری اعتقاد دارند که دست‌کم «ذخیره‌سازهای ابری رایگان ازنظر حریم خصوصی هرگز محافظت‌شده نیستند» (Robison, 2010: 1195,1223) و این در حالی است

1. One Drive.
2. Google Drive.
3. iCloude.
4. Cloud Drive.
5. DropBox.

که حقوقدانان متذکر می‌شوند که بدون تردید، ذخیره‌سازهای ابری، شایستگی حمایت بیشتری نسبت به یک کیف‌دستی ازنظر حریم خصوصی دارا می‌باشند (Couillard, 2009: 2219–2220).

برای بررسی این ادعا که معیار ذهنی و شخصی موجود در دکترین شخص ثالث تغییر یافته است یا خیر، یک پژوهش میدانی و آماری انجام‌شده، نشان می‌دهد که دکترین، از اطلاعاتی به‌عنوان حریم خصوصی دفاع می‌کند که مردم آن‌ها را بسیار کم‌اهمیت‌تر و عمومی‌تر از اطلاعاتی می‌دانند که مورد حمایت این دکترین و اصلاحیه نیست؛ چراکه واقعیت این است که نظارت، دستیابی یا آنالیز متادیتاهای ایمیل، هجمه و تاخت‌وتازهای بسیار وحشتناک‌تری به حریم خصوصی در مقایسه با تفتیش‌های وسایط نقلیه یا بازرسی‌های بدنی انجام می‌دهد (Slobogin, 2008, p. 183)؛ درحالی‌که عموماً در درجه توجه و دغدغه کمتری نسبت به آن‌ها قرار گرفته است. ایراد دیگر که بسیار محل تأمل قرار می‌گیرد این است که دکترین، از شناسایی این امکان و احتمال واقعی که افراد می‌توانند اطلاعاتشان را با اهداف مشخص و به نحو کنترل‌شده‌ای نزد اشخاص ثالث افشا کنند و حق داشته باشند که این افشا نزد شخص ثالث، به معنی افشا برای تمامی جهانیان محسوب نشود، طفره می‌رود و امتناع می‌کند، اما حقیقتاً هیچ دلیلی وجود ندارد که باور داشته باشیم افشای اطلاعات نزد مخاطبین محدود، اخلاقاً و منطقاً با افشای اطلاعات نزد تمام جهان کاملاً برابر باشد (Colb, 2002: 119,122). این عقیده مبنی بر این‌که «یک شخص ممکن است و می‌تواند بپذیرد که از بخشی از اطلاعات محرمانه خود، پس از به اشتراک گذاشته شدن اطلاعاتش با ثالث، صرف‌نظر کرده باشد» (Ibid: 119,122)، بسیار منطقی‌تر از تحمیلِ یک چشم‌پوشیِ اجباری به آن شخص، از تمام حریم خصوصی خود در رابطه با آن اطلاعات خواهد بود و درواقع، یک مفهوم دقیق‌تر و ظریف‌تر از حریم خصوصی زمانی می‌تواند خوشایند و مطلوب باشد که باوجود به اشتراک گذاشتن اطلاعات حساس، حریم خصوصی آن‌ها در شرایطی محفوظ باقی بماند؛ والا ممکن است ما با عصر «زهد

اطلاعاتی»[1] روبرو شویم که در آن مردم از این‌که در جامعه اطلاعاتی مشارکت نمایند، کراهت داشته باشند (Solove, 2004: 217). امری که نباید مورد غفلت قرار بگیرد این است که این راه‌حل تنها یک راهبرد عملی برای اجرای بهتر قانون بدون توجه به سرنوشت هنجارهایی مانند حریم خصوصی است و دکترین شخص ثالث نباید به نحوی تفسیر و یا اجرا شود که حریم خصوصی یا اهداف غایی و هنجارین هر نظام حقوقی مخدوش شود.

اما همان‌گونه که گفته شد، ایراد وارده تنها به بخش نخست این دکترین وارد نمی‌شود. ورود فن‌آوری‌های نوین نیز باعث شده است که انتظار ذهنی متفاوتی که هم‌اکنون نسبت به گذشته ایجاد شده است، باید به‌عنوان انتظارات معقول عینی تلقی شوند. منتقدین دکترین شخص ثالث استدلال می‌کنند که تنها این موضوع مطرح نیست که افراد، توقع داشته باشند که حریم خصوصی آن‌ها در اینترنت محترم شمرده شود، بلکه آن‌ها باید مستحق چنین انتظاری از حفظ حریم خصوصی شناخته شوند. تبادل اطلاعات حساس از طریق اینترنت به روش‌های بسیار، دیگر یک انتخاب نیست. قاضی دیوان عالی، «مارشال» در مخالفتش با دیدگاه‌های مطرح‌شده در پرونده «اسمیت»، چنین نگرانی‌هایی را مطرح نموده است. او می‌گوید «مفهوم ضمنی یا التزام در مفهومِ فرضیه خطر، بدین معنی که شخص در زمان در اختیار قرار دادن اطلاعات خود به ثالث، این خطر را پذیرفته است که ممکن است ثالث اطلاعات را برای دولت افشا نماید، بدین معنا است که شخص در واگذاری خود به ثالث مخیر بوده و حق انتخاب یا رها کردن این گزینه را داشته است {و لذا خود، آن شیوه و آن عواقب احتمالی را انتخاب کرده است}»، وی در ادامه استدلال می‌نماید که این واقعاً یک انتخاب نیست و مردم در انتخاب خود، «ناچار» به نظر می‌رسند و در بیشتر موارد، مردم نمی‌خواهند و رضایت ندارند که این نظارت انجام شود ولی چاره دیگری ندارند. او می‌گوید «این خیلی بی‌معنی به نظر می‌رسد که سخن از «پذیرش ریسک» نماییم، زمانی که مردم در زمان انتخاب، هیچ جانشین واقعی برای آنچه پیش روی خود دارند، نمی‌بینند» (Smith v. Maryland, 1979: 479–750). به نظر می‌رسد استدلال قاضی مارشال، امروزه که شاید بیش از هشتاد درصد مردم روزانه بر اینترنت متکی شده‌اند،

1. Information Age Hermits.

جایگاه ویژه‌ای پیدا کرده است (Tokson, 2010: 588). همان‌گونه که خدمات حیاتی بیشتری به‌صورت آنلاین ارائه می‌شود، دسترسی به خدمات دولتی که امروزه بدون جایگزین دیگری، صرفاً در فضای سایبر ارائه شده و این نحوه‌ی ارائه افزایش می‌یابد (West, n.d.: 2-3)، درخواست کاریابی و یا حتی مکاتبه، همگی بدون استفاده از اینترنت به نحو فزاینده‌ای دشوارتر شده است (Issacharoff & Wirsha, 2016: 996). این مسئله قطعاً، غیرقابل‌انکار است که به چرخش انداختن اطلاعات خصوصی از طریق اینترنت، برای انجام امور عادی و ضروری، به نحوی آشکار، اجتناب‌ناپذیر شده است. بر اساس این اجتناب‌ناپذیری، پروفسور «ریچارد اپستین»[1] با این ایده که «استفاده از واسطه‌ای به نام شخص ثالث برای بهره‌مندی از این خدمات در بستر اینترنت، به‌عنوان رضایت به نظارت دولتی می‌تواند محسوب شود»، به‌شدت مخالفت می‌کند و بالاتر از آن، اعتقاد دارد که این بهره‌مندی از خدمات از طریق ثالث، حتی نمی‌تواند بدین معنی تلقی شود که به‌صورت مشروع و قانونی می‌توانیم فرض نماییم که شخص، پذیرفته است که ممکن است یک احتمال برای نظارت قانونی وجود داشته باشد (Epstein, 2009: 1205). عده‌ای استدلال می‌کنند همین که دولت‌ها به شهروندانشان هشدار دهند که حضور در این فضا به معنای پذیرفتن نظارت مطلق دولت است، برای مشروعیت این نظارت کفایت می‌کند. واقعیت این است که قاعدتاً بسیاری از دولت‌ها می‌توانند برای خودشان قوانینی را وضع نمایند که حریم خصوصی اشخاص را لاغرتر و لاغرتر نماید. به تعبیر دیگر، آن‌ها می‌توانند به نقض حریم خصوصی خود، لباس فاخری از مواد قانونی بپوشانند ولی این کار، تنها مانند این است که بگویند ما به حریم خصوصی شما نظارت خواهیم کرد؛ شما پرده‌های منزل خود را بکشید؛ اما به این دلیل که ما از قبل به‌صورت قانونی، از قبل به شما اعلام کرده‌ایم، پس می‌توانیم داخل منزل شما را نیز زیر نظر بگیریم! (Ibid: 1205) و نیازی به توضیح بیشتر نیست که قانونی بودن رفتارها، هرگز مبنایی برای انسانی و یا عادلانه بودن آن قوانین و آن رفتارها محسوب نمی‌شود. از طرف دیگر، در یک ایده و نظریه‌ی جالب، حق دسترسی به اینترنت، از حقوق اساسی بشر، همانند حق دسترسی به اطلاعات، حق آزادی بیان، حق انتخاب شغل و مانند

1. Richard A. Epstein.

آن‌ها است(Lim & Sexton, 2011: 295,315). لذا لازم است که این حق نوین، یا مصداق نوینی از ترکیبِ چند حقِ از قبل شناخته‌شده، همان حکمی را دارد که سایر حقوق اساسی داشته است؛ یعنی لازم است که با سایر حقوق و آزادی‌ها به تعادل برسد و راهکارِ به تعادل رساندن، با تعطیلی و یا نقض مطلق حق متفاوت است. کما این‌که فرانسه، استونی، فنلاند، یونان، اسپانیا و شورای حقوق بشر ایالات‌متحده آمریکا، دسترسی به اینترنت را ازجمله موارد حقوق بشر اعلام نموده‌اند (Wiebe, 2012: 219).

برآمد؛

در دکترین شخص ثالث، سخت از پذیرفتن ریسک یا خطرِ انتقال اطلاعات توسط ثالث به دولت است. گفته می‌شود که «یک سپرده‌گذار با افشای اطلاعات مربوط به امور تجاری‌اش برای دیگری، این خطر را که اطلاعاتش توسط آن فرد به دولت منتقل شود را می‌پذیرد» (United States v. Miller, 1976). منطبق بر همین رهیافت، بسیار بالاتر از این ایده که «شخص استفاده-کننده از خدمات، احتمال این را می‌داده است که اطلاعاتش منتقل شود»، ادعا شده است که باید بپذیریم «سپرده‌گذار [یا دیگر افراد استفاده‌کننده از خدمات ثالث]، داوطلبانه با افشا موافقت نموده‌اند» (Kerr, 2009: 588–590) ، اما به‌درستی و در تقابل با این ایده، برخی دیگر، قویاً در انتقاد از این ایده، متذکر شده‌اند که «اطلاع از وجود خطر انتقال اطلاعات»، از جنبه تحلیلی و فلسفی و حتی در واقعیت امر، هرگز معادل با «پذیرش رضایتمندانه‌ی افشا و موافقت بر افشای اطلاعات» نخواهد بود و نیست؛ چراکه اشخاص نمی‌توانند خارج از چهارچوب موجود با شخص ثالث قرارداد ببندند و درعین‌حال، باید توجه داشت که ما نهایتاً در این وضعیت، به کمک و به‌وسیله‌ی قانونِ حقوقِ اعتباری در مقابل حقوق طبیعی است که «حکومت فرضیه پذیرش خطر افشا» را بر اشخاص تحمیل خواهیم کرد؛ نه این‌که آن‌ها خود قبول نموده باشند؛ لذا رضایت، مفروض نخواهد بود (Epstein, 2009: 1206). مدافعان دکترین سنتی شخص ثالث، ممکن است این‌گونه پاسخ دهند که یک فرد، درصورتی‌که به دنبال خصوصی نگه‌داشتن اطلاعات است،

می‌تواند به‌راحتی، قید «قرارداد بستن» با طرف‌های ثالث را بزند؛ ولی حتی خود کسانی که این مسئله را مطرح می‌نمایند، اعتراف می‌کنند که چنین گزینه‌ای هیچ‌گاه نمی‌تواند عملی باشد (Georgia v. Randolph, 2006) و قطعاً در دنیای مدرن، حتی یک نوع محروم‌سازی از حقوق اولیه‌ی انسانی و مبتنی بر نسل‌های اول و دوم محسوب می‌شود (US v. Jones, 2012) و برخی از حقوقدانان این مفهوم را که «نظارت الکترونیکی فراگیر، درصورتی‌که از طریق طرف‌های ثالث انجام شود، تحت عنوان رضایت قابل توجیه هستند» را بسیار غریب و ناسازگار معرفی می‌کنند. درحالی‌که تصمیم مأخوذه از پرونده کاتز علیه ایالات‌متحده آمریکا (Katz v. United States, 1967) ، در سال ۱۹۶۷، نزدیک به سه دهه بدین شکل مورد تأسی قرار گرفت که اشخاص هیچ انتظار متعارفی برای رعایت حریم خصوصی خود در خصوص اطلاعاتی که با ارائه‌دهندگان خدماتی چون شرکت‌های تلفن، شرکت‌های ارائه‌دهنده خدمات همگانی، بانک‌ها یا حتی یک حسابدار به اشتراک می‌گذارند نخواهد داشت (Stern, 2013: 378) ، اما به‌تدریج این استدلال قوت گرفت که در قضیه دکترین شخص ثالث، صرفاً یک کاهش انتظار درباره حریم خصوصی وجود دارد و این کاهش، برای تمامی موارد و انواعِ مختلفِ اطلاعات نیز قابل‌اعمال نخواهد بود. واقعیت این است که این موضوع صحیح است که در مقایسه‌ی زمانی که مجرمین امکان بهره‌برداری از فنّاوری را نداشتند با حال حاضر، بدون تردید باید گفت که مقدار قابل‌توجه و فراوانی از رفتارها که در آن موقع قابل‌مشاهده برای دیگران بود، در حال حاضر قابل مخفی کردن است، اما این تنها فقط یک توصیف است و معلوم نیست که چگونه می‌توان این توصیف را مبنایی برای این حکم قرار داد که «در موقعیت‌های دکترین شخص ثالث، انتظار متعارف حریم خصوصی کم شده یا وجود ندارد» و لذا شاید صحیح این باشد برای این‌که تعادل موجود بین حریم خصوصی و میزان و تنوع فعالیت‌های پلیسی را در آن زمان که به آن تعادل سنتی می‌گوییم، در حال حاضر نیز حفظ شود، لازم است که در نگرش دکترین شخص ثالث، برخی ضابطه‌ها تغییر و یا تعریف شوند و رویکردهای نوینی جایگزین رویکردهای سابق شوند

چراکه موضوعات تغییر کرده و یا جایگزین شده‌اند، لذا مناسبات جدیدی نیز ازنظر ضوابط قانونی لازم به تعریف هستند (Kerr, 2011: 482). به‌عبارت‌دیگر، رویه ابتدایی و حتی جاری دکترین شخص ثالث که اطلاعاتِ نزدِ ثالث را خارج از حمایت‌های حریم خصوصی قرار می‌دهد صحیح به نظر نمی‌رسد و شایسته است که اولاً این‌گونه تفتیش‌ها، بسته به موضوع، شرایط و میزان آسیبی که به حریم خصوصی وارد می‌شود، به ترتیب سخت به آسان، در رسته‌های تشریفاتی ذیل قرار گیرد: الف- الزام به اخذ مقام قرار قضایی. ب- الزام به اثبات وجود سبب محتمل. ج- الزام به اثبات ایجاد ظن متعارف در شرایط پیرامونی موضوع تفتیش. درعین‌حال لازم است که برای تمامی موارد، اصل معقول و متعارف بودن تفتیش اثبات گردد. همچنین می‌توان ترتیبات کلی دیگری مانند ضرورت ارسال تقاضانامه برای متصدی خدمات (شخص ثالث) با شرایط متفاوت نسبت به رسته‌ای مختلف فوق برای این‌گونه تفتیش‌ها تعریف نمود. درهرصورت، باید توجه داشت که دستور مقام قضایی یا اقدامات بدون نیاز به قرار قضایی از سوی ضابطین دادگستری، نیازمند رعایت ملاحظات و احتیاط فراوان نسبت به حریم خصوصی اشخاص است؛ زمانی که یک تفتیش بدون قرار انجام می‌شود، قبول این مسئله بسیار دشوار است که به پلیس اجازه داده شود تا برای تمامی اسناد را بررسی نماید تا بفهمد که کدام‌یک از این اسناد بر اساس قوانین حریم خصوصی، غیرقابل‌تفتیش و کدام‌یک قابل‌تفتیش هستند! (Stern, 2013: 394–395) و در نظر نگارنده، سپردن اختیار تشخیص در این حوزه به ضابط قضایی و حتی قاضی دادگستری، در برخی نظام‌های قضایی مانند ایران که از ضعف علمی عمومی قضات و تعداد فراوان پرونده‌ها رنج می‌برد، به‌شدت نگران‌کننده است. درهرصورت، به‌تدریج، این ایده که «یک فرد هیچ انتظار مشروع حریم خصوصی‌ای در مورد اطلاعاتی که داوطلبانه به طرف‌های ثالث می‌دهد ندارد» (Smith v. Maryland, 1979)، صریحاً محکوم شده است. ولی حتی درصورتی‌که یک فرد کلاً فاقد یک انتظار مشروع در زمینه حریم خصوصی نباشد، این لزوماً بدین‌صورت نخواهد شد که انتظار وی در رابطه با حریم خصوصی، به هیچ اندازه‌ای کاهش نیافته

است. پذیرش اینکه انتظارات کاهش‌یافته‌ای، نه اینکه هیچ انتظاری وجود نداشته باشد، درباره حریم خصوصی، برخلاف رویکرد اتخاذی در پرونده‌های «ایالات‌متحده علیه میلر» (United States v. Miller, 1976) و «اسمیت علیه مری‌لند(Smith v. Maryland, 1979) ، در اعتبار یا حساب کاربری اشخاص در نزد ثالث، وجود داشته باشد، حقیقتاً تنها رویکردی است که می‌تواند به مبانی، اصول و اهداف حقوق بشر و به‌طورکلی علم حقوق، نزدیک تلقی شود. همان‌گونه که در رویه قضایی آمریکا و در پرونده «ریلی علیه ایالت کالیفرنیا» (Riley v. California, 2014) در سال ۲۰۱۴ مطرح شد، «این واقعیت که یک فرد دستگیرشده، منافع کاهش‌یافته حریم خصوصی دارد، بدان معنا نیست که اصلاحیه چهارم کلاً بی‌اعتبار شود» و منظور این است که ضوابط معیار انتظار حریم خصوصی برای وی احتمالاً وجود خواهد داشت (Riley v. California, 2014) لذا تا حدود زیادی پذیرفته شده است که افراد نمی‌توانند، یا نباید، واقعاً انتظار خصوصی ماندن تمام اطلاعاتی که قبلاً برای شخص ثالثی افشا شده است را داشته باشند. در پرونده «ریلِی»، قاضی الیتو[1]، هم‌عقیده با رهیافت اتخاذی در پرونده «ایالات‌متحده علیه جونز» (US v. Jones, 2012) ، اذعان نمود که «حتی درصورتی‌که عموم مردم از کاهش حریم خصوصی ناشی از اثرات فنّاوری‌های جدید استقبال نکنند، ولی نهایتاً مجبور هستند که خود را با این پیشرفت‌ها تطبیق دهند» (US v. Jones, 2012)، اما چنین رهیافتی هرگز نباید باعث ایجاد اسقاط حق حریم خصوصی به‌طور مطلق شود و لذا لازم است که نسبت به اطلاعات مختلف، موضوعات مختلف، اشخاص مختلف و مصالح مختلف، تشریفات مختلفی برای افشای اطلاعات موجود در نزد ثالث ترسیم و تعریف شود. درواقع لازم است که ارائه‌دهندگان خدمات در قالب ضوابط مشخصی با مجریان قانون همکاری نمایند ولی این ضوابط هرگز بی‌حدوحصر نیست و همان‌طور که در بند ۴ ماده ۱۹ کنوانسیون جرائم سایبر آمده(جلالی فراهانی (مترجم)، ۱۳۸۹:

1. Samuel Alito

۸۰)، لازم است «متعارف بودن» آن احراز گردد[1] و در تشخیص متعارف بودن، شرایط و موضوعات مختلفی از قبیل تفاوت داده‌های شکلی و محتوایی یا اوضاع‌واحوال پیرامونی و میزان خطرناکی جرم و یا درجه‌ی اهمیت آن ازنظر حریم خصوصی اطلاعاتی اشخاص مورد توجه خواهد گرفت.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

۱. جلالی فراهانی، ۱۳۸۹، ص ۲۸۱

منابع؛

- آشوری، محمد. (۱۳۸۸). *آیین دادرسی کیفری*. (ویرایش چاپ پانزدهم، ج اول). تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- اورین اس. کِر و گروه نویسندگان. (۱۳۸۸). *تفتیش و توقیف رایانه‌ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری*. (امیرحسین، جلالی فراهانی، مترجم). تهران: روزنامه رسمی جمهوری اسلامی ایران.
- ورواییی، اکبر، جهانگیرپور، علی، جربانی، حمید و هاشمی، حمید. (۱۳۸۹). »بازرسی منازل، اماکن و اشیاء اشخاص در حقوق کیفری ایران با رویکرد به اسناد بین‌المللی». *دانش انتظامی*. (۵۱)، ۴۱ – ۸۲
- انصاری، باقر. (۱۳۸۳). «حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران». *مجله دانشکده حقوق و علوم سیاسی*. (۶۶)، صص ۲۰–۲۵.
- انصاری، باقر. (۱۳۸۷). *آزادی اطلاعات*. تهران: دادگستر.
- بوریکان، ژان و سیمون، آن ماری. (۱۳۸۹). *آیین دادرسی کیفری*. (تدین، عباس، مترجم). تهران: خرسندی.
- جلالی فراهانی، امیرحسین. (۱۳۸۹). *درآمدی بر آئین دادرسی کیفری جرائم سایبری*. تهران: خرسندی.
- جلالی فراهانی (مترجم)، امیرحسین. (۱۳۸۹). *کنوانسیون جرائم سایبر و پروتکل الحاقی آن*. تهران: خرسندی.
- خالقی، علی. (۱۳۹۴). *آئین دادرسی کیفری*. (ویرایش یازدهم، ج اول). تهران: موسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
- رحمدل، منصور. (۱۳۹۳). *آیین دادرسی کیفری: تحقیقات مقدماتی، قرارها، صلاحیت و رسیدگی*. (ج دوم). تهران: دادگستر.
- فضلی، مهدی. (۱۳۸۹). *مسئولیت کیفری در فضای سایبر*. تهران: خرسندی.

- مؤذن‌زادگان، حسنعلی. (۱۳۷۲). «اختیارات بی‌رویه مأمورین انتظامی». *حقوقی دادگستری*. (۷)، ۸۵ – ۹۴.

- مرکز پژوهش‌ها - رایانش ابری. (بدون تاریخ). بازیابی ۱۷ مهر ۱۳۹۵، از http://rc.majlis.ir/fa/report/show/800669

- یوسفی، ایمان. (۱۳۹۲). *حقوق جزای تطبیقی: تحقیقات مقدماتی در آیین دادرسی کیفری (ایران، کامن‌لا، رومی- ژرمنی)*. تهران: جاودانه.

- یزدان‌پور (مترجم)، اسماعیل. (۱۳۸۴). *علم در جامعه اطلاعاتی*. تهران: کمیسیون ملی یونسکو در ایران، دبیرخانه شورای عالی اطلاع‌رسانی.

- White ،James B. (1974). *The Fourth Amendment as a Way of Talking about People: A Study of Robinson and Matlock. The Supreme Court Review*. *1974* ، 165–232.

- Aaronson, D. E. & Wallace, R. (1975). "Reconsideration of the Fourth Amendment's Doctrine of Search Incident to Arrest", A Georgetown Law Journal, *64*, 53.

- Abrams, S. E. (1984). "Third-Party Consent Searches, the Supreme Court, and the Fourth Amendment". The Journal Of Criminal Law And Criminology *(1973-)*, *75*(3), 963–994. DOI: 10.2307/1143652

- Amar, A. R. (1996). "The Fourth Amendment, Boston, and the Writs of Assistance". Suffolk University Law Review, *30*, 53.

- American Civil Liberties Union v. Clapper., 959 F. Supp. 2d 724 (Dist. Court December 27, 2013).

- Brattain, B. (2016). "The Electronic Communications Privacy Act: Does The Act Let The Goverment Snoop Through Your Emails And will It Continue?" NCJL & Tech. *On.*, *17*, 185–329.

- Campbell, T. (1992). "Illinois v. Rodriguez: Should Apparent Authority Validate Third-Party Consent Searches". University Of Colorado Law Review, 63, 481.

- Colb, S. (2002). "What is a Search? Two Conceptual Flaws in Fourth Amendment Doctine and Some Hints of a Remedy". Cornell Law Faculty Publications.

- Couch v. United States., 409 US 322 (Supreme Court January 09, 1973).

- Couillard, D. A. (2009). Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing.

- COUNCIL, O. E. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *Explanatory Report. Strasbourg*, *28*.

- Dery, G. M. I. (2014). "Creating the Right to Deny Yourself Privacy: The Supreme Court Broadens Police Search Powers in Consent Cases in Fernandez v. California". Michigan State Law Review, *2014*, 1129.

- Epstein, R. A. (2009). "Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations". Berkeley Technology Law Journal, *24*(3), 1199–1227.

- Fernandez v. California., 134 S. Ct. 1126 (Supreme Court February 25, 2014).

- Fiske, A. (2006). "Disputed-Consent Searches: An Uncharacteristic Step toward Reinforcing Defendants' Privacy Rights". Denver University Law Review, *84*, 721.

- Fox, R. C. (1955). "Evidence: Admissibility in Federal Courts of Record of Telephone Conversation: Meaning of "Interception"". Michigan Law Review, *53*(4), 623–625. DOI: 10.2307/1285264

- Georgia v. Randolph., 547 US 103 (Supreme Court March 22, 2006).

- Gillespie, D. T. (1999). Bright-Line Rules: Development of the Law of Search and Seizure during Traffic Stops. *Loyola University Chicago Law Journal*, *31*, 1.

- Gold, A. J. (2014). "Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts through Locally Installed Software". William & Mary Law Review, *56*, 2321.

- Guest v. Leis., 255 F. 3d 325 (Court of Appeals, 6th Circuit 2001).

- Henderson, S. E. (2004). "Nothing New under the Sun - A Technologically Rational Doctrine of Fourth Amendment Search". Mercer Law Review, *56*, 507.

- Illinois v. Rodriguez., 497 US 177 (Supreme Court June 21, 1990).

- In re US for Historical Cell Site Data., 724 F. 3d 600 (Court of Appeals, 5th Circuit July 30, 2013).

- Issacharoff, L. & Wirsha, K. (2016). "Restoring Reason to the Third Party Doctrine". Minnesota Law Review, *100*, 985.

- Katz v. United States., 389 US 347 (Supreme Court December 18, 1967).

- Kerr, O. S. (2001). Searching and seizing computers and obtaining electronic evidence in criminal investigations. US Department of Justice, Computer Crime and Intellectual Property Section.

- Kerr, O. S. (2005). Searches and Seizures in a Digital World. Harvard Law Review, 119(2), 531–585.

- Kerr, O. S. (2009). The Case for the Third-Party Doctrine. Michigan Law Review, 107(4), 561–601.

- Kerr, O. S. (2011). "An Equilibrium-Adjustment Theory Of The Fourth Amendment". Harvard Law Review, 125(2), 476–543.

- Kerr, O. S. (2012). The Mosaic Theory of the Fourth Amendment.

- Korff, D. (2002). Comparative summary of national laws. Brussels: EC Study On Implementation Of Data Protection Directive.

- Lamparello, A. & MacLean, C. E. (2014). Riley v. California: The New Katz or Chimel?

- Lim, Y. J. & Sexton, S. E. (2011). "Internet as a Human Right: A Practical Legal Framework to Address the Unique Nature of the Medium and to Promote Development". Washington Journal Of Law, Technology & Arts, 7, 295.

- Matasar, E. (2015). "Finest of Fine Lines: Randolph, Fernandez, and What Remains of the Fourth Amendment When a Roommate Consents to a Search". Lewis & Clark Law Review, 19, 203.

- McLaughlin, K. (2006). "The Fourth Amendment and Cell Phone Location Tracking: Where Are We". Hastings Communications And Entertainment Law Journal (Comm/Ent), 29, 421.
- McNeeley, M. E. (2006). "Constitutional Law - Search and Seizure - Validity of Consent to Warrantless Search of Residence When Co-Occupant Expressly Objects". Tennessee Law Review, 74, 259.
- Mulligan, D. K. (2004). "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act". George Washington Law Review, 72, 1557.
- Newfield v. Ryan. (1937) (Vol. 302). Supreme Court.
- Riley v. California., 134 S. Ct. 2473 (Supreme Court June 25, 2014).
- Robison, W. J. (2010). Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act.
- Sánchez Abril, P., Levin, A. & Del Riego, A. (2012). "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee". American Business Law Journal, 49(1), 63–124.
- Slobogin, C. (2008). "Privacy at Risk: The New Government Surveillance and the Fourth Amendment". University of Chicago Press.
- Slobogin, C. (2012). Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory.
- Smith v. Maryland., 442 US 735 (Supreme Court June 20, 1979).
- Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. NYU Press.
- Stern, S. (2013). "The Third-Party Doctrine and the Third Person". New Criminal Law Review: In International And Interdisciplinary Journal, 16(3), 364–412.
- Suo, H., Liu, Z., Wan, J. & Zhou, K. (2013). Security and privacy in mobile cloud computing. In 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 655–659). IEEE.
- Tokson, M. (2010). "Automation and the Fourth Amendment". Iowa Law Review, 96, 581.

- United States v. Beusch., 596 F. 2d 871 (Court of Appeals, 9th Circuit May 10, 1979).
- United States v. Matlock., 415 US 164 (Supreme Court February 20, 1974).
- United States v. Miller., 425 US 435 (Supreme Court April 21, 1976).
- United States v. Robinson., 414 US 218 (Supreme Court December 11, 1973).
- US v. Carey., 172 F. 3d 1268 (Court of Appeals, 10th Circuit April 14, 1999).
- US v. Jones., 132 S. Ct. 945 (Supreme Court January 23, 2012).
- US v. Runyan., 275 F. 3d 449 (Court of Appeals, 5th Circuit December 10, 2001).
- US v. Slanina., 283 F. 3d 670 (Court of Appeals, 5th Circuit February 21, 2002).
- US v. Walser., 275 F. 3d 981 (Court of Appeals, 10th Circuit December 28, 2001).
- Voorheis, P. (2014). "Fernandez v. California: Co-Occupant Consent Searches and the Continued Erosion of the Fourth Amendment". Denver University Law Review, 92, 399.
- Webb, M. W. J. (2008). Third-Party Consent Searches after Randolph: The Circuit Split over Police Removal of an Objecting Tenant. Fordham Law Review, 77, 3371.
- West, D. M. (n.d.). State and Federal Electronic Government in the United States, 2008. Retrieved from http://www.uquebec.ca/observgo/fichiers/65274_PSP-1.pdf
- Wiebe, B. (2012). "BART's Unconstitutional Speech Restriction: Adapting Free Speech Principles to Absolute Wireless Censorship". University Of San Francisco Law Review, 47, 195.
- Winick, R. (1994). "Searches and Seizures of Computers and Computer Data". Harvard Journal Of Law & Technology, 8, 75.
- Ziff, D. J. S. (2005). "Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant". Columbia Law Review, 105(3), 841–872.