ترجمه

پروتکل برکلی

در مورد تحقیقات متن باز دیجیتال

آخرین بازبینی این متن: تابستان ۱۴۰۵

ترجمه حاضر از «پروتکل برکلی در مورد تحقیقات متن‌باز دیجیتال: راهنمای عملی برای استفادهٔ مؤثر از اطلاعات متن‌باز دیجیتال در تحقیقات مربوط به موارد نقض قوانین بین‌المللی کیفری، حقوق بشری و بشردوستانه»، منتشرشده از سوی مرکز حقوق بشر دانشکدهٔ حقوق دانشگاه برکلی و دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد، ترجمه رسمی، مصوب یا تأییدشده توسط سازمان ملل متحد نیست و نباید به‌عنوان نسخه رسمی یا دارای اعتبار رسمی تلقی شود.

این ترجمه صرفاً توسط مرکز اسناد حقوق بشر ایران تهیه شده و در فرآیند ترجمه، نهایت دقت، امانت‌داری حرفه‌ای و وفاداری به متن اصلی به عمل آمده است. با این حال، با توجه به این که این ترجمه از سوی مراجع رسمی ذی‌صلاح تأیید یا گواهی نشده است، هیچ‌گونه وصف رسمی یا حجیت ناشی از ترجمه رسمی برای آن متصور نیست.

ازاین‌رو، در مواردی که استناد حقوقی، قضایی یا اداری به متن ضروری باشد، ملاک، متن اصلی یا ترجمه رسمی مورد تأیید مراجع صلاحیت‌دار خواهد بود و این ترجمه صرفاً با هدف تسهیل مطالعه، پژوهش و بهره‌برداری علمی و تخصصی در اختیار مخاطبان قرار گرفته است.

پروتکل برکلی
در مورد تحقیقات متن باز دیجیتال

راهنمای عملی برای استفادهٔ مؤثر از اطلاعات متن باز دیجیتال در تحقیقات مربوط به موارد نقض قوانین بین‌المللی کیفری، حقوق بشری و بشردوستانه

مرکز حقوق بشر ، دانشکدهٔ حقوق دانشگاه برکلی

دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد

نیویورک و ژنو، 2022

HR/PUB/20/2
ISBN: 978-92-1-154233-2
eISBN: 978-92-1-005343-3
Sales No.: E.20.XIV.4

این اثر توسط سازمان ملل متحد، به نمایندگی از دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد (OHCHR) و مرکز حقوق بشر دانشکده حقوق دانشگاه کالیفرنیا در برکلی، منتشر شده است.

تصویر روی جلد: تصویر ماهواره‌ای دیپ فِیک [جعل عمیق] که توسط احمد الجمال با استفاده از پلتفرم هوش مصنوعی پِلِی فرم (Playform) تولید شده است.

مرکز حقوق بشر دانشکده حقوق دانشگاه کالیفرنیا در برکلی، از حمایت مالی اهداکنندگان زیر سپاسگزاری می‌کند: بنیاد سیگرید راازینگ؛ بنیاد اوک؛ اهداکنندگان فردی در دانشگاه کالیفرنیا، برکلی؛ بنیادهای جامعه باز؛ و مرکز بلاجیو در بنیاد راکفلر.

پیشگفتار

از اوایل دهه ۱۹۹۰، ابزارهای دیجیتال و اینترنت، همانند دوربین و تلفن در دوران پیش از آنها، نحوهٔ دریافت، جمع‌آوری و انتشار اطلاعات در مورد نقض حقوق بشر و سایر موارد نقض جدی حقوق بین‌الملل، از جمله جنایات بین‌المللی را متحول کرده‌اند.

امروزه، محققان می‌توانند از طیف وسیعی از تصاویر ماهواره‌ای عمومی، ویدئوها و عکس‌ها، از جمله موادی که از طریق تلفن‌های هوشمند در اینترنت بارگذاری شده و پست‌های شبکه‌های اجتماعی، دربارهٔ موارد نقض احتمالی حقوق بشر و دیگر موارد نقض جدی قوانین بین‌المللی، از جمله جنایات بین‌المللی، داده‌هایی را به دست آورند. این پیشرفت به محققان کمک کرده است تا با دور زدن دولت‌ها و سایر نگهبانان سنتی اطلاعات، به اطلاعات کلیدی مربوط به تخلفات، حتی در زمان رخ دادن آنها، دسترسی پیدا کنند. این اطلاعات در غیر این صورت از دید عموم پنهان می‌ماند.

با این حال، اطلاعات متن باز دیجیتال عمدتاً به نحوی موردی مورد استفاده قرار گرفته است زیرا سازمان‌های حقوق بشری، نهادهای بین‌دولتی، سازوکارهای تحقیقی و دادگاه‌ها برای تطبیق شیوه‌های کاری خود با روش‌های جدید دیجیتالی جمع‌آوری و تحلیل اطلاعات، به دفعات با چالش مواجه شده‌اند. یکی از بزرگترین چالش‌هایی که این سازمان‌ها با آن روبرو هستند، رسیدگی به کشف و راستی‌آزمایی مطالب مربوط به یک موضوع، در بین مقادیر فزایندهٔ اطلاعات آنلاین، به ویژه عکس‌ها و ویدئوهایی است که توسط تلفن‌های هوشمند و سایر دستگاه‌های همراه ضبط شده‌اند، که برخی از آن‌ها ممکن است مورد دستبرد قرار گرفته یا به ااشتباه به موضوع مورد نظر منتسب شده باشند.

در همین حال، تشکیل شدن دادگاه‌های کیفری بین‌المللی و سازوکارهای تحقیقاتی، و همچنین نهادهای ملی برای رسیدگی جنایات جنگی، نیاز به وجودِ استانداردهای مشترک برای ثبت، حفظ و تحلیل اطلاعات متن باز که می‌توانند به عنوان شواهد و مدارک در محاکمات جنایی ارائه شوند را افزایش داده است. برای اینکه اطلاعات متن باز به عنوان شواهد در دادگاه پذیرفته شوند، دادستان‌ها و وکلای مدافع باید معمولاً بتوانند اصالت و زنجیره حفظ آن را اثبات کنند. مدیریت و پردازش مناسب این مواد، احتمال استفاده از آنها توسط دادستان‌ها و وکلای مدافع را به طور قابل توجهی افزایش خواهد داد. با این حال، اگر روش‌های نادرست جمع‌آوری و حفظ به کار گرفته شوند، اطلاعات حاصله نمی‌تواند برای اثبات حقایق در یک پرونده به عنوان منابع قابل اعتماد در نظر گرفته شود. در ارزیابی اهمیت و اعتبار اطلاعات متن باز، چه به عنوان شواهد ارتباطی و چه به عنوان شواهد مبتنی بر جرم، استفاده از معیارهای واضح و مشخص برای دادگاه‌ها و مکانیسم‌های تحقیقاتی سودمند خواهد بود. . استانداردهای روش‌شناسی معمول برای اصالت‌سنجی و راستی‌آزمایی، به کمیسیون‌های تحقیقاتی حقوق بشر نیز که به طور فزاینده‌ای از مواد متن باز دیجیتال در تحقیقات خود استفاده می‌کنند، کمک خواهد کرد.

کمیسیون‌های تحقیق، واحدهای حقوق بشری ماموریتهای حفاظت از صلح، دفاتر میدانی دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد (OHCHR) و دیگر برنامه‌های نظارتی و تحقیقاتی حقوق بشر سازمان ملل متحد همگی از اصول و روش‌های روش‌شناسی صحیح استفاده می‌کنند تا اعتبار و ارزش یافته‌های آنها افزایش یابد.

برای پاسخ به این نیاز، مؤسسات ما، مرکز حقوق بشر دانشکدهٔ حقوق دانشگاه کالیفرنیا در برکلی، و دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد، با یکدیگر همکاری کرده‌اند تا «*پروتکل برکلی در تحقیقات متن باز دیجیتال:* راهنمای عملی برای استفادهٔ مؤثر از اطلاعات متن باز دیجیتال در تحقیقات مربوط به موارد نقض قوانین بین‌المللی کیفری، حقوق بشری و بشردوستانه » ارا منتشر کنند. مسیری که به انتشار این سند منتهی شد در سال ۲۰۰۹ در دانشگاه برکلی آغاز گردید. در آن زمان، مرکز حقوق بشر دانشگاه برکلی کارشناسان حقوقی، فناوران، روزنامه‌نگاران و فعالان را گرد هم آورد تا استراتژی‌هایی را برای استفاده از فناوری‌ها و روش‌های دیجیتال برای افشای موارد نقض حقوق بشر و مستندسازی آنها به وجود آورند. از آن زمان به بعد، مرکز حقوق بشر، با همکاری مجموعه‌ای از کارشناسان فنی، حقوقی و روش‌شناسی، از جمله کارشناسان دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد، یک سری کارگاه‌های میان‌رشته‌ای را به منظور تبادل افکار، توسعه ابزارهای جدید و شناسایی و حصول معیارها، استانداردها و روش‌های کشف، ارزیابی، تشخیص و حفظ اطلاعات متن باز دیجیتال به منظور مستندسازی موارد نقض حقوق بشر و محاکمهٔ عاملان آنها برگزار کرده است. این فرآیند با تلاش‌های دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد برای تهیهٔ راهنمایی‌ها و ابزارهایی جهت حمایت و مشاوره با کمیسیون‌های تحقیق و هیئت‌های حقیقت‌یاب سازمان ملل متحد و کارکنان دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد در استفادهٔ روزافزون آنها از اطلاعات متن باز در کارهای حقیقت‌یابی و تحقیقی هماهنگ بود.

افرادی با دیدگاه‌های حرفه‌ای متنوع، زمینه‌های حقوقی و فرهنگی مختلف، جنسیت‌ها و ملیت‌های گوناگون در پدید آوردن پروتکل برکلی مشارکت داشتند. این روند شامل بیش از ۱۵۰ جلسهٔ مشورتی با کارشناسان و مشارکت نهادهای اصلی ذینفع، از جمله محققان حقوق بشر سازمان ملل متحد، بوده است. این پروتکل همچنین از تخصص گروه‌های کاری متخصص در بخش روش‌شناسی، آموزشی و پرورشی دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد و دفتر دادستانی دیوان کیفری بین‌المللی بهره برده است. دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد و مرکز حقوق بشر ، پروتکل برکلی را بر اساس استانداردهای بین‌المللی در توسعه روش‌شناسی جدید تحت مراحل دقیق بررسی، بازبینی و ارزیابی قرار دادند.

پروتکل برکلی با تکیه بر این رویکرد همکارانه ، شامل استانداردهای بین‌المللی برای انجام تحقیقات آنلاین در بارهٔ موارد انتسابی نقض قانون بین‌المللی حقوق بشر و حقوق بین‌المللی بشردوستانه و کیفری است. این پروتکل همچنین در مورد روش‌ها و شیوه‌های جمع‌آوری، تحلیل و حفظ اطلاعات دیجیتال به صورت حرفه‌ای، قانونی و اخلاق راهنمایی‌هایی را ارائه می‌دهد. در نهایت، پروتکل برکلی اقداماتی را تعیین می‌کند که محققان آنلاین می‌توانند برای حفاظت از امنیت دیجیتال، جسمی و روانی خود و دیگران، از جمله شهود، قربانیان و پاسخ‌دهندگان اولیه (مانند شهروندان، فعالان و روزنامه‌نگاران) که رفاه خود را برای مستندسازی نقض‌های حقوق بشر و موارد جدی نقض قوانین بین‌المللی به خطر می‌اندازند، انجام دهند.

پروتکل برکلی در ادامهٔ دو پروتکل پیشین سازمان ملل متحد تدوین شده است: پروتکل مینسوتا در مورد تحقیقات مرگ‌های احتمالی غیرقانونی (۱۹۹۱، به‌روزرسانی شده در ۲۰۱۶)، و راهنمای تحقیق و مستندسازی مؤثر شکنجه و سایر رفتارها یا مجازات‌های ظالمانه، غیرانسانی یا تحقیرآمیز (پروتکل استانبول) (۱۹۹۹، به‌روزرسانی شده در ۲۰۰۴). پروتکل مینسوتا که توسط وکلا و دانشمندان پزشکی قانونی که در دهه ۱۹۸۰ در جستجوی افراد ناپدید

شده مشغول بودند، تهیه شده است، استانداردها و شیوه‌های بین‌المللی برای انجام تحقیقات پزشکی قانونی در مورد مرگ‌های مشکوک یا بدون حضور شاهد را تعیین می‌کند و به عنوان ابزاری برای ارزیابی اعتبار چنین تحقیقاتی عمل می‌کند. مشابهاً، پروتکل استانبول به پزشکان و وکلا راهنمایی‌هایی ارائه می‌دهد که چگونه عواقب جسمی و روانی شکنجه را شناسایی و مستندسازی کنند تا این مستندات به عنوان شواهد معتبر در دادگاه یا در زمینه‌های دیگر، از جمله در تحقیقات و نظارت بر حقوق بشر، مورد استفاده قرار گیرند. هر سه پروتکل بر این باور استوارند که علم، فناوری و قانون می‌توانند و باید با یکدیگر در خدمت حقوق بشر عمل کنند. مانند پروتکل‌های قبلی، پروتکل برکلی نیز به زبان‌های رسمی سازمان ملل متحد در دسترس قرار خواهد گرفت تا استفاده و کاربری آن در سراسر جهان تسهیل شود.

امیدواریم که در دنیایی که به طور فزاینده‌ای دیجیتالی شده است، پروتکل برکلی به محققان آنلاین - چه وکلا، مدافعان حقوق بشر، روزنامه‌نگاران یا دیگر افراد - کمک کند تا روش‌های مؤثر برای مستندسازی و تشخیص موارد نقض قانون بین‌المللی حقوق بشر، حقوق بشردوستانه بین‌المللی و حقوق کیفری بین‌المللی را توسعه داده و اجرا کنند و از اطلاعات متن باز دیجیتال استفاده بهینه به عمل آورند تا عدالت در بارهٔ کسانی که مرتکب این نقض‌ها شده‌اند، به اجرا درآید.

امضاء: اریک استوور، رئیس دانشکده، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
امضاء: میشل باچله، کمیسریای عالی حقوق بشر سازمان ملل متحد

چکیـــــده

تحقیقات متن باز تحقیقاتی هستند که تماماً یا بخشی از آن بر اطلاعاتِ موجود در دسترسِ عموم تکیه دارند تا تحقیقاتی رسمی و سیستماتیک را به صورت آنلاین درباره تخلفات انتسابی انجام دهند. امروزه مقادیر زیادی از اطلاعات موجود برای عموم از طریق اینترنت قابل دسترسی است،. این فضای دیجیتال که سریعاً در حال شکل گیری است، منجر به ظهور انواع و منابع جدید اطلاعات شده که می‌توانند در تحقیق درباره نقض‌های انتسابی حقوق بشر و جنایات جدی بین‌المللی کمک کنند. توانایی تحقیق در مورد چنین اتهاماتی برای محققانی که نمی‌توانند به‌موقع به صحنه‌های جرم دسترسی فیزیکی پیدا کنند، اهمیت ویژه‌ای دارد، چنان چه چنین وضعیتی اغلب در تحقیقات بین‌المللی رخ می‌دهد،

اطلاعات متن باز می‌تواند سرنخ‌هایی فراهم کند، از مبنای برون‌داده‌های اطلاعاتی باشدو مستقیماً به عنوان شواهد در دادگاه‌ها مورد استفاده قرار گیرد. با این حال، برای اینکه این اطلاعات در فرآیندهای تحقیقاتی رسمی، از جمله تحقیقات قانونی، کمیسیون‌های حقیقت‌یاب و هیئت‌های تحقیقاتی، مورد استفاده قرار گیرد، محققان باید از روش‌های هماهنگی استفاده کنند که هم دقت یافته‌هایشان را تقویت کرده و هم به قضات و دیگر حقیقت‌یابان اجازه دهد کیفیت فرآیند تحقیق را بهتر ارزیابی کنند. پروتکل برکلی در تحقیقات متن باز دیجیتال برای ارائه استانداردها و راهنمایی‌های بین‌المللی به محققان در زمینه‌های حقوق کیفری بین‌المللی و حقوق بشر به وجود آمد. چنین محققانی از مجموعه‌ای از نهادها، از جمله رسانه‌ها، گروه‌های جامعه مدنی و سازمان‌های غیر دولتی، سازمان‌های بین‌المللی، دادگاه‌ها و آژانس‌های تحقیقاتی ملی و بین‌المللی می‌آیند. ایجاد استانداردهای ثابت و سنجش‌پذیر برای حمایت از این حوزه چندرشته‌ای به معنای حرفه‌ای‌سازی تحقیقات متن باز است.

در حالی که رهنمودها و آموزش‌های مربوط به استفاده از ابزارها و نرم‌افزارهای خاص بخش مهمی از بهبود کیفیت تحقیقات متن باز دیجیتال هستند، پروتکل برکلی بر فناوری‌ها، پلتفرم‌ها، نرم‌افزارها یا ابزارهای خاص تمرکز نمی‌کند، بلکه بر اصول و روش‌های پایه‌ای که می‌توانند به طور ثابت اعمال شوند، حتی با تغییر خود فناوری، تأکید دارد. این اصول، حداقل استانداردهای قانونی و اخلاقی برای انجام تحقیقات مؤثر متن باز را تعیین می‌کنند. با پیروی از راهنمایی‌های موجود در پروتکل برکلی، محققان به تضمین کیفیت کار خود کمک خواهند کرد و در عین حال خطرات فیزیکی، روانی و دیجیتالی برای خود و دیگران را به حداقل می‌رسانند.

پروتکل برکلی به عنوان یک ابزار آموزشی و یک راهنمای مرجع برای محققان متن باز طراحی شده است. به دنبالِ فصل مقدماتی، سه فصل بعد به چارچوب‌های کلی اختصاص داده شده‌اند، از جمله اصول، ملاحظات قانونی و امنیت. فصل‌های باقیمانده بر فرآیند تحقیق تمرکز دارند. این بخش از پروتکل برکلی با فصلی در مورد آمادگی و برنامه‌ریزی استراتژیک آغاز می‌شود و به دنبال آن فصلی به مراحل مختلف تحقیقاتی مورد نیاز - یعنی، پرس و جوهای آنلاین، ارزیابی اولیه، جمع‌آوری، حفظ، تشخیص و تحلیل تحقیقی - اختصاص دارد. این بخش با فصلی درباره روش‌شناسی و اصول گزارش‌دهی درباره یافته‌های یک تحقیق متن باز به پایان می‌رسد.

مشارکت کنندگان و همراهان

کمیته هماهنگی پروتکل برکلی

لینزی فریمن (Lindsay Freeman)، پژوهشگر ارشد حقوقی، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
الکسا کینیگ (Alexa Koenig)، مدیر اجرایی، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
اریک استوور (Eric Stover)، مدیر دانشکده، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق

کمیته ویرایشی پروتکل برکلی

ساریتا اشرف (Sareta Ashraph)، مشاور ارشد حقوقی؛ وکیل، دادگاه گاردن کورت؛ تحلیلگر ارشد سابق، تیم تحقیقاتی سازمان ملل متحد برای ترویج مسئولیت‌پذیری در قبال جنایات ارتکابی توسط داعش/دولت اسلامی در عراق و شام
آلیکس دان (Alix Dunn)، مدیر اجرایی، The Engine Room
ریچارد گلدستون (Richard Goldstone)، قاضی سابق، دادگاه قانون اساسی آفریقای جنوبی؛ دادستان ارشد سابق، دادگاه کیفری بین‌المللی برای یوگسلاوی سابق و دادگاه کیفری بین‌المللی برای رواندا
برندا جی. هالیس (Brenda J. Hollis) ، دادستان مشترک بین‌المللی، شعبه‌های فوق‌العاده در دادگاه‌های کامبوج؛ دادستان ارشد سابق، دادگاه ویژه فعال برای سیرالئون
تانیا کاراناسیوس (Tanya Karanasios)، مدیر برنامه‌ها، WITNESS
انریک پیرس (Enrique Piracés)، مدیر برنامه رسانه‌ها و حقوق بشر، مرکز علوم حقوق بشر، دانشگاه کارنگی ملون
بت ون شاک (Beth Van Schaack)، استاد مهمان حقوق بشر، دانشکده حقوق دانشگاه استنفورد؛ معاون سابق سفیر متولی مسائل جنایات جنگی، دفتر حقوق کیفری جهانی، وزارت امور خارجه ایالات متحده آمریکا

میشل د سمدت (Michel de Smedt)، مدیر بخش تحقیقات، دفتر دادستان، دیوان کیفری بین‌المللی
آلن تیگر (Alan Tieger)، وکیل ارشد محاکمات، دفتر دادستان ویژه کوزوو؛ وکیل ارشد محاکمه سابق، دادگاه کیفری بین‌المللی برای یوگسلاوی سابق
کریستین وناوزر (Christian Wenaweser)، نماینده دائم لیختن‌اشتاین در سازمان ملل متحد؛ رئیس سابق مجمع کشورهای عضو اساسنامه رم دیوان کیفری بین‌المللی
الکس وایتینگ (Alex Whiting)، رئیس تحقیقات، دفتر دادستان ویژه کوزوو؛ استاد حرفه‌ای، دانشکده حقوق هاروارد؛ مسئول سابق هماهنگی پیگردها و هماهنگ‌کننده تحقیقات در دفتر دادستان، دیوان کیفری بین‌المللی
سوزان ولفینبارگر (Susan Wolfinbarger)، مسئول امور خارجه و رهبر تیم تحلیلی، وزارت امور خارجه ایالات متحده؛ مدیر ارشد سابق پروژه، پروژه فناوری‌های جغرافیایی فضایی، انجمن آمریکایی پیشبرد علم

کمیته مشاوره پروتکل برکلی

فدریکا دالساندرا (Federica D'Alessandra)، مدیر اجرایی، برنامه آکسفورد در زمینه صلح و امنیت بین‌المللی، دانشگاه آکسفورد؛ ویراستار کتاب راهنمای گروه حقوق بین‌الملل عمومی و سیاست در مورد مستندسازی موارد جدی نقض حقوق بشر در جامعه مدنی: اصول و بهترین شیوه‌ها
استوارت کیسی-ماسلن (Stuart Casey-Maslen)، استاد افتخاری، دانشکده حقوق، دانشگاه پرتوریا؛ مشارکت‌کننده در پروتکل مینسوتا در مورد تحقیقات مرگ‌های احتمالی غیرقانونی (۲۰۱۶)
آلیسون کول (Alison Cole)، مشاور تخصصی حقوق بشر، وزارت امور کشور، نیوزیلند
فرانسوا همپسن (Francoise Hampson)، استاد بازنشسته، دانشکده حقوق دانشگاه اسکس؛ عضو کمیسیون تحقیق در مورد بوروندی
کریستوف هاینس (Christof Heyns)، استاد حقوق بشر، دانشگاه پرتوریا؛ عضو کمیته حقوق بشر؛ گزارشگر ویژه سابق در مورد اعدام‌های فرا قضایی، شتابزده یا خودسرانه؛ هماهنگ‌کننده پروتکل مینسوتا در مورد تحقیقات مرگ‌های احتمالی غیرقانونی (۲۰۱۶)
وینسنت یاگوپینو (Vincent Iacopino)، مشاور ارشد پزشکی، پزشکان برای حقوق بشر؛ مشارکت‌کننده اصلی در راهنمای تحقیق و مستندسازی مؤثر شکنجه و دیگر رفتارها یا مجازات‌های بی‌رحمانه، غیرانسانی یا تحقیرآمیز (پروتکل استانبول)
کلی ماتسون (Kelly Matheson)، وکیل ارشد و مدیر برنامه، WITNESS؛ نویسنده راهنمای میدانی ویدئو به عنوان مدرک
هانی مگالی (Hanny Megally)، کمیسر کمیسیون بین‌المللی مستقل تحقیق در مورد جمهوری عربی سوریه؛ عضو ارشد، مرکز همکاری بین‌المللی، دانشگاه نیویورک
خوان مندز (Juan Méndez)، استاد حقوق بشر ساکن در کالج حقوق واشنگتن؛ گزارشگر ویژه سابق در مورد شکنجه و دیگر رفتارها یا مجازات‌های بی‌رحمانه، غیرانسانی یا تحقیرآمیز؛ هماهنگ‌کننده پروتکل جهانی برای مصاحبه‌های تحقیقی و تضمین‌های آیین دادرسی
آریه نِیر (Aryeh Neier)، رئیس افتخاری، بنیادهای جامعه باز
ناوی پیلای (Navi Pillay)، رئیس، کمیسیون بین‌المللی علیه مجازات اعدام؛ کمیسر عالی سابق حقوق بشر سازمان ملل متحد؛ قاضی سابق دیوان کیفری بین‌المللی؛ رئیس سابق دادگاه کیفری بین‌المللی برای روآندا
پائولو سرجیو پینهیرو (Paulo Sérgio Pinheiro)، رئیس، کمیسیون بین‌المللی مستقل تحقیق در مورد جمهوری عربی سوریه؛ گزارشگر ویژه سابق در مورد وضعیت حقوق بشر در بوروندی؛ گزارشگر ویژه سابق در مورد وضعیت حقوق بشر در میانمار

توماس پروبرت (Thomas Probert)، مدرس ممتاز مرکز حقوق بشر، دانشگاه پرتوریا؛ دستیار پژوهشی، مرکز حکومت و حقوق بشر، دانشگاه کمبریج؛ مشارکت‌کننده در پروتکل مینسوتا در مورد تحقیقات مرگ‌های احتمالی غیرقانونی (۲۰۱۶)
استفن رپ (Stephen Rapp)، همکار برجسته، مرکز سیمون-اسکیات برای پیشگیری از نسل‌کشی، موزه یادبود هولوکاست ایالات متحده؛ سفیر سیار سابق برای مسائل جنایات جنگی، دفتر عدالت کیفری جهانی، وزارت امور خارجه ایالات متحده؛ دادستان سابق، دادگاه ویژه سیرالئون
کریستینا ریبیرو (Cristina Ribeiro)، هماهنگ‌کننده تحقیقات، دفتر دادستان، دادگاه جنایی بین‌المللی
پاتریشیا سلرز (Patricia Sellers)، مشاور ویژه جنسیت برای دادستان دادگاه جنایی بین‌المللی؛ پژوهشگر مهمان، کالج کلوگ، دانشگاه آکسفورد؛ مشاور حقوقی و وکیل محاکمه سابق، دادگاه جنایی بین‌المللی برای یوگسلاوی سابق و دادگاه جنایی بین‌المللی برای رواندا.

شرکت‌کنندگان در کارگاه

کارگاه در باره پزشکی قانونی نوین: استفاده از اطلاعات متن باز برای تحقیق در مورد جنایات سنگین (بلاجیو، ایتالیا، ۲۰۱۷)

هادی الخطیب (Hadi Al Khatib)، آرشیو سوریه
استوارت کیسی-ماسلن (Stuart Casey-Maslen)، دانشگاه پرتوریا
ایوان کویپرز (Yvan Cuypers)، دادگاه جنایی بین‌المللی
اسکات ادواردز (Scott Edwards)، سازمان عفو بین‌الملل
لیندزی فریمن (Lindsay Freeman)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
الکسا کینیگ (Alexa Koenig)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
استیو کوستاس (Steve Kostas)، طرح عدالت جامعه باز
آندریا لمپروس (Andrea Lampros)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
کلی ماتسون (Kelly Matheson)، WITNESS
فلیم مک‌ماهون (Félim McMahon)، دیوان کیفری بین‌المللی
جولیان نیکولز (Julian Nicholls)، دیوان کیفری بین‌المللی
توماس پروبرت (Thomas Probert)، دانشگاه کمبریج
کریستینا ریبیرو (Cristina Ribeiro)، دیوان کیفری بین‌المللی
گوین شریدان (Gavin Sheridan)، Vizlegal
اریک استوور (Eric Stover)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
آلن تایگر (Alan Tieger)، دادگاه جنایی بین‌المللی برای یوگسلاوی سابق
مارک واتسون (Mark Watson)، کمیسیون عدالت و مسئولیت بین‌المللی
گای ویلوبی (Guy Willoughby)، انجمن مطالعات جنایات جنگی

کارگاه درباره ایجاد چارچوب اخلاقی برای تحقیقات متن باز (دانشگاه اسکس، بریتانیا، ۲۰۱۹)

فرد آبراهامز (Fred Abrahams)،دیده‌بان حقوق بشر
لینا بسونی (Leenah Bassouni)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق

فدریکا دالساندرا (Federica D’Alessandra)، دانشگاه آکسفورد
سم دابربلی (Sam Dubberley)، عفو بین‌الملل
جنیفر ایستردی (Jennifer Easterday)، آزمایشگاه‌های JustPeace
اسکات ادواردز (Scott Edwards)، عفو بین‌الملل
لینزی فریمن (Lindsay Freeman)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
جف گیلبرت (Geoff Gilbert)، دانشگاه اسکس
کریستوفر "کیپ" هیل (Christopher “Kip” Hale)، کمیسیون عدالت و مسئولیت بین‌المللی
ایوانا هو (Evanna Hu)، Omelas
گابریلا ایونس (Gabriela Ivens)، عضو Mozilla و WITNESS
الکسا کوئنیگ (Alexa Koenig)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
مت محمودی (Matt Mahmoudi)، دانشگاه کمبریج
لرنا مک‌گرگور (Lorna McGregor)، دانشگاه اسکس
دارا موری (Daragh Murray)، دانشگاه اسکس
ویوین نگ (Vivian Ng)، دانشگاه اسکس
انریک پیرس (Enrique Piracés)، مرکز علوم حقوق بشر، دانشگاه کارنگی ملون
زارا رحمان (Zara Rahman)، The Engine Room
ساشا روبهمد (Sasha Robehmed)، The Engine Room
ایلیا سیاتیتسا (Ilia Siatitsa)، Privacy International
نماینده دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد (OHCHR representative)، از بخش روش‌شناسی، آموزش و پرورش

میزگرد در مورد مسائل حقوقی ناشی از تحقیقات متن باز (لاهه، ۲۰۱۹)

دیوید آکرسون (David Akerson)، تیم تحقیقاتی سازمان ملل متحد برای ترویج مسئولیت‌پذیری در قبال جنایات ارتکابی توسط داعش/دولت اسلامی در عراق و شام
ساریتا اشرف (Sareta Ashraph)، دادگاه گاردن کورت
دانیا چایکل (Danya Chaikel)، دفتر دادستان ویژه کوزوو
آلن کلارک (Alan Clark)، دیوان کیفری بین‌المللی
فدریکا دالساندرا (,Federica D’Alessandra)، دانشگاه آکسفورد
نیکو دکینز (Nico Dekens)، Bellingcat
کریس انگلس (Chris Engels)، کمیسیون عدالت و مسئولیت بین‌المللی
لینزی فریمن (Lindsay Freeman)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
اما اروینگ (Emma Irving)، دانشگاه لایدن
میشل جارویس (Michelle Jarvis)، مکانیزم بین‌المللی، بی‌طرف و مستقل برای کمک به تحقیقات و پیگرد افرادی که بر طبق حقوق بین‌الملل مسئول جنایات جدی هستند که در جمهوری عربی سوریه از مارس ۲۰۱۱ ارتکاب یافته‌اند.
ادوارد جرمی (Edward Jeremy)، دیوان کیفری بین‌المللی
اشلی جوردانا (Ashley Jordana)، Global Rights Compliance
سانگ-مین کیم (Sang-Min Kim)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق

الکسا کوئنیگ (Alexa Koenig)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
نیکلاس کومجیان (Nicholas Koumjian)، مکانیزم تحقیقاتی مستقل برای میانمار
باستیان ون در لاکن (Bastiaan Van Der Laaken)، مکانیزم بین‌المللی، بی‌طرف و مستقل برای کمک به تحقیقات و پیگرد افرادی که مسئول جنایات جدی تحت حقوق بین‌الملل مرتکب شده در جمهوری عربی سوریه از مارس ۲۰۱۱ هستند
دیربلا مینوگ (Dearbhla Minogue)، شبکه اقدام حقوق جهانی
نیک اورتز (Nick Ortiz)، دانشگاه لایدن
ماتیوز پزدیرک (Matevz Pezdirc)، شبکه نسل‌کشی آژانس اتحادیه اروپا برای همکاری قضایی جنایی
سانجا پوپوویچ (Sanja Popovic)، دفتر دادستان ویژه کوزوو
استیون پاولز (Steven Powles)، دادگاه‌های داوتی استریت؛ کمیته جنایات جنگی انجمن بین‌المللی وکلای دادگستری
استیون رپ (Stephen Rapp)، مرکز سیمون-اسکیات برای پیشگیری از نسل‌کشی، موزه یادبود هولوکاست ایالات متحده
کریستینا ریبیرو (Cristina Ribeiro)، دیوان کیفری بین‌المللی
مارک رابسون (Mark Robson)، کمیسیون عدالت بین‌المللی و مسئولیت پذیری
براد ساموئلز (Brad Samuels)، SITU Research
دالیلا سوانه (Dalila Seoane)، Civitas Maxima
کارستن استاهن (Carsten Stahn)، دانشگاه لایدن
ملیندا تیلور (Melinda Taylor)، دیوان کیفری بین‌المللی
آلن تایگر (Alan Tieger)، دفتر دادستان ویژه کوزوو
راکوئل وازکز لورنت (Raquel Vázquez Llorente)، eyeWitness to Atrocities [شهود عینی فجایع]

دیگر کارشناسان مسئول بازبینی

الیس بیکر (Elise Baker)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
شان بروکس (Sean Brooks)، مرکز امنیت سایبری بلند مدت، دانشگاه کالیفرنیا، برکلی
استفانی کرفت (Stephanie Croft)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
سم دابرلی (Sam Dubberley)، عفو بین‌الملل
توماس ایوینگ (Thomas Ewing)، مرکز مطالعات پیشرفته دفاعی
کریستوفر "کیپ" هیل (Christopher “Kip” Hale)، کمیسیون عدالت بین‌المللی و پاسخگویی
گابریلا ایونس (Gabriela Ivens)، دیدبان حقوق بشر
فلیم مک‌ماهون (Felim McMahon)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
دارا موری (Daragh Murray)، دانشگاه اسکس
ایوون نگ (Yvonne Ng)، WITNESS
زارا رحمان (Zara Rahman)، The Engine Room
مارک رابسون (Mark Robson)، کمیسیون عدالت بین‌المللی و پاسخگویی
جاستین سیتز (Justin Seitz)، Hunchly
آندریا تروینارد (Andrea Trewinnard)، مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق
استیو تراش (Steve Trush)، مرکز امنیت سایبری بلند مدت، دانشگاه کالیفرنیا، برکلی
راکوئل وازکز لورنت (Raquel Vázquez Llorente)، eyeWitness to Atrocities [شهود عینی فجایع]

تشکر ویژه

از اعضای گروه کاری تحقیقات آنلاین، دفتر دادستان، دیوان کیفری بین‌المللی به ویژه سپاسگزاری می کنیم.
همچنین از بسیاری از همکاران در دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد که تلاش‌هایشان منجر به تحقق انتشار این سند مشترک شد، قدردانی می‌شود.*

* بر اساس سیاست دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد(OHCHR) ، مشارکت در انتشارات این دفتر، به کارکنان آن نسبت داده نمی‌شود.

اختصارات و سرواژه‌ها

HTML	Hypertext Markup Language	اچ تی ام ال، زبان نشانه گذاری ابرمتنی (یک زبان استاندارد برای طراحی صفحات وب)، زنگام
ICRC	International Committee of the Red Cross	آی سی آر سی، کمیتهٔ بین المللی صلیب سرخ
ICT	information and communications technology	آی سی تی، فناوری اطلاعات و ارتباطات
IP	Internet Protocol	آی پی، قرارداد مبادلهٔ اطلاعات در شبکه های اینترنتی، پروتکل اینترنت
ISP	Internet service provider	آی اس پی، رسانندهٔ خدمات اینترنتی یا رسا
NGO	non-governmental organization	ان جی او، سازمان غیر دولتی
OHCHR	Office of the United Nations High Commissioner for Human Rights	دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد
PDF	Portable Document Format	پی دی اف، فورمت متن قابل انتقال
URI	uniform resource identifier	یو آر آی، شناسانهٔ منبع یکسان
URL	uniform resource locator	یو آر ال، مکان‌یاب منبع یکسان، نشانی وب، آدرس اینترنتی
وی پی اِن	virtual private network	وی پی ان، شبکهٔ خصوصی مجازی، شبکهٔ خم

1. مقدمه

خلاصهٔ این فصل

- هدف
- مخاطَبان
- تعاریف

1. پروتکل برکلی درباره تحقیقات دیجیتال متن باز، استانداردهای حرفه‌ای را که باید در شناسایی، جمع‌آوری، حفظ، تحلیل و ارائه اطلاعات دیجیتال متن باز و استفاده از آن در تحقیقات کیفری بین‌المللی و حقوق بشر اعمال شوند، توصیف می‌کند. اطلاعات متن باز، اطلاعاتی است که هر عضو جامعه می‌تواند مشاهده، خریداری یا درخواست کند، بدون اینکه نیاز به وضعیت حقوقی خاص یا دسترسی غیرمجاز داشته باشد. اطلاعات دیجیتال متن باز، اطلاعاتی است که به صورت دیجیتال در دسترس عموم قرار دارد و به طور کلی از اینترنت به دست می‌آید. اطلاعات دیجیتال متن باز شامل داده‌هایی است که هم توسط کاربران و هم توسط کامپیوترها تولید شده است و برای مثال ممکن است شامل: محتوای منتشر شده در شبکه‌های اجتماعی؛ اسناد، تصاویر، ویدئوها و فایل‌های صوتی در وب‌سایت‌ها و پلتفرم‌های به اشتراک‌گذاری اطلاعات؛ تصاویر ماهواره‌ای؛ و داده‌های منتشر شده توسط دولت باشد.[1] تحقیقات دیجیتال متن باز، تحقیقاتی است که بر اساس اطلاعات دیجیتال متن باز انجام می‌شود. برای سهولت در خواندن، پروتکل حاضر از این پس به اطلاعات دیجیتال متن باز و تحقیقات دیجیتال متن باز به ترتیب به عنوان «اطلاعات متن باز» و «تحقیقات متن باز» اشاره خواهد کرد.

2. اگرچه استفاده از اطلاعات متن باز در تحقیقات، موضوع جدیدی نیست، اما حجم و تنوع منابع باز به دلیل استفاده روزافزون از اینترنت و منابع دیجیتال دیگر برای به اشتراک‌گذاری اطلاعات، از جمله گسترش رسانه‌های اجتماعی، افزایش یافته است. این پروتکل به پیچیدگی‌هایی که در برخورد با اطلاعات دیجیتال ایجاد می‌شود و چالش‌های منحصربه‌فردی که در ارزیابی منابع و تأیید اطلاعات یافت شده در تریبون‌های آزاد آنلاین به وجود می‌آید، می‌پردازد.

3. در حالی که تعداد فزاینده‌ای از محققان بین‌المللی جرایم و حقوق بشر اکنون برای تسهیل کار خود از اینترنت استفاده می‌کنند، هیچ مرجع، راهنما یا استاندارد جهانی برای تحقیقات متن باز وجود ندارد. این پروتکل در تلاش است تا شکاف موجود را با تعیین اصول و روش‌هایی که به محققان کمک می‌کند تا کار خود را به صورت حرفه‌ای انجام دهند و در صورت لزوم، حفظ اطلاعات متن باز را برای استفاده احتمالی توسط سازوکارهای پاسخگویی تسهیل نمایند، پر کند.

4. پروتکل حاضر به طور خاص بر تحقیقات متن باز که با هدف تضمین عدالت و پاسخگویی بین‌المللی انجام می‌شوند، تمرکز دارد. این تحقیقات به طور کلی شامل موارد زیر می‌شوند: مستندسازی حقوق بشری، حفظ، جمع‌آوری شواهد و حقیقت‌یابی؛ تحقیقاتِ هیئت‌های تحقیق و کمیسیون‌های

[1] این یک فهرست جامع نیست.

حقیقت‌یاب[2]؛ انواع دیگر تحقیقات و بررسی‌های بین‌المللی[3]؛ فرآیندهای حقیقت و آشتی؛ دعوی‌های مدنی؛ و محاکمات کیفری، از جمله دادرسی‌های کیفری بین‌المللی. از آنجا که تحقیقات متن باز می‌توانند به انواع مختلفی از تلاش‌ها برای تضمین پاسخگویی کمک کنند[4]، روش‌شناسی و الزامات مستندسازی که در پروتکل مشخص شده‌اند ممکن است دقیق‌تر از آنهایی باشند که به طور سنتی در زمینه‌های دیگر، مانند روزنامه‌نگاری و حمایت از حقوق بشر، به کار می‌روند. محققان متن باز، صرف نظر از هدف تحقیقاتشان، با رعایت اصول روش‌شناسی که در پروتکل آمده‌اند و حول استانداردهای قانونی مشترک طراحی شده‌اند، کیفیت بالای کار خود را تضمین کرده و استفاده از اطلاعات جمع‌آوری شده را در دادگاه‌ها، محکمه‌ها و دیگر فرآیندها را به حداکثر رسانده تا از پاسخگویی اطمینان حاصل کنند.

5. علاوه بر این، پروتکل برکلی بر استانداردهای تحقیقاتی در زمینه نقض قوانین بین‌المللی، از جمله نقض حقوق بشر و نقض قوانین کیفری بین‌المللی، مانند جنایات جنگی، جنایات علیه بشریت و نسل‌کشی تأکید دارد. همچنین، راهنمایی‌های ارائه شده توسط پروتکل می‌توانند به انواع دیگر تحقیقات، از جمله تحقیقات برای دادگاه‌های ملی یا محلی هم اعمال شوند.

6. نهایتاً پروتکل برکلی برای این تهیه شده است تا به محققان متن باز کمک کند که کار خود را مطابق با روش‌شناسی حرفه‌ای که به طور گسترده با الزامات قانونی و هنجارهای اخلاقی سازگار است، انجام دهند. همچنین هدف این پروتکل کمک به کاربران مختلف فرآیند تحقیقاتی، از جمله وکلا و قضات و سایر تصمیم‌گیرندگان است تا تکنیک‌های تحقیق متن باز را بهتر درک و ارزیابی نمایند. این پروتکل به عنوان یک منبع برای متخصصان با تجربه و نیز یک ابزار آموزشی و پرورشی برای کسانی که می‌خواهند نحوه انجام تحقیقات متن باز در مورد موارد انتسابی نقض قوانین بین‌المللی را بیاموزند، در نظر گرفته شده است.[5]

---

[2] هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب نهادهایی هستند که ممکن است توسط دولت‌ها یا سازمان‌های بین‌المللی برای بررسی مسائل مختلف تأسیس شوند. هیئت‌های تحقیق یا کمیسیون‌های حقیقت‌یاب یافته‌های واقعی را گزارش می‌کنند، نتیجه‌گیری‌های حقوقی ارائه می‌دهند و توصیه‌هایی می‌نمایند. اگرچه یافته‌های هیئت‌های بین‌المللی تحقیق یا کمیسیون‌های حقیقت‌یاب از نظر قانونی الزام‌آور نیستند، اما می‌توانند بسیار تأثیرگذار باشند. با این حال، در برخی حوزه‌های قضایی، یافته‌های هیئت‌های ملی تحقیق ممکن است الزام‌آور باشند. برای اطلاعات بیشتر در مورد هیئت‌های بین‌المللی تحقیق و کمیسیون‌های حقیقت‌یاب، نگاه کنید به شورای حقوق بشر، «هیئت‌های بین‌المللی تحقیق، کمیسیون‌های حقوق بشر، کمیسیون‌های حقیقت یاب و تحقیقات دیگر» [International commissions of inquiry, commissions on human rights, fact-finding missions and other investigations] ، قابل دسترسی در www.ohchr.org/EN/HRBodies/HRC/Pages/COIs.aspx.

[3] برای مثال نگاه کنید به گزارش کمیسریای عالی حقوق بشر سازمان ملل متحد در مورد وضعیت حقوق بشر در جمهوری بولیواری ونزوئلا [A/HRC/41/18] که به دنبال قطعنامه 39/1شورای حقوق بشر ارائه شده است. همچنین نگاه کنید به قطعنامه 41/2 شورای حقوق بشر که در آن شورا از کمیسریای عالی خواست گزارشی در مورد وضعیت حقوق بشر در فیلیپین تهیه کند.

[4] به عنوان مثال، اطلاعات منبع باز توسط کمیسیون بین‌المللی مستقل حقیقت‌یاب در مورد میانمار، در کنار منابع دست اول و سایر اطلاعات، در مراحل اثبات و نیز در یافته‌ها و نتیجه‌گیری‌های آن مورد استفاده قرار گرفت. گزارش نهایی کمیسیون حقیقت‌یاب [A/HRC/42/50] یکی از عواملی بود که منجر به تأسیس «مکانیسم مستقل تحقیقاتی برای میانمار» توسط شورای حقوق بشر شد، که مأموریت انجام تحقیقات قضایی به آن واگذار شد. همچنین به کمیسیون حقیقت‌یاب مأموریت داده شد تا اطلاعات خود، از جمله محتوای تحقیقات منبع باز را به «مکانیسم مستقل تحقیقاتی برای میانمار» تحویل دهد. گزارش‌های این کمیسیون حقیقت‌یاب نیز در پرونده‌ای که توسط گامبیا علیه میانمار در دیوان بین‌المللی دادگستری برای نقض «کنوانسیون پیشگیری و مجازات جنایت نسل‌کشی» توسط میانمار مطرح شد، مورد استناد قرار گرفت. این نشان می‌دهد که چگونه اطلاعات جمع‌آوری‌شده برای یک هدف ممکن است در نهایت به یک فرآیند دیگر برای پاسخگویی قانونی کمک کند.

[5] این پروتکل همچنین چندین الگو برای تحقیقات منبع باز و یک واژه‌نامه فراهم می‌کند. (به فصل 8 در زیر نگاه کنید).

الف) هدف

7. اگرچه بسیاری از محققان از مدت‌ها پیش به اطلاعات منابع باز تکیه کرده‌اند، اما بهره‌برداری سیستماتیک از این منابع در اوایل تا اواسط قرن بیستم با تمرکز بر استخراج اطلاعات از پخش‌های رادیویی خارجی و روزنامه‌های چاپی شدت پیدا کرد.[6] با به وجود آمدن شبکه جهانی وب (اینترنت) در دهه ۱۹۹۰ و به دنبال آن محبوبیت یافتن رسانه‌های اجتماعی و تلفن‌های همراه هوشمند در دهه ۲۰۰۰، کمیت و کیفیت اطلاعات منابع باز به طور چشمگیری تغییر یافت. امروزه، هر فردی که به گوشی هوشمند و اینترنت دسترسی داشته باشد، می‌تواند محتوای دیجیتالی تولید کند و آن را در سطح جهان پخش نماید، هرچند که کیفیت، صحت و شفافیت این محتواها متفاوت است. افزایش حجم داده‌ها و سرعت انتقال و اشتراک‌گذاری آنها، فرصت‌های جدیدی برای محققان منابع باز فراهم کرده تا اطلاعاتی در مورد جنایات بین‌المللی و نقض حقوق بشر جمع‌آوری و تحلیل کنند. در عین حال، تولیدکنندگان محتوا نیز می‌توانند به راحتی اطلاعات نادرست را منتشر کرده و داده‌های دیجیتال را دستکاری کنند. این پروتکل تلاشی است برای پاسخ به این محیط جدید و پیچیدگی‌های مرتبط با این فرصت‌ها و چالش‌ها.

8. اطلاعات منابع باز در همه گونه تحقیقات مفید هستند، اما در تحقیقات کیفری بین‌المللی و حقوق بشری نقشی به‌ویژه حیاتی ایفا می‌کنند. این امر به دلایل متعددی صادق است. نخست آنکه تحقیقات بین‌المللی که توسط نهادهایی چون هیئت‌های تحقیق سازمان ملل و کمیسیون‌های حقیقت‌یاب صورت می‌گیرند یا آنهایی که توسط دیوان بین‌المللی مجوز دارند، به فرآیندهای قانونی و سیاسی‌ای بستگی دارند که امکان انجام تحقیق را فراهم می‌کنند.[7] بنابراین، تحقیقات مزبور اغلب مدت‌ها پس از وقوع رویدادها انجام می‌شوند. دوم اینکه بسیاری از تحقیقات بین‌المللی ممکن است برای مثال به دلیل عدم همکاری یا امتناع یک دولت از اعطای دسترسی، امکان دسترسی فیزیکی به مکان وقوع حوادث را نداشته باشند. سوم، حتی در صورتی که دسترسی به یک منطقه یا قلمرو اعطا شود، محققان ممکن است دسترسی فیزیکی محدودی به محل مورد نظر داشته باشند یا به دلیل نگرانی‌های امنیتی قادر به انجام تحقیقات میدانی یا مصاحبه‌های حضوری نباشند. در نهایت، بیشتر محققان از قدرت کامل ظابطان قضائی در مناطقی که جنایات یا موارد نقض ادعا شده رخ داده است برخوردار نیستند و بنابراین ممکن است نتوانند اطلاعات لازم را جمع‌آوری کنند. حتی در مواردی که همکاری دولتی وجود دارد، جمع‌آوری شواهد فرامرزی می‌تواند فرآیندی سخت و پیچیده باشد و به خاطر تشریفات اداری کند شود. همه این عوامل نشان می‌دهند که چرا تکنیک‌های تحقیقات منابع باز، که می‌توانند از راه دور و هم‌زمان با وقوع رویدادها انجام شوند، هم قدرتمند و هم ضروری هستند.

9. این پروتکل برای گروه متنوعی از محققان طراحی شده است که در زمینه‌های مختلف با مأموریت‌ها، توان تحقیقاتی و منابع متفاوت فعالیت می‌کنند. در نتیجه، این پروتکل رویکردی انعطاف‌پذیر اتخاذ می‌کند که پیش‌بینی نمی‌کند همه محققان کار خود را به طور یکسان انجام دهند، بلکه روش‌های تحقیقاتی را

---

[6] نیکیتا مهاندرو و الکسا کینیگ «فناوری‌های اطلاعات و ارتباطات، رسانه‌های اجتماعی و آیندهٔ حقوق بشر» [Nikita Mehandru and Alexa Koenig, "ICTs, social media, & the future of human rights", Duke Law & Technology Review، جلد 17، شماره 1، ص 129.

[7] هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب که توسط سازمان ملل متحد مأموریت یافته‌اند، از جمله توسط شورای امنیت، مجمع عمومی، شورای حقوق بشر و دبیرکل تأسیس شده‌اند. برای دادگاه جنایی بین‌المللی، دفتر دادستان می‌تواند بر اساس ارجاع کشورهای عضو یا شورای امنیت، یا به ابتکار خود و با مجوز قضات، تحقیقات را آغاز کند.

متناسب با هر محیط کاری منحصربه‌فرد تطبیق می‌دهد. همچنین، با توجه به اینکه فناوری‌ها، ابزارها و تکنیک‌هایی که به تحقیقات منابع باز کمک می‌کنند به طور مداوم در حال تغییر و تکامل هستند، این پروتکل بر ابزارها، پلتفرم‌ها، وب‌سایت‌ها، نرم‌افزارها یا منابع خاصی که ممکن است تغییر کنند تمرکز نمی‌کند، بلکه بر اصول و رویه‌های اساسی که باید راهنمای تحقیقات منابع باز باشند تأکید دارد.

10. این پروتکل به‌منظور استانداردسازی رویه‌ها و ارائه راهنمایی‌های روش‌شناختی در تحقیقات، نهادها و حوزه‌های قضایی مختلف طراحی شده است تا به محققان منابع باز کمک کند اهمیت موارد زیر را درک کنند:
(الف) ردیابی منشأ محتوای آنلاین و انتساب آن به منبع اصلی، تا حد امکان؛
(ب) ارزیابی اعتبار و قابلیت اطمینان منابع آنلاین؛
(ج) راستی آزمایی محتوای آنلاین و بررسی صحت و قابلیت اعتماد آن؛
(د) رعایت الزامات قانونی و هنجارهای اخلاقی؛
(ه) به حداقل رساندن هرگونه خطر آسیب برای خود، سازمان‌هایشان و اشخاص ثالث؛
(و) محافظت بهتر از حقوق بشرِ منابع، از جمله حق حریم خصوصی.

ب) مخاطبان

11. مخاطبان این پروتکل شامل افراد و سازمان‌هایی هستند که به منظور تحقیق درباره جنایات بین‌المللی یا نقض حقوق بشر، اطلاعات منابع باز را شناسایی، جمع‌آوری، حفظ و یا تحلیل می‌کنند تا عدالت و پاسخگویی را تضمین کنند. این گروه شامل محققان، وکلا، بایگان‌ها و تحلیل‌گرانی است که در دادگاه‌های کیفری بین‌المللی، منطقه‌ای و ترکیبی؛ واحدهای ملی جنایات جنگی ؛ هیئت‌های تحقیق؛ کمیسیون‌های حقیقت‌یاب؛ ساز و کارهای تحقیقاتی مستقل؛ سازمان‌های بین‌المللی؛ مکانیزم‌های عدالت انتقالی؛ و سازمان‌های غیردولتی (NGOها) فعالیت می‌کنند. همچنین، کارمندان مکانیزم‌های متنوع بین‌المللی و منطقه‌ای که تحقیقات منابع باز قضایی و شبه‌قضایی درباره نقض قوانین بین‌المللی را انجام می‌دهند، می‌توانند از این پروتکل بهره‌مند شوند.[8] این پروتکل همچنین می‌تواند برای پاسخ‌دهندگان اولیه دیجیتال، مانند سازمان‌های محلی و محققان مستقل که اغلب نخستین کسانی هستند که یافته‌های مبتنی بر اطلاعات منابع باز را منتشر می‌کنند و کارشان نقشی کلیدی در شکل‌گیری تحقیقات منابع باز رسمی دارد، آموزنده باشد. مخاطبان مورد نظر همچنین شامل افراد و سازمان‌هایی هستند که از قربانیان در ارائه دعاوی مدنی علیه عاملان یا دولت‌ها حمایت می‌کنند. به‌طور کلی، این پروتکل می‌تواند به کسانی که بر اساس تحقیقات منابع باز نتیجه‌گیری‌های واقعی یا قانونی می‌کنند کمک کند تا محتوای هر تحقیقی که به آن تکیه یا ارزیابی کرده را بهتر مورد بررسی قرار دهند.

12. اشخاص ذینفع بالقوه دیگر ممکن است شامل ارائه‌دهندگان خدمات مبتنی بر وب مانند پلتفرم‌های رسانه‌های اجتماعی باشند که حجم زیادی از داده‌ها را ذخیره می‌کنند و می‌توانند در حفظ داده‌ها نقشی

[8] برای مثال نگاه کنید به گزارش‌های ارتباطات و بازدیدهای سازوکارهای ویژه شورای حقوق بشر. قابل دسترسی در: www.ohchr.org/en/hrbodies/sp/pages/welcomepage.aspx. همچنین نگاه کنید به: فعالیت‌های کمیته‌های تحریم که توسط شورای امنیت ایجاد شده‌اند. قابل دسترسی در: www.un.org/securitycouncil/content/repertoire/sanctions-and-other-committees.

کلیدی ایفا کنند. همچنین، تولید کنندگان نرم‌افزارهای تقویت تکنیک‌ها و فرآیندهای تحقیقات منابع باز نیز جزء این گروه قرار دارند.

پ) تعاریف

13. برای ارائه استانداردها و راهنمایی‌های عملی در تحقیقات منابع باز، محققان باید درک مشترکی از اصطلاحات خاص داشته باشند. در این بخش، اصطلاحات کلیدی که در سراسر پروتکل مورد استفاده قرار گرفته‌اند مشخص می‌شوند. از جمله تفاوت‌های بین اصطلاحاتی که اغلب به اشتباه یکسان در نظر گرفته می‌شوند، شرح داده شده‌اند.[9]

1- اطلاعات منابع باز در مقابل اطلاعات منابع بسته

14. اطلاعات منابع باز شامل اطلاعاتی است که به‌صورت عمومی در دسترس هستند و هر فردی از عموم مردم می‌تواند آن را مشاهده، خریداری یا درخواست کند، بدون اینکه نیاز به اجازهٔ قانونی خاص یا دسترسی غیرمجاز داشته باشد. اطلاعات منابع بسته شامل اطلاعاتی است که دسترسی به آنها محدود یا توسط قانون محافظت شده است،[10] اما می‌توان آنها را به طور قانونی از طریق کانال‌های خصوصی مانند فرآیندهای قضایی یا به‌صورت داوطلبانه به‌دست آورد. با وجود این تعریف ساده، تعیین اینکه در زمینه محتوای آنلاین چه چیزی اطلاعات منابع باز را تشکیل می‌دهد، پیچیده‌تر از آن است که در ابتدا به نظر می‌رسد. در اینترنت، حجم فزاینده‌ای از داده‌ها به‌صورت عمومی در دسترس قرار گرفته است، بدون اینکه صاحبان آنها رضایت داده باشند؛ مانند اطلاعاتی که هک شده، افشا شده، به‌دلیل ضعف‌های امنیتی نمایان شده یا توسط اشخاص ثالث بدون مجوزهای لازم منتشر شده است. هرچند این اطلاعات به‌صورت عمومی در دسترس هستند و قاعدتاً به‌عنوان اطلاعات منابع باز در نظر گرفته می‌شوند، ممکن است در مورد استفاده از آنها محدودیت‌های قانونی و اخلاقی وجود داشته باشد. علاوه بر این، برخی از اطلاعات دیجیتال ممکن است برای افرادی که مهارت‌های فنی خاص و آموزش‌های تخصصی دارند قابل دسترسی باشد، اما افراد عادی احتمال یا امکان دسترسی به آنها را نداشته باشند.[11] به‌عنوان مثال، می‌توان به اطلاعاتی که فقط در دارک وب یا وب تاریک (dark web) قابل دسترسی است، اشاره کرد – یعنی بخشی از اینترنت که تنها از طریق نرم‌افزارهای خاصی مانند مرورگر تور (Tor) می‌توان به آن دسترسی داشت.[12] هرچند وب تاریک امکانِ ناشناس بودن را فراهم آورده و آن را به مکانی جذاب برای فعالیت‌های غیرقانونی تبدیل کرده است، استفاده از مرورگر تور و جستجو در وب تاریک در بیشتر کشورها قانونی است. پروتکل برکلی این اطلاعات را تا زمانی که دسترسی غیرمجاز به آنها صورت نگرفته باشد به‌عنوان اطلاعات «منابع باز» در نظر می‌گیرد. واضح‌ترین تمایز این است که اطلاعات منابع باز

[9] برای مجموعهٔ جامع‌تر اصطلاحات و تعاریف مرتبط، نگاه کنید به فصل 8.

[10] برای مثال، اطلاعات محرمانه و اطلاعات طبقه‌بندی‌شده.

[11] برخی اقدامات ممکن است ناقض شرایط خدمات یک وب‌سایت باشند، اما ذاتاً غیرقانونی نباشند. به عنوان مثال، نقض شرایط خدمات یک وب‌سایت برای استخراج داده‌ها یک عمل غیرمجاز است و ممکن است منجر به ممنوعیت استفاده از آن وب‌سایت شود.

[12] وب تاریک به آن بخش از اینترنت اشاره دارد که فقط از طریق نرم‌افزارهای تخصصی قابل دسترسی است. مرورگر Tor یکی از نمونه‌های این نوع نرم‌افزارهاست.

شامل تعامل با کاربران اینترنت یا درخواست اطلاعات از آنها نمی‌شود.[13] به‌دست آوردن اطلاعات از سایر کاربران اینترنت از طریق ارتباط با آنها به‌عنوان اطلاعات منابع بسته در نظر گرفته می‌شود.

15. اطلاعات منابع باز دیجیتال،[14] اطلاعات منابع بازِ موجود در اینترنت است که می‌تواند، به‌عنوان مثال، از طریق وب‌سایت‌های عمومی، پایگاه‌های داده‌های اینترنتی یا پلتفرم‌های رسانه‌های اجتماعی در دسترس قرار گیرد. مطالب زیر، روش‌های مختلفِ به‌دست آوردن اطلاعات منابع باز را شرح می‌دهد.

2- به‌دست آوردن اطلاعات منابع باز دیجیتال

(الف) مشاهده

16. در بسیاری از پلتفرم‌ها، محتوا به‌سادگی با پیمایش به سایت مربوطه از طریق هر یک از مرورگرهای رایگان قابل دسترسی است. برخی از پلتفرم‌های آنلاین دیگر از کاربران می‌خواهند که برای دسترسی و مشاهده محتوا وارد حساب کاربری شده یا ثبت‌نام کنند. این نوع محتوا تا زمانی که این فرآیندها برای همه کاربران در حوزه‌های قضایی که دسترسی به این اطلاعات در آنها قانونی است، باز باشد و هنگام دسترسی و مشاهده هیچگونه قوانین حفظ حریم خصوصی یا امنیتی نقض نشود، به‌عنوان اطلاعات منابع باز محسوب می‌شوند. با این حال، برخی محتوا که با این تعریف مطابقت دارند، ممکن است به‌عنوان منابع باز در نظر گرفته نشوند؛ مثلاً اطلاعات ویژه، طبقه‌بندی‌شده (محرمانه) یا اطلاعاتی که به‌صورت قانونی محافظت‌شده اند. در چنین مواردی، هرچند این اطلاعات برای هر فردی از عموم قابل مشاهده است، استفاده از آن به‌عنوان مدرک در پرونده‌های قضایی ممکن است محدود باشد. همچنین در مورد استفاده از چنین موادی ممکن است ملاحظات اخلاقی یا روش‌شناختی از قبیل ناتوانی در انتساب یا تأیید آن محتوا وجود داشته باشد.

(ب) خرید

17. چندین منبع داده برای تحقیقات منابع باز در پلتفرم‌هایی قرار دارند که نیاز به پرداخت دارند، یا از یک مدل ترکیبی رایگان و پولی استفاده می‌کنند که در آن عملکرد اضافی و دسترسی به داده‌ها با هزینه مالی همراه است. شمار فزاینده‌ای از کسب‌وکارها وجود دارند که داده‌های عمومی را جمع‌آوری کرده و خدمات رایگان و پولی برای دسترسی به آنها ارائه می‌دهند. بسیاری از اطلاعاتی که برای محققان منابع باز مفید است، در پایگاه‌های داده و پلتفرم‌هایی وجود دارند که فقط از طریق پرداخت پول قابل دسترسی هستند. برای اهداف این پروتکل، اطلاعات منابع باز شامل آن دسته از خدمات غیر رایگانی می‌شود که برای عموم مردم قابل دسترسی باشد، اما شامل خدماتی نمی‌شود که دسترسی را به گروه‌های خاصی مانند نیروهای قوۀ مجریه یا محققان خصوصی دارای مجوز محدود می‌کنند.

(پ) درخواست

[13] در حالی که خرید اطلاعات از یک پایگاه دادۀ خصوصی یا ارسال درخواست اطلاعات از یک نهاد دولتی عمومی نیاز به مقداری تبادل آنلاین دارد، این فرآیند اغلب خودکار است و با نوع تعامل با سایر کاربران فردی اینترنت که در اینجا توصیف شده است، تفاوت دارد.

[14] در این پروتکل، به اطلاعات منبع باز ممکن است به عنوان محتوای آنلاین، مطالب آنلاین یا داده‌های آنلاین نیز اشاره شود.

18. در این زمینه، اصطلاح «درخواست» به درخواست‌هایی اشاره دارد که هر فردی می‌تواند برای دریافت اطلاعات عمومی از نهادهای دولتی تحت قوانین آزادی اطلاعات یا دسترسی به اطلاعات ارسال نماید. این اصطلاح به درخواست از افراد، شرکت‌ها یا سازمان‌ها برای تحویل داوطلبانه اطلاعات خود اشاره ندارد و محدود به درخواست‌هایی از نهادهای دولتی است که به‌طور قانونی موظف به پاسخ دادن به تمامی افراد به‌صورت یکسان هستند. تحقیقات منابع باز ممکن است به فعالیت‌های تحقیقاتی آنلاین دیگری مانند تعامل با منابع خارجی از طریق خدمات پیام‌رسانی، اتاق‌های گفتگو، انجمن‌ها یا ایمیل منجر شود. چنین تعاملاتی فراتر از حوزه تحقیقات منابع باز است که در این پروتکل به آن پرداخته شده است.

3- اطلاعات محرمانهٔ منابع باز

19. اطلاعات محرمانهٔ منابع باز به زیرمجموعه‌ای از اطلاعات منابع باز گفته می‌شود که اغلب در زمینه‌های نظامی یا سیاسی به‌منظور کمک به تصمیم‌گیری و سیاست‌گذاری، جمع‌آوری و استفاده می‌شود. در حالی که اطلاعات منابع باز شامل همه اطلاعات عمومی موجود است که هر فردی می‌تواند به صورت قانونی به آنها دسترسی داشته باشد، اطلاعات محرمانهٔ منابع باز زیرمجموعه‌ای از آن اطلاعات است که «که در زمان مناسب جمع‌آوری، بهره‌برداری و توزیع می‌شود تا برای پاسخگویی به یک نیاز اطلاعاتی خاص به مخاطب مناسب ارائه شود».[15] در زمینه پرونده‌های کیفری بین‌المللی و حقوق بشری، اطلاعات محرمانهٔ منابع باز به‌عنوان اطلاعات زمینه‌ای برای تصمیم‌گیری استفاده می‌شود – مثلاً برای اطلاع‌رسانی درباره فعالیت‌های مرتبط با امنیت، مانند محافظت از شاهدان و اعضای تیمی که برای تحقیقات میدانی می‌روند و یا برای ردیابی افراد مورد نظر – نه برای اقدامات مربوط به جمع‌آوری اطلاعات مرتبط با فرآیندهای تحقیقاتی، از قبیل اثبات عناصر مختلف جرم.

4- تحقیقات منابع باز

20. تحقیقات منابع باز به استفاده از اطلاعات منابع باز گفته می‌شود که به منظور جمع‌آوری اطلاعات و شواهد به کار گرفته می‌شود.

5- شواهد منابع باز

21. اصطلاح «شواهد» باید از «اطلاعات» متمایز شود.[16] شواهد عموماً در حوزه‌های قضایی به‌عنوان اثبات واقعیاتِ مورد استفاده در تحقیقات یا ارائه شده در جلسات قضایی، مانند یک محاکمه، تعریف می‌شود. شواهد منابع باز به آن دسته از اطلاعات منابع باز اطلاق می‌شوند که ارزش اثباتی دارند و می‌توانند در روندهای قانونی برای اثبات واقعیات پذیرفته شوند. مهم است که هنگام اشاره به «اطلاعات» به‌طور کلی، از اصطلاح «شواهد» سوءاستفاده یا استفادهٔ بیش از حد نشود.

6- اطلاعات منابع باز در مقابل نرم‌افزار متن‌باز

[15] سازمان ملی منبع باز، «دستورالعمل اطلاعاتی جامعه» شماره 301، 11 ژوئیه 2006، ص 8 (پاورقی حذف شده است).
[16] فدریکا دآلساندرا و دیگران (ویراستاران)، «راهنمای مستندسازی نقض‌های جدی حقوق بشر توسط جامعهٔ مدنی: اصول و بهترین روش‌ها» (لاهه، گروه حقوق بین‌الملل عمومی و سیاست، 2016)، ص 17.

22. اصطلاح «متن‌باز» اغلب برای توصیف نرم‌افزار یا کدی استفاده می‌شود که به‌صورت آزاد در دسترس است و بدون محدودیت‌های مربوط به حق نشر، حق اختراع یا دیگر کنترل‌های قانونی، قابل استفاده و انتشار مجدد است. نرم‌افزار متن‌باز از کد منبعی ساخته شده است که هر کسی با دسترسی به آن می‌تواند آن را بررسی کند، ویرایش نماید و بهبود بخشد.[17] این کد معمولاً برای کاربران قابل مشاهده نیست، اما توسط برنامه‌نویسان رایانه‌ای قابل تنظیم و انطباق است. نرم‌افزار متن‌باز از اطلاعات منابع باز متمایز است، هرچند که محققان منابع باز اغلب از نرم‌افزارها و ابزارهای متن‌باز برای یافتن، جمع‌آوری، حفظ و تحلیل اطلاعات منابع باز استفاده می‌کنند.

7- اعتبار در مقابل قابلیت اطمینان

23. در مورد شواهد مبتنی بر شهادت در محاکمات کیفری بین‌المللی، قضات «اعتبار شاهد» و «قابلیت اطمینان شهادت او» را ارزیابی می‌کنند.[18] در تحقیقات هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب سازمان ملل و تحقیقات مشابه، دستورالعمل‌ها تصریح می‌کنند که «مصاحبه‌گر باید اعتبار و قابلیت اطمینان مصاحبه‌شونده را ارزیابی کند»[19]. این دستورالعمل توضیح می‌دهد که «ارزیابی شامل بررسی ارتباط اطلاعات با موضوع تحقیق است. همچنین قابلیت اطمینان منبع و اعتبار یا صحت اطلاعات را بررسی خواهد کرد».[20] پروتکل برکلی از این اصطلاحات به‌صورت زیر استفاده می‌کند:

(الف) «اعتبار» به معنای باورپذیری یا قابل اعتماد بودن است؛
(ب) «قابلیت اطمینان» به توانایی ارائه عملکرد به گونه‌ای که دارای همخوانی و سازگاری باشد، قابل اعتماد یا بر طبق انتظار باشد اشاره دارد؛
(ج) «صحت» یا «اعتبار» به معنای دقت، صداقت یا انطباق با واقعیت‌ها است.

---

[17] نگاه کنید به Opensource.com «منبع باز چیست؟»

[18] دیوان کیفری بین‌المللی، «دادستان علیه بوسکو نتگاندا» [Prosecutor v. Bosco Ntaganda] ، پرونده شماره ICC-01/04-02/06، حکم مورخ 8 ژوئیه 2019، بند 53.

[19] دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد (OHCHR)، «هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب در مورد حقوق بشر بین‌المللی و حقوق بشردوستانه: راهنما و رویه» [OHCHR, Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice] (نیویورک و ژنو، 2015)، ص 52. قابل دسترسی در: www.ohchr.org/Documents/Publications/CoI_Guidance_and_Practice.pdf.

[20] همان

2. اصول

خلاصهٔ این فصل

- برای رعایت اصول حرفه‌ای مرتبط با تحقیقات منابع باز دیجیتال، محققان باید اطمینان حاصل کنند که مسئولیت‌پذیر، شایسته و بی‌طرف باشند و کار آنها مطابق با قوانین و با در نظر گرفتن ملاحظات امنیتی انجام شود.

- محققان همچنین باید روش‌هایی که در تمام مراحل چرخه تحقیق استفاده می‌کنند را مدنظر قرار دهند. اصول روش‌شناختی مربوطه حداقل شامل دقت، حداقل‌سازی داده‌ها، حفظ داده‌ها و امنیت از همان ابتدای برنامه ریزی می‌شود.

- در نهایت، همه محققان باید از ملاحظات اخلاقی پیروی کنند. این ملاحظات حداقل شامل محافظت از کرامت تمام افرادی است که در یک تحقیق شرکت می‌کنند یا به نوعی در آن دخیل هستند، و همچنین اطمینان از تواضع، همه شمول بودن، استقلال و شفافیت.

24. در حالی که فناوری‌ها، ابزارها و تکنیک‌های مورد استفاده در تحقیقات منابع باز تغییر خواهند کرد، برخی از اصول کلی روش‌شناختی و اخلاقی باید پایدار بمانند. شناسایی این اصول گامی مهم در جهت حرفه‌ای‌سازی حوزه تحقیقات منابع باز است. این اصول، که در پی خواهد آمد ،برای تضمین کیفیت تحقیقات منابع باز بنیادین هستند و منجر بهتقویت اعتبار، قابل اطمینان بودن و سودمند بودن بالقوهٔ آنها به منظور اطمینان حاصل کردن از پاسخگویی و به حداقل رساندن آسیب‌های احتمالی به اشخاص ذینفع مختلف خواهند شد.

الف) اصول حرفه‌ای

1- پاسخگویی

25. محققان منابع باز باید نسبت به اقدامات خود پاسخگو باشندو این امر اغلب از طریق مستندسازی شفاف، نگهداری سوابق و نظارت تضمین می‌شود. شفافیت در روش‌ها و مراحل تحقیقاتی یک عنصر اساسی در تضمین پاسخگویی است. بنابراین، تا حد امکان و معقول، محققان منابع باز باید = فعالیت‌های خود را ثبت کنند. مراحل تحقیق منابع باز – از شناسایی مطالب مرتبط تا جمع‌آوری، تجزیه و تحلیل و تهیهٔ گزارش – باید به طور مداوم و واضح مستند شوند. هر فردی که در جمع‌آوری یا مدیریت اطلاعات آنلاین مشارکت دارد، باید آگاه باشد که ممکن است روش‌شناسی او زیر سوال برود، از جمله اینکه احتمال دارد برای شهادت به دادگاه احضار شود. مستندسازی تحقیقات منابع باز ممکن است به صورت دستی یا با استفاده از فرآیندهای خودکار که توسط نرم‌افزارهای مختلف ارائه می‌شوند، انجام شود. مادامی که مستندسازی به طور یکدست و به اندازه کافی کامل باشد، می‌توان از روش‌های دستی یا خودکار استفاده کرد. فرآیندها و نرم‌افزارهای خودکار باید برای کاربران قابل درک باشند و بتوان آنها را در دادگاه توسط کاربران یا تهیه کنندگان توضیح داد. علاوه بر این، محققان منابع باز باید هر ابزار یا نرم‌افزاری که در طول کار خود استفاده می‌کنند را ثبت کنند.

2- صلاحیت

26. محققان منابع باز باید آموزش‌های مناسب و مهارت‌های فنی لازم را برای فعالیت‌هایی که انجام می‌دهند داشته باشند. آنها باید فعالیت‌های آنلاین خود را به صورت حرفه‌ای و اخلاقی انجام دهند، از تصاحب کار دیگران خودداری کنند؛ از تمام کسانی که در یک تحقیق مشارکت می‌کنند (در صورتی که ایمن باشد و خود افراد تمایل داشته باشند) تقدیر کنند؛ و داده‌ها را به‌دقت گزارش کنند، از جمله به هرگونه نارسایی احتمالی در محتوای آنلاین اذعان کنند. محققان منابع باز و فرآیندهای تحقیقاتی آنها باید انعطاف‌پذیر باشند، خود را با پیشرفت‌های جدید به‌روز کنند و فناوری‌ها و تکنیک‌های جدید را به‌طور مناسب به کار گیرند. علاوه بر این، سازمان‌ها و تیم‌های تحقیقاتی باید مکانیزم‌هایی داشته باشند تا از اجرای هماهنگ تمام مراحل و رعایت دقیق آنها مطمئن بشوند.

3- بیطرفی

27. بیطرفی یک اصل بنیادین است که در تمامی تحقیقات، چه آنلاین و چه آفلاین، اعمال می‌شود. محققان منابع باز باید از جانبداری‌های شخصی، فرهنگی و ساختاری که ممکن است بر کار آنها تأثیر بگذارد آگاه

باشند. آنها باید در مورد نیاز به اتخاذ تدابیری برای تضمین بیطرفی نیز مطلع باشند. محققان منابع باز باید اطمینان حاصل کنند که در تحقیقات خود رویکردی بیطرفانه در پیش می‌گیرند ، فرضیه‌های متعددی را به وجود آورده و به پیش می‌برند و از مرجح دانستن هیچ نظریهٔ خاصی به منظور توضیح موارد کاریِ خود، اجتناب می‌نمایند. در تحقیقات منابع باز که به صورت آنلاین انجام می‌شوند، به دلیل نحوهٔ ساختار و ارائهٔ اطلاعات اینترنتی به کاربران، بیطرفی باهمیت ویژه‌ای دارد. حتی زمانی که پرسش اصلی یکسان باشد، مرورگر، موتور جستجو، اصطلاحات جستجو و نحوه نگارش آنها ممکن است به نتایج بسیار متفاوتی منجر شوند. سوگیری‌های ذاتی در طراحی اینترنت و الگوریتم‌هایی که توسط موتورهای جستجو و وب‌سایت‌ها به کار گرفته می‌شوند می‌توانند واقعیت نتایج جستجو را به مخاطره بیاندازند.[21] نتایج جستجو ممکن است همچنین تحت تأثیر چندین عامل فنی، از جمله دستگاه مورد استفاده، مکان آن، و تاریخچه جستجوی قبلی و فعالیت اینترنتی کاربر قرار گیرند. محققان منابع باز باید با استفاده از روش‌شناسی‌هایی برای تضمین تنوع هرچه بیشتر نتایج جستجو، این سوگیری‌ها را خنثی کنند؛ به عنوان مثال، با اجرای چندین جستجو با پرسش‌های متفاوت و استفاده از موتورهای جستجو و مرورگرهای متنوع.[22] محققان باید آگاه باشند که نتایج جستجو ممکن است تحت تأثیر عوامل دیگری نیز قرار گیرند، از جمله به دلیل اختلاف در محیط دیجیتال که در آن اطلاعات آنلاین ممکن است از برخی گروه‌ها یا بخش‌های جامعه به‌طور نابرابر در دسترس باشد.[23] در نهایت، محققان باید همواره تلاش کنند از جانبداری‌های خود، چه آگاهانه باشد و چه ناخودآگاه، مطلع باشند و آنها را اصلاح کنند.[24]

---

[21] نگاه کنید به: صفیه نوبل، «الگوریتم‌های سرکوب: چگونه موتورهای جستجو نژادپرستی را تقویت می‌کنند» (نیویورک، انتشارات دانشگاه نیویورک، ۲۰۱۸) [Safiya Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (New York, New York University Press, 2018)]؛ ویرجینیا یوبانکس، «خودکار کردنِ نابرابری: چگونه ابزارهای پیشرفته تکنولوژی فقرا را پروفایل، کنترل و مجازات می‌کنند» (نیویورک، پیکادور، ۲۰۱۹) [Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York, Picador, 2019)].

[22] برای مثال نگاه کنید به: پاول مایرز، «چگونه می‌توان از روش‌های منبع باز برای کشف اطلاعات استفاده کرد»، در کتاب «شاهد دیجیتال: استفاده از اطلاعات منبع باز برای تحقیقات حقوق بشری، مستندسازی و پاسخگویی»، به ویراستاری سم دابرلی، آلکسا کوئینگ و دارا مورای (آکسفورد، انتشارات دانشگاه آکسفورد، ۲۰۲۰) [Paul Myers, "How to conduct discovery using open source methods", in Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020)] (به بررسی روش‌هایی می‌پردازد که انتخاب موتورهای جستجو و عبارات جستجو می‌تواند نتایج تحقیقات منبع باز را تحت تأثیر قرار دهد).

[23] برای مثال نگاه کنید به: آلکسا کینیگ و اولیک ایگن، «مخفی شده در معرض دید: استفاده از اطلاعات منبع باز آنلاین برای تحقیق در مورد خشونت جنسی و جرایم مبتنی بر جنسیت»، در کتاب «فناوری‌های نمایندگی حقوق بشر»، به ویراستاری جیمز داوس و الکساندرا اس. مور [Alexa Koenig and Ulic Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes", in Technologies of Human Rights Representation, James Dawes and Alexandra S. Moore, eds.] (در دست انتشار) (بررسی می‌کند که چگونه عدم دسترسی نسبی زنان به گوشی‌های هوشمند و استفاده از زبان کدگذاری شده توسط بازماندگان خشونت جنسی و جنسیتی، ممکن است میزان و دسترسی به اطلاعات منبع باز مربوط به چنین جرایمی را کاهش دهد — و همچنین اینکه چگونه حضور غالبِ مردان در موقعیت‌های مرتبط با فناوری و به عنوان محققان جرایم جنگی ممکن است بر احتمال تولید اطلاعات منبع باز مرتبط با جرایم جنسیتی در فرآیندهای شناسایی خودکار و/یا دستی تأثیر منفی بگذارد). برای بحث بیشتر درباره تعصب، نگاه کنید به فصل II.C زیر درباره اصول اخلاق و فصل V.B زیر درباره ارزیابی چشم‌انداز [فعالیت‌های] دیجیتال.

[24] برای مثال نگاه کنید به: «بازرس علوم پزشکی قانونی، اثرات تعصب شناختی مربوط به تحقیقات علوم پزشکی قانونی»، FSR-G-217 (بیرمنگام، بریتانیا، ۲۰۱۵) [Forensic Science Regulator, Cognitive Bias Effects Relevant to Forensic Science Investigations, FSR-G-217 (Birmingham, United Kingdom, 2015)]، (بحث در مورد دسته‌بندی‌های مختلف تعصب شناختی که می‌تواند بر کیفیت تحقیقات تأثیر منفی بگذارد، از جمله تعصب انتظارات، تعصب تأییدی، اثر لنگر انداختن، تعصب زمینه‌ای، و اثرات نقش و بازسازی)؛ وین ای. والاس، «اثر تعصب تأییدی بر تصمیم‌گیری‌های تحقیقاتی جنایی» [Wayne A. Wallace, The Effect of Confirmation Bias on Criminal

4- مشروعیت قانونی

28. تحقیقات منابع باز باید با قوانین مربوطه مطابقت داشته باشند، به این معنا که محققان باید از قوانین مربوط به کار خود درکی ابتدایی داشته باشند. محققان به ویژه باید از قوانین محافظت از داده‌ها و حق حفظ حریم خصوصی که بر طبق قوانین بین‌المللی حقوق بشری محافظت می‌شود، آگاه باشند.[25] حتی اگر اطلاعات به‌طور عمومی در دسترس باشد به این معنا نیست که در جمع‌آوری و استفاده از آن در ارتباط با حریم خصوصی هیچ پیامدی وجود ندارد. محققان منابع باز باید در اقدامات خود عواقب مربوط به حریم خصوصی، از جمله انتظار معقول افراد برای حفظ حریم خصوصی خود در فضاهای دیجیتالی مختلف را در نظر بگیرند. همچنین، محققان باید از اثر ترکیبی داده‌ها آگاه باشند، که طبق آن داده‌های عمومی، حتی زمانی که ناشناس‌سازی شده باشند، ممکن است در صورت انتشار یا ترکیب مجموعهٔ داده‌های مشابه یا مکمل، در معرض شناسایی مجدد قرار گیرند.[26] علاوه بر این، محققان باید

[Investigative Decision Making] (مینیاپولیس، Walden University ScholarWorks، ۲۰۱۵) (توضیح تعصب تأییدی به عنوان فرآیندی که طی آن محققان به دنبال اطلاعاتی می‌گردند یا به آن اعتقاد دارند که از نظریه مورد علاقه آنها در یک پرونده پشتیبانی می‌کند «در حالی که شواهد مخالف را نادیده می‌گیرند یا توجیه می‌کنند»)؛ مایکل پیتارو، «تعصب ضمنی در سیستم حقوق جنایی» [Michael Pittaro, "Implicit bias within the criminal justice system"]، Psychology Today، ۲۱ نوامبر ۲۰۱۸ (درباره تعصب‌هایی که می‌تواند به طور کلی بر تحقیقات جنایی تأثیر بگذارد بحث می‌کند و تکنیک‌های شناخته‌شده برای کاهش تعصب را پیشنهاد می‌کند)؛ جان اس. بیرد، «تعصب تأییدی، اخلاق و اشتباهات در علوم پزشکی قانونی» [Jon S. Byrd, "Confirmation bias, ethics, and mistakes in forensics"]، Forensic Pathways، ۲۱ مارس ۲۰۲۰ (درباره خطاهای شناختی و اخلاقی که می‌تواند تحلیل‌های پزشکی قانونی را تحریف کند، و تکنیک‌هایی برای اجتناب از این خطاها را توضیح می‌دهد). همچنین نگاه کنید به: ایوون مک‌درموت، دارا مورای و آلکسا کینیگ، «همایش پاسخگویی دیجیتال: داستان‌های چه کسانی بیان می‌شود و توسط چه کسانی؟ نمایندگی در تحقیقات حقوق بشری منبع باز» [Yvonne McDermott, Daragh Murray and Alexa Koenig, "Digital accountability symposium: whose stories get told, and by whom? Representativeness in open source human rights investigations"]، Opinio Juris، ۱۹ دسامبر ۲۰۱۹ (توضیح می‌دهد که چگونه روش‌های تحقیقات منبع باز ممکن است بر «انواع نقض‌های گزارش‌شده، قربانیان و شهودی که فرصت ابراز دارند، و چگونگی ساختار روایات نقض‌های گسترده حقوق بشر» تأثیر منفی می‌گذارد)؛ و پروژه‌ای که به رهبری ایوون مک‌درموت با عنوان «آینده تحقیقات حقوق بشری: استفاده از اطلاعات منبع باز برای تحول در مستندسازی و کشف موارد نقض حقوق بشر» انجام می‌شود.

[25] ماده ۱۲ اعلامیه جهانی حقوق بشر تصریح می‌کند که هیچ‌کس نباید در معرض دخالت خودسرانه در حریم خصوصی، خانواده، خانه یا مکاتبات خود و همچنین حملات به حیثیت و شهرت خود قرار گیرد. هر کس حق دارد در برابر چنین دخالت‌ها یا حملاتی از حمایت قانون برخوردار باشد. میثاق بین‌المللی حقوق مدنی و سیاسی نیز در ماده ۱۷ مقرر می‌دارد که هیچکس نباید در معرض دخالت‌های خودسرانه یا غیرقانونی در حریم خصوصی، خانواده، خانه یا مکاتبات خود و همچنین حملات غیرقانونی به حیثیت و شهرت خود قرار گیرد. همچنین در ماده ۱۷ بیان می‌شود که هر فردی حق دارد در برابر چنین دخالت‌ها یا حملاتی از حمایت قانون برخوردار باشد.

[26] «مفهوم اثر موزاییکی از نظریه موزاییکی جمع‌آوری اطلاعات مشتق شده است، که در آن قطعات پراکنده اطلاعات – اگرچه به‌صورت فردی ارزش محدودی دارند – هنگامی که با انواع دیگر اطلاعات ترکیب می‌شوند، اهمیت پیدا می‌کنند (پوزن ۲۰۰۵). وقتی این مفهوم در داده‌های قابل استفاده عمومی به‌کار می‌رود، اثر موزاییکی نشان می‌دهد که حتی داده‌های ناشناس‌شده، که ممکن است به‌صورت مستقل بی‌ضرر به نظر برسند، ممکن است در صورت انتشار تعداد کافی از مجموعه داده‌هایی که حاوی اطلاعات مشابه یا مکمل هستند، در معرض خطر شناسایی مجدد قرار گیرند.» نگاه کنید به: جان چایکا و دیگران، «به حداقل رساندن ریسک افشای اطلاعات در ابتکارات داده‌های باز HHS» (واشنگتن، دی.سی، مطالعات سیاست‌گذاری ماتماتیکا، ۲۰۱۴) [John Czajka and others, Minimizing Disclosure Risk in HHS Open Data Initiatives (Washington, D.C., Mathematica Policy Research, 2014)]، پیوست E، ص E-7. قابل دسترسی در https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf. همچنین نگاه کنید به: دیوید ای. پوزن، «نظریه موزاییکی، امنیت ملی و قانون آزادی اطلاعات»، مجله حقوق ییل [David E. Pozen, "The mosaic theory, national security, and the Freedom of Information Act", Yale Law Journal]، جلد ۱۱۵، شماره ۳ (دسامبر ۲۰۰۵)، صص ۶۲۸-۶۷۹.

آگاه باشند که در برخی حوزه‌های قضایی، نظارت مداوم و مستمر بر افراد در فضای آنلاین، یا جمع‌آوری سیستماتیک و نگهداری بلندمدت داده‌های شخصی ممکن است به دلیل نگرانی‌های شدیدتری که اینگونه فعالیت‌ها در مورد حفظ حریم خصوصی در بر دارند، به مجوزها و تدابیر حفاظتی اضافی نیاز داشته باشد.[27]

5- آگاهی نسبت به مسائل امنیتی

29. اگرچه موضوع امنیت ذاتاً[28] به طراحی و زیرساخت های یک تحقیق و نیز هر گونه فعالیت جانبیِ مربوط به آن می پردازد اما اصل آگاهی نسبت به مسائل امنیتی بر ملاحظاتی توجه دارد که افراد باید در حین کار خود در نظر بگیرند – به ویژه آگاهی از رفتارهای آنلاین خود. تمام افرادی که تحقیقات آنلاین انجام می‌دهند باید در زمینهٔ امنیت عملیاتی، از یک آگاهی پایه‌ای برخوردار باشند تا اطمینان حاصل کنند که ردپای دیجیتال خود را به حداقل رسانده و از خطرات احتمالی آگاه باشند. سازمان‌هایی که تحقیقات منابع باز انجام می‌دهند باید اطمینان حاصل کنند که محققان آنها آموزش‌های امنیت اطلاعات را برای درک خطراتی که ممکن است با آنها روبرو شوند، دریافت کرده‌اند و با سه ستون اصلی امنیت اطلاعات آشنا هستند: (الف) محرمانه بودن (برای مثال، فقط به کاربران مجاز اجازه دسترسی به داده‌ها داده شود)؛ (ب) یکپارچگی (اطمینان از اینکه داده‌ها توسط کاربران غیرمجاز دستکاری یا تغییر نکرده‌اند)؛ و (ج) در دسترس بودن (اطمینان از اینکه سیستم‌ها و داده‌ها به هنگام نیاز، در دسترس کاربران مجاز قرار دارند). آموزش‌ها باید همچنین بر ساختار حاکمیت اینترنت متمرکز باشد. ارزیابی تهدیدات و ریسک‌ها باید قبل از شروع فعالیت‌های تحقیقاتی آنلاین انجام شود و مرتباً بازبینی و در صورت نیاز اصلاح شود. امنیت مسئولیت همه است، نه فقط واحدهای فناوری اطلاعات یا مدیران ریسک امنیتی.

ب) اصول روش‌شناسی

1- دقت

30. یک ضرورت روش‌شناسی و اخلاقی وجود دارد تا دقت – و در نتیجه کیفیت – تحقیقات فقط با تکیه بر مطالب معتبر تضمین شود. محققان منابع باز باید تلاش کنند تا در طول تحقیقات خود و در ارائه نتایج، تا حد امکان صادق و دقیق باشند، به‌ویژه زمانی که نوبت به اذعان به نقاط ضعف داده‌های اولیه یا کل پرونده می‌رسد. دقت اغلب از طریق استفاده و آزمایش فرضیه‌های کاری متعدد و/یا بررسی موارد مشابه بهبود می‌یابد، که هر دو می‌توانند کمک کنند تا احتمال طرفداری در انتخاب، تفسیر و ارائه داده‌ها به حداقل برسد. نتیجه‌گیری‌های تحلیلی نباید اغراق‌آمیز یا بیش از حد مبالغه آمیز باشند. استفاده از زبان

---

[27] برای مثال، در پادشاهی متحد بریتانیای کبیر و ایرلند شمالی(، قانون تصریح می کند که «داده‌های شخصی پردازش‌شده برای ... مقاصد اجرای قانون نباید بیش از مدت زمان لازم برای هدفی که برای آن پردازش می‌شود، نگهداری شوند» (فصل ۱۲ قانون حفاظت از داده‌ها ۲۰۱۸، بخش ۳، فصل ۳، ماده ۳۹ (۱)). مطابق با مقررات ۲۰۱۶/۶۷۹ پارلمان اروپا و شورای ۲۷ آوریل ۲۰۱۶ در خصوص حفاظت از اشخاص طبیعی در ارتباط با پردازش داده‌های شخصی و ارسال آزادانه این داده‌ها، و لغو دستورالعمل EC/۴۶/۹۵ (مقررات عمومی حفاظت از داده‌ها)، داده‌های شخصی فقط می‌توانند برای «اهداف مشخص، صریح و مشروع» جمع‌آوری شوند، باید به اطلاعاتی محدود شوند که برای هدف جمع‌آوری لازم هستند و باید تنها به مدت زمان لازم برای اهداف جمع‌آوری، قابل شناسایی باقی بمانند (مواد ۶-۵).

[28] نگاه کنید به پاراگراف ۳۳ در زیر.

شفاف، واقع‌گرایانه و مبتنی بر حقایق و اجتناب از زبان احساسی، عینیت واقعی و ادراک‌شدهٔ یک تحقیق و نتایج آن را حفظ خواهد کرد.

2- حداقل‌سازی داده‌ها

31. اصل حداقل‌سازی داده‌ها مقرر می‌کند که اطلاعات دیجیتال تنها در صورتی باید جمع‌آوری و پردازش شوند که: (الف) برای یک هدف قابل‌بیان توجیه‌شده باشند؛ (ب) برای دستیابی به آن هدف ضروری باشند؛ و (ج) با توانایی تحقق آن هدف متناسب باشند.[29] در زمینه تحقیقات منابع باز، محتوای آنلاین تنها در صورتی باید جمع‌آوری شود که با یک تحقیق خاص مرتبط باشد. این اصل، جمع‌آوری دستی و موردی را بر جمع‌آوری خودکار و حجیم ترجیح می‌دهد، هرچند که در برخی موارد جمع‌آوری خودکار ممکن است مناسب باشد. اعمال این اصل در جمع‌آوری محتوای آنلاین به جلوگیری از جمع‌آوری بیش از حد کمک می‌کند، که این امر به چند دلیل اهمیت دارد. جمع‌آوری بیش از حد [داده‌ها] – که به‌ویژه در هنگام استفاده از فرآیندهای جمع‌آوری خودکار نگران‌کننده است – ممکن است آسیب‌پذیری‌های امنیتی[30] را ایجاد یا تشدید کند، به‌ویژه اگر باعث شود محققان از انواع اطلاعاتی که در اختیار دارند آگاه نباشند. جمع‌آوری بیش از حد همچنین در صورتی که یک فرآیند خودکار بین انواع محتوا تمایز قائل نشود، می‌تواند در مورد حریم خصوصی و حفاظت از داده‌ها مشکلاتی را ایجاد کند. در نهایت، اجتناب از جمع‌آوری بیش از حد، می تواند در عمل به اهدافی همچون کاهش هزینه‌های ذخیره‌سازی و جلوگیری از ایجاد تنگناها در مراحل مختلف چرخه تحقیقات مانند بازبینی، تحلیل و در صورت منجر شدن تحقیقات به مراحل قانونی، به افشاگری کمک کند.

3- حفظ و نگهداری

32. جلوگیری از جمع‌آوریِ کمتر از حدِ اطلاعات مرتبط به همان اندازه مهم است که اجتناب از جمع‌آوری بیش از حد. این موضوع به‌ویژه در زمینه اطلاعات آنلاین نگران‌کننده است، زیرا ماندگاری و دسترسی به این اطلاعات اغلب ناپایدار است. اصل حفظ و نگهداری برای جلوگیری از جمع‌آوری کمتر از حد طراحی شده است تا از از دست دادن مدارک مرتبط و بالقوه ارزشمند جلوگیری شود. به عنوان مثال، پلتفرم‌های رسانه‌های اجتماعی ممکن است محتوایی را که با شرایط خدمات آنها مغایرت دارد حذف کنند، حتی اگر آن محتوا برای محققان ارزش بالقوه‌ای داشته باشد. اگر درخواست حفظ به‌موقع به پلتفرم ارائه نشود یا محققان به نحوی دیگر محتوا را حفظ نکنند، ممکن است این اطلاعات برای همیشه از دست برود. علاوه بر این، کاربران ممکن است تصمیم بگیرند محتوای خود را حذف یا ویرایش کنند، و در نتیجه اطلاعاتی که قبلاً در دسترس عموم بود غیرقابل دسترس شود. همچنین اطلاعات در اینترنت به‌راحتی می‌تواند از بستر اصلی خارج شود، از بین برود، پاک شود یا خراب شود. اگر قرار است مطالب دیجیتال برای مکانیزم‌های پاسخگویی آینده قابل دسترس و قابل استفاده باقی بمانند، باید هم در کوتاه‌مدت و هم در دراز مدت فعالانه و با دقت حفظ شوند.[31]

4- امنیتِ طراحی شده

[29] این پروتکل، اصل به حداقل رساندن داده‌ها را از مقررات عمومی حفاظت از داده‌های اتحادیه اروپا استخراج کرده، اما آن را برای تطبیق با زمینه تحقیقات منبع باز سازگار کرده است (نگاه کنید به ماده ۵ مقررات).

[30] برای مثال‌هایی از آسیب‌پذیری‌های امنیتی، نگاه کنید به فصل 4 در زیر درباره امنیت.

[31] برای جزئیات بیشتر در مورد حفاظت و نگهداری، نگاه کنید به فصل D.6 در زیر.

33. اصل امنیتِ طراحی شده ایجاب می‌کند که اطلاعات دیجیتال و عملیات آنلاین تا حد امکان به‌صورت برنامه ریزی شده، امن باشند. سازمان‌هایی که تحقیقات منبع باز آنلاین انجام می‌دهند باید در جهت انجام تدابیر فنی و ساختاریِ مناسب اقدام کنند تا اطمینان حاصل شود که زیرساخت‌ها – از جمله سخت‌افزار و نرم‌افزار – در هنگام استفاده آنلاین توسط محققان به‌طور صحیح و خود به خود ناشناس و غیرقابل ردگیری باشند. تمامی تجهیزات باید دارای نرم‌افزار به‌روز شده برای محافظت در برابر بدافزار و تنظیمات مناسب برای حفظ حریم خصوصی و امنیت باشند. تدابیر امنیتی باید قبل از شروع فعالیت‌های تحقیقاتی آنلاین برقرار شوند؛ این تدابیر باید به‌طور مداوم نظارت، به‌روز و در صورت نیاز تنظیم شوند. محققان، تیم‌های تحقیقاتی یا سازمان‌ها ممکن است بخواهند برای آزمایش مداوم سیستم‌های امنیتی خود، از جمله آزمون نفوذ،[32] اقدام کنند تا اطمینان حاصل نمایند که سیستم‌های امنیتی آنها همان‌طور که طراحی شده‌اند، عمل می‌کنند.

پ) اصول اخلاقی

1- کرامت

34. تحقیقات باید با آگاهی و حساسیت نسبت به هرگونه مسائل مرتبط با کرامت انسانی انجام شوند، به‌ویژه آن دسته از منافعی که تحت قوانین بین‌المللی حقوق بشر محافظت می‌شوند. برای مثال، محققان باید به اصول عدم تبعیض پایبند باشند، که ممکن است بر اینکه چه چیزی تحقیق می‌شود و چه کسی تحقیق را انجام می‌دهد یا به عنوان محقق شناخته می‌شود تأثیر بگذارد. آنها باید همچنین تدابیری برای حفاظت از امنیت دیجیتال، فیزیکی و روانی شهود، بازماندگان، سایر محققان، متهمان و افراد دیگری که ممکن است از این جریانات دچار تأثیرات منفی شوند، اتخاذ کنند. پایبندی به اصل کرامت ممکن است همچنین بر آنچه که به‌صورت عمومی از یک تحقیق به اشتراک گذاشته می‌شود، از جمله در نوشتار یا مطالب تصویری، تأثیر بگذارد – به عنوان مثال، نشان ندادن کامل ابعاد رنج یا خشونت در صورتی که ضروری نباشد. این اصل تضمین می‌نماید که هنجارهای حقوق بشر به عنوان مجموعه‌ای از معیارهای راهنما برای انجام تحقیقات اخلاقی منبع باز به کار گرفته شوند.

2- تواضع

35. محققان منابع باز باید فروتن باشند، محدودیت‌های خود را بشناسند و بر آنچه که نمی‌دانندآگاهی داشته باشند. درک و تفسیر صحیح اطلاعات منبع باز ممکن است به آموزش‌های تخصصی یا مشاوره با کارشناسان نیاز داشته باشد. فروتنی همچنین به معنای پذیرفتن مسئولیت اشتباهات است. اگر محققان متوجه شوند که مرتکب اشتباهی شده‌اند، آن اشتباه باید اصلاح گردد یا به کسانی گزارش داده شود که می‌توانند آسیب‌های ناشی از آن را به حداقل برسانند. در حالت ایده‌آل، به‌ویژه برای تحقیقاتی که عمومی بوده و به‌طور گسترده منتشر می‌شوند، باید مکانیزمی برای گزارش دادنِ اشتباهات و اقدام برای اصلاح آنها وجود داشته باشد.

3- شمول‌گرایی

[32] آزمون نفوذ، یک حملهٔ سایبری شبیه‌سازی‌شده است که با مجوز انجام می‌شود تا امنیت یک سیستم را آزمایش کند.

36. محققان منابع باز باید اطمینان حاصل کنند که طیف گسترده‌ای از دیدگاه‌ها و تجربیات در تحقیقات لحاظ می‌شود. عواملی که ممکن است بر شمول‌گرایی کلی یک تحقیق آنلاین تأثیر بگذارند، شامل گستره جغرافیایی آن، نقض‌ها و/یا جنایات بین‌المللی مورد تحقیق و آگاهی از نابرابری اطلاعات آنلاین در ارتباط با بخش‌های مختلف جامعه هستند.[33] تیم‌های تحقیقاتی نیز باید متنوع باشند، از جمله با داشتن توازن جنسیتی. علاوه بر این، اصل شمول‌گرایی، همراه با اصل کرامت، ممکن است بر مطالبی که یک محقق برای جمع‌آوری و استفاده در یک تحقیق و نحوه ارائه آن‌ها به مخاطبان مختلف انتخاب می‌کند، تأثیر بگذارد.

4- استقلال

37. محققان منابع باز باید از خود و تحقیقاتشان در برابر اعمال نفوذ محافظت کنند. آنها باید تضاد واقعی یا احتمالی منافع را شناسایی و از آنها اجتناب کنند و برای کاهش تضادهایی که نمی‌توان از آنها پیشگیری کرد، تدابیری را اتخاذ نمایند. شفافیت مراحل، روش‌ها و منابع مالی می‌تواند به ارزیابی استقلال کمک کرده و از استقلال، چه در عمل و چه از منظر برداشت عموم، ، محافظت نماید.

5- شفافیت

38. در حالی که اصل پاسخگویی، یک محقق را ملزم می دارد که در روش‌ها و نتایج خود شفاف باشد، اصل اخلاق شفافیت به چگونگی رفتار محققان منابع باز به‌صورت آنلاین و در ارتباط با دنیای بیرونی اشاره دارد. این به معنای اجتناب از کژنمایی‌است.[34] در حالی که ناشناس‌ماندن و عدم‌نسبت‌دادن هویت – از جمله استفاده از هویت‌های مجازی[35] – می‌تواند به دلایل امنیتی مهم باشد، محققان باید از پیامدهای منفی احتمالی کژنمایی، مانند آسیب‌زدن به اعتبار و حیثیت یک تحقیق، تیم یا سازمان، یا آلوده کردن اطلاعات جمع‌آوری‌شده آگاه باشند. به‌دست‌آوردن اطلاعات از طریق کژنمایی ممکن است حق حریم خصوصی فرد مورد هدف را نقض کند و یا به تحقیق آسیب برساند، به‌ویژه اگر این کژنمایی در حوزه قضایی مربوطه غیرقانونی باشد.

[33] در مورد بررسی چشم انداز دیجیتال، نگاه کنید به فصل B.5 درزیر.
[34] برای مثال، با تلاش برای پیوستن به گروه‌های بسته یا ایجاد ارتباط در شبکه‌های اجتماعی و با ادعاهای نادرست.
[35] برای بحث در مورد هویت‌های مجازی، نگاه کنید به فصل C.4 در زیر که دربارهٔ ملاحظات مرتبط با زیرساخت‌ها است.

3. چارچوب قانونی

خلاصهٔ این فصل

- تعیین اینکه چه قوانینی اعمال می‌شوند، در تصمیم‌گیری درباره جمع‌آوری اطلاعات و بهترین روش‌های انجام آن حیاتی است. این موضوع بسته به هویت محققان، هویت افراد یا موضوعات مورد نظر آنها، هدف تحقیقات و حوزه‌های قضایی که محققان، اهداف، داده‌ها و فرآیندهای قانونی در آن قرار دارند، متفاوت خواهد بود.

- حفظ مواد دیجیتال به گونه‌ای که اصالت آنها حفظ شود و زنجیره حفظ و انتقال آنها مستند شود، احتمال پذیرفته‌شدن آنها به عنوان مدرک در دادگاه را افزایش می‌دهد.

- شناسایی نوع تحقیق و هدف نهایی آن (برای مثال، دادرسی‌های جنایی، دعاوی مدنی، فرآیند عدالت انتقالی و غیره) آستانه اثبات مورد نیاز را تعیین خواهد کرد.

- نقض حق حریم خصوصی یک فرد ممکن است منجر به حذف مدرک شود.

39. محققان منابع باز باید چارچوب‌های قانونی که در آن فعالیت می‌کنند را به‌خوبی درک کنند. این شامل آگاهی از مجموعه قوانین قابل شمول در رابطه با تحقیقات آنها و نیز چارچوب‌های قانونی حوزه‌های قضایی است که در آن فعالیت‌های تحقیقاتی انجام می‌دهند. آگاهی از قوانین ماهوی مربوط به تحقیقات، از جمله عناصر نقض‌های احتمالی یا جرایم[36]، و همچنین آگاهی از انواع مسئولیت‌ها[37]، می‌تواند به تحقیقات متمرکزتری منجر شود و احتمال اینکه اطلاعات جمع‌آوری‌شده و نتیجه‌گیری‌های تحلیلی انجام‌شده در تلاش برای دستیابی به عدالت و پاسخگویی مفید باشند را افزایش دهد. به همین ترتیب، آگاهی از قوانین آیین دادرسی و قوانین ادله در حوزه‌های قضایی مربوطه به محققان اجازه می‌دهد تا کار خود را به شیوه‌ای انجام دهند که با الزامات استفاده از اطلاعات منبع باز در رسیدگی‌های قانونی همخوانی داشته باشد.

40. برای تحقیقات کیفری بین‌المللی، چارچوب قانونی توسط ابزارهای قانونی مربوط به دادگاه یا سیستم قضایی تعیین می‌شود.[38] در مواردی مانند هیئت‌های تحقیق، که توسط نهادهای بین‌المللی ایجاد شده‌اند، مجموعه قوانین قابل اجرا ، گستره جغرافیایی و زمانی تحقیقات از جمله مواردی هستند که از سوی مکانیزم تاسیس تحقیقات تعیین می‌شوند.[39] برای سایر تحقیقات، از جمله آنهایی که توسط

---

[36] برای مثال، در صورتی که موضوع تحقیق نفرت‌پراکنی و تحریک به خشونت باشد، محققان باید نوع رفتاری که به آستانهٔ بالا در ماده 20(2) میثاق بین‌المللی حقوق مدنی و سیاسی می‌رسد را درک کنند. نگاه کنید به «برنامه عملی رباط در مورد ممنوعیت نفرت پراکنی ملی، نژادی یا مذهبی که تحریک به تبعیض را دشمنی یا خشونت محسوب می‌کند» (A/HRC/22/17/Add.4، پیوست)، پاراگراف‌های ۱۱ و ۲۹ و آزمون آستانه آن بر مبنای حقوق بشر که به ۳۲ زبان موجود است. قابل دسترسی در www.ohchr.org/EN/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx. در خصوص نفرت‌پراکنی، نگاه کنید به «راهبرد و برنامه عملی سازمان ملل در مورد نفرت‌پراکنی» (۲۰۱۹). قابل دسترسی در www.un.org/en/genocideprevention/hate-speech-strategy.shtml.

[37] در قانون کیفری، مرتکبین ممکن است بر اساس چندین شیوه مسئولیت که در اساسنامه مربوطه تعریف شده‌اند، پاسخگو شناخته شوند. این شیوه‌های مسئولیت شامل ارتکاب مستقیم و غیرمستقیم، مشارکت در جرم، معاونت در جرم و مسئولیت فرماندهی است. نگاه کنید به: ژروم دِ همتن، روبرت روث و الیس وان سلیدرِگت، ویراستاران، «شیوه‌های مسئولیت در قانون جنایی بین‌المللی» [Jérôme de Hemptinne, Robert Roth and Elies van Sliedregt, eds., Modes of Liability in International Criminal Law] (کمبریج، بریتانیا، انتشارات دانشگاه کمبریج، ۲۰۱۹) [Cambridge, United Kingdom, Cambridge University Press, 2019].

[38] برای مثال نگاه کنید به: دیوان کیفری بین‌المللی، «قوانین آیین دادرسی و ادله» (۲۰۱۳)؛ دادگاه بین‌المللی برای یوگسلاوی سابق، «قوانین آیین دادرسی و ادله» (۸ ژوئیه ۲۰۱۵)؛ دادگاه بین‌المللی کیفری برای رواندا، «قوانین آیین دادرسی و ادله» (۱۳ مه ۲۰۱۵)؛ دادگاه ویژه باقی‌مانده برای سیرالئون، «قوانین آیین دادرسی و ادله» (۳۰ نوامبر ۲۰۱۸)؛ دادگاه ویژه لبنان، «قوانین آیین دادرسی و ادله» (۱۰ آوریل ۲۰۱۹)؛ شعب فوق‌العاده در دادگاه‌های کامبوج، «قوانین داخلی» (۳ اوت ۲۰۱۱).

[39] برای مثال، هیئت حقیقت‌یاب بین‌المللی مستقل در مورد جمهوری بولیواری ونزوئلا که در سپتامبر ۲۰۱۹ تأسیس شد، مأموریت دارد که اعدام‌های فراقانونی، ناپدیدشدن‌های اجباری، بازداشت‌های خودسرانه، شکنجه و سایر رفتارهای ظالمانه، غیرانسانی یا تحقیرآمیز از سال ۲۰۱۴ به بعد را بررسی کرده و گزارشی از یافته‌های خود به شورا ارائه دهد (قطعنامه 42/25 شورای حقوق بشر، پاراگراف ۲۴). هیئت تحقیق بین‌المللی مستقل در مورد جمهوری عربی سوریه که در سال ۲۰۱۱ تأسیس شد، مأموریت دارد که تمامی موارد انتسابی نقض قانون بین‌المللی حقوق بشر از مارس ۲۰۱۱ در جمهوری عربی سوریه را بررسی کرده، حقایق و شرایطی که ممکن است به حد نقض‌های مذکور و جرائم ارتکابی برسند را مشخص کند و در صورت امکان، افراد مسئول را شناسایی نماید (قطعنامه S-17/1 شورای حقوق بشر، پاراگراف ۱۳). تیم بین‌المللی کارشناسانی که در سال ۲۰۱۷ به منطقه کاسای در جمهوری دموکراتیک کنگو اعزام شد، مأموریت داشت که اطلاعات مربوط به موارد انتسابی نقض حقوق بشر و اذیت و آزار و نقض قانون بین‌المللی بشردوستانه در مناطق کاسای را جمع‌آوری و حفظ کرده و نتایج این تحقیق را به مقامات قضایی جمهوری دموکراتیک کنگو ارسال کند (قطعنامه 35/33 شورای حقوق بشر، پاراگراف ۱۰).

سازمان‌های غیردولتی انجام می‌شوند، نهاد تحقیق‌کننده ممکن است چارچوب قانونی خود را تعیین کند.[40]

41. این فصل طراحی شده است تا به محققان منابع باز کمک کند که ارزش و اهمیت کاربردهای نهایی احتمالی کار خود را بهتر درک کنند و تکنیک‌های تحقیقاتی خود را متناسب با آن تطبیق دهند. از آنجا که قوانین قابل اجرا بر اساس حوزه قضایی، نوع تحقیق و اختیارات قانونی نهاد تحقیقاتی متفاوت است، بخش‌های زیر یک نمای کلی از ملاحظات اصلی در تحقیق درباره نقض‌های احتمالی قوانین بین‌المللی ارائه می‌دهند. توصیه می‌شود که محققان، در صورت امکان، از وکلایی که با حوزه‌های قضایی و موضوعات مربوطه آشنایی دارند، مشاوره حقوقی تخصصی دریافت کنند.

الف) حقوق بین‌الملل عمومی

42. این پروتکل بر سه مجموعه از حقوق بین‌الملل عمومی که دارای هم‌پوشانی قابل‌توجهی هستند تمرکز دارد: حقوق بشردوستانه بین‌المللی، قانون بین‌المللی حقوق بشر و قانون کیفری بین‌المللی. این سه مجموعه به طور متقابل یکدیگر را تقویت می‌کنند؛ در واقع، اِعمال حقوق بشردوستانه بین‌المللی و/یا قانون کیفری بین‌المللی، دولت‌ها را از انجام تعهدات خود در چارچوب قانون بین‌المللی حقوق بشر معاف نمی‌کند. آنچه در ادامه آمده است، نمایی کلی از هر یک از این حوزه‌ها ، از جمله منابع حقوق و تمایزات میان آنها را نشان می‌دهد تا محققان منابع آزاد بدانند که کدام مراجع باید راهنمای کار آنها باشد.

1- قانون بشردوستانهٔ بین‌المللی

43. حقوق بشردوستانه بین‌المللی یا «حقوق مخاصمات مسلحانه» رفتارهای مربوط به درگیری‌های نظامی را تنظیم کرده و مسائل بشردوستانه‌ای را که در طی این مخاصمات به وجود می‌آید حل می‌کند. این مخاصمات ممکن است بین‌المللی یا غیر بین‌المللی باشند.[41] حقوق بشردوستانه بین‌المللی زمانی اعمال می‌شود که یک مخاصمهٔ مسلحانه آغاز می‌شود و تا زمانی که صلح برقرار شود ادامه دارد، هرچند این مرزها همیشه مشخص یا ساده نیستند.[42] منابع اصلی حقوق بشردوستانه بین‌المللی شامل

---

[40] برخی سازمان‌ها، از جمله سازمان‌های غیردولتی (NGOها)، اغلب روش‌شناسی‌های داخلی خاص خود را دارند که آنها را ملزم می‌کند بر یک حوزه خاص از قانون تمرکز کنند، برای مثال در رابطه با شکنجه یا خشونت جنسی و جنسیتی، که این روش‌ها همچنین راهنمایی‌هایی برای تمرکز بر بخش‌های خاصی از تحقیقات ارائه می‌دهند.

[41] تفاوت بین مخاصمات مسلحانه بین‌المللی و غیربین‌المللی بر دو عامل استوار است: ساختار و وضعیت طرف‌های درگیر. مخاصمات مسلحانه بین‌المللی شامل دولت‌های حاکم می‌شود، در حالی که منازعات مسلحانه غیربین‌المللی شامل دولت‌ها و گروه‌های مسلح سازمان‌یافته است. نگاه کنید به: اندرو کلاپام، پائولا گائتا و مارکو ساسولی، ویراستاران، «کنوانسیون‌های ژنو ۱۹۴۹، تفسیر» (آکسفورد، انتشارات دانشگاه آکسفورد، ۲۰۱۵) [Andrew Clapham, Paola Gaeta and Marco Sassòli, eds., The 1949 Geneva Conventions, A Commentary (Oxford, Oxford University Press, 2015)]، فصل‌های ۱ و ۱۹.

[42] در حالی که آغاز یک مخاصمه بین‌المللی نسبتاً مشخص است، زیرا با هرگونه استفاده از زور بین دو دولت شروع می‌شود، آغاز یک مخاصمه مسلحانه غیربین‌المللی کمتر مشخص است. مخاصمه مسلحانه غیربین‌المللی تنها در صورتی وجود دارند که گروه‌های مسلح به اندازه کافی سازمان‌یافته باشند و سطح خشونت به شدت معینی برسد – دو عاملی که نیاز به تحلیل دقیق واقعی بر اساس هر مورد خاص دارند. نگاه کنید به: سیلوین ویت، «طبقه‌بندی مخاصمات مسلحانه در حقوق بشردوستانه بین‌المللی: مفاهیم قانونی و موقعیت‌های واقعی»، مجلهٔ بازنگری بین‌المللی صلیب سرخ [Sylvain Vité, “Typology of armed conflicts in international humanitarian law: legal concepts and actual situations”, International Review of the Red Cross]، جلد ۹۱، شماره ۸۷۳ (مارس ۲۰۰۹)، صص ۷۲ و ۷۶-

کنوانسیون‌های لاهه سال‌های 1899 و 1907[43]، کنوانسیون‌های ژنو مورخ 12 اوت 1949[44] و پروتکل‌های الحاقی آنها در سال 1977[45]، و همچنین چند معاهده است که قوانینِ استفاده از برخی از انواع سلاح‌ها را تعیین می‌کنند.[46] قوانین عرفی نیز منبع مهمی از حقوق بشردوستانه بین‌المللی است، زیرا خلأهایی که در معاهدات وجود دارد را پر می‌کند. حقوق بشردوستانه عرفی بین‌المللی برای تمامی طرف‌های یک مخاصمه الزام‌آور است و به‌ویژه برای مخاصمات مسلحانه غیر بین‌المللی هم اهمیت دارد، زیرا قواعد آنها در مقایسه با حقوق بشردوستانهٔ بین‌المللیِ مبتنی بر معاهده، دارای جزئیات بیشتری است.[47] تا اوایل دهه 1990، مکانیسم‌های اصلی اجرای حقوق بشردوستانه بین‌المللی، دادگاه‌های نظامی ملی بودند که دولت‌ها اعضای ارتش و افسران خود را در آنها تحت محاکمه قرار می‌دادند. با ظهور دادگاه‌های کیفری بین‌المللی، برخی از نقض‌های جدی قانون بشردوستانه بین‌المللی در اساسنامه‌های تأسیس این دادگاه‌ها به عنوان جنایات جنگی[48] قید شدند، که راه جدیدی برای اجرای قانون بشردوستانه بین‌المللی در سطح جهان فراهم کرد. برخی از کشورها نیز جنایات جنگی را در قوانین ملی خود لحاظ کرده‌اند[49] تا بتوان چنین مواردی را به جای دادگاه‌های نظامی در سیستم قضایی عادی آن کشورها

---

۷۷. همچنین اختلافاتی درباره زمان پایان یک مخاصمه مسلحانه و دستیابی به صلح وجود دارد. در حالی که توافقات آتش‌بس یا صلح ممکن است پایان مخاصمه مسلحانه را نشان دهند، اما قطعی نیستند. معیارهای مختلفی برای پایان یک منازعه مسلحانه پیشنهاد شده است، از جمله پایان عمومی عملیات نظامی پس از دستیابی به نتیجه کلی صلح، وجود یک راه‌حل مسالمت‌آمیز و پایان یافتن عواملی که برای شناسایی وجود مخاصمه مورد استفاده قرار می‌گیرند. نگاه کنید به: ناتالی ویزمن، «پایان مخاصمه مسلحانه، پایان مشارکت در مخاصمه مسلحانه و پایان درگیری‌ها: پیامدهای عملیات بازداشت تحت اجازهٔ استفاده از نیروی نظامی سال 2001»، مجلهٔ بازنگری قانون حقوق بشر کلمبیا [Nathalie Weizmann, "The end of armed conflict, the end of participation in armed conflict, and the end of hostilities: implications for the detention operations under the 2001 AUMF", Columbia Human Rights Law Review]، جلد ۴۷، شماره ۳ (۲۰۱۶)، صفحات ۲۲۴-۲۲۱.

[43] به ترتیب، «کنوانسیون مربوط به قوانین و عرف جنگ در خشکی» (کنوانسیون دوم لاهه) و «کنوانسیون مربوط به قوانین و عرف جنگ در خشکی» (کنوانسیون چهارم لاهه).

[44] نگاه کنید به «کنوانسیون ژنو برای بهبود وضعیت مجروحان و بیماران نیروهای مسلح در میدان نبرد» (کنوانسیون ژنو 1)؛ «کنوانسیون ژنو برای بهبود وضعیت مجروحان، بیماران و بازماندگان سوانح نیروهای مسلح در دریا» (کنوانسیون ژنو 2)؛ «کنوانسیون ژنو مربوط به رفتار با اُسرای جنگی» (کنوانسیون ژنو 3)؛ «کنوانسیون ژنو مربوط به حمایت از افراد غیرنظامی در زمان جنگ» (کنوانسیون ژنو 4).

[45] نگاه کنید به «پروتکل الحاقی کنوانسیون‌های ژنو ۱۹۴۹ به تاریخ ۱۲ اوت ۱۹۴۹ و مربوط به حمایت از قربانیان منازعات مسلحانه بین‌المللی» (پروتکل ۱)؛ «پروتکل الحاقی کنوانسیون‌های ژنو به تاریخ ۱۲ اوت ۱۹۴۹ و مربوط به حمایت از قربانیان منازعات مسلحانه غیربین‌المللی» (پروتکل ۲).

[46] برای مثال نگاه کنید به: «کنوانسیون منع توسعه، تولید و انباشت سلاح‌های میکروبی (بیولوژیکی) و سمی و نابودی آنها»؛ «کنوانسیون منع یا محدودیت استفاده از برخی سلاح‌های معمول که ممکن است به شدت آسیب‌زا یا دارای اثرات غیرقابل کنترل باشند»؛ «کنوانسیون منع توسعه، تولید، انباشت و استفاده از سلاح‌های شیمیایی و نابودی آنها»؛ «کنوانسیون منع استفاده، انباشت، تولید و انتقال مین‌های ضدنفر و نابودی آنها»؛ «کنوانسیون منع سلاح‌های خوشه‌ای». همچنین نگاه کنید به کمیته بین‌المللی صلیب سرخ (ICRC)، «سلاح‌ها»، ۳۰ نوامبر ۲۰۱۱. قابل دسترسی در www.icrc.org/en/document/weapons.

[47] نگاه کنید به کمیته بین‌المللی صلیب سرخ (ICRC)، «حقوق بشردوستانه بین‌المللی عرفی» [ICRC, "Customary international humanitarian law"]، ۲۹ اکتبر ۲۰۱۰. قابل دسترسی در www.icrc.org/en/document/customary-international-humanitarian-law-0. همچنین نگاه کنید به کمیته بین‌المللی صلیب سرخ (ICRC)، «به پایگاه داده حقوق بشردوستانه عرفی خوش آمدید» [ICRC, "Welcome to the Customary IHL Database"]. قابل دسترسی در https://ihl-databases.icrc.org/customary-ihl/eng/docs/home.

[48] برای مثال، ماده ۸ اساسنامه رم دادگاه جنایی بین‌المللی، در تعریف جنایات جنگی، حقوق بشردوستانه بین‌المللی را مدون می‌کند.

[49] برای مثال نگاه کنید به: استرالیا (قانون جنایات جنگی ۱۹۴۵، اصلاح‌شده، بخش ۷)؛ بوسنی و هرزگوین (قانون جنایی، مواد184-171)؛ کنیا (قانون جنایات بین‌المللی ۲۰۰۸، بخش (ج)(1)6و (4)-(2))؛ نیوزیلند (قانون جنایات بین‌المللی و دادگاه جنایی بین‌المللی ۲۰۰۰، بخش ۱۱)؛ آفریقای جنوبی (قانون اجرای کنوانسیون‌های ژنو ۲۰۱۲).

محاکمه کرد. این موارد ممکن است در کشور محل وقوع درگیری، و یا آن گونه که فزونی یافته، در کشورهای دیگر و تحت اصل صلاحیت قضایی جهانی مورد رسیدگی قرار بگیرند.[50] تعدادی از کشورها برای تعقیب قانونیِ چنین مواردی، واحدهای ویژۀ جنایات جنگی تأسیس کرده‌اند. دادگاه‌های جنایی بین‌المللی و محاکم ملی به این مجموعۀ رو به رشدِ رویه قضایی در قانون بشردوستانه بین‌المللی کمک می‌کنند، که این رویه نیز به عنوان منبع مهمی از قانون عمل می‌کند، و بسته به صلاحیت قضایی ممکن است قواعد آن الزام‌آور باشد.

2- قانون بین‌المللی حقوق بشر

44. کشورها بر طبق حقوق بین‌الملل برای احترام، محافظت و تحقق حقوق بشر وظایف و تعهداتی دارند. اعلامیه جهانی حقوق بشر که در سال 1948 به تصویب رسید، پایه و اساس قانون بین‌المللی حقوق بشر را فراهم می‌کند. در حالی که این اعلامیه آرمان‌گرا بوده و از جهت قانونی الزام‌آور نیست، برخی از مواد آن بخشی از حقوق عرفی بین‌المللی را تشکیل می‌دهند.[51] این اعلامیه همچنین الهام‌بخش دو میثاق و نیز مجموعه‌ای غنی از معاهدات حقوق بشری بوده است.[52] کشورها تنها به میثاق‌ها و معاهداتی که امضا و تصویب کرده‌اند متعهد هستند، مگر اینکه هنجارهای موجود در آن اسناد به مرحلۀ حقوق عرفی بین‌المللی دست یافته باشند.[53] قانون بین‌المللی حقوق بشر همچنین در چارچوب قانونی بسیاری از دادگاه‌های کیفری بین‌المللی ادغام شده است. علاوه بر این، چندین دادگاه حقوق بشری منطقه‌ای هم وجود دارند که توسط کنوانسیون‌های بین‌المللی تأسیس شده‌اند و مأموریت دارند تا در مورد پرونده‌های

---

[50] بر اساس «صلاحیت قضایی جهانی»، یک دادگاه ملی ممکن است افرادی را به‌خاطر ارتکاب جنایات جدی علیه حقوق بین‌الملل – مانند جنایات علیه بشریت، جنایات جنگی، نسل‌کشی و شکنجه – که خارج از مرزهای آن کشور رخ داده است، مورد پیگرد قرار دهد. این اصل بر این مبنا استوار است که چنین جنایاتی به جامعه بین‌المللی و نظم بین‌المللی آسیب می‌رساند و کشورها می‌توانند برای حفاظت از آن اقدام کنند. نگاه کنید به مرکز منابع عدالت بین‌المللی، «صلاحیت قضایی جهانی» [International Justice Resource Center, Universal jurisdiction]، قابل دسترسی در https://ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction.

[51] کشورهای متعدد، مقامات سازمان ملل متحد و پژوهشگران اظهار کرده‌اند که اگر نه تمامی مواد اعلامیه جهانی حقوق بشر، اما اکثر مواد آن، حقوق بین‌الملل عرفی را تشکیل می‌دهند. به طور خاص، ممنوعیت‌هایی علیه برده‌داری، محرومیت خودسرانه از زندگی، شکنجه، بازداشت خودسرانه و تبعیض نژادی که در اعلامیه جهانی حقوق بشر مدون شده‌اند، به عنوان حقوق بین‌الملل عرفی پذیرفته شده‌اند. نگاه کنید به: هرست هنوم، «وضعیت اعلامیه جهانی حقوق بشر در حقوق ملی و بین‌المللی»، مجله حقوق بین‌الملل و تطبیقی جورجیا [Hurst Hannum, "The status of the Universal Declaration of Human Rights in national and international law", Georgia Journal of International and Comparative Law]، جلد ۲۵، شماره ۱ (۱۹۹۶)، صص ۳۲۱–۳۳۲ و ۳۴۱–۳۴۶.

[52] نگاه کنید به: «کنوانسیون بین‌المللی رفع تمامی اشکال تبعیض نژادی»؛ «میثاق بین‌المللی حقوق مدنی و سیاسی»؛ «میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی»؛ «کنوانسیون رفع تمامی اشکال تبعیض علیه زنان»؛ «کنوانسیون منع شکنجه و سایر رفتارها یا مجازات‌های ظالمانه، غیرانسانی یا تحقیرآمیز»؛ «کنوانسیون حقوق کودک». برای اطلاعات بیشتر درباره معاهدات اصلی حقوق بشر سازمان ملل متحد، نگاه کنید به: دفتر کمیسریای عالی حقوق بشر سازمان ملل متحد (OHCHR)، «اسناد اصلی بین‌المللی حقوق بشر و نظارت بر آن‌ها» [The core international human rights instruments and their monitoring]. قابل دسترسی در www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx.

[53] حقوق بین‌الملل عرفی به تعهدات بین‌المللی‌ای اشاره دارد که از رویه‌های تثبیت‌شدۀ بین‌المللی ناشی می‌شوند تا از تعهداتی که از کنوانسیون‌ها و معاهدات رسمی و کتبی به وجود می‌آیند. این حقوق نتیجه یک رویه عمومی و مستمر دولت‌هاست که یک حس تعهد قانونی را دنبال می‌کنند. یکی از اجزای اساسی حقوق بین‌الملل عرفی، اصول و ضوابط لازم‌الرعایۀ حقوق بین‌الملل است که به اصول بنیادی و برتر حقوق بین‌الملل اشاره دارد. برای مثال نگاه کنید به: مؤسسه اطلاعات حقوقی، «حقوق بین‌الملل عرفی» و «اصول و ضوابط لازم‌الرعایۀ حقوق بین‌الملل»، دانشکده حقوق کرنل [Legal Information Institute, "Customary international law" and "Jus cogens", Cornell Law School]. قابل دسترسی در www.law.cornell.edu/wex.

نقض قانون بین‌المللی حقوق بشر علیه دولت‌های عضو آن کنوانسیون‌ها حکم صادر کنند، از جمله دادگاه حقوق بشر و مردم آفریقا[54]، دادگاه اروپایی حقوق بشر[55]، و دادگاه بین آمریکایی حقوق بشر[56]. همچنین نهادهای حقوق بشری دیگری نیز در سطح منطقه‌ای وجود دارند، از جمله کمیسیون حقوق بشر و مردم آفریقا، کمیته اروپایی حقوق اجتماعی، و کمیسیون حقوق بشر قارهٔ آمریکا که همگی به توسعهٔ رویهٔ حقوقی در زمینه قانون بین‌المللی حقوق بشر ادامه می‌دهند.

45. سازمان‌های بین‌المللی نیز در توسعه و تعیین استانداردهای حقوق عرفی بین‌المللی در زمینه حقوق بشر ، نقشی کلیدی ایفا می‌کنند.[57] کمیساریای عالی حقوق بشر سازمان ملل متحد (OHCHR) و همچنین سایر نهادهای بین‌المللی، گزارش‌های موضوعی در حوزه‌های حقوقی منتشر می‌کنند که به تعیین استانداردها و توسعهٔ حقوق نرم کمک می‌کنند. نهادهای مربوط به معاهدات حقوق بشر [58]گزارش‌ها[59]، رویه‌های قضایی[60] و دیگر اَشکال راهنمایی، از جمله تفسیرهای عمومی و توصیه‌های عمومی[61] را منتشر می‌کنند که به توسعه و درک مواد معاهدات مربوطه‌شان کمک می‌کنند. به همین ترتیب، رویه‌های ویژه شورای

---

[54] بر اساس منشور حقوق بشر و حقوق ملت‌های آفریقا (منشور بانجول) ایجاد شده.

[55] بر اساس کنوانسیون حفاظت از حقوق بشر و آزادی‌های اساسی (کنوانسیون اروپایی حقوق بشر) ایجاد شده.

[56] بر اساس کنوانسیون آمریکایی حقوق بشر (پیمان سن خوزه) ایجاد شده.

[57] نمونه‌هایی از سازمان‌های بین‌المللی شامل دادگاه جنایی بین‌المللی، سازمان بین‌المللی مهاجرت و سازمان منع سلاح‌های شیمیایی است، همچنین مکانیزم‌های حقوق بشری مانند کارشناسان ویژه و هیئت‌های تحقیق شورای حقوق بشر یا معادل‌های آنها. کارشناسان ویژه وظایف خود را در ارتباط با تمام کشورهای عضو سازمان ملل متحد انجام می‌دهند و به تصویب معاهده خاصی وابسته نیستند. در این مکانیزم‌های حقوق بشری، تفاوت‌هایی در هنجارهای قانونی و ساختار و همچنین در روش‌ها و استانداردهای جمع‌آوری اطلاعات وجود دارد. برای مثال، روش اصلی گروه کاری بازداشت‌های خودسرانه دریافت اطلاعات از افراد ذیربط، خانواده‌ها یا نمایندگان آنها، دولت‌ها، سازمان‌های غیردولتی و نهادهای ملی درباره موارد فردی است. این گروه کاری سپس موارد گزارش‌شده را از طریق تماس و مکاتبه بررسی می‌کند که شامل بازدیدهای کشوری نیز می‌شود. برای جدیدترین روش‌های کاری گروه‌های کاری، به سند A/HRC/36/38 نگاه کنید. در مقابل، هیئت‌های تحقیق توسط شورای حقوق بشر به‌صورت موردی تأسیس می‌شوند و معمولاً تحقیقات خود را بر اساس مفاد وظایف‌شان آغاز می‌کنند، که اغلب شامل بازدید از کشورها می‌شود و در طول این بازدیدها، از جمله با شهود مصاحبه‌هایی انجام می‌دهند. برای مثال نگاه کنید به مفاد حدود وظایف و اختیارات هیئت تحقیق درباره بوروندی. قابل دسترسی در:
www.ohchr.org/Documents/HRBodies/HRCouncil/CoIBurundi/TermsofreferenceCOIBurundiENGL.pdf.

[58] برای مثال، نگاه کنید به: کمیساریای عالی حقوق بشر (OHCHR)، «نهادهای معاهده حقوق بشر» [“Human rights treaty bodies”]. قابل دسترسی در www.ohchr.org/EN/HRBodies/Pages/TreatyBodies.aspx.

[59] گزارش‌ها می‌توانند به صورت ملاحظات نهایی باشند، که در آن یک نهاد معاهده گزارش‌های ارائه‌شده توسط دولت‌های عضو و سایر منابع ذی‌نفع را در مورد اجرای تعهدات دولت‌ها تحت یک معاهده خاص بررسی می‌کند. برخی از نهادهای معاهده هم قادر به صدور گزارش‌هایی درباره تحقیقات هستند. برای مثال، نگاه کنید به: کمیته رفع تبعیض علیه زنان، «رویه تحقیق» [Committee on the Elimination of Discrimination against Women, “Inquiry procedure”]. قابل دسترسی در www.ohchr.org/EN/HRBodies/CEDAW/Pages/InquiryProcedure.aspx.

[60] نهادهای معاهده در پاسخ به موارد خاص، نظرات خود را در مورد شکایات فردی صادر می‌کنند. به طور کلی، نگاه کنید به: کمیساریای عالی حقوق بشر (OHCHR)، «نهادهای معاهده حقوق بشر - ارتباطات فردی» [Human rights treaty bodies – individual communications]. قابل دسترسی در
www.ohchr.org/EN/HRBodies/TBPetitions/Pages/IndividualCommunications.aspx#procedureregenerale

[61] نگاه کنید به کمیساریای عالی حقوق بشر (OHCHR)، «نهادهای معاهده حقوق بشر - تفسیرهای کلی» [Human rights treaty bodies – general comments]. قابل دسترسی در
www.ohchr.org/EN/HRBodies/Pages/TBGeneralComments.aspx.

حقوق بشر نیز در تکامل هنجارهای تعیین استاندارد در قوانین بین‌المللی حقوق بشر[62] نقش دارند، همان‌گونه که سایر سازوکارها از جمله کمیسیون‌های حقیقت یاب و هیئت‌های تحقیق در این امر دخیل هستند.

46. همانند قانون بشردوستانهٔ بین‌المللی ، قانون بین‌المللی حقوق بشر نیز بخشی از چارچوب قانونی بسیاری از کشورها شده است، چه به دلیل سنت‌های حقوقی یگانه‌گرا که در آن تعهدات بین‌المللی را مستقیماً در حوزه ملی اعمال می‌کنند، چه از طریق ادغام مستقیم قانون بین‌المللی در قوانین ملی، و چه از طریق اعمال صلاحیت قضایی جهانی، که در نتیجه آن، تفاسیر حقوقی مهمی در بارهٔ این قانون به وجود آمده است.[63]

3- قانون کیفری بین‌المللی

47. قانون کیفری بین‌المللی هم در زمان صلح و هم در دوران مخاصمات مسلحانه اعمال می‌شود و افرادی را که طبق قانون بین‌المللی مرتکب جرایم می‌شوند، از جمله جنایات جنگی، جنایات علیه بشریت و نسل‌کشی، دارای مسئولیت کیفری می‌داند.[64] این جرایم گاهی به طور جمعی به عنوان «جنایات فجیع»[65] یا «جنایات شدید بین‌المللی» شناخته می‌شوند و بخش عمده‌ای از آنها در اساسنامه رم ،که به طور گسترده منعکس کنندهٔ قانون عرفی جنایی بین‌المللی است، تعریف شده‌اند. قانون کیفری بین‌المللی همچنین شامل جرایمی نظیر تروریسم که در اساسنامه رم تدوین نشده‌اند نیز می‌شود[66]. ممکن است بین قانون کیفری بین‌المللی و حوزه مرتبط با قانون جنایی فراملی همپوشانی که اعمال فرامرزی مانند قاچاق انسان، مواد مخدر، اسلحه و سایر کالاهای غیرقانونی را جرم تلقی می‌کند، همپوشانی‌هایی وجود داشته باشد.[67] بر خلاف قانون بشردوستانه بین‌المللی و قانون بین‌المللی حقوق بشر، تمرکز قانون کیفری بین‌المللی بر مسئولیت کیفری فردی است، نه مسئولیت دولتی. پرونده‌های قانون کیفری بین‌المللی ممکن است در دادگاه‌های کیفری ملی، دادگاه‌های کیفری ترکیبی،[68] دادگاه‌ها یا دیوان‌های کیفری

---

[62] به طور کلی، نگاه کنید به کمیسریای عالی حقوق بشر (OHCHR)، «کارشناسان ویژه شورای حقوق بشر» [Special procedures of the Human Rights Council]. قابل دسترسی در www.ohchr.org/en/HRBodies/SP/Pages/Welcomepage.aspx.

[63] سازمان عفو بین‌الملل، «صلاحیت قضایی جهانی: بررسی ابتدایی قانون‌گذاری در سراسر جهان – به‌روزرسانی ۲۰۱۲» (لندن، ۲۰۱۲)، صفحات ۱–۲.

[64] رابرت کرایر، دریل رابینسون و سرگئی واسیلیوف، «مقدمه‌ای بر قانون و آیین دادرسی جنایی بین‌المللی» [Robert Cryer, Darryl Robinson and Sergey Vasiliev, An Introduction to International Criminal Law and Procedure]، ویرایش چهارم (کمبریج، بریتانیا، انتشارات دانشگاه کمبریج، ۲۰۱۹)، فصل ۱۵.

[65] اگرچه اصطلاح «پاکسازی قومی» در اساسنامه رم ذکر نشده و به عنوان یک جرم مستقل در حقوق بین‌الملل تعریف نشده است، اما به عنوان یکی از «جرایم فجیع» در نظر گرفته شده است. در این زمینه، نگاه کنید به: سازمان ملل متحد، «چارچوب تحلیل برای جرایم فجیع: ابزاری برای پیشگیری» [United Nations, “Framework of analysis for atrocity crimes: a tool for prevention”]، ص ۱. قابل دسترسی در www.un.org/en/genocideprevention/documents/about-us/Doc.3_Framework%20of%20Analysis%20for%20Atrocity%20Crimes_EN.pdf.

[66] نگاه کنید به قطعنامه ۱۷۵۷ (۲۰۰۷) شورای امنیت، پیوست، ضمیمه (اساسنامه دادگاه ویژه لبنان)، ماده ۲.

[67] کرایر، رابینسون و واسیلیوف، «مقدمه‌ای بر قانون و آیین دادرسی جنایی بین‌المللی»، فصل ۱۵.

[68] این اصطلاح از جمله شامل شعب فوق‌العاده در دادگاه‌های کامبوج، دادگاه ویژه سیرالئون، دادگاه ویژه لبنان، شعب ویژه کوزوو و دفتر دادستانی، و دادگاه جنایی ویژه جمهوری آفریقای مرکزی می‌شود.

بین‌المللی،[69] از جمله دیوان کیفری بین‌المللی، یا دادگاه‌های داخلی که از صلاحیت قضایی جهانی استفاده می‌کنند، تحت رسیدگی قرار گیرند. منابع قانون کیفری بین‌المللی شامل اسناد تأسیسی دادگاه‌ها و دیوان‌ها (برای مثال، قطعنامه‌های شورای امنیت، اساسنامه‌ها، قوانین دادرسی و ادله و مقررات دادگاه‌ها) و قوانین ملی کشورهایی است که در مورد جرایم بین‌المللی صلاحیت قضایی اعمال می‌کنند. منبع مهم دیگر در قانون کیفری بین‌المللی، رویه‌های قضایی هستندکه بسته به صلاحیت قضایی ممکن است الزام‌آور یا تأثیرگذار باشند.[70]

ب) حوزهٔ قضایی و پاسخگویی

48. صلاحیت قضایی یک اصطلاح حقوقی است که به اختیاراتی اشاره دارد که به یک نهاد حقوقی، مانند دادگاه یا دیوان، اعطا می‌شود تا قانونی را وضع، رسیدگی و اعمال کند. عدالت و پاسخگویی در پروتکل به‌طور گسترده تعریف شده و به انواع مختلف فرآیندهای قضایی و غیرقضایی اشاره دارد. پاسخگویی در قبال جنایات بین‌المللی و نقض‌های قانون بین‌المللی حقوق بشر و/یا قانون بشردوستانه بین‌المللی ممکن است از طریق دادرسی‌های حقوقی، اعم از کیفری، مدنی یا اداری، و همچنین از طریق فرآیندهای غیرالزام‌آور حقوقی، مانند گزارش‌های تحقیقات بین‌المللی حقوق بشر، از جمله هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب و دیگر سازوکارهای عدالت انتقالی، از جمله ابتکاراتی که بر جستجوی حقیقت تمرکز دارند، به دست آید. محققان باید تلاش کنند تا در صورت امکان، دامنه‌ای از صلاحیت‌های قضایی ممکن که می‌توان در آن‌ها به دنبال پاسخگویی بود را در نظر بگیرند.

49. محققان منابع باز باید آن دسته از سازوکارهای پاسخگویی که ممکن است با کار آنها مرتبط باشد و نیز راه‌های احتمالی که ممکن است از طریق آنها مدارک جمع‌آوری‌شده برای اثبات حقایق پذیرفته شوند را شناسایی کنند. با این حال، در مراحل اولیه تحقیقات بین‌المللی، این موارد ممکن است نامشخص یا مبهم باشند. این موضوع به‌ویژه زمانی صادق است که دولت محل ارتکاب جنایات دارای نظام قضایی فعال و کارآمد نباشد یا زمانی که جامعه بین‌المللی هنوز به‌طور کامل برای بررسی این موضوع اقدام نکرده باشد. علاوه بر این، ممکن است پیش‌بینی تمام حوزه‌های قضایی که ممکن است در آینده با آن پرونده مرتبط باشند، ممکن نباشد. هنگامی که محققان منابع باز از سازوکار یا صلاحیت قضایی خاصی اطلاع ندارند، باید تلاش کنند تا اطلاعات را به گونه‌ای جمع‌آوری و حفظ کنند که استفاده از آن در حداکثر حوزه‌های قضایی بالقوهٔ مرتبط با موضوع، امکان‌پذیر باشد. اگر محققان از الزامات مربوط به مرجعی که پرونده در نهایت در آن رسیدگی خواهد شد آگاه باشند، باید فرآیندهای خود را با آن الزامات خاص تطبیق دهند.

50. صلاحیت قضایی می‌تواند به روش‌های زیر تعیین شود:

الف) صلاحیت قضایی حوزه‌ای (قلمرو): اختیار دادگاه برای رسیدگی به پرونده‌هایی است که به اقداماتی که در یک قلمرو مشخص رخ داده‌اند، مربوط می‌شود. در مورد دادگاه‌های بین‌المللی، صلاحیت قضایی حوزه‌ای معمولاً به قلمروهای کشورهای عضو که معاهده تأسیس آن دادگاه را تصویب کرده‌اند، محدود می‌شود؛

---

[69] این اصطلاح شامل دیوان کیفری بین‌المللی که دائمی است و دادگاه‌های بین‌المللی موردی برای یوگسلاوی سابق، دادگاه کیفری بین‌المللی برای رواندا، و سازوکار بین‌المللی باقی‌مانده برای دادگاه‌های کیفری بین‌المللی می‌شود.

[70] نگاه کنید به: رزا تئوفانیس، «اصل امر مختومه در قانون کیفری بین‌المللی»، فصلنامه بررسی قانون کیفری بین‌المللی [Rosa Theofanis, “The doctrine of res judicata in international criminal law”, *International Criminal Law Review*]، جلد ۳، شماره ۳ (۲۰۰۳).

ب) صلاحیت قضایی زمانی: اختیار دادگاه برای رسیدگی به پرونده‌هایی است که در آن اَعمالِ انتسابی در یک دوره زمانی مشخص رخ داده‌اند؛
ج) صلاحیت قضایی شخصی: اختیار دادگاه برای اتخاذ تصمیمات در مورد یکی از طرفین دعوی است؛
د) صلاحیت قضایی موضوعی: اختیار دادگاه برای رسیدگی به پرونده‌هایی است که از نوع خاصی باشند یا پرونده‌هایی که به موضوع خاصی مربوط می‌شوند؛
هـ) صلاحیت قضایی جهانی: ادعای اختیار توسط یک دادگاه برای رسیدگی به پرونده فرد متهم، بدون توجه به اینکه جرم انتسابی در کجا رخ داده و بدون توجه به تابعیت، کشور محل اقامت یا هر رابطه دیگری که فرد متهم با نهاد پیگرد کننده داشته باشد.

پ) اختیارات و وظایف تحقیقاتی

51. اختیارات تحقیقاتی رسمی، آن دسته از اختیاراتی هستند که برای انجام تحقیقات در یک حوزه قضایی معین توسط قانون به یک نهاد خاص واگذار می‌شوند. مشابه محدودیت‌های اعمال شده بر اختیارات مقامات قضایی، یک نهاد قضایی یا دادستانی تنها تا حدی که قانون به آن اجازه می‌دهد می‌تواند به تحقیقات بپردازد.[71] قدرت‌های تحقیقاتی ممکن است شامل توانایی احضار شهود، درخواست اسناد و اجرای حکم تبازرسی باشند. یک نهاد تحقیقاتی ممکن است بر اساس قانون موظف باشد که از رویه‌های سختگیرانه‌ای پیروی کند یا در برخی موارد بتواند رویه‌های خود را تعیین کند.[72]

52. بیشتر کسانی که در حال تحقیق درباره موارد نقض قانون بین‌المللی هستند، معمولاً دارای اختیارات تحقیقاتی یا ابزارهای اجرایی برای جمع‌آوری شواهد، مانند احضاریه یا حکم تفتیش نخواهند بود. بنابراین، آنها ممکن است به‌طور کامل به اطلاعات منابع باز و اطلاعاتی که به‌طور داوطلبانه ارائه می‌شود، مانند اسناد، فایل‌های دیجیتال و شهادت شهود، متکی باشند.

53. به طور کلی، اختیارات تحقیقاتی با وظایف مشخصی همراه هستند.[73] اگرچه برخی از محققان ممکن است از اختیارات پلیس یا سایر اختیارات قانونی برخوردار نباشند، توصیه می‌شود تا حد امکان، تمامی محققان تلاش کنند تا با وظایف اصلی محققان قانونی تطابق داشته باشند تا کیفیت تحقیقات تضمین شود. وظایف و تعهدات رایج محققان قانونی و دادستان‌ها شامل وظیفه تحقیق در مورد جزئیات دال بر جرم و یا برائت ، وظیفه محافظت از شهود، وظیفه حفظ شواهد، وظیفه تضمین عدالت در دادرسی‌ها و تعهد به احترام به حقوق متهمان است.

54. در محاکمات کیفری، دادستان‌ها موظف هستند اطلاعات و شواهد مربوطه را در اختیار وکلای مدافع قرار دهند.[74] این امسئله فقط شامل شواهدی که در دادگاه ارائه می‌شود نیست، بلکه شامل هرگونه

---

[71] نگاه کنید به: جاستیا [Justia]، «تحقیقات سازمانی» [Agency investigations]. قابل دسترسی در www.justia.com/administrative-law/agency-investigations.

[72] همان.

[73] برای مثال، ماده ۵۴ اساسنامه رم وظایف و اختیارات دادستان را در مورد تحقیقات مشخص می‌کند و توانایی دادستان را، از جمله، برای انجام تحقیقات، جمع‌آوری و بررسی شواهد، مصاحبه با قربانیان و شهود و همکاری با دولت‌ها و سازمان‌های بین‌المللی تعیین می‌کند.

[74] برای مثال، نگاه کنید به: دادگاه بین‌المللی برای یوگسلاوی سابق، «قوانین آیین دادرسی و ادله»، قاعده 66(A)؛ دادگاه کیفری بین‌المللی برای روآندا، «قوانین آیین دادرسی و ادله»، قاعده 66(A)؛ دادگاه ویژه لبنان، «قوانین آیین دادرسی و ادله»، قاعده 110(A).

اطلاعات جمع‌آوری‌شده در طول تحقیق می‌شود که ممکن است دال بر جرم یا برائت باشد، از جمله اطلاعات مربوط به اعتبار شهود.[75] برخی استثنائات وجود دارند که شامل اطلاعات محرمانه یا اطلاعاتی می‌شوند که ممکن است شخصی را در معرض خطر قرار دهد. دادگاه ممکن است دستور عدم افشای هویت قربانی یا شاهدی را صادر کند که ممکن است در صورت افشا با خطر مواجه شود، اما این امر هرگز تضمین‌شده نیست.[76] بسیاری از حوزه‌های قضایی کیفری دارای قوانین حاکم بر افشاگری هستند که دادستان‌ها را ملزم می‌کنند هرگونه اطلاعاتی که ممکن است دال بر برائت باشد را در اختیار قرار دهند.[77] محققان منابع باز که روی پرونده‌هایی کار می‌کنند که حتی اندک احتمالی برای رسیدگی در دادگاه دارند، باید این تعهدات مربوط به افشاگری را در کار خود در نظر داشته باشند.[78] دلایل دیگری نیز وجود دارد که چرا محققان باید به احتمال افشای اطلاعات توجه کنند. به عنوان مثال، اگر دادستان‌ها موظف به بررسی تمامی مدارک جمع‌آوری‌شده در یک تحقیق باشند، محققان باید از جمع‌آوری حجم زیادی از اطلاعات خودداری کنند، زیرا حجم زیاد ممکن است بار بیش از حدی ایجاد کند یا حتی مرور و پردازش آن غیرممکن باشد. این موضوع همچنین در مورد حفظ و ذخیره اطلاعات جمع‌آوری‌شده نیز اهمیت دارد، از جمله برچسب‌گذاری صحیح، که برای کسانی که در آینده به دنبال بازیابی و بررسی مواد هستند، بسیار مفید خواهد بود.

ت) قوانین آیین دادرسی و ادله

55. هنگام کار در چارچوب یک تحقیق حقوقی، وظیفه اصلی محققان منابع باز جمع‌آوری اطلاعات مرتبط و موثق است تا بتوان از آن برای دستیابی به نتایج واقعی و حقوقی استفاده کرد. به‌ویژه در دادگاه‌ها و دیوان‌های بین‌المللی، محققان باید تلاش نمایند تا اطمینان حاصل کنند که هرگونه مدرک منبع باز جمع‌آوری‌شده قابل پذیرش، مرتبط، قابل اعتماد و دارای ارزش اثباتی باشد. تحقیقات کیفری با تحقیقات انجام‌شده برای سایر اهداف متفاوت است، زیرا استاندارد اثبات بالاتری برای آنها اعمال

---

[75] برای مثال، نگاه کنید به: دیوان کیفری بین‌المللی، «قوانین آیین دادرسی و ادله»، قواعد 84-76؛ دادگاه بین‌المللی برای یوگسلاوی سابق، «قوانین آیین دادرسی و ادله»، قاعده (ii) (A) 66؛ دادگاه کیفری بین‌المللی برای رواندا، «قوانین آیین دادرسی و ادله»، قاعده (ii) (A) 66؛ دادگاه ویژه سیرالئون، «قوانین آیین دادرسی و ادله»، قاعده (ii) (A) 66؛ دادگاه ویژه لبنان، «قوانین آیین دادرسی و ادله»، قاعده (ii) (A) 110؛ هیئت‌های ویژه برای جرایم جدی در تیمور شرقی، «قوانین انتقالی آیین دادرسی کیفری»، بخش ۲۴.۴.

[76] برای مثال، نگاه کنید به: دیوان کیفری بین‌المللی، «قوانین آیین دادرسی و ادله»، قاعده (۴)81؛ دادگاه بین‌المللی برای یوگسلاوی سابق، «قوانین آیین دادرسی و ادله»، قاعده ۶۹؛ دادگاه جنایی بین‌المللی برای رواندا، «قوانین آیین دادرسی و ادله»، قاعده ۶۹؛ دادگاه ویژه سیرالئون، «قوانین آیین دادرسی و ادله»، قاعده ۶۹؛ دادگاه ویژه لبنان، «قوانین آیین دادرسی و ادله»، قواعد ۱۱۶–۱۱۵؛ هیئت‌های ویژه برای جرایم جدی در تیمور شرقی، «قوانین انتقالی آیین دادرسی کیفری»، بخش ۲۴.۶.

[77] برای مثال، نگاه کنید به: دادگاه بین‌المللی برای یوگسلاوی سابق، «قوانین آیین دادرسی و ادله»، قاعده ۶۸؛ دادگاه کیفری بین‌المللی برای رواندا، «قوانین آیین دادرسی و ادله»، قاعده ۶۸؛ دادگاه ویژه سیرالئون، «قوانین آیین دادرسی و ادله»، قاعده ۶۸؛ دادگاه ویژه لبنان، «قوانین آیین دادرسی و ادله»، قاعده ۱۱۳؛ اساسنامه رم دیوان کیفری بین‌المللی، ماده 67(۲)؛ هیئت‌های ویژه برای جرایم جدی در تیمور شرقی، «قوانین آیین دادرسی و ادله»، قاعده (ج) ۲۴.۴، شواهد تبرئه‌کننده شواهدی هستند که ممکن است متهم را از اتهام مبری کنند. در ایالات متحده، اصل بریدی یک قاعده کشف پیش از محاکمه است که توسط دادگاه عالی ایالات متحده تأسیس شده و مستلزم آن است که دادستان تمامی شواهد تبرئه‌کننده را در پرونده‌های کیفری به متهم ارائه دهد. نگاه کنید به: پرونده بریدی علیه مریلند [Brady v. Maryland]، 83 U.S. 378(1963).

[78] از آنجا که تعهدات افشای اطلاعات ممکن است مستلزم آن باشد که برخی یا همه مواد جمع‌آوری‌شده به وکلای مدافع ارائه شوند، توانایی محققان منابع باز در حفاظت از هویت‌ها و سایر اطلاعات حساس ممکن است از بین برود.

می‌شود[79] و قوانین آیین دادرسی و ادلهٔ آنها دارای سختگیری بیشتری است، از جمله مقررات مربوط به قابل قبول بودن مدارک، تا از حقوق افراد متهم در ارتباط با ضمانت‌های آیین دادرسی و محاکمهٔ عادلانه محافظت شود.[80] در حالی که استاندارد پذیرش مدارک در دادگاه‌ها و دیوان‌های کیفری بین‌المللی به‌طور کلی پایین‌تر از برخی دادگاه‌های ملی است، اما روش‌های جمع‌آوری مدارک همچنان بر اهمیتی که قضات برای آن مدارک قائل می‌شوند، تأثیر می‌گذارد. این موضوع در تمامی حوزه‌های قضایی صدق می‌کند. در دورانی که با افزایش چشمگیر اطلاعات دیجیتال، از جمله اطلاعات نادرست و گمراه‌کننده مواجه هستیم،[81] ضروری است که محققان بتوانند تشخیص دهند آیا اطلاعات منابع باز معتبر است و با دقت کافی صحت آن را اثبات یا رد کنند.[82]

56. در دادرسی‌های قضایی، «قابل قبول بودن مدرک» به این موضوع اشاره دارد که آیا یک مورد ارائه‌شده توسط یکی از طرفین دعوی می‌تواند به عنوان مدرک در پرونده پذیرفته شود یا خیر. به طور کلی، دیوان‌های جنایی بین‌المللی پذیرش یک مدرک پیشنهادی را با استفاده از یک آزمون سه‌عاملی ارزیابی می‌کنند: (الف) مرتبط بودن با موضوع؛ (ب) ارزش اثباتی؛ و (ج) ارزش اثباتی در مقایسه با هر گونه تأثیر زیان‌بخش احتمالی آن بر عادلانه بودن محاکمه.[83] مدرکِ ارائه‌شده در صورتی مرتبط خواهد بود که به افزایش یا کاهش احتمال یک واقعیت کمک کند، در حالی که ارزش اثباتی آن به این مطلب اشاره دارد که آیا مدرک مورد مذکور به اثبات یا رد یک واقعیت مورد بحث در پرونده کمک می‌کند یا خیر. در تحقیقات غیرقضایی نیز ارزیابی مشابهی برای قابلیتِ قبول یک مدرک اِعمال می‌شود. هر بخش از اطلاعات باید از نظر قابلیت اعتماد، مرتبط بودن با موضوع و ارزش اثباتی ارزیابی شود تا مشخص گردد که آیا و چگونه باید در تعیین نتیجه‌گیری های حقوقی و/یا نتیجه‌گیری های مربوط به داده‌ها مورد استفاده قرار گیرد.[84]

---

[79] برای مثال، در حالی که دادگاه‌های بین‌المللی معمولاً از استاندارد اثبات کیفری «فراتر از شک معقول» استفاده می‌کنند، هیئت‌های تحقیق و نهادهای مشابه معمولاً استاندارد پایین‌تری تحت عنوان «دلایل معقول برای باور» را برای پایه‌گذاری نظرات خود اتخاذ کرده‌اند. برای اطلاعات بیشتر، نگاه کنید به: کمیساریای عالی حقوق بشر (OHCHR)، «هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب در مورد حقوق بشر بین‌المللی و حقوق بشردوستانه: راهنما و عملکرد» [Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice]، صص ۶۳–۶۲.

[80] دیوان کیفری بین‌المللی، دادستان علیه ژان-پی‌یر بمبا [Prosecutor v. Jean-Pierre Bemba]، پرونده شماره ICC-01/05-01/08 A، «حکم در مورد تجدیدنظر آقای ژان-پی‌یر بمبا گومبو علیه حکم شعبه 3 دادگاه بر اساس ماده ۷۴ اساسنامه»، ۸ ژوئن ۲۰۱۸، شعبه تجدیدنظر، نظر جداگانه قاضی ون دن وینگارت و قاضی موریسون، پاراگراف ۵.

[81] اطلاعات نادرست به اطلاعاتی گفته می‌شود که نادرست هستند، اما قصد آسیب‌رسانی ندارند. برای مثال، افرادی که نمی‌دانند یک اطلاعات نادرست است ممکن است آن را در شبکه‌های اجتماعی به اشتراک بگذارند، به این امید که مفید واقع شوند. اطلاعات گمراه‌کننده اطلاعات نادرستی هستند که به‌طور عمدی با هدف خاصی برای آسیب‌رسانی تولید یا منتشر می‌شوند. تولیدکنندگان اطلاعات گمراه‌کننده معمولاً انگیزه‌های سیاسی، مالی، روان‌شناختی یا اجتماعی دارند. نگاه کنید به: کلر واردل، «بی‌نظمی اطلاعات: واژه‌نامه ضروری» (کمبریج، ماساچوست، مرکز شورنستاین برای رسانه، سیاست و سیاست‌گذاری عمومی، ۲۰۱۸) [Claire Wardle, “Information disorder: the essential glossary” (Cambridge, Massachusetts, Shorenstein Center on Media, Politics and Public Policy, 2018)]. قابل دسترسی در https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x32994.

[82] همان.

[83] بر اساس اساسنامه رم (مواد (الف)(۹) 64 و (4)69)، شعبه محاکمه دیوان کیفری بین‌المللی این «اختیار را دارد که بنا به درخواست یکی از طرفین یا به ابتکار خود... طبق قوانین آیین دادرسی و ادله، در مورد قابل‌قبول بودن یا ارتباط ادله تصمیم‌گیری کند... از جمله با در نظر گرفتن ارزش اثباتی ادله و هرگونه پیش‌داوری که چنین ادله‌ای ممکن است به دادرسی عادلانه یا ارزیابی منصفانه از شهادت شهود وارد کند».

[84] برای مثال، نگاه کنید به: کمیساریای عالی حقوق بشر (OHCHR)، «هیئت‌های تحقیق و کمیسیون‌های حقیقت‌یاب در مورد حقوق بشر بین‌المللی و حقوق بشردوستانه: راهنما و عملکرد»، به‌ویژه فصل 4-سی درباره جمع‌آوری و ارزیابی اطلاعات.

57. اهمیت مدرک به ارزشی اشاره دارد که به یک مدرک داده می‌شود و میزان اعتمادی که در نهایت در نتیجه‌گیری‌های حقوقی یا واقعی بر آن مدرک استناد می‌شود. تعیین میزان اهمیت باید یک ارزیابی جامع باشد که تا حدی به سایر اطلاعاتی بستگی دارد که ممکن است از واقعیت مورد نظر حمایت کند، آن را تأیید یا رد نماید. در بسیاری از دادرسی‌های حقوقی، پذیرش و اهمیت مدارک به‌طور جداگانه ارزیابی می‌شوند. در سایر زمینه‌ها، در مواقعی که قابلیت ارائهٔ مدرک عامل مهمی نیست، محققان حقوق بشر نیز از رویکردی مشابه برای ارزیابی اهمیتی که باید به اطلاعات داده شود استفاده می‌کنند.

58. قوانین آیین دادرسی و ادله که در دادرسی‌های کیفری بین‌المللی اعمال می‌شوند را می‌توان در اسناد تأسیس هر دادگاه، که معمولاً شامل قوانین آیین دادرسی و ادله آن دادگاه‌ها هستند، پیدا نمود. رویه‌های قضایی نیز راهنمایی‌های بیشتری ارائه می‌کنند. بسته به ماهیت تحقیق، ممکن است مشاوره با یک کارشناس حقوقی ارزشمند باشد. این موضوع به‌ویژه زمانی حائز اهمیت می‌شود که تحقیقِ مورد نظر قرار است برای دادرسی به دادگاه ارائه شود.

59. اطلاعات منابع باز ممکن است ترکیبی از شواهد مستند و شهادت شهود باشد. برای مثال، اصالتِ ویدیویی که شخصی در آن اظهاراتی مطرح می‌کند، باید سنجیده و تأئید شود و اظهارات موجود در آن نیز به صورت جداگانه تأیید شوند.[85] بنابراین، ممکن است روش‌های سنجش اعتبار یک مدرک دیجیتال به عنوان یک سند یا ارزیابی قابلیت اعتماد و قابلیت پذیرفته شدن آن به عنوان مدرک شهادت یک شاهد، اعمال شوند. محققان باید از نحوه برخورد با هر نوع مدرک در حوزه قضایی مربوطه آگاه باشند.
مستندات ممکن است حتی اگر تهیه کنندهٔ آن ناشناخته باشد یا نتواند برای شهادت حاضر شود، قابل پذیرش باشند. همچنین ممکن است بدون نیاز به معرفی سند از طریق شاهدی که بتواند اعتبار آن را تأئید کند، پذیرفته شود، مشروط بر اینکه طرف ارائه‌دهنده بتواند به‌وضوح و با دقت نشان دهد که این سند چگونه و به چه بخشی از پرونده مربوط می‌شود.[86]

---

[85] نگاه کنید به مرکز حقوق بشر، دانشگاه کالیفرنیا، برکلی، دانشکده حقوق، «رد پاهای دیجیتال: استفاده از شواهد الکترونیکی برای پیشبرد پیگردها در دادگاه جنایی بین‌المللی» [Human Rights Center, University of California, Berkeley, School of Law, “Digital fingerprints: using electronic evidence to advance prosecutions at the International Criminal Court] (برکلی، ۲۰۱۴). قابل دسترسی در www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. شواهد شنیداری (شواهد مبتنی بر شنیده‌ها)اطلاعاتی هستند که خارج از دانش مستقیم شاهدی که شهادت می‌دهد، می‌باشند. در برخی از حوزه‌های قضایی، شواهد شنیداری غیرقابل‌قبول هستند، مگر اینکه استثنای خاصی به آن تعلق گیرد. در سایر حوزه‌ها، شواهد شنیداری قابل‌قبول هستند، اما به دلیل این که نمی‌توان آنها را به درستی در بررسی متقابل توسط دادستان یا وکلای مدافع رسیدگی کرد، اعتبار کمی به آنها داده می‌شود. بر اساس گزارش سازمان امنیت و همکاری اروپا، «در حالی که شواهد شنیداری به طور کلی در حوزه‌های قضایی مبتنی بر حقوق عرفی در غیاب شرایط خاص قابل‌قبول نیستند، هیچ ممنوعیتی علیه شواهد شنیداری در حوزه‌های حقوق مدنی یا در دادگاه‌های بین‌المللی وجود ندارد». نگاه کنید به سازمان امنیت و همکاری اروپا، هیئت اعزامی به بوسنی و هرزگوین، «راهنمای تحقیقات برای جنایات جنگی، جنایات علیه بشریت و نسل‌کشی در بوسنی و هرزگوین» [Organization for Security and Cooperation in Europe, Mission to Bosnia and Herzegovina, Investigation Manual for War Crimes, Crimes Against Humanity and Genocide in Bosnia and Herzegovina] (سارایوو، ۲۰۱۳)، ص ۲۶. قابل دسترسی در www.osce.org/bih/281491?download=true. علیرغم فقدان این محدودیت‌ها در حوزه‌های قضایی حقوق مدنی و دادگاه‌های بین‌المللی، کلاً شواهد شنیداری به عنوان گروه خاصی از شواهد غیر مستقیم و غیرقابل‌اعتماد در نظر گرفته می‌شوند و قضات معمولاً اعتبار نسبتاً کمی به آنها می‌دهند.

[86] برای مثال، نگاه کنید به: دادگاه بین‌المللی یوگسلاوی سابق، دادستان علیه پاوله استروگار [Prosecutor v. Pavle Strugar]، پرونده شماره IT-01-42-T، «تصمیم در مورد قابل‌قبول بودن برخی اسناد»، ۲۶ مه ۲۰۰۴، شعبه 2 دادگاه، و دادستان علیه میلان میلوتینویچ و دیگران [Prosecutor v. Milan Milutinović et al]، پرونده شماره IT-05-87-T،

60. در شرایطی که مسئولیت جنایات و نقض‌ها به افراد بالاتر در ساختار فرماندهی نسبت داده می‌شود، اطلاعات جمع‌آوری‌شده ممکن است نه تنها برای اثبات «اساس جنایت» (در ادامه توضیح داده شده) استفاده شود، بلکه ممکن است برای اثبات نوع مسئولیت[87] فرد یا افراد متهم[88] نیز موضوعیت داشته باشد. زمانی که هر عنصری از جرم یا نقض حقوق، از جمله اعمال مجرمانه (actus reus) و حالت ذهنی متهم (mens rea) بر اساس استاندارد اثباتی که در آن مورد قابل اِعمال است، نشان داده شود، افراد ممکن است مسئول شناخته شوند. برای اتخاذ این تصمیم، دادگاه به اطلاعات ارائه‌شده در مورد هر عنصر نقض حقوق یا جرم توجه خواهد کرد. محققان باید با جرایم یا نقض‌های انتسابی، عناصر هر یک، افرادی که به ارتکاب آنها متهم هستند و نظریه‌ای که بر اساس آن مسئولیت بر عهدهٔ شخص خاصی قرار می‌گیرد، آشنا باشند. در پرونده‌های قانون کیفری بین‌المللی، مسئولان معمولاً شواهد «مبتنی بر جرم» را از شواهد «پیوندی» جدا می‌کنند. این دو مفهوم به شرح زیر توضیح داده می‌شوند:

الف) شواهد مبتنی بر جرم، شواهدی هستند که به جنایاتی که اتهامات بر اساس آنها بنا شده‌اند، مربوط می‌شوند، از جمله اطلاعات درباره اینکه جنایات توسط چه کسی، با چه چیزی، در کجا و در چه زمانی رخ داده‌اند.[89] به عنوان مثال، اگر اتهامِ شخص، ارتکاب قتل به عنوان یک جنایت علیه بشریت باشد، هرگونه اطلاعاتی که اثبات کند قتلی رخ داده است، به عنوان شواهد مبتنی بر جرم در نظر گرفته می‌شود. ب) شواهد پیوندی، شواهدی است که مسئولیت فرد متهم را در قبال جنایات ارتکاب‌یافته نشان می‌دهد، که این امر به‌ویژه زمانی اهمیت دارد که فرد متهم به‌طور مستقیم مرتکب جنایت نشده باشد.[90] به عبارت دیگر، شواهد پیوندی، شواهدی است که فرد مسئول را به جنایت متصل می‌کند. به‌عنوان مثال، در مواردی که اتهام بر این است که یک فرمانده نتوانسته از وقوع موارد نقض‌حقوق جلوگیری کند یا عاملان آنها را مجازات کند، با اینکه از آنها آگاه بوده است، شواهد پیوندی اثبات می‌کنند

«تصمیم در مورد درخواست دادستان برای پذیرش شواهد مستند»، ۱۰ اکتبر ۲۰۰۶، دادگاه؛ دادگاه جنایی بین‌المللی برای روآندا، دادستان علیه ادوارد کارمرا و دیگران [Prosecutor v. Edouard Karemera et al.]، پرونده شماره ICTR-98-44-T، «تصمیم در مورد درخواست ژوزف نزیرورا برای پذیرش اسناد ارائه شده بدون حضور شهود: اظهارات عمومی و صورتجلسات»، ۱۴ آوریل ۲۰۰۹، شعبه 3 دادگاه؛ دادگاه کیفری بین‌المللی، دادستان علیه توماس لوبانگا دیلو [Prosecutor v. Thomas Lubanga Dyilo]، پرونده شماره ICC-01/04-01/06، «تصمیم در مورد پذیرش اسناد ارائه شده بدون حضور شهود »، ۲۴ ژوئن ۲۰۰۹؛ دادگاه بین‌المللی یوگسلاوی سابق، دادستان علیه رادوان کارادیچ [*Prosecutor v. Radovan Karadžić*]، پرونده شماره IT-95-5/18-PT، «دستور در مورد درخواست دادستان برای توضیح و پیشنهاد درباره رهنمودها برای اجرای محاکمه»، ۲۰ اکتبر ۲۰۰۹، دادگاه، و دادستان علیه رادوان کارادیچ [*Prosecutor v. Radovan Karadžić*]، پرونده شماره IT-95-5/18-T، «تصمیم در مورد اولین درخواست دادستان در مورد پذیرش اسناد ارائه شده بدون حضور شهود »، ۱۳ آوریل ۲۰۱۰، شعبه محاکمه؛ دادگاه جنایی بین‌المللی، دادستان علیه ژرمن کاتانگا و ماتیو نگودجولو چوی [Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui]، پرونده شماره ICC-01/04-01/07، «تصمیم در مورد درخواست‌های دادستان در مورد پذیرش اسناد ارائه شده بدون حضور شهود »، ۱۷ دسامبر ۲۰۱۰، شعبه 2 دادگاه.

[87] کرایر، رابینسون و واسیلیوف، «مقدمه‌ای بر قانون و آیین دادرسی جنایی بین‌المللی»، فصل ۱۵.

[88] نگاه کنید به: کمیساریای عالی حقوق بشر (OHCHR)، «چه کسی مسئول است؟ انتساب مسئولیت فردی برای نقض حقوق بشر بین‌المللی و حقوق بشردوستانه در هیئت‌های تحقیق، کمیسیون‌های حقیقت‌یاب و سایر تحقیقات سازمان ملل متحد» [Who's Responsible? Attributing Individual Responsibility for Violations of International Human Rights and Humanitarian Law in United Nations Commissions of Inquiry, Fact-Finding Missions and Other Investigations] (نیویورک و ژنو، ۲۰۱۸). قابل دسترسی در https://ohchr.org/Documents/Publications/AttributingIndividualResponsibility.pdf.

[89] کلی متیسون، «راهنمای میدانی ویدئو به عنوان مدرک» [Kelly Matheson, Video as Evidence Field Guide] (WITNESS، ۲۰۱۶)، ص ۴۲. قابل دسترسی در https://vae.witness.org/video-as-evidence-fieldguide.

[90] همان.

که او از این نقض‌ها آگاه بوده یا اینکه آن فرمانده بر روی شخصی که مرتکب مستقیم جنایت بوده، «کنترل مؤثر» داشته است.

ث) حق حریم خصوصی و حفاظت از داده‌ها

61. حق حریم خصوصی از جمله حقوق بنیادین بشر است.[91] یکی از عناصر مهم این حق، حق حفاظت از داده‌های شخصی است که در قوانین مختلف حفاظت از داده‌ها تبیین شده است.[92] قوانین حفاظت از داده‌ها و حریم خصوصی به‌ویژه در تحقیقات مربوط به استفاده از فناوری اطلاعات و ارتباطات دیجیتال (ICT) اهمیت فزاینده‌ای دارند. در ادامه مروری کلی بر مفاهیم حق بین‌المللی حریم خصوصی و چارچوب جهانی برای حفاظت از داده‌ها، امنیت داده‌ها و اشتراک‌گذاری داده‌ها ارائه می‌شود که محققان منابع باز باید از آنها آگاه باشند. در محیط دیجیتال، حریم خصوصی اطلاعاتی که شامل اطلاعاتی است که در مورد یک شخص وجود دارد یا می‌تواند از آن استخراج شود، دارای اهمیت ویژه‌ای است.[93]

62. محققان منابع باز باید به حقوق بشر احترام بگذارند و به‌ویژه به حق حریم خصوصی که اغلب در زمینه اطلاعات دیجیتال مطرح می‌شود، حساس باشند. به عنوان مثال، نقض حق حریم خصوصی یکی از معدود دلایلی است که بر اساس آن قضات دادگاه جنایی بین‌المللی ممکن است شواهد را رد کنند.[94] حریم خصوصی، کرامت انسانی و سایر ارزش‌های کلیدی مانند آزادی انجمن و آزادی بیان را حمایت و محافظت می‌کند. دادگاه اروپایی حقوق بشر برخی از قوی‌ترین تفسیرها از قوانین حریم خصوصی را به همراه مجموعهٔ فزاینده‌ای از رویه‌های قضایی در زمینه حقوق دیجیتال ارائه می‌دهد. نقض چنین حقوق بنیادینی به طور اجتناب‌ناپذیری منجر به اعتراضات وکلای مدافع در دادرسی‌های کیفری خواهد شد و حتی ممکن است به دعاوی مدنی علیه طرف‌های تحقیقاتی منجر شود. علاوه بر قوانین حریم خصوصی، قوانین و مقررات متعددی برای حفاظت از داده‌ها وجود دارند که امنیت داده‌های شخصی را تضمین می‌کنند. به‌ویژه، محققان منابع باز باید از مقررات 2016/679 پارلمان اروپا و مقررات 27 آوریل 2016 شورای اروپا درباره حفاظت از اشخاص حقیقی در ارتباط با پردازش داده‌های شخصی و جابه‌جایی آزاد این داده‌ها و لغو دستورالعمل 95/46/EC (مقررات عمومی حفاظت از داده‌ها - GDPR) و رویکرد آن نسبت به حفاظت از داده‌های فردی آگاه باشند، زیرا این قانون استاندارد بالایی تعیین کرده و کشورهای دیگر نیز در حال بررسی تصویب قوانین مشابه هستند.[95] با این حال، مقررات حفاظت از داده‌ها در بین

---

[91] حق حریم خصوصی در بسیاری از اسناد حقوق بشری و در قوانین اساسی بیش از ۱۳۰ کشور گنجانده شده است. برای مثال، نگاه کنید به: اعلامیه آمریکایی حقوق و وظایف انسان، ماده 5؛ کنوانسیون اروپایی حقوق بشر، ماده ۸؛ کنوانسیون آمریکایی حقوق بشر، ماده ۱۱؛ کنوانسیون حقوق کودک، ماده ۱۶؛ کنوانسیون بین‌المللی حمایت از حقوق همه کارگران مهاجر و اعضای خانواده‌هایشان، ماده ۱۴؛ منشور آفریقایی حقوق و رفاه کودک، ماده ۱۰؛ منشور عربی حقوق بشر، مواد ۱۶ و ۲۱؛ اعلامیه حقوق بشر انجمن کشورهای جنوب شرق آسیا، ماده ۲۱. همچنین نگاه کنید به: سازمان بین‌المللی حریم خصوصی، «حریم خصوصی چیست؟»، ۲۳ اکتبر ۲۰۱۷. قابل دسترسی در https://privacyinternational.org/explainer/56/what-privacy.

[92] در بیش از ۱۰۰ کشور و در بسیاری از اسناد بین‌المللی و منطقه‌ای قوانین حفاظت از داده‌ها وجود دارد. برای مثال، نگاه کنید به: سازمان همکاری و توسعه اقتصادی، «رهنمودهایی درباره حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی»؛ شورای اروپا، «کنوانسیون حفاظت از افراد در ارتباط با پردازش خودکار داده‌های شخصی»؛ منشور حقوق اساسی اتحادیه اروپا؛ چارچوب حریم خصوصی همکاری اقتصادی آسیا-اقیانوسیه (APEC)؛ قانون تکمیلی حفاظت از داده‌های شخصی در جامعه اقتصادی کشورهای غرب آفریقا.

[93] به طور کلی، نگاه کنید به سند A/HRC/39/29، پاراگراف ۵.

[94] نگاه کنید به: اساسنامه رم، ماده 69(۷).

[95] این مقررات اظهار می‌دارد که اشخاص حقیقی دارای حقوق مرتبط با حفاظت از داده‌های شخصی، حفاظت از پردازش داده‌های شخصی و جریان آزاد داده‌های شخصی در داخل اتحادیه اروپا هستند. حقوق مشابهی نیز در کنوانسیون حفاظت

کشورها متفاوت هستند و تنوع زیادی دارند و حتی در برخی موارد قوانین ممکن است به‌طور مستقیم با یکدیگر در تضاد باشند. محققان منابع باز باید برای آگاهی از قوانین و مقررات حفاظت از داده‌های قابل اِعمال در حوزه‌های قضایی که در آنها فعالیت می‌کنند، با یک کارشناس حقوقی مشورت کنند.

63. در نهایت، محققان منابع باز باید از ممنوعیت کلی دسترسی غیرمجاز به داده‌ها و شبکه‌ها آگاه باشند. به عنوان مثال، این شامل استفاده از رمز عبوری است که از طریق نفوذ به یک مجموعه دادهٔ به بیرون درز کرده و برای دسترسی به محتوای محرمانه به کار می‌رود. همچنین دسترسی غیرمجاز به اطلاعات محرمانه از طریق فریب و سایر روش‌های مهندسی اجتماعی [دستکاری روانشناختی افراد] نیز در این دسته قرار می‌گیرند.[96]

ج) سایر ملاحظات حقوقی مربوطه

64. در جریان تحقیقات منابع باز، قوانین دیگری نیز ممکن است مرتبط باشند. فهرست زیر شامل برخی از ملاحظات حقوقی است که محققان منابع باز باید از آنها آگاه باشند، اگرچه این فهرست جامع نیست.

1- نقض شرایط خدمات

65. برخی از تکنیک‌های رایج در تحقیقات منابع باز ، نقض شرایط خدمات یک وب‌سایت یا پلتفرم است. به عنوان مثال، استخراج داده‌ها یا استفاده از هویت مجازی (نه هویت واقعی) شرایط خدمات پلتفرم‌ها و به‌ویژه پلتفرم‌های رسانه‌های اجتماعی را نقض می‌کند.[97] نقض شرایط خدمات، نقض قرارداد محسوب می‌شود. محققان باید بررسی کنند که آیا این نقض ممکن است در حوزه‌های قضایی که در آن کار می‌کنند، به عنوان یک عمل غیرقانونی تلقی شود یا خیر. نیاز به رعایت اصول امنیتی که می‌تواند از طریق استفاده از هویت‌های مجازی تأمین شود، باید در مقابل آسیب‌های احتمالی ناشی از نقض قرارداد، سنجیده شود، که رایج‌ترین جریمه در این شرایط، متوقف نمودنِ دسترسی کاربر به یک پلتفرم است. با وجود این، اگرچه هویت‌های مجازی صرفاً برای جستجو و نظارت در منابع باز ضروری هستند، همان‌طور که در بالا ذکر شد، نباید از هویت‌های مجازی برای دسترسی به محتوای موجود در شبکه‌های اجتماعی که تحت

از افراد در ارتباط با پردازش خودکار داده‌های شخصی، به ویژه پروتکل ۲۰۱۸ آن، در نظر گرفته شده است. این کنوانسیون نه تنها کشورهای عضو شورای اروپا، بلکه تعدادی از کشورهای دیگر را نیز متعهد می‌سازد.

[96] بر اساس تعریف مؤسسه ملی استانداردها و فناوری ایالات متحده، مهندسی اجتماعی «عمل فریب دادن فرد برای افشای اطلاعات حساس از طریق ایجاد ارتباط با آن فرد به منظور جلب اعتماد و اطمینان» است (پل ای. گراسی، مایکل ای. گارسیا و جیمز ال. فنتون، «راهنمای هویت دیجیتال» [Paul A. Grassi, Michael E. Garcia and James L. Fenton, Digital Identity Guidelines] (گیدرزبرگ، مریلند، مؤسسه ملی استانداردها و فناوری، ۲۰۱۷) [Gaithersburg, Maryland, National Institute of Standards and Technology]، ص ۵۴). همچنین نگاه کنید به: مایکل ورکمن، «دستیابی به اطلاعات با مهندسی اجتماعی: مطالعه‌ای تجربی درباره تهدید»، امنیت سیستم‌های اطلاعاتی، جلد ۱۶، شماره ۶ (۲۰۰۷) [Michael Workman, “Gaining access with social engineering: an empirical study of the threat”, Information Systems Security]. برای بحث بیشتر درباره دسترسی غیرمجاز و فریبنده، به پاراگراف ۶۵ در ادامه مراجعه کنید. برای بحث درباره استتار کاربر، به پاراگراف ۱۰۷ در ادامه مراجعه کنید.

[97] برای مثال، شرایط خدمات فیس‌بوک از کاربران می‌خواهد که «از همان اسمی که در زندگی روزمره استفاده می‌کنند، استفاده کنند»، «اطلاعات دقیق درباره خود ارائه دهند» و «فقط یک حساب (حساب خودشان) را ایجاد کنند و از تایم‌لاین برای مقاصد شخصی استفاده کنند». نگاه کنید به www.facebook.com/terms.php. جعل هویت، قوانین و سیاست‌های توییتر را نقض می‌کند. نگاه کنید به «سیاست جعل هویت» [Impersonation policy] در https://help.twitter.com/en/rules-and-policies/twitter-impersonation-policy.

کنترل‌های محدودیتِ دسترسی هستند، استفاده کرد یا به عنوان بهانه‌ای برای استخراج مستقیمِ اطلاعات از یک شخص تحت پوشش هویت جعلی به کار برد. چنین رفتاری محققان را از حوزه تحقیقات منابع باز خارج کرده، اصول اخلاق را نقض می‌کند[98] و ممکن است قانون را نیز زیر پا بگذارد.[99]

2- قوانین مالکیت فکری

66. محققان باید از هرگونه مجوز مالکیت فکری که ممکن است برای انتشار، توزیع و/یا استفاده قانونی از اطلاعات جمع‌آوری‌شده در طول تحقیقات مورد نیازشان باشد، مطلع باشند. قوانین مربوطه از یک حوزه قضایی به حوزه دیگر متفاوت است، اگرچه اکثر حوزه‌های قضایی حداقل نوعی حفاظت از حق نسخه‌برداری را برای خالق یک اثر، مانند ویدیو، عکس یا متن منتشرشده آنلاین، فراهم می‌کنند. «خالق» معمولاً به عنوان فردی تعریف می‌شود که واقعاً آن محتوا را ایجاد کرده است – به عنوان مثال، با گرفتن عکس، ضبط ویدیو یا نوشتن متن اصلی – و نه کسی که آن را بارگذاری کرده است، اگرچه این دو می‌توانند یک نفر باشند. کاربر نهایی ممکن است برای جلوگیری از نقض حق نسخه‌برداری، نیاز به دریافت رضایت خالق برای استفادهٔ مورد نظر داشته باشد (مثلاً در صورت استفاده از محتوا در یک گزارش عمومی یا داستان ژورنالیستی) – دریافت رضایت بارگذارکننده، اگر آن شخص خالق محتوا نباشد، معمولاً برای جلوگیری از نقض قانون کافی نیست. این یکی دیگر از دلایلی است که محققان باید تلاش کنند تا منبع اصلی هر بخش از محتوایی را که به دست می‌آورند پیدا کنند. برخی از حوزه‌های قضایی (اما نه همه)، زمانی که ویدیوها، عکس‌ها، متن‌ها و اطلاعات دیگر برای اهداف اجتماعی مفید مانند آموزش، اجرای قانون یا روزنامه‌نگاری استفاده می‌شوند، استثنائاتی برای نیاز به دریافت رضایت ارائه می‌دهند – که اغلب به آنها استثنائات «استفاده منصفانه» یا «معامله منصفانه» گفته می‌شود. با این حال، این استثنائات، در صورت اعمال، معمولاً بسیار محدود هستند، بنابراین هر استفاده خاص نباید بدون بررسی دقیق، مشمول چنین استثنائاتی فرض شود. مکانیزم‌هایی که گاهی می‌توانند به کاهش احتمال و/یا گستره تخلف کمک کنند شامل این موارد می‌شود: گذاشتن لینک مربوط به محتوای اصلی در یک گزارش دیجیتال بدون آنکه مطلب فوق از منبع اصلی حذف شود؛ اعتبار دادن به خالق اثر؛ و استفاده از بخش کوچکی از محتوای اصلی – با این حال، این موارد نیز به زمینه و حوزه قضایی مربوطه بستگی دارد. اطلاعاتی که تحت مجوزهای خلاقانه عمومی (Creative Commons Licenses) یا سایر مجوزهای رایگان قرار دارند ممکن است دارای طیف وسیعی از استفاده‌های مجاز بدون هزینه باشند. با این وجود، اگر چنین مجوزهای رایگانی اعمال شود، رعایت شرایط مجوز، ضروری است و نباید با محتوا به گونه‌ای برخورد شود که گویی نیازی به اجازه ندارد.

[98] برای بحث در مورد اطلاعات گمراه کننده، به فصل (ج)2 در بالا درباره اصول اخلاقی مراجعه کنید.
[99] نگاه کنید به فصل (هـ)3 در بالا درباره حق حریم خصوصی و حفاظت از داده‌ها.

4. امنیت

خلاصهٔ این فصل

- همه، و نه فقط متخصصان فناوری اطلاعات، مسئولیت دارند که امنیت یک تحقیق و افراد تأثیر پذیرفته از آن را تضمین کنند.

- ملاحظات امنیتی باید دو جنبه داشته باشند: (الف) با زیرساخت‌ها، از جمله سخت‌افزار، نرم‌افزار و شبکه‌ها مرتبط باشد؛ و (ب) با رفتار، از جمله رفتار محققان و تمام کسانی که با آنها در تعامل هستند، مرتبط باشد.

- ارزیابی‌های امنیتی باید در سه سطح انجام شوند، از جمله در سطح سازمان، تحقیق/پرونده خاص و فعالیت‌ها/وظایف خاص.

- تدابیر حفاظتی، همانطور که در ارزیابی خطرات تحقیق شناسایی شده‌اند، باید برای کاهش خطرات و تهدیدها طراحی شوند.

- ارزیابی‌های امنیتی باید همه انواع آسیب‌ها را در نظر بگیرند، از جمله آسیب‌های دیجیتال، مالی، قانونی، جسمی، روانی و آسیب‌های حیثیتی.

- برخی از بزرگ‌ترین آسیب‌پذیری‌ها در تحقیقات منبع باز به اتصالات اینترنتی/آدرس‌های آی.پی (پروتکل اینترنت)، دستگاه‌ها و ویژگی‌های آنها، و رفتار کاربران مربوط می‌شود.

- محققان و سازمان‌های تحقیقاتی باید به طور مداوم در آموزش امنیتی مداوم شرکت کنند و بسته به ماهیت متغیر هر گونه تهدید و آسیب پذیری، تدابیر حفاظتیِ در حال تکاملی را به کار گیرند.

67. این فصل شامل مروری بر ملاحظات امنیتی آنلاین و آفلاین مرتبط با تحقیقات منبع باز است. با آمادگی مناسب، سرمایه‌گذاری و تمرکز بر ارزیابی تهدید و کاهش خطر، محققان منبع باز باید بتوانند خطر آسیب به افراد، داده‌ها و سایر دارایی‌ها را به حداقل برسانند. زیرساخت‌های امنیتی، از جمله سخت‌افزار، نرم‌افزار و پروتکل‌های مربوط به رفتار کاربران، باید تا حد امکان پیش از آغاز تحقیق ایجاد شوند، به‌طور منظم ارزیابی شوند و در صورت لزوم به‌روزرسانی گردند. اندازه و منابع یک سازمان ممکن است بر امکان‌پذیر بودنِ برخی از تدابیر حفاظتی تأثیر بگذارد؛ بنابراین، این فصل شامل استانداردهای انعطاف‌پذیری است که باید بر اساس نیازهای خاص یک سازمان و یک تحقیق، اتخاذ شوند. سازمان‌هایی که تحقیقات پرخطر انجام می‌دهند – مانند تحقیقاتی که شامل قربانیان به‌ویژه آسیب‌پذیر هستند یا در شرایطی که مجرمانِ انتسابی از مقامات دولتی و/یا افراد شناسایی‌شده باشند – باید از خدمات افراد حرفه‌ای باتجربه در حوزه امنیت سایبری بهره‌مند شوند. علاوه بر این، یک چارچوب امنیتی قوی باید شامل نوعی مکانیزم حسابرسی مستقل و آموزش‌های مداوم باشد تا کاربران بتوانند در جریان تحولات جدید فناوری و بهترین شیوه‌ها قرار داشته باشند.

الف) حداقل استانداردها

68. از آنجا که زیرساخت‌های امنیتی و بهترین شیوه‌های مربوط به رفتار کاربران به‌طور مداوم در حال تغییر هستند، این پروتکل اصول کلی را ارائه می‌دهد تا به محققان منبع باز در تفکر درباره امنیت کمک کند. محققان باید مسئول امنیت خود باشند، از جمله میزان خطری که در نتیجهٔ رفتارشان ایجاد می‌شود را ارزیابی کنند و تدابیر کافی برای کاهش خطر و محافظت را به اجرا درآورند. علیرغم نیاز به رویکردی اختصاص یافته و فردی در امنیت، حداقل استانداردهایی وجود دارند که محققان منبع باز باید همیشه در کار خود از آنها استفاده کنند تا با اصول امنیتی تطابق داشته باشند:

(الف) محققان منبع باز باید از افشای عناصر قابل شناسایی درباره خود، سازمان‌هایشان و هرگونه شریک یا منبعی به اشخاص ثالث خودداری کنند، مگر اینکه این امر یک هدف یا الزام تحقیقاتی باشد. بنابراین، محققان باید هویت خود را در اقدامات آنلاین محفوظ نگاه داشته و اطمینان حاصل کنند که فعالیت‌های آنلاین آنها تا حد امکان غیرقابل ردیابی باقی بماند.

(ب) محققان منبع باز باید فعالیت‌های آنلاین خود را با این انتظار انجام دهند که این فعالیت‌ها ممکن است توسط اشخاص ثالث زیر نظر گرفته شده و تحلیل شوند. از این رو، آنها باید فعالیت‌های آنلاین خود را به گونه‌ای انجام دهند که با هویت‌های مجازی‌شان سازگار باشد و هویت یا اهداف تحقیقاتی آنها را فاش نسازد و همچنین منابع انسانی یا اشخاص ثالث دیگر را به خطر نیندازد.

(ج) محققان منبع باز باید آگاه باشند که استفاده بیش از حد از یک منبع آنلاین اطلاعات، مانند یک سایت خاص، ممکن است خطر کنترل کردن و تحلیل توسط اشخاص ثالث را افزایش دهد. بنابراین، آنها باید راه‌هایی را برای به حداقل رساندن این احتمال اجرا کنند، مانند تنوع بخشیدن به منابع دیجیتال.

(د) محققان منبع باز باید از الگوهای رفتاری قابل شناسایی یا پیش‌بینی‌پذیر، مانند الگوهای جستجوی تکراری بر روی دستگاه‌های قابل شناسایی، خودداری کنند، زیرا این موارد ممکن است به شناسایی

اهداف تحقیق توسط اشخاص ثالث کمک کرده و محققان را برای حملات فیشینگ و انواع دیگر مهندسی اجتماعی، آسان‌تر هدف قرار دهند.[100]

(ه) محققان منبع باز باید کار حرفه‌ای خود را از فعالیت‌های شخصی آنلاین جدا نگه دارند. حساب‌های شخصی آنلاین و، تا حد امکان، تجهیزات شخصی نباید برای تحقیقات حرفه‌ای استفاده شوند و تجهیزات حرفه‌ای نیز هرگز نباید برای فعالیت‌های شخصی آنلاین به کار گرفته شوند.[101]

(و) محققان منبع باز که چندین تحقیق را انجام می‌دهند نباید تحقیقات خود را با یکدیگر درآمیزند. بنابراین، آنها باید زمان‌های شروع و پایان متفاوتی برای هر فعالیت تحقیقاتی در نظر بگیرند، داده‌ها و مستندات مربوط به هر تحقیق را در مکان‌های جداگانه نگهداری کنند و در صورت لزوم از هویت‌های مجازی متفاوت استفاده نمایند.[102]

(ز) محققان منبع باز باید از سیستم‌ها یا محیط‌های فنی‌ای استفاده کنند که به گونه‌ای طراحی شده‌اند که از ورود احتمالی نرم‌افزارهای مخرب یا عوامل مخرب دیگر که ممکن است در طول فعالیت‌هایشان با آنها مواجه شوند، حداقل تأثیرپذیری را داشته باشند.

ب) ارزیابی‌های امنیتی

69. برای توسعه یک چارچوب امنیتی مناسب و مؤثر، محققان منبع باز باید مفاهیم کلیدی امنیت سایبری و مدیریت ریسک را درک کنند. آنها همچنین باید بتوانند دارایی‌هایی را که نیاز به حفاظت دارند و آسیب‌های احتمالی را شناسایی کرده و تهدیدها، ریسک‌ها و آسیب‌پذیری‌های احتمالی را ارزیابی کنند.

70. ریسک به معنای احتمال از دست دادن، آسیب یا تخریب یک دارایی به دلیل خطرِ سوء استفاده از یک موقعیت آسیب‌پذیر است. هر یک از این اصطلاحات در ادامه تعریف شده‌اند. از آنجا که تحقیقات منبع باز که در اینترنت انجام می‌شوند، نسبت به تحقیقات سنتی دارای روش‌های متفاوتی برای جمع‌آوری اطلاعات هستند، انواع مختلفی از ریسک‌ها را به همراه دارند. شناسایی و ارزیابی این ریسک‌ها بخشی اساسی از برنامه‌ریزی و آماده‌سازی برای یک تحقیق است. برخی از نمونه‌های رایج ریسک‌ها در تحقیقات منبع باز شامل موارد زیر می‌شوند: توانایی‌های فنی و آگاهی از هدف یک تحقیق، یا نهادهای پشتیبان آن هدف هستند که می‌توانند باعث دور شدن از آن تحقیق یا گمراه کردن آن شوند؛ مشکلات در تنظیمات فنی محیط آنلاین مورد استفاده برای تحقیق که می‌تواند منجر به افشای اطلاعاتی شود که تحقیق را به خطر بیندازد؛ نرم‌افزار یا کدهای مخرب که ممکن است سیستم‌های کامپیوتری، فعالیت‌ها، هویت یا داده‌های جمع‌آوری‌شده محقق را به خطر بیندازد؛ یا ویژگی‌های فنی مانند ردیاب‌ها، کوکی‌ها، بیکن‌ها و تحلیل‌ها که می‌توانند فعالیت‌های تحقیقی را به خطر بیندازند.

[100] به توضیحاتی که در ادامه درباره حملات فیشینگ و مهندسی اجتماعی ارائه شده است، نگاه کنید.
[101] اگر استفاده از تجهیزات شخصی اجتناب‌ناپذیر است، کاربران باید تحقیقات حرفه‌ای و فعالیت‌های شخصی خود را در محیط‌های آنلاین جداگانه، مثلاً با استفاده از یک ماشین مجازی برای تحقیقات خود انجام دهند.
[102] علاوه بر کاهش خطر اشتباه در تحقیقات، این روش‌ها به حفظ مؤثر زنجیره نگهداری [شواهد و مدارک] نیز کمک خواهند کرد.

71. بخش زیر به توضیح مفاهیم اصلی و نحوه به‌کارگیری آنها در تحقیقات منبع باز می‌پردازد و در نتیجه، راهنمایی برای ارزیابی تهدیدها و ریسک‌ها فراهم می‌کند.

1- دارایی‌ها

72. دارایی به هر چیزی که نیاز به حفاظت دارد اطلاق می‌شود، از جمله افراد،[103] اموال و اطلاعات. در زمینه تحقیقات منبع باز، افرادی که نیاز به محافظت دارند ممکن است شامل محققان یا تیم‌های تحقیقاتی و همچنین هر کسی که با آن‌ها همکاری می‌کند (مانند همکاران داخلی یا شرکای خارجی، چه افراد محلی و چه آنهایی که در تحقیقات میدانی هستند)، نویسندگان یا منابع اطلاعات، شهود، قربانیان، متهمان و ناظران باشد. اموال شامل اقلام ملموس و غیرملموس است که می‌توان ارزشی به آنها اختصاص داد.[104] دارایی‌های ملموس شامل ساختمان‌ها، تجهیزات و اسناد هستند، در حالی که دارایی‌های غیرملموس شامل اعتبار و اطلاعات اختصاصی، مانند داده‌های دیجیتال، فراداده، پایگاه‌های داده، کد نرم‌افزار و سوابق می‌شود.

2- آسیب

73. آسیب به معنای خسارت یا صدمه فیزیکی یا ذهنی به دارایی‌ها یا از بین رفتن آنهاست. این آسیب می‌تواند شامل خسارت‌های دیجیتال، مالی، حقوقی، فیزیکی، روانی-اجتماعی یا آسیب به اعتبار و وِجهه باشد.

(الف) آسیب دیجیتال

74. آسیب دیجیتال به خسارت وارد شده به هرگونه اطلاعات یا زیرساخت دیجیتال گفته می‌شود. آسیب‌های احتمالی دیجیتال می‌تواند شامل تخریب، دستکاری یا از دست دادن دسترسی به داده‌ها، یا اختلال در خدمات سیستم‌ها و پلتفرم‌های کامپیوتری باشد.

(ب) آسیب مالی

75. آسیب مالی می‌تواند از منابع مختلفی ناشی شود، از جمله آسیب‌های حقوقی و اعتباری مرتبط با یک تحقیق. محققان، اهداف تحقیق و ناظران همگی ممکن است با چنین آسیبی مواجه شوند. علاوه بر این، آسیب مالی می‌تواند زمانی رخ دهد که محققان نتوانند هزینه‌های درازمدت یک تحقیق را به‌درستی ارزیابی کنند.

(پ) آسیب حقوقی

76. محققان منبع باز ممکن است به دلیل فرایند یا نتایج کار خود با مسئولیت حقوقی مواجه شوند. محققان باید از محدودیت‌های قانونی فعالیت‌های خود و پیامدهای حقوقی اقداماتشان آگاه باشند تا ریسک

---

[103] اشاره به افراد به عنوان دارایی تنها در زمینه انجام ارزیابی‌های امنیتی انجام می‌شود.

[104] نگاه کنید به گروه تحلیلی تهدید (Threat Analysis Group)، «تهدید، آسیب‌پذیری، ریسک - اصطلاحاتی که اغلب اشتباه گرفته می‌شوند» [Threat, vulnerability, risk – commonly mixed up terms]. قابل دسترسی در: www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms.

مسئولیت حقوقی برای خود و یا اشخاص ثالث را به حداقل برسانند. تحقیقات همچنین می‌توانند منجر به آسیب حقوقی برای افرادی شوند که موضوع این تحقیقات هستند. حتی افراد حاضر در صحنه، که ممکن است در جریان تحقیق و با افشای تخلفات قانونی درگیر شوند، در معرض آسیبهای حقوقی هستند.[105]

(ت) آسیب فیزیکی

77. آسیب فیزیکی می‌تواند شامل خسارت به افراد یا اموال باشد. اگرچه محققان منبع باز معمولاً از دفتر یا خانه کار می‌کنند و نه در محل موضوع تحقیقات، ارزیابی آسیب فیزیکی همچنان به‌عنوان یک پیامد احتمالی فعالیت‌های آنلاین ضروری است. اقدامات در فضای مجازی می‌توانند منجر به پیامدهایی در دنیای واقعی بشوند که محققان باید از آنها آگاه باشند و برای مقابله با آنها آمادگی داشته باشند. برای مثال، محققان منبع باز باید به افرادی که ممکن است در محیط‌های ناامن باشند، مانند همکاران، کاربران آنلاین در کشورهای مورد نظر یا دیگران، توجه داشته باشند، زیرا رفتار آنلاین محقق می‌تواند آنها را در معرض خطر آسیب فیزیکی قرار دهد. محققان آنلاین یک وظیفه اخلاقی – و در برخی موارد قانونی – برای مراقبت از دیگران دارند[106] تا اطمینان حاصل کنند افرادی که در معرض خطر آسیب فیزیکی هستند، به دلیل فعالیت‌های آنها در خطر بیشتری قرار نگیرند. خطرات فیزیکی باید به‌عنوان بخشی از یک ارزیابی جامع خطرات، قبل از آغاز کار در نظر گرفته شوند و در طول دوره انجام تحقیقات نیز به‌طور مداوم بازبینی شوند.

(ث) آسیب روانی

78. آسیب روانی می‌تواند از ناراحتی روانی تا ضربه روانی را شامل شود و ممکن است هر یک از اعضای تیم تحقیق و/یا افرادی که به‌نوعی در تحقیق دخیل یا تحت تأثیر آن هستند، از جمله موضوعات تحقیق و ناظران را تحت تأثیر قرار دهد. علاوه بر اهمیت اخلاقی و معنوی حفاظت از خود و دیگران در برابر آسیب‌های روانی، انسان‌ها گاهی می‌توانند آسیب‌پذیرترین حلقه در عملکرد مؤثر هر سازمانی باشند. فردی که دچار آسیب روانی می‌شود ممکن است به‌ویژه آسیب‌پذیر باشد و فرصت‌های جدیدی برای عوامل تهدید ایجاد کند تا از آن سوءاستفاده کنند یا خطراتی برای امنیت فیزیکی و دیجیتال به وجود آید، به‌ویژه اگر تأثیرات منفی روانی باعث کاهش عملکرد، مانند رعایتِ کمتر از حد معمولِ پروتکل‌های امنیتی شود. تماشای حجم زیادی از ویدئوهای خشونت‌آمیز یا حاوی تصاویر دلخراش دیگر مخصوصا دشوار است و می‌تواند باعث ناراحتی روانی یا ضربه روانی شود که ممکن است نیاز به حمایت حرفه‌ای داشته باشد. نشانه‌های ضربه روانی ثانویه می‌تواند شامل تغییر در رفتار، نوسانات خُلقی، تغییر در عادات غذا خوردن یا نوشیدن، ناتوانی در خوابیدن، تمایل به خواب بیشتر از حد معمول یا کابوس باشد.[107] راهبردهایی برای

---

[105] برای بحث بیشتر در مورد ملاحظات قانونی مربوطه، نگاه کنید به فصل‌های E.۴ و F.۴ در بالا.

[106] اساسنامه رم، ماده (ب) (۱) ۵۴.

[107] نگاه کنید به: مرکز دارت برای روزنامه‌نگاری و تروما، «کار با تصاویر آسیب‌زننده» [Dart Center for Journalism and Trauma, "Working with traumatic imagery"]، ۱۲ اوت ۲۰۱۴ (قابل دسترسی در: https://dartcenter.org/content/working-with-traumatic-imagery)؛ سام دابرلی، الیزابت گریفین و هالوک مرت بال، «ایجاد تمرکز بر تروماهای ثانویه: مطالعه‌ای درباره رسانه‌های شاهد عینی و تروماهای جانبی در خط مقدم دیجیتال» [Sam Dubberley, Elizabeth Griffin and Haluk Mert Bal, Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline] (Eyewitness Media Hub، ۲۰۱۵) (قابل دسترسی در: http://eyewitnessmediahub.com/research/vicarious-trauma). سام دابرلی و میشل گرانت، «روزنامه‌نگاری

کاهش آسیب‌های روانی در بخش مربوط به آماده‌سازی و ایجاد یک برنامه مقاومت و مراقبت از خود توضیح داده شده‌اند.[108]

(ج) آسیب به اعتبار

79. در زمینه تحقیقات منبع باز، آسیب به اعتبار می‌تواند به‌ویژه برای محققان منبع باز و/یا سازمان‌های آنها شدید باشد، مثلاً هنگامی که محققان اطلاعات نادرستی منتشر کنند، اصول اخلاقی را نقض کنند یا محتوایی تولید میکنند که مشکل‌ساز است. آسیب به اعتبار ممکن است همچنین به افراد مورد تحقیق نیز وارد شود و ممکن است به دلیل رفتارهایی که به آنها نسبت داده شده، پس از عمومی شدن آن رفتارها، بدنام شوند. این موضوع به‌ویژه زمانی نگران‌کننده است که اتهاماتی علیه افراد یا سازمان‌ها مطرح شود که بعداً نادرستی آنها ثابت شود.

3- اقدامات حفاظتی

80. اقدامات حفاظتی تلاش‌هایی هستند که برای پیشگیری یا به حداقل رساندن آسیب‌پذیری‌ها انجام می‌شوند و ممکن است شامل اقدامات فیزیکی، فناوری و سیاست‌گذاری باشند. حفاظت فیزیکی می‌تواند شامل قفل‌های ایمنی برای ساختمان‌ها، اتاق‌ها یا کابینت‌هایی باشد که اسناد حساس در آنها نگهداری می‌شود. اقدامات فناوری ممکن است شامل استفاده از گذرواژه‌ها، رمزگذاری و احراز هویت چندگانه در دستگاه‌ها یا کنترل‌های دسترسی در سیستم‌های داده باشد. اقدامات مربوط به سیاست و خط مشی شامل قوانین داخلی و خارجی و قوانین و سازوکارهای اجرایی می‌شوند، مانند قوانینی که ارسال محتوای کاری داخلی از ایمیل کاری به ایمیل شخصی را ممنوع می‌کنند یا سیاست‌هایی که استفاده از حساب‌های شخصی شبکه‌های اجتماعی بر روی کامپیوتر کاری را منع می‌کنند.

4- تهدیدها

81. تهدیدها مواردی هستند که دارایی‌ها باید در برابر آنها محافظت شوند. تهدید می‌تواند هر چیزی باشد که به‌طور عمدی یا تصادفی از یک وضعیت آسیب‌پذیر، سوءاستفاده کرده و یک دارایی را به دست می‌آورد، به آن آسیب می‌زند یا آن را نابود می‌کند. تهدیدها می‌توانند نسبت به یک سازمان یا تحقیق، داخلی یا

و تروماهای جانبی: راهنمایی برای روزنامه‌نگاران، سردبیران و سازمان‌های خبری» [Sam Dubberley and Michele Grant, "Journalism and vicarious trauma: a guide for journalists, editors and news organisations" (First Draft News، ۲۰۱۷) (قابل دسترسی در: https://firstdraftnews.org/wp-content/uploads/2017/04/vicarioustrauma.pdf). مرکز حقوق بشر و عدالت جهانی، «پروژه تاب‌آوری حقوق بشر وب‌سایت جدیدی راه‌اندازی می‌کند» [Center for Human Rights and Global Justice, "Human rights resilience project launches new website"]، ۲۱ می ۲۰۱۸ (قابل دسترسی در: https://chrgj.org/2018/05/21/human-rights-resilience-project-launches-resources-for-resilience-website).

کرامت ریتر و الکسا کونینگ، «چالش‌ها و استراتژی‌های تحقیق درباره تروما» [Keramet Reiter and Alexa Koenig, "Reiter and Koenig on challenges and strategies for researching trauma"]، Palgrave MacMillan (قابل دسترسی در: www.palgrave.com/gp/blogs/social-sciences/reiter-and-koenig-on-researching-trauma).

[108] برای اطلاعات بیشتر درباره مراقبت از خود، به فصل (د) (۵) در پایین مراجعه کنید.

خارجی باشند و ممکن است توسط افراد، گروه‌ها، مؤسسات یا شبکه‌ها اجرا شوند. محققان منبع باز باید از جمله از تهدیدهای زیر آگاه باشند.

(الف) حملات توزیع شده محروم سازی از خدمت

82. حملات توزیع شده محروم سازی از خدمت نوعی از حملات سایبری هستند که برای مختل کردن دسترسی شخص یا سیستمی که هدف قرار گرفته به یک دستگاه یا شبکه طراحی شده‌اند. باید سیستمی برای کاهش چنین حملاتی برای دارایی‌های عمومی مانند وب‌سایت‌ها و پورتال‌های دسترسی از راه دور ایجاد شود. علاوه بر این، باید سیستمی برای ثبت وقایع به وجود آورد تا در صورت وقوع حمله برای ثبت تمامی اقدامات و عوامل مربوطه مورد استفاده قرار گیرد.

(ب) حملات فیشینگ

83. فیشینگ یا سرقت آنلاین اقدامی کلاهبردارانه برای به دست آوردن اطلاعات حساس، مانند نام کاربری، گذرواژه و جزئیات کارت اعتباری، با جعل هویت یک نهاد معتبر در یک ارتباط الکترونیکی است.[109] حملات فیشینگ یا کلاهبرداری‌های تلفنی برای به دست آوردن اطلاعات محرمانه یا آزار محققان استفاده می‌شوند. حساب‌های شخصی نسبت به حساب‌های حرفه‌ای معمولاً در معرض خطر بیشتری قرار دارند؛ بنابراین، استفاده از آنها می‌تواند تحقیقات یا محتوای کاری را به خطر بیندازد.

(پ) حملات مرد میانی

84. حملات مرد میانی نوعی از حملات سایبری هستند که در آن عوامل مخرب خود را میان ارتباط بین دو طرف قرار می‌دهند، هویت هر دو طرف را جعل می‌کنند و به اطلاعاتی که دو طرف قصد دارند با یکدیگر رد و بدل کنند دسترسی پیدا می‌کنند.[110] این حمله به عامل مخرب اجازه می‌دهد تا داده‌هایی را که برای دیگری در نظر گرفته شده یا اصلاً نباید ارسال می‌شده را رهگیری، ارسال و دریافت کند، بدون اینکه هیچیک از طرفین از این موضوع آگاه شوند، تا زمانی که دیگر خیلی دیر شده باشد.[111]

(ت) مهندسی اجتماعی

85. مهندسی اجتماعی به معنای دستکاری روان‌شناختی افراد است تا آنها را وادار به انجام عملی مانند افشاط اطلاعات محرمانه کنند که بالقوه مضر باشد. نمونه‌های مختلفی از مهندسی اجتماعی نظیر فیشینگ هدفمند وجود دارد.[112] از آنجا که تاکتیک‌های مهندسی اجتماعی به‌طور مداوم تطبیق یافته و تکامل می‌یابند، محققان باید برای شناسایی و اجتناب از این تاکتیک‌ها مرتباً آموزش‌هایی دریافت کنند.

(ث) بدافزار

---

[109] نگاه کنید به Phishing.org، «فیشینگ چیست؟» قابل دسترسی در: www.phishing.org/what-is-phishing.

[110] نگاه کنید به Veracode، «حمله مرد میانی (MITM)» [Man in the middle (MITM) attack]. قابل دسترسی در: www.veracode.com/security/man-middle-attack.

[111] همان.

[112] فیشینگ هدفمند (Spear Phishing) به معنای عمل متقلبانه ارسال ایمیل‌هایی است که ظاهراً از طرف یک فرستنده آشنا یا مورد اعتماد ارسال شده‌اند، با این هدف که افراد خاص به افشای اطلاعات محرمانه ترغیب شوند.

86. بدافزار، مخفف نرم‌افزار مخرب، به برنامه‌های کامپیوتری‌ای گفته می‌شوند که برای نفوذ و آسیب رساندن به سیستم‌های کامپیوتری بدون رضایت کاربر طراحی شده‌اند. انواع مختلفی از بدافزار وجود دارند، از جمله جاسوس‌افزار و باج‌افزار.

5- عوامل تهدید

87. عامل تهدید یا عامل مخرب شخص یا نهادی است که مسئول یک رویداد یا حادثه‌ای است که بر ایمنی یا امنیت یک نهاد یا فرد دیگر تأثیر می‌گذارد یا می‌تواند تأثیر بگذارد. در تحقیقات کیفری بین‌المللی و حقوق بشری، عوامل تهدید معمولاً متهمان، اهداف تحقیق، از جمله دولت‌ها یا حامیان آنها هستند. برای محققان منبع باز مهم است که عوامل تهدید بالقوه را شناسایی کرده و توانایی‌ها و احتمال حملات آنها را درک کنند.

6- آسیب‌پذیری‌ها

88. آسیب‌پذیری به معنای ضعف یا خلأ در اقدامات حفاظتی است که می‌تواند در حوزه‌های دیجیتال و فیزیکی وجود داشته باشد. در فعالیت‌های آنلاین، آسیب‌پذیری‌ها می‌توانند شامل این موارد باشد: ضعف در تدابیر حفاظتی امنیتی که ممکن است برای دسترسی غیرمجاز به یک دارایی مورد سوءاستفاده قرار گیرند، نقص‌های امنیتی در نرم‌افزار، طراحی ناامن، یا کاربران و کدهایی که دسترسی بیش از حد به منابع دارند. در حوزه آفلاین، این آسیب‌پذیری‌ها می‌توانند شامل ضعف در افراد نیز باشند، مانند یک عضو تیم که در برابر اخاذی یا زورگویی آسیب‌پذیر است، یا کسی که به دلیل مواجهه بیش از حد با محتوای خیلی دلخراش یا شرایط کاری دشوار، دچار آسیب‌پذیری می‌شود.[113] آسیب‌پذیری‌های جدید ممکن است از طریق افشای اینکه یک تحقیق در حال انجام است یا فاش کردن دامنه تحقیق به اشخاصِ هدف قرار گرفته ایجاد شوند. در نهایت، آسیب‌پذیری‌های امنیتی ممکن است از تهدیدات خارجی مانند بدافزارها و ویروس‌های جدید ناشی شوند که محققان باید از آنها آگاه باشند. نقشه‌برداری امنیتی و ارزیابی ریسک باید این نوع آسیب‌پذیری‌ها را در نظر بگیرد.

89. محققان منبع باز باید از آسیب‌پذیری‌های آنلاین زیر نیز آگاه باشند.

(الف) کوکی‌ها

90. کوکی یک فایل کوچک است که اغلب از طریق یک وب‌سایت ارسال شده و در حافظه کامپیوتر کاربر یا روی دیسک کامپیوتر ذخیره می‌شود تا توسط مرورگر استفاده شود. کوکی‌ها اغلب برای عملکرد صحیح یک وب‌سایت ضروری هستند؛ برای مثال، با ذخیره تنظیمات ترجیحی کاربر و جزئیات هویتی او، تا نیازی به وارد کردن مکرر داده‌ها در بازدیدهای بعدی نباشد. کوکی‌ها به‌گونه‌ای توسعه یافته‌اند که می‌توانند داده‌های مهم – و اغلب حساس – درباره بازدیدکنندگان و بازدیدهای آنها را جمع‌آوری و ذخیره کنند. برخی از آنها به ابزارهای اصلی تبدیل شده‌اند که می‌توانند برای جمع‌آوری داده‌ها و ایجاد تصویری از

[113] برای اطلاعات بیشتر درباره تاب‌آوری و مراقبت از خود، به فصل (د) (۵) در پایین مراجعه کنید.

علایق و عادات جستجوی کاربر استفاده شوند. یک کوکی ممکن است تا زمان انقضا یا حذف شدن توسط کاربر در کامپیوتر باقی بماند.

(ب) ردیاب‌ها

91. ردیاب نوعی کوکی است که از قابلیت مرورگر برای ثبت صفحات بازدید شدهٔ وب، معیارهای جستجوی وارد شده و غیره بهره می‌برد. ردیاب‌ها کوکی‌های ماندگاری هستند که یک گزارش مداوم از رفتار بازدیدکننده وب‌سایت نگه می‌دارند. در ساده‌ترین شکل، ردیاب‌ها یک هویت منحصر به فرد به مرورگر کاربر اختصاص می‌دهند و سپس این هویت را به تمام فعالیت‌های مرور و جستجوی بعدی (از جمله معیارهای جستجو، صفحات بازدید شده، و ترتیب بازدید از صفحات) پیوند می‌زنند. این قابلیت به مالک ردیاب اجازه می‌دهد بازدیدهای قبلی و بعدی از یک وب‌سایت (یا مجموعه‌ای از وب‌سایت‌های وابسته) را به هم پیوند دهد و تصویری دقیق از کاربران و عادات جستجوی آنها ایجاد کند. ردیاب‌ها اغلب در تبلیغات تعبیه شده‌اند که سپس در چندین وب‌سایت توزیع می‌شوند و به ردیاب شانس بیشتری برای ثبت فعالیت‌ها و رفتار کاربر می‌دهند. حتی بازدید از یک وب‌سایت «مطمئن» ممکن است منجر به نصب ردیاب‌ها بر روی کامپیوتر کاربران و پیگیری فعالیت‌های بعدی آنها در اینترنت شود.

(پ) بیکن‌ها

92. بیکن مکانیزمی برای ردیابی فعالیت‌ها و رفتار کاربران است. بیکن‌ها از یک عنصر کوچک و نامحسوس (اغلب نامرئی) در یک صفحه وب ساخته شده‌اند، مانند یک پیکسل شفاف که وقتی توسط مرورگر نمایش داده می‌شود، اطلاعاتی درباره آن مرورگر و کامپیوتر مرتبط را به یک شخص ثالث ارسال می‌کند. بیکن‌ها می‌توانند همراه با کوکی‌ها استفاده شوند تا جمع‌آوری و انتقال داده‌ها را فعال کرده و کاربران را به‌طور منحصربه‌فرد شناسایی کرده و عادات جستجوی آنها را ثبت کنند. بیکن‌ها ارتباط نزدیکی با سایت‌های شبکه‌های اجتماعی دارند و شناسایی روابط و شبکه‌ها بخشی کلیدی از ساختار این سایت‌ها را تشکیل می‌دهد. و در پایان باید گفت که بیکن‌ها می‌توانند در ایمیل‌های مبتنی بر HTML برای جمع‌آوری و گزارش اطلاعات هویتی کاربر و دسترسی به کوکی‌هایی که قبلاً روی آن کامپیوتر ذخیره شده‌اند، استفاده شوند.

(ت) کدها و اسکریپت‌های دیگر

93. شمار فزاینده‌ای از وب‌سایت‌ها از تکه‌های کوچکی از کد استفاده می‌کنند که توسط مرورگرِ بازدیدکننده دانلود می‌شوند و قابلیت ذخیره اطلاعات مربوط به آن بازدید را دارند. این کدها می‌توانند بر نحوه نمایش وب‌سایت، واکنش وب‌سایت به ورودی‌ها و پاسخ مرورگر به وب‌سایت تأثیر بگذارند. کدها همچنین می‌توانند داده‌های حساس مرتبط با اطلاعات هویتی،فعالیت‌های بازدیدکنندگان و موضوعات دیگر را ذخیره کنند. جمع‌آوری داده‌ها ممکن است مداوم باشد و اطلاعات به یک شخص ثالث ارسال شود.

(پ) ملاحظات مربوط به زیرساخت

94. منظور از زیرساخت، سازه‌ها، امکانات و سیستم‌ها، از جمله نرم‌افزار و سخت‌افزار هستند که برای انجام تحقیقات منبع باز مورد نیازند. زیرساخت باید تدابیر امنیتی کافی را برای محافظت و نگهداری دارایی‌ها و

داده‌های یک سازمان فراهم کند (و به آنها مجهز باشد). برای مقاوم‌سازی زیرساخت، باید اقدامات کاهش خطر به‌منظور تضمین تداوم در صورت وقوع هر یک از موارد زیر انجام شود.

الف) اختلال یا قطع اتصال اینترنت؛

ب) اختلال یا از دست دادن دسترسی به داده‌های ذخیره‌شده؛

پ) از دست دادن، خراب شدن یا از بین رفتن داده‌ها؛

ت) اختلال یا از دست دادن خدمات نرم‌افزاری؛

ث) آسیب به یا از دست دادن سخت‌افزار؛

ج) دسترسی غیرمجاز به دستگاه‌ها؛

چ) دسترسی غیرمجاز به شبکه؛

ح) حذف یا دستکاری تصادفی داده‌ها؛

خ) تخریب یا دستکاری عمدی داده‌ها؛

د) نشت داده‌ها یا گروگان‌گیری داده‌ها.

95. معماری مورد نیاز بر اساس مقیاس فعالیت‌های تحقیقی آنلاین، ماهیت تحقیق و موضوع مورد نظر، و همچنین منابع مالی موجود برای ساخت، حفظ و در صورت لزوم اصلاح زیرساخت، تعریف می‌شود.

1- زیرساخت

96. زیرساخت‌های مورد استفاده برای تحقیقات منبع باز با ویژگی‌های اضافی‌ای که به استراتژی‌های تحقیقاتی خاص مربوط هستند، حداقل شامل اجزای زیر خواهند بود.

(الف) دستگاه‌ها

97. محققان منبع باز باید برای دسترسی به محتوای آنلاین، تجهیزاتی مانند کامپیوتر دسکتاپ، لپ‌تاپ، تبلت یا گوشی هوشمند داشته باشند. سخت‌افزار و تجهیزات باید با گذرواژه محافظت شوند، تمام دیسکها به طور کامل رمزگذاری شوند و در حالت ایده‌آل از احراز هویت چندمرحله‌ای استفاده کنند.[114] تمام تجهیزات باید به‌طور منظم پشتیبان‌گیری (بَک آپ) شوند. زمانی که از سخت‌افزار استفاده نمی‌شود، باید به‌صورت ایمن نگهداری شوند و دسترسی به آنها تنها به کاربر و افراد مجاز محدود شود. تجهیزات شخصی نباید برای فعالیت‌های مربوط به کار استفاده شوند. به همین ترتیب، تجهیزات مربوط به تحقیق هم نباید برای فعالیت‌های شخصی استفاده شوند، زیرا خطر پیوند دادن شبکه‌های اجتماعی شخصی با هویت‌های مجازی که برای اهداف تحقیق ایجاد شده‌اند وجود دارد.[115]

---

[114] احراز هویت چندگانه (Multifactor Authentication) سطح بالاتری از اجرای امور امنیتی است که از کاربر می‌خواهد برای ورود به یک حساب کاربری، دو نوع اعتبارنامه ارائه دهد. برای مثال، ارائه همزمان یک رمز عبور و یک داده بیومتریک (مانند اثر انگشت) یا کارت هوشمند. نگاه کنید به: ایالات متحده، مؤسسه ملی استاندارد و فناوری (NIST)، «بازگشت به اصول: احراز هویت چندعاملی (MFA)» [United States, National Institute of Standards and Technology, "Back to basics: multi-factor authentication (MFA)]. قابل دسترسی در: www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

[115] این توصیه ممکن است در طول سفر دشوار باشد، زیرا بسیاری از محققان دستگاه کاری خود را همراه دارند اما می‌خواهند یا نیاز دارند که در خارج از ساعات کاری به امور شخصی بپردازند. بنابراین، سازمان‌هایی که تحقیقات منبع باز انجام می‌دهند باید خط مشی‌های معقولی برای دوران سفر تدوین کنند.

(ب) اتصال اینترنت

98. در حالت ایده‌آل، محققان باید یک اتصال اینترنتی قوی، پایدار و خصوصی داشته باشند و از استفاده از شبکه‌های Wi-Fi عمومی خودداری کنند. اگرچه Wi-Fi عمومی رایگان – از جمله شبکه‌های نیمه‌خصوصی مانند آنهایی که توسط هتل‌ها یا کافی‌نت‌ها ارائه می‌شوند – گزینه‌ای راحت است، اما بسیار ناامن بوده و در معرض تهدیدات زیادی قرار دارند که بزرگ‌ترین آنها توانایی هکرها در قرار گرفتن بین کاربر و نقطه اتصال است. استفاده از یک هات‌اسپات شخصی با محافظت گذرواژه‌ای نیاز به سرمایه‌گذاری مالی دارد، اما برای انجام فعالیت‌های تحقیقی آنلاینِ امن، ضروری است. علاوه بر این، اگرچه همیشه یک اتصال اینترنتی قوی و پایدار تحت کنترل محقق نیست، اما از نظر عملکرد و امنیت بهتر است. در صورتی که از یک شبکه خصوصی مجازی (وی پی اِن) روی یک اتصال ناپایدار استفاده شود، محققان باید از یک مکانیزم ایمنی استفاده کنند تا در صورت قطع شدن اتصال، آدرس IP آنها فاش نشود.

(پ) مرورگرهای وب

99. یکی از ابزارهای اصلی مورد استفاده در تحقیقات آنلاین، مرورگر وب است که برای جستجو، یافتن و دسترسی به وب‌سایت‌های منتشر شده در اینترنت استفاده می‌شود. مرورگرها به‌عنوان رابط اصلی بین محققان و اینترنت عمل می‌کنند، اما اغلب به‌عنوان یک منبع خطر نادیده گرفته می‌شوند. مرورگرهای مدرن به‌طور مداوم در حال تغییر هستند و طیف گسترده‌ای از قابلیت‌های از پیش تعبیه شده را دارند تا نیازهای مختلف را برآورده کنند. مرورگرها همچنین هدف اصلی افرادی هستند که قصد دارند وضعیتی را زیر نظر بگیرند یا حملاتی علیه حریف خود انجام دهند، زیرا قابلیت‌های آنها می‌تواند به‌راحتی مورد سوءاستفاده قرار گیرد و قابلیت‌های اضافی نیز به‌سادگی می‌توانند اضافه شوند. یک مرورگر به‌طور همزمان به اینترنت و به کامپیوتر دسترسی دارد و در نتیجه ممکن است اطلاعات شناسایی‌کننده‌ای درباره کاربر داشته باشد. نشت داده‌ها از طریق مرورگر می‌تواند به اندازهٔ کافی اطلاعاتی را افشا کند تا شخص یا نهاد مورد تحقیق را از این جریان مطلع سازد. مرورگرهای مدرن دارای چندین ویژگی تعبیه شده در خود هستند و می‌توانند ویژگی‌های اضافی متعددی را اضافه کنند که به عنوان افزونه‌های مرورگر شناخته می‌شوند. این افزونه‌ها، به‌طور فردی یا جمعی، ممکن است باعث نشت داده‌ها شوند و منجر به شناسایی یک تحقیق، محقق یا خط تحقیقی و فعالیت‌های جستجوی مربوطه شوند. مرورگرها به‌طور پیش‌فرض قادر به دانلود و اجرای کدهای کامپیوتری گرفته‌شده از یک وب‌سایت هستند. وجود و/یا عملکرد کدهای کامپیوتری ممکن است برای محققان آشکار نباشد، اما این کدها می‌توانند محتوای دیجیتال ارائه‌شده به آنها را تغییر دهند، به قابلیت‌ها و داده‌های موجود در کامپیوترهایشان دسترسی پیدا کنند و حتی باعث شوند که کامپیوترها به روشی متفاوت از آنچه پیش‌بینی شده است عمل کنند. محققان منبع باز باید با استفاده از مرورگرهای ایمن و به‌روزرسانی‌شده که به‌طور منظم بررسی می‌شوند و با نصب نرم‌افزارها و افزونه‌های مناسب برای مقابله با برخی از خطراتی که در بالا ذکر شد، تلاش کنند تا این خطرات را به حداقل برسانند.[116]

2- اقدامات امنیتی

[116] برای راهنمایی‌های به‌روز درباره مرورگرها و سایر اقدامات امنیت عملیاتی، نگاه کنید به مرکز منابع امنیت رایانه‌ای مؤسسه ملی استاندارد و فناوری ایالات متحده [Computer Security Resource Center of the United States National Institute of Standards and Technology] (https://csrc.nist.gov)

100. این عناصر اساسی زیرساخت می‌توانند برای شناسایی کاربران و محل آنها مورد استفاده قرار گیرند. برای رعایت اصل ناشناس بودن و عدم انتساب، محققان باید از راهبردهای زیر برای استتار اتصالات اینترنتی خود استفاده کنند. این راهبردها محل و آدرس IP را پنهان کرده و کامپیوتر، ویژگی‌های شناسایی‌کننده دستگاه، سیستم‌عامل و مرورگر را استتار می‌کنند.

(الف) استتار اتصال

101. یک آدرس IP می‌تواند اطلاعاتی را فاش کند که ممکن است برای هدف قرار دادن پایه و اساس یک سازمان مورد استفاده قرار گیرد. محققان منبع باز باید از وی پی اِن‌ها، پروکسی‌ها یا نرم‌افزارهای دیگر برای پنهان کردن آدرس‌های IP کامپیوترهای خود استفاده کنند، به این معنا که آدرس‌های IP فاش‌شده در اینترنت به محققان یا سازمان‌های آنها ارتباطی نداشته باشند. وی پی اِن‌ها یک کانال رمزگذاری‌شده برای ارتباطات بین کامپیوتر محقق و سِرورِ وی پی اِن ایجاد می‌کنند، به‌گونه‌ای که شبکه‌ها یا گره‌هایی که اتصال از آنها عبور می‌کند تنها داده‌های رمزگذاری‌شده را مشاهده می‌کنند و این یک لایه حفاظتی اضافی فراهم می‌کند. با این حال، استفاده از برخی وی پی اِن‌ها توسط بعضی کشورها و وب‌سایت‌ها مسدود می‌شود و ممکن است فعالیت‌های تحقیقی را برای اشخاص ثالث به‌عنوان فعالیت‌های مشکوک نشان دهد. در حالت ایده‌آل، وی پی اِن‌ها باید این امکان را برای محققان فراهم کنند که از چندین آدرس IP استفاده کرده و در صورت لزوم به سرعت آنها را تعویض کنند. آدرس‌های IP نباید به یک کشور خاص قابل ردیابی بشوند، بلکه باید به‌گونه‌ای تقسیم شوند که مکان‌های متعددی در سراسر جهان را منعکس کنند.

(ب) استتار دستگاه

102. برای پنهان کردن ویژگی‌هایی که ممکن است برای شناسایی کاربران استفاده شوند، محققان می‌توانند از ماشین‌های مجازی استفاده کنند؛ یعنی برنامه‌های نرم‌افزاری یا سیستم‌های عاملی که رفتار کامپیوترهای مجزا را شبیه‌سازی می‌کنند. استفاده از ماشین مجازی در اصل یک کامپیوتر جدید درون یک کامپیوتر ایجاد می‌کند، یک محیط کاملاً جدا از سایر بخش‌های کامپیوتر. یک ماشین مجازی همچنین قادر است وظایفی مانند اجرای برنامه‌ها و نرم‌افزارها را انجام دهد، گویی یک کامپیوتر کاملاً جداگانه است،[117] و باعث می‌شود محققی که از آن استفاده می‌کند به‌صورت یک کاربر متفاوت در فضای آنلاین ظاهر شود. محققان هنگام استفاده از ماشین مجازی، سیستمی دارند که می‌تواند مرورگر، عامل کاربر، نرم‌افزار، پورت‌های باز، سیستم‌عامل و سایر اطلاعات مربوط به دستگاه را تغییر دهد تا هر بار که آنها آنلاین می‌شوند به‌صورت یک کاربر متفاوت ظاهر شوند. در حالت ایده‌آل، زیرساخت باید به محقق اجازه دهد از یک ماشین مجازی استفاده کند که دستگاه واقعی در حال استفاده را پنهان کند. ماشین‌های مجازی می‌توانند نابود و دوباره ایجاد شوند، به مرحله قبلی بازگردانده و احیا شوند، به روش‌های مختلف پیکربندی شوند، برای پرونده‌های جدید تکثیر شوند یا برای نیازهای آینده حفظ شوند. در غیر این صورت، محققان می‌توانند رویکردی پرزحمت‌تر اما نسبتاً مؤثر را در پیش بگیرند و ظاهر خود را به‌صورت دستی تغییر دهند؛ مانند استفاده از مرورگرهای مختلف هر بار که آنلاین می‌شوند، تغییر تنظیمات تا منحصربه‌فرد بودنِ ردپایِ دستگاه‌هایشان را محدود کنند و استفاده از افزونه‌هایی که مانع ردیابی می‌شوند.

3- زیرساخت‌های دیگر

[117] نگاه کنید به Techopedia، «ماشین مجازی» (VM) ، ۲۱ می ۲۰۲۰. قابل دسترسی در: www.techopedia.com/definition/4805/virtual-machine-vm.

103. محققان باید پیش از آغاز کار برای حفاظت از شبکه‌ها و زیرساخت‌های خود، سایر زیرساخت‌ها را در نظر بگیرند، از جمله سیستم‌های زیر:
الف) سیستم‌های پشتیبان؛
ب) سیستم‌های ثبت گزارش برای بررسی فعالیت‌ها و ردیابی اقدامات کاربران؛
پ) سیستم‌های ذخیره‌سازی مجزا و مکان‌های ذخیره‌سازی مناسب برای جمع‌آوری مواد دیجیتالی شناسایی‌شده در حین جستجوها. برای محافظت از داده‌ها در برابر تهدیدات خارجی، سازمان‌ها باید پلتفرم‌هایی (مانند مخازن شواهد، پایگاه‌های داده یا دیگر سیستم‌های مدیریت اطلاعات) داشته باشند که از شبکه‌های اصلی جدا نگه داشته شوند. این پلتفرم‌ها باید دو بخش اصلی داشته باشند: یکی متصل به اینترنت و دیگری بدون اتصال به اینترنت. در برخی موارد، ممکن است مناسب باشد که داده‌ها را هرچه زودتر از زیرساخت متصل به اینترنت به یک شبکه/مخزن امن‌تر منتقل کنند تا اطلاعات در وضعیت امن بررسی شوند.

ت) ملاحظات مربوط به کاربران

104. یکی از بزرگترین نقاط ضعف هر چارچوب امنیتی، کاربر است. حتی با وجود زیرساخت‌های کامل، بدون تغییر رفتار کاربران از طریق آموزش منظم و نظارت، اصول امنیتی رعایت نخواهند شد. امنیت مسئولیت همگان است. افراد نباید بدون آموزش مناسب در مورد چگونگی کاهش این خطرات، فعالیت‌هایی را انجام دهند که ممکن است داده‌ها یا افراد را در معرض خطر قرار دهد. محققان باید آموزش ببینند که تشخیص دهند کدام رفتار در هنگام انجام فعالیت‌های مختلف آنلاین مناسب است.

105. در مواقعی که یک عامل تهدید تلاش می‌کند منشاء فعالیت را به شبکه یا کاربر ردیابی کند، ناشناس ماندن می‌تواند به کاهش آسیب کمک کند.[118] هر فعالیت آنلاین در معرض ردیابی توسط اشخاص ثالث قرار دارد؛ بنابراین، محققان باید هنگام انجام فعالیت‌های آنلاین فرض کنند که چنین تهدیدی وجود دارد. رایج‌ترین هدف‌های ردیابی شامل آدرس‌های IP، مرورگرها و وضوح صفحه نمایش (که برای شناسایی تجهیزات استفاده می‌شود) و همچنین زمان ناوبری و فعالیت در وب‌سایت‌ها (مانند عبارات جستجو شده یا صفحات بازدید شده) هستند. یک عامل تهدید ممکن است تلاش کند منبع فعالیت آنلاین را شناسایی کند. اگر تلاشی برای ردیابی انجام شود، باید عامل تهدید از موقعیت یا هویت واقعی محقق یا نهاد تحقیقاتی منحرف شود. این کار می‌تواند با اتخاذ تدابیری صورت گیرد که به نظر برسد دسترسی به اینترنت از جای دیگری انجام می‌شود، مثلاً با استفاده از وی پی اِن، یا به‌صورت شخص دیگری، از طریق ایجاد و استفاده از هویت‌های مجازی.[119]

106. پنهان کردن اتصال و دستگاه مورد استفاده در یک تحقیق آنلاین حفاظت مهمی را فراهم می‌کند، اما اگر کاربران با شناسایی خود در یک وب‌سایت یا، برای مثال، با استفاده از اطلاعات شخصی برای ثبت‌نام یا ورود به یک شبکه اجتماعی یا حساب خصوصی دیگر هویت خود را فاش کنند، این حفاظت ممکن است تضعیف شود. محققان هرگز نباید از حساب‌های شخصی خود برای تحقیق استفاده کنند یا در

[118] ردیابی کردن به معنای کشف نقطه آغاز یا منبع اصلی یک شخص یا چیزی، با دنبال کردن یک مسیر اطلاعاتی یا سلسله‌ای از رویدادها به صورت معکوس است.
[119] برای بحث درباره هویت‌های مجازی، همچنین به فصل‌های (پ) (۲)، (ج) (۳)، و (الف) و (پ) (۴) در بالا مراجعه کنید.

مرورگری که برای تحقیقات منبع باز استفاده می‌شود به حساب‌های شخصی وارد شوند. برخی حساب‌ها ممکن است در زمان ایجاد به استفاده از عکس، شماره تلفن یا ایمیل نیاز داشته باشند. عکس‌ها، شماره‌های تلفن، ایمیل‌ها یا داده‌هایی که شخصی هستند یا قابل انتساب به محققان یا افراد دیگر هستند، هرگز نباید مورد استفاده قرار گیرند.

استتار کاربر

107. هویت مجازی[120] یک هویت یا پروفایل آنلاین ساختگی است که می‌تواند برای انجام فعالیت‌های تحقیقی امن در پلتفرم‌های شبکه‌های اجتماعی و دیگر پلتفرم‌های مبتنی بر وب که برای دسترسی به محتوا نیاز به ورود دارند، استفاده شود. این همچنین می‌تواند شامل یک حساب مجازی یا یک سرویس ایمیل یا پیام‌رسان، پایگاه داده، محصول یا برنامه‌ای باشد که از یک هویت آنلاین ساختگی به‌جای هویت واقعی استفاده می‌کند. از نظر امنیتی، محققان منبع باز باید هویت‌های مجازی ایجاد کرده و از آنها برای فعالیت‌های تحقیقی آنلاین که به محتوای منبع باز مربوط است، استفاده کنند. این کار برای اطمینان از این است که اگر یک عامل تهدید تلاش کند فعالیت‌های آنلاین آن پروفایل را ردیابی کند، با اطلاعاتی منسجم و قانع‌کننده بر اساس هویت مجازی مواجه شود که اطلاعات واقعی درباره محقق یا نهاد تحقیقاتی، یا اطلاعاتی درباره محتوا یا محور تحقیق را فاش نکند. این امر همچنین برای حفاظت از افرادی که امکان دارد از تحقیق حمایت کنند، یک اقدام امنیتی مهم است. پروفایل‌ها و حساب‌های مجازی و فعالیت‌هایی که با استفاده از آنها انجام می‌شوند باید برنامه‌ریزی شوند،[121] و سوابق مربوط به اطلاعات استفاده‌شده برای ایجاد حساب‌ها باید نگهداری شوند و فعالیت‌های انجام‌شده با استفاده از این حساب‌ها باید ثبت شوند، به‌طوری‌که بعداً در صورت نیاز، مثلاً در دادگاه، بتوان در بارهٔ آنها توضیح داد.[122]

[120] هرگونه استفاده از هویت‌های مجازی باید نیاز به امنیت را با اصل اخلاقی شفافیت متعادل کند. نگاه کنید به فصل (پ) (۲) در بالا درباره اصول اخلاقی.

[121] نگاه کنید به فصل (پ) (۵) در پایین درباره طرح تحقیق آنلاین.

[122] نگاه کنید به فصل (ت) (۶) در پایین درباره نگهداری.

5- آماده‌سازی

خلاصهٔ این فصل

- آماده‌سازی و برنامه‌ریزی استراتژیک برای انجام یک تحقیق جامع و امن خیلی ضروری هستند.

- آماده‌سازی شامل سه فرآیند است: الف) ارزیابی تهدیدها و ریسک‌ها و طراحی برنامه‌ای برای کاهش آنها؛ ب) ارزیابی فضای اطلاعاتی؛ و پ) توسعه یک برنامه تحقیقاتی. این فرآیندها ممکن است در طول چرخه تحقیق با یکدیگر همپوشانی داشته و/یا تکرار شوند.

- آماده‌سازی شامل تدوین برنامه‌ای برای مقابله با جنبه‌های روانی منفی ناشی از تحقیق می‌شود، مانند آنچه ممکن است از مواجهه با محتوای دلخراش یا مواد بالقوه آسیب‌زا ایجاد شود.

- آماده‌سازی شامل تدوین برنامه‌ای برای نحوه مدیریت اطلاعات جمع‌آوری‌شده در طول چرخه حیات آن است، از جمله زمان و شرایط حذف آن، نحوه و شرایط اشتراک‌گذاری آن و اینکه چه کسانی باید به آن دسترسی داشته باشند.

- آماده‌سازی باید شامل ارزیابی نرم‌افزارها و ابزارهای احتمالاً مفید باشد. محققان باید از مزایا و معایب منابع تجاری، سفارشی و منبع باز آگاه باشند.

108. محققان منابع باز باید فعالیت‌های تحقیقاتی آنلاین خود را تنها پس از اتخاذ برخی تدابیر مقدماتی آغاز کنند. مراحل مقدماتی باید شامل ارزیابی تهدید و ریسک دیجیتال و ارزیابی چشم‌انداز دیجیتال باشد.[123] سپس محققان باید برنامه‌های تحقیقاتی آنلاین را با استفاده از اطلاعات به‌دست‌آمده از این ارزیابی‌ها تدوین کنند. هر یک از این فعالیت‌ها در ادامه به تفصیل شرح داده شده است.

109. در سطح سازمانی نیز مهم است که پیش از جمع‌آوری و نگهداری اطلاعات، سیاست‌هایی درباره نگهداری داده‌ها، حذف داده‌ها، دسترسی به داده‌ها و اشتراک‌گذاری داده‌ها تدوین شود، همان‌طور که در ادامه به تفصیل آمده است.

الف) ارزیابی تهدید و ریسک دیجیتال

110. اندیشیدن به تهدیدهای احتمالی و اتخاذ استراتژی برای مدیریت ریسک – چه فیزیکی، دیجیتال یا روانی باشد، موجب اطمینان از رعایت اصول امنیتی و اخلاقی خواهد شد. در ابتدا، باید ارزیابی تهدید و ریسک دیجیتال انجام شود تا تهدیدهای کلی و مربوط به پرونده که ممکن است به دلیل فعالیت‌های آنلاین به وجود آیند، شناسایی شوند، به‌ویژه هنگام بازدید از وب‌سایت‌های هدف، زیر نظر گرفتنِ مستمر منابع خاص یا استخراج داده‌ها از رسانه‌های اجتماع گوناگون. این ارزیابی باید شامل عناصر تحلیل تهدیدهای همیشگی باشد، مانند شناسایی تمام عوامل بالقوهٔ تهدید، ارزیابی منافع و توانایی‌های این عوامل تهدید، و احتمال وقوع حمله، با در نظر گرفتن آسیب‌پذیری‌ها و اتخاذ تدابیر حفاظتی برای به حداقل رساندن این آسیب‌پذیری‌ها. در یک چنین ارزیابی‌ای، مشاوره با کارشناسان امنیتی، به‌ویژه افراد دارای تخصص در امنیت سایبری، مفید خواهد بود.[124] این ارزیابی باید به‌صورت دوره‌ای بازبینی شده و در صورت لزوم به‌روزرسانی شود. علاوه بر این، برای بررسی انواع خاصی از فعالیت‌های آنلاین یا ورود تهدیدهای بالقوهٔ جدید، ممکن است ارزیابی‌های بیشتری مورد نیاز باشد.[125]

ب) ارزیابی چشم‌انداز دیجیتال

111. محققان منابع باز باید محیط دیجیتال مربوط به موضوع مورد تحقیق را درک کنند. نوع فناوری‌های موجود و مورد استفاده، از جمله کاربران آنها، بر نوع داده‌های دیجیتالی که قابل دسترسی هستند، تأثیر خواهد گذاشت. این امر مستلزم شناسایی پلتفرم‌های آنلاین، خدمات ارتباطی، رسانه‌های اجتماعی، فناوری‌های موبایل و برنامه‌های موبایلی است که در منطقه جغرافیایی مورد تحقیق به‌طور معمول استفاده می‌شوند. برای مثال، در تحقیقات مربوط به جنایات جنگی، محققان باید از انواع وسایل حمل‌ونقل، فناوری اطلاعات و ارتباطات (ITC) و رسانه‌های دیجیتالی که توسط تمام طرف‌های درگیر در مخاصمه مسلحانه و همچنین شاهدان یا ناظران استفاده می‌شوند، آگاهی داشته باشند تا بتوانند تشخیص دهند که کدام نوع اطلاعات احتمال بیشتری دارد که ثبت و به صورت آنلاین منتشر شود.

---

[123] نگاه کنید به ضمیمه ۲ درباره الگوی ارزیابی تهدیدها و ریسک‌های دیجیتال و ضمیمه ۳ درباره الگوی ارزیابی نمای کلی دیجیتال.

[124] برای اطلاعات کلی درباره تهدیدها و ریسک‌ها در تحقیقات منبع‌باز، نگاه کنید به فصل ۴ در بالا درباره امنیت.

[125] نگاه کنید به ضمیمه ۲ درباره الگوی ارزیابی تهدیدها و ریسک‌های دیجیتال.

112. محققان باید طبقات افرادی که از هر یک از این فناوری‌ها در آن منطقه جغرافیایی استفاده می‌کنند یا به آنها دسترسی دارند را بررسی کنند. محققان در ارتباط با این موضوع باید آگاه باشند که محتوای دیجیتال تولیدشده توسط کاربران و قابل دسترسی عمومی، از جمله پست‌های رسانه‌های اجتماعی و اطلاعات به‌اشتراک‌گذاشته‌شده از طریق پلتفرم‌های ارتباطی، ممکن است به طور یکسان گسترهٔ کامل نقض حقوق‌ها علیه همه افراد و گروه‌ها را منعکس نکند. این امر به این دلیل است که استفاده از فناوری‌های دیجیتال ممکن است بر اساس عواملی مانند جنسیت،[126] هویت قومی، مذهب، عقیده، سن، وضعیت اجتماعی-اقتصادی، عضویت در اقلیت نژادی، زبانی،[127] قومی یا مذهبی، هویت بومی، وضعیت مهاجرت و موقعیت جغرافیایی[128] متفاوت باشد. این نابرابری ممکن است ناشی از نبود دسترسی به دستگاه‌ها، امکانات یا منابع[129] باشد که باعث می‌شود این افراد فرصت ایجاد یا بارگذاری اطلاعات آنلاین درباره مسائل یا نقض‌های مرتبط با خود را نداشته باشند. عامل دیگر می‌تواند این باشد که افراد مذکور، علاوه بر دیگر عوامل، ممکن است به آموزش برابر دسترسی نداشته و در نتیجه از نظر مهارت‌های فنی توانایی کمتری داشته باشند. در نتیجهٔ انواع گوناگون تبعیض که با هم همپوشانی دارند، برخی از بخش‌های جامعه ممکن است به‌طور مضاعف در فضای آنلاین نادیده گرفته شوند. مثلاً اطلاعات مربوط به زنان و دخترانی که به یکی از گروه‌های به حاشیه رانده شدهٔ مذکور تعلق دارند، ممکن است حتی کمتر در منابع باز نمایان باشد. این عوامل می‌توانند به این معنا باشند که چنین افرادی نه خالق محتوا هستند و نه توسط محتوا بازنمایی می‌شوند، و در نتیجه باعث انحراف نتایج هرگونه تحقیق آنلاین می‌گردند.

113. علاوه بر این، دسترسی نابرابر به فناوری در میان تمام بخش‌های جامعه ممکن است نه تنها تمرکز بر اینکه چه کسانی در محتوای آنلاین نمایان می‌شوند را منحرف کند، بلکه همچنین نوع نقض‌هایی که به صورت آنلاین موجود هستند، به‌ویژه در ارتباط با محتوای تولیدشده توسط کاربران را هم تحریف نماید. برای مثال، زمانی که زنان از تلفن‌های همراه متعلق به اعضای مرد خانواده خود استفاده می‌کنند یا یک حساب کاربری را با دیگران به اشتراک می‌گذارند، ممکن است درباره مسائل حساس، مانند خشونت جنسی و جنسیتی یا مسائل مربوط به سلامت جنسی و باروری صحبت نکنند. علاوه بر این، محتوای تولیدشده توسط کاربران در رسانه‌های اجتماعی، از جمله عکس‌ها و ویدئوها، ممکن است برخی از انواع نقض‌ها را آسان‌تر از دیگر موارد نشان دهد. برای مثال، خشونت جنسی و جنسیتی که ممکن است در محیط‌های خصوصی رخ دهد، ممکن است سخت‌تر از تصاویری مانند تخلیه اجباری به تصویر کشیده شوند.

---

[126] برای مثال، زنان، دختران و افراد همجنس‌گرا، دوجنس‌گرا، تراجنسیتی و بیناجنسی ممکن است به تلفن همراه خانوادگی دسترسی نداشته باشند یا مالک آن نباشند. برای بحث بیشتر درباره آنچه به عنوان «شکاف دیجیتال جنسیتی» شناخته می‌شود، نگاه کنید به سند A/HRC/35/9. همچنین نگاه کنید به قطعنامه شماره 13/32 شورای حقوق بشر و کتاب «ارزیابی: داده‌ها و شواهد درباره برابری جنسیتی در دسترسی دیجیتال، مهارت‌ها و رهبری» [Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership] نوشته عربا سی و نانسی هافکین [Araba Sey and Nancy Hafkin] (ماکائو، چین، مشارکت جهانی EQUALS و دانشگاه سازمان ملل متحد، 2019). قابل دسترسی در: www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf

[127] افراد متعلق به اقلیت‌های زبانی ممکن است با موانعی در دسترسی به فضای آنلاین مواجه شوند، زیرا این فضا معمولاً به زبان غالب اداره می‌شود. با این حال، برخی از اقلیت‌های زبانی ممکن است فضای آنلاین خود را داشته باشند که توسط خودشان اداره شده یا از زبان‌های خودشان استفاده کند. بنابراین، ممکن است محققان نیاز داشته باشند در زبان‌های اقلیت (از جمله زبان‌های بومی) جستجو کنند.

[128] برای مثال، در مناطق روستایی، اتصال به اینترنت ممکن است کمتر باشد.

[129] مانند نداشتن دسترسی فیزیکی به اتصال اینترنت پرسرعت یا ناتوانی در تأمین هزینه خرید دستگاه‌ها یا پرداخت هزینه‌های اشتراک.

114. در حالی که برخی از این عوامل را می‌توان با تلاش برای دسترسی به گسترهٔ متنوعی از اطلاعات آنلاین، نه فقط محتوای تولیدشده توسط کاربران، کاهش داد، اما باید همین عوامل را هنگام تحلیل انواع دیگرِ اطلاعات منبع باز نیز مدنظر قرار داد. برای مثال، هنگام دسترسی به داده‌ها و آمارهای تولیدشده توسط دولت، محققان باید همواره این پرسش را مطرح کنند که آیا این داده‌ها تمامی بخش‌ها و جنبه‌های جامعه را دقیقاً شامل شده‌اند یا خیر.[130] تعدادی از مسائل کلیدی و فناوری‌ها وجود دارند که بسته به ارتباط آنها با یک تحقیق خاص و بر اساس گستره جغرافیایی و زمانی آن قابل ارزیابی هستند. محققان باید جنسیت، سن، جغرافیا، نابرابری‌های اجتماعی-اقتصادی و سایر اطلاعات جمعیت شناسی مربوطه را مدنظر قرار دهند. هدف از این ارزیابی بهبود درک محققان از وضعیتی است که مورد تحقیق قرار گرفته تا بتوانند استراتژی‌های مؤثر تحقیقاتی آنلاین طراحی کنند و نیز محققان را وادار سازند که از ابتدا به سوگیری‌های احتمالی موجود در داده‌های آنلاین توجه کنند. تمام این دسته‌بندی‌ها ممکن است به همه تحقیقات مرتبط نباشند، بنابراین محققان باید با توجه به نیازهای موردی خود، ارزیابی فضای دیجیتال را تطبیق دهند. [131]برای فهرست کامل دسته‌بندی‌های اطلاعاتی که می‌توان در ارزیابی چشم‌انداز دیجیتال گنجاند، به ضمیمه 3 در ادامه مراجعه کنید.

پ) برنامهٔ تحقیق آنلاین

115. پیش از آغاز یک تحقیق منبع باز، باید یک برنامه تحقیق آنلاین[132] تدوین شود که (الف) استراتژی کلی تحقیق و (ب) فعالیت‌های تحقیقاتی آنلاین مشخصی را پوشش دهد. اگر تحقیقات آنلاین بخشی از یک تحقیق گسترده‌تر با استفاده از تکنیک‌های سنتی مانند گرفتن اظهارات شهود یا جمع‌آوری شواهد فیزیکی باشد، برنامه تحقیق آنلاین باید در برنامه اصلی تحقیق ادغام شود. محققان باید دیدگاه جنسیتی را در برنامه تحقیق ادغام کنند تا اطمینان حاصل شود که تحقیق تمامی نگرانی‌های مربوط به جنسیت را در بر می‌گیرد و به ماهیت متفاوتِ دسترسی به فناوری توجه می‌کند.[133] برنامه تحقیق آنلاین باید موضوعات زیر را مورد توجه قرار دهد.

1- اهداف و فعالیت‌های برنامه‌ریزی‌شده

116. برنامه باید اهداف و اولویت‌های تحقیق منبع باز، استراتژی پیشنهادی برای دستیابی به این اهداف و جدول زمانی اجرای آنها را مشخص کند.

2- استراتژی مدیریت ریسک

[130] به طور کلی نگاه کنید به: کمیساریای عالی حقوق بشر سازمان ملل متحد (OHCHR)، «یک رویکرد مبتنی بر حقوق بشر، به داده‌ها: جا نگذاشتن هیچ‌کس در دستور کار ۲۰۳۰ برای توسعه پایدار» [A human rights-based approach to data: leaving no one behind in the 2030 Agenda for Sustainable Development] (ژنو، ۲۰۱۸). قابل دسترسی در:
www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

[131] برای الگو، نگاه کنید به ضمیمه ۳ در ادامه.

[132] نگاه کنید به ضمیمه ۱ در ادامه، درباره الگوی برنامه‌ریزی تحقیقات آنلاین.

[133] برای راهنمایی بیشتر درباره چگونگی ادغام دیدگاه جنسیتی، نگاه کنید به ادغام دیدگاه جنسیتی در تحقیقات حقوق بشری: راهنما و عملکرد [Integrating a Gender Perspective into Human Rights Investigations: Guidance and Practice] (انتشارات سازمان ملل متحد، شماره فروش: 19.XIV.2).

117. برنامه باید شامل یافته‌های اصلی در مورد ارزیابی تهدید و ریسک دیجیتال باشد، از جمله تهدیدات سایبری احتمالی، همراه با استراتژی مدیریت ریسک که نحوه شناسایی، پاسخ‌دهی و ترمیم آسیب‌ها یا حملات را مشخص کند.

3- شناسایی نقش آفرینان و فرصت‌های همکاری

118. محققان منابع باز ممکن است بخواهند سایر عواملی که در حال انجام تحقیقات مشابه یا هم‌پوشان هستند را شناسایی کنند تا ارزیابی کنند که فعالیت‌های هر یک از آنها چگونه ممکن است بر یکدیگر تأثیر بگذارد و همچنین به بررسی امکان مشارکت و فرصت‌های همکاری بپردازند. این امر ممکن است شامل شناسایی بایگان‌های دیجیتال، روزنامه‌نگاران یا سایر گروه‌ها و افرادی باشد که محتوای آنلاین مربوط به تحقیق را حفظ می‌کنند. این شناسایی باید تعصب‌های احتمالی و محدودیت‌های سایر عوامل را نیز در نظر بگیرد، زیرا این موارد ممکن است به نتایج جانبی منجر شوند که پیچیدگی‌های یک وضعیت خاص را به‌طور کامل نشان ندهند یا به دلیل سوگیری‌های ذاتی در فضای دیجیتال، همان طور که پیشتر توضیح داده شد، گروه‌های خاصی را حذف کنند. اگر چنین همکاری‌هایی شکل گیرد، تنظیم یک توافقنامهٔ کتبی برای به‌اشتراک‌گذاری اطلاعات مفید خواهد بود.

4- منابع

119. برنامه باید منابع مورد نیاز برای انجام فعالیت‌های برنامه‌ریزی‌شده، از جمله نیروی انسانی، آموزش، ابزارها و تجهیزات را مشخص کند. ارزیابی نیازهای مربوط به کارکنان می‌تواند شامل تعداد اعضای تیم مورد نیاز برای انجام وظایف، مهارت‌های آنها، فراگیر بودن و تنوع اعضای تیم و همچنین ارزیابی نیازهای آموزشی اضافی باشد. این ارزیابی ممکن است شامل بررسی زیرساخت‌های لازم، از جمله سخت‌افزار و نرم‌افزار، و هزینه‌های مالی نگهداری مطالب دیجیتال در دراز مدت باشد. این برنامه همچنین باید اطمینان حاصل کند که منابع مشخصی برای رفاه روانی مرتبط با جنسیت محققان اختصاص داده شده است، به‌ویژه در شرایطی که تحقیق منبع باز با محتوای خیلی دلخراش سروکار دارد یا زمانی که محققان یا اشخاص ثالث مربوطه ممکن است در صورت افشا شدن هویت یا حریم خصوصی‌شان به‌طور خاص در معرض خطر اقدامات تلافی‌جویانه قرار گیرند.[134]

5- نقش‌ها و مسئولیت‌ها

120. اگر کار به‌صورت تیمی یا با شرکای خارجی انجام می‌شود، نقش‌ها و مسئولیت‌های محققان منابع باز باید به‌طور دقیق تعریف شوند، و هماهنگی فعالیت‌ها، از جمله جلوگیری از تکرار فعالیت‌ها و جمع‌آوری داده‌ها در نظر گرفته شوند. به علاوه ، این بخش از برنامه باید در نظر بگیرد که برای یک تحقیق خاص

[134] برای مثال، محققان ممکن است با سخنان نفرت‌انگیز یا آزار و اذیت آنلاین مواجه شوند و این حملات ممکن است بر اساس جنسیت انجام شوند (برای مثال، زنان و محققان همجنس‌گرا، دوجنس‌گرا، تراجنسیتی، دگرباش و بیناجنسی ممکن است نسبت به میزان معمول با خطرات بیشتری، مانند سخنان نفرت‌آمیز آنلاین، افشای اطلاعات شخصی (doxing)، تهدید به تجاوز و سایر تهدیدات خشونت‌آمیز مبتنی بر جنسیت یا مسائل جنسی روبه‌رو شوند). برای مثال نگاه کنید به: سازمان عفو بین‌الملل [Amnesty International]، «توییتر سمی – مکانی مسموم برای زنان» (Toxic Twitter – a toxic place for women). قابل دسترسی در: www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

چه حوزه‌های تخصصی ممکن است مورد نیاز باشد و اینکه در صورتی که یک تخصص در تیم موجود نباشد آیا محققان باید با یک کارشناس مشورت کنند یا وی را به کار بگیرند یا خیر. حوزه‌های تخصصی ممکن است شامل پزشکی قانونی دیجیتال، تحلیل تصاویر ماهواره‌ای و علم داده‌ها باشد. در برخی حوزه‌های تخصصی، ممکن است تلاش‌هایی همراه با آینده نگری برای شناسایی کارشناسان از جنسیت‌ها و پیشینه‌های متنوع لازم باشد تا فراگیری و تنوع تیم تحقیق و تحلیل‌های آن تضمین شود.

6- مستندسازی

121. تحقیقات منابع باز باید به گونه‌ای مستند شوند که مدیریت مؤثر آنها و رعایت اصل پاسخگویی را امکان‌پذیر کند. در صورت رسیدگی‌های قانونی، این مستندسازی باید به محققان امکان دهد تا نشان دهند که شواهد جمع‌آوری‌شده مرتبط و دارای ارزش اثباتی هستند و گام‌هایی که در طول فعالیت‌های آنلاین برداشته شده یا نشده و دلایل آن را توضیح دهند. چه به صورت مستقل عمل کنید و چه از سوی یک سرپرست مأموریت دریافت کرده باشید، سیستم باید مکانیزمی برای ایجاد وظایف مرتبط با فعالیت‌های تحقیقاتی خاص، از جمله فعالیت‌های آنلاین، مانند درخواست برای تحقیق درباره یک شخص خاص یا سایر پرس‌وجوها داشته باشد. نتایج حاصل از انجام این فعالیت، از جمله گزارش‌ها، باید روش‌ها و تکنیک‌های به کار گرفته شده را قید کند. گزارش‌دهی باید اطلاعات عملیاتی که ممکن است برای حفاظت از منابع و روش‌های تحقیق محرمانه نگه داشته شود را از اطلاعات تحقیقاتی که باید در جریان رسیدگی‌های قانونی افشا شوند، جدا کند.

122. برنامه تحقیق آنلاین باید به صورت منظم بازبینی شود و در صورت لزوم اصلاح گردد. برای قالب برنامه تحقیق آنلاین، به ضمیمه 1 در ادامه مراجعه کنید.

ت) طرح پایداری و مراقبت از خود

123. در حالی که محققان ممکن است مصاحبه‌های حضوری انجام ندهند یا به صورت فیزیکی از صحنه‌های جرم بازدید نکنند، ویژگی‌های خاص تحقیق دیجیتال به این معناست که آنها ممکن است در معرض مشاهده، جمع‌آوری و تحلیل مقادیر قابل توجهی از اطلاعات دیجیتال دلخراش یا اطلاعاتی که به‌شکلی دیگر آسیب‌زننده هستند، قرار بگیرندکه این امر می‌تواند منجر به بروز آسیب روانی ثانویه و سایر مشکلات شود. محققان منبع‌باز باید با اصول مراقبت از خود[135] آشنا باشند، و مدیران تحقیقات باید محیطی سازمانی ایجاد کنند که به مراقبت از خود، حساسیت‌های جنسیتی و فرهنگی اهمیت دهد. این امر باید در مرحله آمادگی یک تحقیق، از طریق تدوین برنامه‌ای که به تقویت تاب‌آوری و کاهش اثرات منفی روانی تحقیقات بپردازد، نهادینه شود. این اثرات ممکن است بسته به جنسیت، فرهنگ و سن متفاوت باشند. چنین برنامه‌ای از نظر اخلاقی ضروری است، چرا که بخشی از ارتقا و احترام به حقوق بشر هر یک از اعضای تیم تحقیق محسوب می‌شود. این برنامه همچنین برای به حداکثر رساندن امنیت فیزیکی و دیجیتال ضروری است. حتی با وجود آموزش‌های مناسب، یک فرد تحت استرس می‌تواند به نقطه ضعفی برای ایمنی تیم، امنیت اطلاعات و کیفیت کار مبدّل شود. زمان و منابع مشخصی باید

[135] برای گفتگوی بیشتر درباره اهمیت مراقبت از خود برای افرادی که در زمینه تحقیقات حقوق بشری فعالیت می‌کنند، نگاه کنید به کمیساریای عالی حقوق بشر سازمان ملل متحد (OHCHR)، راهنمای پایش حقوق بشر [Manual on Human Rights Monitoring] (ژنو، ۲۰۱۱)، فصل ۱۲ درباره آسیب روانی و مراقبت از خود، صص ۲۰–۳۹. قابل دسترسی در: www.ohchr.org/Documents/Publications/Chapter12-MHRM.pdf

اختصاص داده شود تا اجرای صحیح این برنامه تضمین گردد، به‌ویژه زمانی که پیش‌بینی می‌شود یک تحقیق آنلاین شامل مشاهده حجم زیادی از تصاویر دلخراش، از جمله محتوای خشونت‌آمیز یا به‌گونه‌ای دیگر آزاردهنده باشد. روش‌های کاهش تأثیرات منفی احتمالی مشاهده چنین محتوای دلخراشی متنوع هستند، اما معمولاً در سه دسته قرار می‌گیرند: آگاهی فردی، راهکارهای به حداقل رساندن مواجهه با اینگونه محتوا و حمایت اجتماعی.

124. نخست آنکه محققان باید از رفتارهای معمول خود و اعضای تیم‌شان، از جمله الگوهای کاری، تفریح، خواب و غذا خوردن، آگاهی داشته باشند تا بتوانند تغییرات را شناسایی و به آنها رسیدگی کنند. وجود سیاستی که بر اساس آن محققان به صورت زوجی کار کنند می‌تواند در شناسایی این انحرافات مفید باشد، چرا که افراد ممکن است تغییرات رفتاری خود را تشخیص ندهند یا نخواهند آن را بپذیرند، اما این تغییرات ممکن است برای دیگران آشکارتر باشد. اعضای تیم باید نسبت به تفاوت‌های واکنش‌ها در مواجهه با مطالب دلخراش یا دیگر مواردی که ممکن است احساسات قوی را برانگیزند، حساس باشند، به آن احترام بگذارند، و بپذیرند که این تفاوت‌ها ممکن است بین افراد، جنسیت‌ها و گروه‌های فرهنگیِ گوناگون، متفاوت باشد. همچنین این واکنش‌ها می‌توانند در طول زمان برای افراد خاص، به دلیل میزان استرسی که تحمل می‌کنند یا عوامل موقعیتی دیگر، تغییر کنند. محققان باید این نکته را نیز درک کنند که داشتن واکنش احساسی نسبت به محتوای دلخراش یا شدید اغلب کاملاً طبیعی است و نشانه ضعف نیست، بلکه می‌تواند نشان‌دهندهٔ عملکرد سالم – و حتی قدرت – باشد.

125. دوم، برای به حداقل رساندن مواجهه با محتوای مضر باید از راهکارهایی استفاده شود. راهبردهای رایج در این زمینه شامل این موارد است: خاموش کردن صدا هنگام مشاهده محتوای بالقوه دلخراش برای اولین بار یا زمانی که صدا برای تجزیه و تحلیل فوری ضروری نیست (زیرا بسیاری از محتواهای احساسی در صدا گنجانده شده است)، کوچک کردن اندازه صفحه‌نمایش تا حد امکان، پوشاندن محتوای فجیع هنگام بررسی زمینه یک عمل خاص و نه خود عمل، علامت‌گذاری محتوای دلخراش در مجموعه داده‌ها به‌گونه‌ای که افراد قبل از مشاهده بدانند چه چیزی را خواهند دید، هشدار دادن به یکدیگر هنگام به اشتراک گذاشتن محتوای فجیع برای کاهش غافلگیری، کار کردن به صورت زوجی، اجتناب از کار در انزوا یا دیرهنگام در شب و استراحت کردن به طور منظم و در هنگام نیاز.

126. سوم، افراد و سازمان‌ها باید حس همبستگی اجتماعی را در میان اعضای تیم تقویت کنند، چرا که این حس می‌تواند اثر محافظتی داشته باشد – و به نوعی همان حس رفاقتی را بازتولید کند که هنگام انجام تحقیقات میدانی ایجاد می‌شود. این هدف می‌تواند از طریق جلسات منظم گزارش‌دهی محقق شود، که می‌تواند میزان انزوا را کاهش دهد و به محققان کمک کند تا تأثیرات مثبت کار خود را بهتر درک کنند. همچنین برگزاری گردهمایی‌های تیمی، از جمله جشن گرفتن دستاوردهای مهم تحقیقاتی؛ و آموزش تیم در مورد راهکارهای تقویت تاب‌آوری از دیگر راههای تحقق این هدف است. تلاش‌ها برای افزایش تاب‌آوری می‌تواند به‌ویژه زمانی تأثیرگذار باشد که در سطوح فردی، فرهنگی و ساختاری مورد توجه قرار گیرد: برای مثال، با توانمندسازی افراد به طوری که هنگام کار روی یک تحقیق، نسبت به نیازهای روانی خود عمیقاً فکر کنند و نیز ایجاد محیطی که در آن جنبه‌های روانی کار جدی گرفته شود، شیوه‌های حمایتی هم به‌صورت آشکار و هم ضمنی تشویق شوند و شمول و تنوع مورد پذیرش قرار گیرند.

ث) سیاست ها و ابزارهای مدیریت داده

127. سیاست‌هایی در مورد نحوه مدیریت، نگهداری و از بین بردن داده‌ها باید در طول یک تحقیق تدوین، اجرا و رعایت شوند. سازمان‌ها باید سیاست‌هایی برای حفظ اطلاعات (سیاست‌های نگهداری) و حذف اطلاعات (سیاست‌های حذف) در مواقع مناسب، همچنین سیاست‌هایی در مورد دسترسی به اطلاعات (به‌صورت داخلی) و به اشتراک‌گذاری اطلاعات (به‌صورت خارجی) تدوین کنند. علاوه بر این، تدوین سیاست‌های خاص در مورد ایجاد و استفاده از هویت‌های مجازی، دسترسی به نرم‌افزارهای تأییدشده و ابزارهای مورد استفاده نیز می‌تواند مفید باشد.

1- سیاست‌های مدیریت داده

(الف) سیاست‌های نگهداری داده‌ها

128. سیاست‌های نگهداری داده‌ها برای رعایت بسیاری از قوانین حفاظت از داده و مقررات مربوط به نگهداری داده‌ها بسیار مهم هستند. در برخی موارد، حداقل مدت زمانی که داده‌ها باید نگهداری شوند تعیین شده است، در حالی که در شرایط دیگر، حداکثر مدت زمان نگهداری داده‌ها محدود شده است. این سیاست‌ها باید با رعایت الزامات قانونی و بایگانی داده‌های تجاری، روش‌هایی را برای ذخیره داده‌های ماندگار و مدیریت سوابق مشخص کنند. سیاست‌های مختلف نگهداری داده‌ها، ملاحظات قانونی و حریم خصوصی را در برابر ملاحظات اقتصادی و نیاز به دسترسی متعادل می‌کنند تا زمان‌های نگهداری، قوانین بایگانی، فرمت‌های داده و روش‌های مجاز برای ذخیره‌سازی، دسترسی و رمزگذاری را تعیین کنند.[136] درک قوانین مربوطه برای تدوین چنین سیاست‌هایی ضروری خواهد بود.

(ب) سیاست‌های حذف داده‌ها

129. حذف بخش‌هایی از یک مجموعه داده بدون وجود سیاست‌های روشن در مورد حذف و نگهداری داده‌ها و بدون ثبت سوابقی از اینکه چه چیزی حذف شده، توسط چه کسی، در چه زمانی و با چه هدفی، می‌تواند مشکلات قابل توجهی ایجاد کند، به‌ویژه زمانی که اطلاعات ممکن است در دادگاه مورد استفاده قرار گیرد. محققان باید از مقررات مربوط به حذف داده‌های دیجیتال تبعیت کنند و آگاه باشند که استفاده از یک روش به‌جای روش دیگر ممکن است مسائل قانونی به همراه داشته باشد.

(پ) سیاست‌های دسترسی به داده‌ها

130. سازمان‌هایی که به جمع‌آوری و پردازش داده‌ها، به‌ویژه داده‌های حساس می‌پردازند، باید سیاست مشخصی در مورد اینکه چه کسی می‌تواند به انواع مختلف داده‌ها دسترسی پیدا کند، داشته باشند. هرگونه تنظیمات در پایگاه‌های داده یا سیستم‌ها باید به‌گونه‌ای تنظیم شود که این سیاست را منعکس نماید.

---

[136] ایوان نگ [Yvonne Ng]، «چگونه اطلاعات منبع‌باز را به‌طور مؤثر حفظ کنیم» ["How to preserve open source information effectively"]، در کتاب شاهد دیجیتال: استفاده از اطلاعات منبع‌باز برای تحقیقات، مستندسازی و پاسخگویی حقوق بشری [Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability]، به ویراستاری سم دوبِرلی، آلکسا کینیگ و دارا موری [Sam Dubberley, Alexa Koenig and Daragh Murray] (آکسفورد، انتشارات دانشگاه آکسفورد، ۲۰۲۰)، صص ۱۴۳–۱۶۴.

(ت) سیاست‌های به‌اشتراک‌گذاری داده‌ها

131. سازمان‌ها ممکن است بخواهند سیاستی برای به‌اشتراک‌گذاری داده‌ها با عوامل خارجی تدوین کنند. در صورت همکاری با شرکای خارجی، لازم است تفاهم‌نامه‌های همکاری یا قراردادهایی تنظیم شوند تا اطمینان حاصل شود که شرکا از این سیاست‌ها تبعیت می‌کنند.

2- مدیریت اطلاعات

132. پیش از آغاز تحقیقات منبع‌باز، به‌ویژه در زمینه جمع‌آوری و نگهداری مواد دیجیتال، محققان، تیم‌ها و سازمان‌ها باید یک سیستم مدیریت اطلاعات ایجاد کنند. برای چنین سیستمی گزینه‌های متنوعی وجود دارد و این پروتکل از یک گزینه خاص حمایت نمی‌کند. در عوض، موارد زیر به عنوان قابلیت‌های اصلی ارائه می‌شوند که می‌توانند برای فرآیند تحقیق مفید باشند و در برخی زمینه‌ها ممکن است الزامی باشند. علاوه بر این، همان‌طور که در فصل چهارم شرح داده شد، زیرساخت‌ها و پروتکل‌های امنیتی باید از قبل آماده باشند.

(الف) سامانه مدیریت تحقیقات

133. سامانه مدیریت تحقیقات سیستمی است برای مستندسازی فعالیت‌هایی که به عنوان بخشی از یک تحقیق انجام می‌شوند. همه سازمان‌هایی که تحقیقات انجام می‌دهند از چنین سامانه‌هایی برخوردار نیستند، اما استفاده از آنها، به‌ویژه برای سازمان‌ها یا تیم‌های تحقیقاتی بزرگ‌تر به‌شدت توصیه می‌شود. چنین سامانه‌هایی می‌توانند برای تخصیص وظایف و گزارش‌دهی درباره فعالیت‌ها مورد استفاده قرار گیرند، به‌گونه‌ای که فرآیند تحقیق ساختارمند و تا حد ممکن کارآمد باشد، زیرا این کار می‌تواند به کاهش تکرار فعالیت‌ها کمک کند.

(ب) سامانه‌های مدیریت اطلاعات و شواهد

134. سامانه‌های مدیریت اطلاعات برای ذخیره داده‌هایی که به عنوان بخشی از تحقیقات جمع‌آوری شده‌اند، استفاده می‌شوند. سامانه مدیریت اطلاعات باید قادر به انجام دو وظیفه مجزا باشد: (الف) پیگیری فرآیند جمع‌آوری و مدیریت مواد، و (ب) تفکیک موادی که ممکن است به عنوان شواهد مورد استفاده قرار گیرند.

3- زیرساخت – ملاحظات تدارکاتی و امنیتی

135. چه در حال طراحی زیرساخت برای سازمانی که در تحقیقات منبع‌باز فعالیت می‌کند باشید و چه به عنوان یک محقق مستقل در حال انتخاب ابزارهای مورد استفاده باشید ، ملاحظات تدارکاتی و امنیتی مهمی وجود دارد که باید در نظر گرفته شوند. به طور کلی، برای توسعه سامانه‌ها سه رویکرد وجود دارند: (الف) ساخت سفارشی سامانه‌ها و ابزارها؛ (ب) استفاده از ابزارها و نرم‌افزارهای منبع‌باز یا رایگان که در اینترنت مجود هستند؛ یا (پ) خرید محصولات تجاری از شرکت‌های ثالث. هر یک از این رویکردها مزایا و معایب خاص خود را دارند و موفقیت آنها به شرایط و زمینه‌ای که محققان در آن فعالیت می‌کنند بستگی دارد. در اینجا نیز، این پروتکل از هیچ رویکردی نسبت به دیگری حمایت

نمی‌کند، بلکه مزایا و معایب هر یک را ارائه می‌دهد و همچنین عوامل خاصی را که باید هنگام تصمیم‌گیری درباره استفاده از محصولات در نظر گرفته شوند، مورد بررسی قرار می‌دهد.

(الف) محصولات تجاری

136. مزیت محصولات تجاری این است که یک شرکت خصوصی ممکن است زیرساخت بهتری برای امنیت داشته باشد و بتواند پشتیبانی فنی مداوم و قابل اعتمادی ارائه دهد. با این حال، محصولات تجاری دارای معایب آشکاری از جمله هزینه هستند. علاوه بر این، تعامل با طرف‌های ثالث و وابستگی به آنها می‌تواند برای سازمان‌هایی که سعی در حفظ محرمانگی تحقیقات خود دارند یک مشکل باشد. بسیاری از محصولات تجاری دارای کد منبع بسته هستند تا از مالکیت فکری خود محافظت کنند. این محصولات ممکن است نگرانی‌هایی در مورد مالکیت داده‌ها، قابلیت انتقال و بُرون بُردِ داده‌ها، و سازگاری با سایر سامانه‌ها ایجاد کنند. علاوه بر این، شرکت‌ها ممکن است در برابر فشارهای دولتی برای دسترسی به اطلاعات خصوصی واکنش نشان دهند. یکی از نگرانی‌های اصلی این است که، اگرچه شرکت‌ها تیم‌های امنیتی برای حفاظت از محصولات و کاربران خود دارند، کاربران باید به این اعتماد کنند که شرکت‌ها سامانه‌های خود را به‌درستی طراحی کرده‌اند و به‌درستی نگهداری خواهند کرد و اینکه در مراحل بعدی هزینه‌های پنهانی وجود نخواهد داشت.

(ب) ابزارهای سفارشی ساخته شده یا انطباق داده شده

137. مزیت ساخت یک ابزار از ابتدا یا انطباق دادن ابزاری که از قبل وجود دارد این است که محققان یا سازمان‌ها کنترل کامل بر کل سامانه و داده‌های خود را حفظ می‌کنند و در نتیجه می‌توانند از تعامل با طرف‌های ثالث اجتناب کنند. سامانه‌های سفارشی‌ساخته شده همچنین می‌توانند با سایر سامانه‌های اختصاصی نیزآسان‌تر ادغام شوند. عیب این رویکرد زمان، هزینه و تخصص مورد نیاز برای ساخت و پشتیبانی چنین سامانه‌هایی است،که برای اکثر سازمان‌ها چالشی بزرگ محسوب می‌شود. علاوه بر این، یک سامانهٔ بسته، با تعداد محدود کاربران و آزمایش‌کنندگان نسخهٔ بتا، ممکن است شناسایی نقاط ضعف یا دریافت بازخورد کافی برای بهینه‌سازی عملکرد را دشوار کند.

(پ) ابزارهای منبع‌باز و رایگان

138. ابزارهای منبع‌باز ابزارهایی هستند که سازندگان آنها کدهای منبع را به‌صورت عمومی منتشر کرده‌اند تا هر کسی بتواند آزادانه از آنها استفاده یا آنها را تغییر دهد. برخی از محصولات تجاری با کدهای منبع‌باز وجود دارند و برخی ابزارهای رایگان نیز با کدهای منبع بسته در دسترس هستند، اما این موارد استثنا هستند. ابزارهای منبع‌باز معمولاً رایگان هستند. برای سازمان‌های کوچک با بودجه محدود و همچنین سازمان‌های بزرگ‌تر که فرآیندهای خرید محصولات پولی در آنها پیچیده و زمان‌بر است، ابزارهای رایگان می‌توانند گزینه‌ای مهم برای در نظر گرفتن باشند. با این حال، ابزارهایی که برای کاربران رایگان هستند ممکن است از روش‌های دیگری مانند فروش داده‌ها و تحلیل‌های کاربران کسب درآمد کنند، که این مسئله می‌تواند مشکلاتی در زمینه امنیت و حریم خصوصی ایجاد کند. علاوه بر این، استفاده از این ابزارها نیازمند تحقیقات قبلی است تا مشخص شود چه کسی آنها را ایجاد کرده است، آیا به‌طور مستقل مورد ارزیابی قرار گرفته‌اند و آیا ماندگار هستند یا خیر. هر سه این جنبه‌ها می‌توانند اعتبار یک تحقیق را تضعیف کنند. به‌ویژه در زمینه‌های قانونی، اگر پرونده‌ای به دادگاه برود و ابزار مورد استفاده توسط

طرف مقابل به چالش کشیده شود، این ابزارها می‌توانند مشکل‌ساز شوند. به علاوه، اگر این سامانه‌ها و ابزارهای نرم‌افزاری منسوخ شوند یا سازندگان آنها در دسترس نباشند، باید برای مقابله با آن، یک برنامه پشتیبان و یک سیستم مهاجرت داده و سیستم پشتیبان داشته باشند. در حالی که ابزارهای منبع‌باز ممکن است به دلیل استفاده سایر گروه‌های مشابه، برای سازمان‌ها جذاب باشند، محققان باید ارزیابی‌های کامل و مستقلی از نحوه عملکرد این ابزارها و پیامدهای استفاده از آنها در یک زمینه خاص انجام دهند.

139. هنگام تصمیم‌گیری درباره اینکه آیا یک ابزار را به صورت اختصاصی بسازند، از نرم‌افزارهای رایگان یا منبع‌باز استفاده کنند یا محصولی را خریداری کنند، محققان باید راهنمایی‌های مربوط به دقت لازم که در ضمیمه 5 در ادامه آمده را دنبال کنند.

6- فرآیند تحقیق

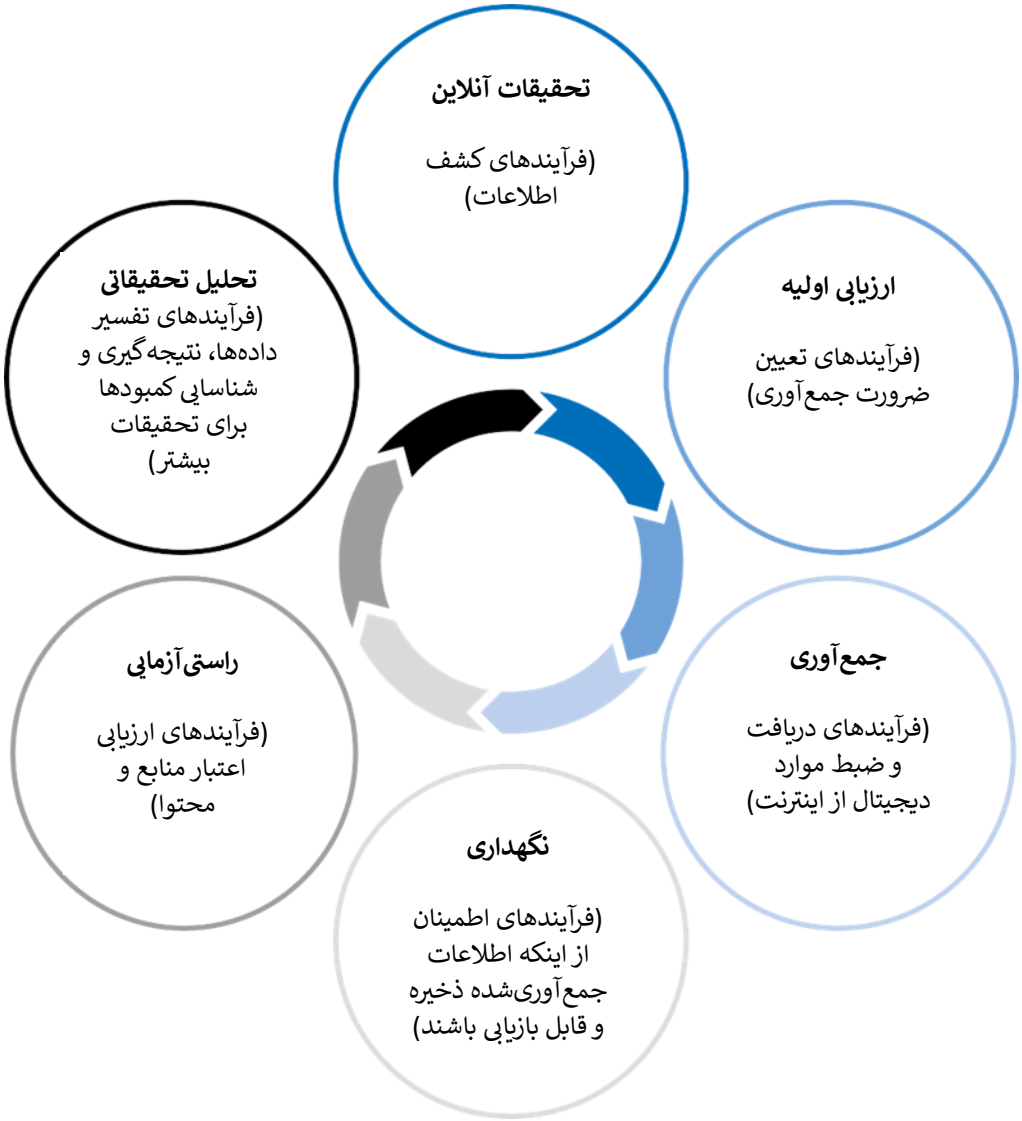
خلاصهٔ این فصل

- شش مرحله اصلی در فرآیند تحقیق وجود دارد که عبارت‌اند از: (الف) تحقیق آنلاین؛ (ب) ارزیابی اولیه؛ (پ) جمع‌آوری؛ (ت) نگهداری؛ (ث) تأیید؛ و (ج) تحلیل تحقیقاتی. این مراحل به‌صورت جمعی بخشی از یک چرخه هستند که ممکن است در طول یک تحقیق بارها تکرار شوند، زیرا اطلاعات تازه کشف‌شده به خطوط تحقیق جدید منجر می‌شوند.

- محققان باید فعالیت‌های خود را در هر مرحله مستندسازی کنند. این کار به قابلیت درک و شفافیت تحقیقات آنها، از جمله زنجیره‌های نگهداری، و همچنین به کارایی و اثربخشی تحقیقات آنها، از جمله تکمیل فرآیندها و ارتباط میان اعضای تیم، کمک می‌کند.

140. تحقیقات منبع‌باز نیازمند مشاهده دقیق و بررسی‌های سیستماتیک هستند تا در یک محیط دیجیتال پیچیده و پویا، حقایق را مشخص کنند. محققان منبع‌باز باید با دیدی انتقادی به ارزیابی محتوای آنلاین بپردازند و توانایی بررسی روش‌هایی را داشته باشند که ممکن است مطالب دیجیتال به آن روش‌ها تحریف یا دستکاری شوند. آنها همچنین باید از یک رویکرد ساختاریافته برای جستجو در اینترنت استفاده کنند و جانبداری الگوریتمی و نابرابری در دسترسی به اطلاعات منبع‌باز که به گروه‌های خاص و ماهیت پویای اطلاعات آنلاین مربوط می‌شود را مدنظر قرار دهند. هر ادعایی در بارهٔ یک واقعیت باید به‌طور دقیق مورد بررسی قرار گیرد. این فصل یک رویکرد ساختاریافته برای تحقیقات منبع‌باز ارائه می‌دهد. نمودار زیر چرخه تحقیقات منبع‌باز را نشان می‌دهد. لازم به ذکر است که تحقیقات منبع‌باز به‌ندرت به‌صورت خطی انجام می‌شوند و اغلب به دلیل ماهیت چرخه‌ای ایجاد پرونده، نیاز به تکرار این فرآیند دارند. همچنین ممکن است دلایل موجهی برای انحراف از این ترتیب وجود داشته باشد.

چرخه تحقیقات منبع‌باز



الف) پرس و جوی آنلاین

141. دو فرآیند اصلی برای بررسی‌های آنلاین وجود دارد: الف) جستجو، یعنی کشف اطلاعات و منابع اطلاعاتی از طریق استفاده از روش‌های جستجوی عمومی یا پیشرفته؛ و ب) پایش [رصد]، یعنی یافتن اطلاعات جدید از طریق بررسی مداوم و پیوسته مجموعه‌ای از منابع ثابت.

1- جستجو

142. جستجوی آنلاین یک فعالیت مبتنی بر مأموریت است که با هدف کشف اطلاعات جدید مرتبط با یک هدف مشخص یا یک پرسش تحقیقاتی انجام می‌شود. جستجوها باید ساختاریافته و سیستماتیک باشند، به این معنا که با یک پرسش تحقیقاتی روشن و پارامترهای جستجو، همراه با کلمات کلیدی و عملگرها[137]آغاز شوند. نتایج جستجو در موتورهای جستجو، ابزارهای جستجو، عبارات جستجو و عملگرهای مختلف، متفاوت خواهد بود؛ بنابراین، محققان باید با خلاقیت و پشتکار مسیرها و کانال‌های مختلف را برای یافتن اطلاعات مرتبط دنبال کنند. علاوه بر موتورهای جستجویی که برای یافتن اطلاعات در وب‌سایت‌های ایندکس‌شده استفاده می‌شوند، جستجوی ساختاریافته می‌تواند در پلتفرم‌های رسانه‌های اجتماعی و پایگاه‌های داده نیز به کار گرفته شود. با توجه به نیاز به اتخاذ رویکردی متنوع، چندجانبه و مرتبط با هر مورد خاص، محققان باید فرآیندهای خود را با دقت مستند کنند تا بتوانند آنها را در بخش روش‌شناسی گزارش‌ها توضیح دهند یا در جریان دادرسی‌های قانونی به آنها استناد کنند. این فرآیند ممکن است به‌صورت بازنگری به گذشته انجام شود و لزوماً به‌طور هم‌زمان با خود تحقیق پیش نرود. با این حال، مستندسازی باید تا حد امکان به‌صورت هم‌زمان انجام شود. مستندسازی جستجوهای ساختاریافته باید شامل اطلاعات زیر باشد:

(الف) هدف و پرسش‌های تحقیق: پرسش‌هایی را که جستجوی آنلاین به دنبال پاسخ دادن به آنهاست، به‌طور دقیق بیان کنید و اصل بی‌طرفی که پیش‌تر ذکر شد را در نظر داشته باشید.

(ب) حقایق، فرضیات و مجهولات: از نقطه‌ای شروع کنید که حقایق مشخص شده‌اند، البته در صورتی که چنین حقایقی اثبات شده باشند. همچنین، ممکن است مفید باشد که بر اساس اطلاعات اولیه یا فرضیات منطقی کار کنید، حتی اگر هنوز این اطلاعات تأیید نشده باشند. با این حال، ضروری است که هرگونه فرضیه به‌عنوان فرضیه ثبت شود. در نهایت، مفید خواهد بود که در ابتدای تحقیق، نقص‌های موجود در آنچه می‌دانیم یا سایر «مجهولات» مشخص شوند. تفکیک و دسته بندی اطلاعات به جلوگیری از نتایج جانبدارانه یا تحریف‌شده کمک می‌کند، زیرا اصطلاحات جستجو و مبانی آنها را شفاف می‌سازد.

(پ) اصطلاحات و کلمات کلیدی جستجو: برای انجام یک جستجوی هدفمند، محققان باید فهرستی از کلمات کلیدی تهیه کنند که با اصل بی‌طرفی و بر اساس نظریه یا نظریه‌های مختلف مرتبط با پرونده مطابقت داشته باشد. ایده‌آل این است که محققان از کلمات کلیدی در تمام زبان‌ها و متون مربوطه

[137] عملگرهای بولی کلمات ساده‌ای مانند «و» (and)، «یا» (or) و «نه» (not) هستند که می‌توانند برای «ترکیب یا حذف کلمات کلیدی در یک جستجو به کار روند که نتایجی دقیق‌تر و مؤثرتر به وجود می‌آورند». نگاه کنید به کتابخانه دانشگاه بین‌المللی الیانت، «عملگر بولی چیست؟» [“What is a Boolean operator?”] قابل دسترسی در: https://library.alliant.edu/screens/boolean.pdf.

استفاده کنند و نسبت به احتمال نتایج جستجوی بیش از حد گسترده یا بسیار محدود محتاط باشند. با وجود تفاوت‌های موجود بین پرونده‌ها، موضوعات کلی مشخصی وجود دارند که باید در فهرست کلمات کلیدی گنجانده شوند، مانند مکان‌های مهم، نام‌ها، سازمان‌ها، تاریخ‌ها و هشتگ‌های مرتبط. همچنین ممکن است مفید باشد که اطلاعاتی را که در زمینه یک تحقیق خاص می‌تواند به‌عنوان شواهد مجرمانه یا تبرئه‌کننده تلقی شود، شناسایی کنید.

(ت) جستجوها و موتورهای جستجو: محققان باید جستجوهای خود را پیگیری کرده و مسیرهای منتهی به مطالب مربوط را ثبت کنند، از جمله اصطلاحات، عملگرها و موتورهای جستجویی که به آن محتوا منتهی شده‌اند. لزومی ندارد محققان تمام نتایج جستجو را ثبت کنند، زیرا این کار می‌تواند بیش از حد دشوار و از نظر ارزش اثباتی کم‌اهمیت باشد.

2- پایش

143. پایش شامل دنبال کردن یک منبع اطلاعاتی مشخص، برای مثال یک موضوع خاص، در طول زمان است. هدف این است که محتوای متغیری که توسط یک منبع ثابت تولید می‌شود را ردیابی کنیم. پایش آنلاین باید یک فعالیت ساختاریافته باشد که از فهرست منابع آنلاین شناخته‌شده و قبلاً ارزیابی‌شده، مانند وب‌سایت‌ها یا حساب‌های رسانه‌های اجتماعی، و همچنین جستجوهایی که به‌صورت مستمر بر روی اهداف تعریف‌شده انجام می‌شود، استفاده کند. برای مثال به منابع زیر نگاه کنید:

(الف) وب‌سایت‌ها و حساب‌های رسانه‌های اجتماعی: محققان باید فهرست‌های فعالی از وب‌سایت‌ها و پروفایل‌ها (حساب‌های کاربری‌ای) که باید پایش شوند را حفظ کنند. این فهرست‌ها باید شامل توجیهی برای دلیل پایش، شخص مسئول پایش، فردی که پایش را انجام می‌دهد، و همچنین دفعات پایش باشند.

(ب) هشتگ‌ها و کلمات کلیدی: محققان همچنین باید فهرستی کاری از هشتگ‌ها و کلمات کلیدی که پایش می‌شوند را حفظ کرده و به‌طور منظم به‌روزرسانی کنند.

(پ) خودکاری: پایش ممکن است شامل استفاده از ابزارهای خودکار باشد که، برای مثال، به‌صورت دوره‌ای جستجویی را در سایت‌های مشخص یا با استفاده از پارامترهای خاص انجام می‌دهند. استفاده از این ابزارها، از جمله نام و نسخه آنها و اطلاعات واردشده در آنها، باید همیشه مستند شود.

3- سوگیری

144. هنگام انجام جستجوی ساختاریافته و فعالیت‌های پایش، محققان منابع باز باید همواره نسبت به سوگیری هوشیار باشند – هم سوگیری شناختی خود و هم سوگیری ذاتی موجود در اطلاعات آنلاین. برای مثال، اگر یک محقق در حال جستجوی اطلاعات درباره تجاوز جنسی باشد، بیشتر داده‌ها یا موضوعات مطرح‌شده به احتمال زیاد مربوط به تجاوز جنسی علیه زنان در سنین باروری و در خارج از روابط زناشویی خواهد بود. نتایج جستجو ممکن است انواعِ کمتر دیده‌شده یا گزارش‌شدهٔ تجاوز جنسی را کمتر منعکس کنند. خشونت جنسی علیه مردان و پسران، افراد همجنس‌گرای مؤنث و مذکر، دوجنس‌گرا، تراجنسیتی، دوجنسه ، زنان مسن‌تر و موارد تجاوز جنسی در چارچوب زناشویی از این قبیل هستند.

145. مثال دیگر، تحقیقات درباره خشونتی است که به تحریک سخنان نفرت‌پراکنانهٔ آنلاین انجام شده است، زیرا این‌گونه سخنان اغلب شامل زبان و نمادهای رمزگذاری‌شده‌ای هستند که به‌راحتی توسط محققان یا ماشین‌ها قابل شناسایی نیستند. به‌ویژه زمانی که محققان متعلق به جوامع هدف قرار گرفته نباشند، ممکن است از استفاده فرهنگی و به کار گرفتن اصطلاحات و نمادهای مربوط به یک زمینهٔ بخصوص که برای تحریک نفرت یا خشونت به کار می‌روند، بی‌اطلاع باشند. این موضوع زمانی پیچیده‌تر می‌شود که سخنان نفرت‌انگیز آنلاین اغلب به‌طور عمدی طراحی می‌شوند تا توسط ماشین‌ها یا ناظران انسانی شناسایی نشوند و از حذف شدن از پلتفرم‌های آنلاین در امان بمانند، در حالی که هدف اصلی آنها تحریک خشونت یا تبعیض علیه جمعیتی است که هدف قرار گرفته است. برای کمک به غلبه بر دشواری در شناسایی کردنِ تحریک به تبعیض، خصومت یا خشونت، محققان باید از یک آزمون مبتنی بر حقوق بشر استفاده کنند، مانند آنچه در برنامه عمل رباط برای منع طرفداری از نفرت ملی، نژادی یا مذهبی که تحریک تبعیض، خصومت یا خشونت محسوب می‌شود، ارائه شده است[138].

146. در نهایت، بهترین راه برای محققان جهت مقابله با «سوگیری در ماشین» همراه با سوگیری‌های خودشان، آگاهی از امکان وجود چنین سوگیری‌هایی، شناسایی خطرات و در صورت امکان اتخاذ اقدامات فعال برای متعادل کردن سوگیری‌ها است. این اقدامات شامل تحقیق درباره اصطلاحات و نمادهای مربوط به یک زمینه خاص یا مجموعه‌ای از جرائم یا حوادث و گسترش و تنوع‌بخشی به بررسی‌های آنلاین می‌باشد. در مواردی که شامل خشونت جنسی و جنسیتی می‌شود، همچنین سایر جرائمی که در آنها بازماندگان مورد بدنامی قرار می‌گیرند و از زبان رمزگذاری‌شده استفاده می‌شود، محققان باید با کارشناسانی مشورت کنند که ممکن است بتوانند زبان رمزگذاری‌شده و شیوه‌های ارتباطی را که این بازماندگان و مرتکبان اغلب در فضاهای آنلاین استفاده می‌کنند، شناسایی و به اشتراک بگذارند.[139]

ب) ارزیابی اولیه

147. پیش از جمع‌آوری محتوا از اینترنت، محققان منابع باز باید در مورد هرگونه محتوایی که شناسایی می‌کنند ارزیابی اولیه‌ای انجام دهند تا از جمع‌آوری بیش از حد جلوگیری کرده و با اصول کاهش داده‌ها و تحقیق متمرکز مطابقت داشته باشند و همچنین اطمینان حاصل کنند که جمع‌آوری این محتوا حقوق حریم خصوصی افراد را نقض نمی‌کند. محققان منابع باز باید عوامل زیر را برای تعیین اینکه آیا یک مورد دیجیتال باید از اینترنت جمع‌آوری شود یا نه، در نظر بگیرند.

1- ربط داشتن

[138] نگاه کنید به کمیساریای عالی حقوق بشر سازمان ملل متحد (OHCHR)، «آزادی بیان در مقابل نفرت‌پراکنی: کمیساریای عالی حقوق بشر و برنامه اقدام رباط» [“Freedom of expression vs incitement to hatred: OHCHR and the Rabat Plan of Action”]، قابل دسترسی در: www.ohchr.org/EN/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx.

[139] برای مثال نگاه کنید به: کینیگ و اِگن «پنهان در برابر دیدگان: استفاده از اطلاعات منبع باز آنلاین برای تحقیق درباره خشونت جنسی و جرایم مبتنی بر جنسیت» [Koenig and Egan, “Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes”].

148. تحقیقات منابع باز باید تعیین کنند که آیا یک مورد دیجیتال در وهلهٔ اول به یک تحقیق خاص مربوط است یا خیر. ارتباط هر مورد به محتوای آن، منبع آن، اهداف تحقیق و اطلاعات موجود درباره یک وضعیت بستگی دارد. در مراحل اولیه یک تحقیق، ممکن است تشخیص اینکه چه چیزی مربوط است دشوار باشد، که این امر می‌تواند منجر به جمع‌آوری بیش از حد توسط محققان شود. با این حال، محققان منابع باز باید بتوانند توضیح دهند که چرا معتقدند یک مورد بالقوه مرتبط است، و این ارزیابی باید ثبت شود (برای مثال، از طریق یک سیستم برچسب‌گذاری یا ذخیره‌سازی ساده و کاربرپسند که اطلاعات جمع‌آوری‌شده را به‌عنوان نمونه به یک مکان، تاریخ، حادثه، فرد یا نوع تخلف مورد تحقیق مربوط می‌کند).

2- قابلیت اطمینان

149. محققان منابع باز باید تعیین کنند که آیا اطلاعات یا ادعاهای موجود در محتوای دیجیتال در ظاهرِ امر، قابل اطمینان هستند یا خیر، و این امر با بررسی و ارزیابی محتوا و اطلاعات زمینه‌ای موجود در فایل انجام می‌شود. این می‌تواند شامل بررسی فرا داده‌های نهفته، اطلاعات مرتبط و منبع باشد.[140] این فرآیند باید شامل تلاش برای شناسایی منبع اصلی محتوا باشد، که ممکن است مستلزم ردیابی منشأ آنلاین داده‌ها، آپلودکننده (بارگذاری کنند) یا نویسنده آن باشد.

3- حذف

150. محققان منابع باز باید ارزیابی کنند که آیا احتمال دارد یک مورد دیجیتال از اینترنت یا دسترسی عمومی حذف شود یا خیر. زمانی که احتمال حذف محتوا وجود دارد، باید قابل‌اعتمادترین نسخه شناخته‌شده محتوا جمع‌آوری شود، حتی در حالی که تأیید و بررسی‌های بیشتر در مورد نسخه‌های قبلی یا بهتر انجام می‌شود. احتمال حذف محتوا را می‌توان بر اساس عوامل مختلفی ارزیابی کرد، از جمله هویت فرضی منبع، محل قرارگیری محتوا و سازگاری محتوا با شرایط خدمات ارائه‌دهنده سرویس. برای مثال، محتوای دلخراش یا توهین‌آمیز، که می‌تواند ارزش اثباتی بالایی برای اثبات جرائم یا تخلفات داشته باشد، از جمله محتویاتی است که بیشترین احتمال حذف را دارد.

4- ایمنی

151. محققان منابع باز باید تعیین کنند که آیا جمع‌آوری یک مورد دیجیتال ایمن است یا اینکه اقدامات احتیاطی بیشتری لازم و قابل انجام است. نگرانی‌ها به احتمال زیاد زمانی ایجاد می‌شوند که جمع‌آوری از وب‌سایتی انجام شود که ممکن است حاوی موارد خراب باشد که می‌تواند به سیستم داخلی آسیب برساند.

5- وظایف بعدی

[140] نگاه کنید به فصل ۶ (ث) در زیر درباره راستی‌آزمایی.

152. محققان منابع باز باید تعیین کنند که در صورت نگهداری یک مورد دیجیتال، چه وظایفی ممکن است بر عهده آنها قرار گیرد، به عنوان مثال، وظیفه حفظ آن مورد به‌صورت ایمن برای رعایت قوانین حفاظت از داده‌ها[141].

پ) جمع‌آوری

153. جمع‌آوری عبارت است از به‌دست آوردن اطلاعات آنلاین از طریق گرفتن اسکرین‌شات، تبدیل کردن به فایل پی.دی.اف (PDF) ، دانلود جرم‌شناسانه (forensic) یا سایر روش‌های ضبط اطلاعات. پس از شناسایی محتوای دیجیتال و تأیید مرتبط بودن آن با تحقیق و همچنین اینکه در ظاهر مربوط بوده و برای هدف موردنظر قابل اطمینان باشد، محقق باید روش مناسب جمع‌آوری آن را تعیین کند.
روش‌های جمع آوری اطلاعات بسته به اهداف زیر ممکن است متفاوت باشد؛ اگر محتوای آنلاین قرار باشد برای مقاصد تصمیم‌گیری مورد استفاده یا استناد قرار گیرد، آیا دارای ارزش احتمالی اثباتی در فرآیندهای قضایی خواهد بود، یا اینکه صرفاً به محصولات کاری داخلی کمک می‌کند. در مواردی که صرفاً شامل محصولات کاری است، گرفتن اسکرین‌شات یا تبدیل به فایل پی.دی.اف ممکن است کافی باشد، در حالی که محتوایی که دارای ارزش احتمالی اثباتی است ممکن است به یک روش ثبت کامل‌تر و مطمئن‌تر نیاز داشته باشد (برای مثال از طریق اختصاص یک کد هش – به توضیحات زیر مراجعه کنید).

154. جمع‌آوری محتوای آنلاین می‌تواند به‌صورت دستی، با پیروی از یک دستورالعمل عملیاتی استاندارد، یا به‌صورت خودکار با استفاده از ابزارها یا اسکریپت‌های مختلف انجام شود. صرف‌نظر از مراحل انجام آن، اطلاعات ذکرشده در زیر باید ترجیحاً در زمان جمع‌آوری ثبت شوند. این اطلاعات ممکن است برای اثبات اصالت یک مورد دیجیتال مفید باشد. این امر ممکن است به‌ویژه در موارد دادرسی‌های قانونی که یک مورد به‌عنوان مدرک ارائه می‌شود، اهمیت داشته باشد، به‌خصوص اگر نویسنده یا خالق آن شناسایی نشده، در دسترس نباشد یا نتواند شهادت دهد. محققان منابع باز باید محتوای آنلاین را در قالب اصلی آن یا در حالتی که تا حد امکان به قالب اصلی نزدیک باشد، جمع‌آوری کنند. هرگونه تغییر، تبدیل یا دگرگونی که در نتیجه فرآیند جمع‌آوری ایجاد شود، باید مستند شود.

155. موارد زیر درباره اینکه چه چیزی را جمع‌آوری کنید و چگونه آن را جمع‌آوری کنید، راهنمایی‌هایی را ارائه می‌دهد. ابزارهای مختلفی برای ثبت اطلاعات زیر وجود دارد یا این کار می‌تواند به‌صورت دستی نیز انجام شود. در حالی که جمع‌آوری تمام اطلاعات زیر به‌عنوان یک رویه مطلوب در نظر گرفته می‌شود، سه مورد اول (نشانی وب(URL) ، اچ.تی.ام.ال یا کد منبع فرامتن (HTML) و ثبت کامل صفحه) به‌عنوان استاندارد حداقلی برای ارائه شواهد در دادگاه محسوب می‌شوند. البته چنین استانداردهایی در زمینه‌های مختلف متفاوت خواهند بود، اما ثبت تمام عناصر ذکرشده در زیر، در همهٔ زمینه‌ها پایه و اساسی قوی فراهم می‌کند:

(الف) نشانی وب هدف: نشانی وب محتوای جمع‌آوری‌شده، که به‌عنوان نشانی وب (URL)یا شناسه (URI)نیز شناخته می‌شود، باید ثبت شود؛

[141] نگاه کنید به فصل ۶ (د) در زیر درباره حفاظت.

(ب) کد منبع: محققان باید کد منبع HTML صفحه وب را در صورت امکان ثبت کنند. کد منبع HTML شامل اطلاعات بیشتری نسبت به بخش قابل‌مشاهده وب‌سایت است. کد منبع HTML به احراز هویت محتوای جمع‌آوری‌شده کمک می‌کند؛

(پ) ثبت کامل صفحه: محققان باید ابتدا یک تصویر از صفحهٔ وب مورد نظر با ذکر تاریخ و زمان ثبت کنند. دلیل این فرآیند، داشتن بهترین نمای ممکن از چیزی است که در زمان جمع‌آوری مشاهده شده است؛

(ت) فایل‌های رسانه‌ای جاسازی‌شده (نهفته): در صورت دانلود یک صفحه وب که برای مثال شامل ویدیوها یا تصاویر است، آن موارد خاص نیز باید از صفحه وب استخراج و جمع‌آوری شوند؛

(ث) فراداده‌های جاسازی‌شده: محققان باید فراداده‌های اضافی مربوط به مطلب دیجیتال مورد نظر را، در صورت موجود بودن و کاربردی بودن، جمع‌آوری کنند. فراداده‌ها بسته به منابع متفاوت هستند، اما فراداده‌های رایج شامل شناسه کاربری آپلودکننده، شناسه پست، تصویر یا ویدیو، تاریخ و زمان آپلود، برچسب جغرافیایی، هشتگ، نظرات و توضیحات هستند؛

(ج) داده‌های زمینه‌ای: محتوای زمینه‌ای نیز باید در صورتی که به درک مطلب دیجیتال مربوط باشد، جمع‌آوری شود. این محتوا می‌تواند شامل نظرات درباره یک ویدیو، تصویر یا پست؛ اطلاعات آپلود؛ و/یا اطلاعات آپلودکننده/کاربر مانند نام کاربری، نام واقعی یا بیوگرافی باشد. اینکه آیا اطلاعات پیرامون آن مورد باید جمع‌آوری شود یا خیر باید بر اساس جزئیات پرونده و مورد دیجیتال تعیین شود؛

(چ) داده‌های جمع‌آوری: محققان منابع باز باید تمام داده‌های مرتبط با جمع‌آوری را ثبت کنند، از جمله نام جمع‌آوری‌کننده، آدرس IP دستگاهی که برای جمع‌آوری اطلاعات استفاده شده است، هویت مجازی در صورت استفاده، و مهر زمانی. محققان باید اطمینان حاصل کنند که ساعت سیستم دقیق است، ترجیحاً با همگام‌سازی آن با یک سرور پروتکل زمان شبکه (NTP). دلیل این مرحله اطمینان از این است که فراداده‌های مربوط به زمان به‌طور دقیق در فایل‌های جمع‌آوری‌شده نمایش داده شوند. در صورتی که از یک هویت مجازی برای دسترسی به اطلاعات جمع‌آوری‌شده استفاده شده باشد، آن نیز باید یادداشت شود؛

(ح) کد هش: کدهای هش یک نوع منحصر به فرد از شناسایی دیجیتال هستند که از طریق استفاده از رمزنگاری تأیید می‌کنند محتوای جمع‌آوری‌شده منحصر به فرد است و از زمان جمع‌آوری تغییری نکرده است. محققان منابع باز باید در زمان جمع‌آوری، به‌صورت دستی کد هش را اضافه کنند یا ابزار جمع‌آوری به‌طور خودکار این کد را اضافه کند. انواع مختلفی از هش وجود دارد که می‌توان از بین آنها انتخاب کرد و استانداردها در طول زمان تکامل یافته‌اند. محققان باید بر اساس استانداردهای پذیرفته‌شده فعلی ارزیابی کنند که از کدام نوع هش استفاده کنند.[142]

156. در موارد جمع‌آوری خودکار، برخی از فرآیندهای توضیح داده‌شده می‌توانند توسط ابزارهایی که برای جمع‌آوری محتوای مرتبط و فراداده طراحی شده‌اند، اجرا شوند. برای هر موردِ جمع‌آوری‌شده باید یک

[142] مؤسسه ملی استانداردها و فناوری ایالات متحده یکی از سازمان‌هایی است که می‌توان برای دریافت راهنمایی در مورد استانداردهای فعلی به آن مراجعه کرد. نگاه کنید به: www.nist.gov.

گزارش فنی تهیه شود که شامل اطلاعات ذکرشده باشد تا اصالت آن مورد در آینده تأیید شود. اطلاعات زمینه‌ای و تمام انواع فراداده باید همان‌طور که در بخش بعدی توضیح داده شده است، همواره همراه با مورد دیجیتال ذخیره و حفظ شوند.

ت) حفظ و نگهداری

157. ماندگاری و در دسترس بودنِ اطلاعات آنلاین اغلب وضعیت نامطمئنی دارد. پلتفرم‌های رسانه‌های اجتماعی ممکن است محتوایی را طبق شرایط استفاده خود حذف کنند، یا کاربران ممکن است محتوای بارگذاری‌شده خود را حذف یا ویرایش کنند. علاوه بر این، اطلاعات آنلاین به‌راحتی می‌توانند از زمینهٔ مربوطه خارج شوند، گم، پاک یا خراب شوند. [143]اگر قرار است مواد دیجیتال برای مقاصد تضمین مسئولیت قانونی در دسترس و قابل استفاده باقی بمانند، باید برای کوتاه‌مدت و دراز مدت حفظ شوند.[144]به‌طور کلی، هدف از حفظ دیجیتال، حفظ دسترسی‌پذیری است.[145] با این حال، هنگامی که مواد دیجیتال به منظور تضمین پاسخگویی در برابر قانون، حفظ و نگهداری می‌شوند، هدف این است که مواد دیجیتال به گونه‌ای مدیریت و نگهداری شوند که دسترسی‌پذیری، اصالت، و قابلیت استفاده از آنها توسط سازوکارهای پاسخگویی، از جمله قابلیت پذیرش آنها در فرآیندهای قانونی، تضمین شود.

158. برای نگهداری در دراز مدت، ممکن است سخت‌افزارهای ذخیره‌سازی و فرمت‌ها نیاز به به‌روزرسانی داشته باشند تا اطمینان حاصل شود که مواد با استفاده از دستگاه‌های معاصر قابل دسترسی باقی می‌مانند.

1- ویژگی‌های یک مورد دیجیتال که باید در طول زمان حفظ و محافظت شوند:

159. طبق نظر بایگانان، ویژگی‌های یک مورد دیجیتال که باید در طول زمان حفظ و محافظت شوند عبارتند از: اصالت، دسترسی‌پذیری، هویت، پایداری، قابلیت نمایش و قابلیت درک، که به‌طور مختصر در زیر توضیح داده شده‌اند.

(الف) اصالت

160. اصالت یعنی توانایی اثبات این موضوع که یک مورد دیجیتال از زمانی که جمع‌آوری شده است بدون تغییر باقی مانده است. این امر مستلزم آن است که یک مورد دیجیتال در آرشیو بدون تغییر بماند یا اینکه اگر هرگونه تغییری در آن ایجاد شده، مستند شود.[146]

---

[143] نگاه کنید به: Ng، «چگونه اطلاعات منبع باز را به‌طور مؤثر حفظ کنیم» [How to preserve open source information effectively].

[144] همان، ص ۱۴۳. نگاه کنید به: سازمان آموزشی، علمی و فرهنگی ملل متحد (یونسکو)، «مفهوم حفاظت دیجیتال» [United Nations Educational, Scientific and Cultural Organization, “Concept of digital preservation”]، قابل دسترسی در: www.unesco.org/new/en/communication-and-information/access-to-knowledge/preservation-of-documentary-heritage/digital-heritage/concept-of-digital-preservation.

[145] نگاه کنید به: Ng، «چگونه اطلاعات منبع باز را به‌طور مؤثر حفظ کنیم» [How to preserve open source information effectively].

[146] همان. توجه داشته باشید که استفاده از اصطلاح «اصالت» در این زمینه با کاربرد آن در زمینه حقوقی متفاوت است.

(ب) دسترسی‌پذیری

161. دسترسی‌پذیری به معنای موجود بودن یک مورد دیجیتال در ساده‌ترین مفهوم آن، یعنی به‌طور مداوم وجود داشتن و قابل بازیابی بودن، و همچنین در مفهوم قانونی، یعنی تأمین حقوق مالکیت فکری مناسب برای دسترسی و استفاده از آن مورد است.[147]

(پ) هویت

162. هویت یعنی توانایی یک مورد دیجیتال برای اینکه بتوان به آن ارجاع داد.این مورد دیجیتال باید قابل شناسایی و متمایز از سایر موارد دیجیتال باشد، برای مثال از طریق ثبت شدن با یک شناسه، مانند یک شماره شناسایی منحصربه فرد.[148]

(ت) پایداری

163. پایداری یعنی یکپارچگی و قابلیت بقای یک مورد دیجیتال از نظر فنی. توالی بیت‌های یک مورد دیجیتال باید دست‌نخورده، قابل پردازش و قابل بازیابی باشند.[149]

(ث) قابلیت نمایش

164. قابلیت نمایش به توانایی انسان یا ماشین برای استفاده یا تعامل با یک مورد دیجیتال با استفاده از سخت‌افزار و نرم‌افزار مناسب اشاره دارد.[150]

(ج) قابلیت درک

165. قابلیت درک، به معنای توانایی کاربران موردنظر برای تفسیر و درک یک مورد دیجیتال است.[151]

2- مسائل خاص تحقیق

166. محققان باید مسائل خاص تحقیق را که احتمالاً یا قطعاً در طی فرآیند حفظ و نگهداری اتفاق خواهند افتاد، در نظر گرفته و برای آنها برنامه‌ریزی کنند.

(الف) زنجیرهٔ حفظ و نگهداری شواهد

---

147 همان.
148 همان.
149 همان.
150 همان.
151 همان

167. زنجیره حفظ شواهد به مستندسازی نگهدارندگان اطلاعات یا شواهد، با حفظ ترتیبِ زمانی اشاره دارد و شامل مستند نمودن کنترل، تاریخ و زمان، انتقال، تحلیل و سرنوشت نهایی اینگونه شواهد است. زنجیره حفظ شواهد یک مورد دیجیتال باید پس از جمع‌آوری، از طریق ایجاد یک سیستم مناسب برای حفظ و ابقای موارد دیجیتال، نگهداری و مراقبت شود.

(ب) نسخهٔ قابل ارائه به عنوان مدرک

168. نسخه اثباتی، مورد دیجیتالی است که توسط یک محقق در قالب اصلی خود جمع‌آوری شده و نباید تغییر یابد یا اصلاح شود. موارد دیجیتال باید در قالب اصلی خود ذخیره شوند. این به معنای حفظ یک نسخه اصلی و دست‌نخورده از مورد دیجیتال جمع‌آوری‌شده در تمام فرمت‌هایی است که در آن جمع‌آوری شده است.

(پ) نسخه های کاری

169. یک یا چند نسخه از مورد دیجیتال باید به منطور تجزیه و تحلیل ایجاد شده و به‌صورت جداگانه ذخیره شوند تا محققان بتوانند با نسخهٔ ایجاد شده کار کنند، نه با نسخهٔ اصلی. این روش باعث می‌شود دست‌کاری نسخه اصلی به حداقل برسد و خطر آسیب‌دیدگی یا تغییر آن کاهش یابد. ایجاد هرگونه تغییر در مطلب دیجیتال، از جمله ایجاد نسخه‌ها، باید مستند شود. در صورت امکان باید سیستم‌های ذخیره‌سازی جداگانه‌ای برای نسخه‌های اثباتی و نسخه‌های کاری استفاده شود.

(ت) ذخیره‌سازی

170. ذخیره‌سازی کمک می‌کند تا از پایدار ماندنِ مطالب دیجیتال و قابلیتِ پیدا کردن و بازیابی آنها اطمینان حاصل کنیم . ذخیره‌سازی نباید به‌عنوان یک فرآیند غیرفعال در نظر گرفته شود، بلکه یک فرآیند فعال بوده که شامل وظایف و مسئولیت‌های مداوم و مدیریت‌شده است. این فرآیند شامل ذخیره‌سازی دائمی است که در آن رسانه‌های ذخیره‌سازی نقش دارند، اما همچنین مدیریت سلسله‌مراتب ذخیره‌سازی، جایگزینی رسانه‌ها، بررسی خطا، بررسی ثبات (تأیید اینکه مورد تغییری نکرده است)، بازیابی پس از فاجعه، و یافتن محل اشیای ذخیره‌شده و بازگرداندن آنها را نیز در بر می‌گیرد.[152] اطلاعات دیجیتال ممکن است به‌صورت محلی (آنلاین یا آفلاین) یا در مکانی دور از محل (آنلاین یا آفلاین) ذخیره شوند.[153]گزینه‌های ذخیره‌سازی برای محتوای دیجیتال شامل یک هارد دیسک محلی یا دستگاه‌های ذخیره‌سازی قابل حمل محلی، یک درایو شبکه‌ای که بخشی از شبکه محلی است، یا یک سرور راه دور یا سیستم ذخیره‌سازی ابری می‌شود. در انتخاب روش ذخیره‌سازی باید موضوعات زیر را در نظر گرفت؛ ظرفیت ذخیره‌سازی (فضا)، دسترسی و کنترل، سیستم پشتیبان، قوانین مربوطه، و امنیت اطلاعات و حفاظت از داده‌ها. همچنین در انتخاب روش ذخیره‌سازی باید سرعت، دسترسی‌پذیری، هزینه، قابلیت دوام و پایداری، مدیریت ذخیره‌سازی و سیستم‌های بازیابی اطلاعات نیز مورد توجه قرار گیرند.[154]

---

[152] همان، ص 154.

[153] نگاه کنید به: شایرا شایندلین و دانیل جی. کاپرا، «کشف الکترونیکی و شواهد دیجیتال به‌طور مختصر» [Shira Scheindlin and Daniel J. Capra, *Electronic Discovery and Digital Evidence in a Nutshell*]، (سنت پل، انتشارات آکادمیک وست [Saint Paul, West Academic Publishing]، ۲۰۰۹)، صص. ۲۱–۲۲.

[154] نگاه کنید به: Ng، «چگونه اطلاعات منبع باز را به‌طور مؤثر حفظ کنیم» [How to preserve open source information effectively].

(1) تهیه نسخه پشتیبان (بکاپ)

171. اگر از دست رفتن داده‌ها یا خطاهایی رخ دهد، یک بایگان یا تکنیسین می‌تواند تلاش کند تا داده‌ها را بازیابی کند. در حالت ایده‌آل، داده‌ها قبلاً در مکانی جداگانه پشتیبان‌گیری یا تکثیر شده‌اند. کارشناسان فناوری اطلاعات توصیه می‌کنند که حداقل سه نسخه از داده‌ها، روی حداقل دو نوع مختلف از حافظه ذخیره‌سازی، و حداقل یک نسخه به‌صورت جغرافیایی جدا از نسخه‌های دیگر نگهداری شود.

(2) فرسایش (افت کیفیت)

172. یکی از چالش‌های ذخیره‌سازی این است که رسانه‌ها با گذر زمان دچار افت کیفیت می‌شوند. بایگان‌ها می‌توانند با استفاده از انواع رسانه‌های به‌ویژه بادوام، خطر خرابی ذخیره‌سازی را کاهش دهند؛ با این حال، هر دستگاه ذخیره‌سازی در نهایت دچار نقص، فرسودگی یا خرابی تصادفی خواهد شد. حتی بدون خرابی کامل، ممکن است خطاهای داده یا خراب شدن فایل به دلیل فرسودگی رسانه‌های ذخیره‌شده رخ دهد. بنابراین، حفظ نسخه‌های پشتیبان و نظارت منظم بر زیرساخت‌های ذخیره‌سازی و پایداری فایل‌های ذخیره‌شده بسیار مهم است. این کار می‌تواند شامل بررسی منظم کدهای هش نمونه‌های تصادفی باشد تا اطمینان حاصل شود که هیچ گونه افت کیفیت رخ نداده است.

(3) فرسودگی تکنولوژیکی و از کارافتادگی

173. فایل‌های دیجیتال زمانی منسوخ می‌شوند که سخت‌افزار مورد نیاز برای دسترسی به داده‌ها دیگر به‌طور منطقی در دسترس نباشد یا نگهداری آن دیگر به طریق معقول امکان‌پذیر نباشد. صرف‌نظر از میزان دوام هر رسانه ذخیره‌سازی، این رسانه نیز در معرض خطر منسوخ شدن قرار دارد، که ممکن است بازیابی داده‌های ذخیره‌شده را دشوار یا غیرممکن کند. بنابراین، تحقیقات باید اطمینان حاصل کنند که رسانه‌های ذخیره‌سازی را نگهداری کرده و در صورت لزوم به‌روزرسانی کنند تا قابلیت استفاده و دسترسی به داده‌ها حفظ شود.

(4) بازیابی

174. فایل‌های دیجیتال ممکن است به‌صورت تصادفی یا عمدی حذف شوند. زمانی که کاربر فایلی را در کامپیوتر "حذف" می‌کند، محتوای فایل حذف‌شده همچنان روی رسانه ذخیره‌سازی باقی می‌ماند، مگر این که داده‌های جدیدی روی محل ذخیره‌سازی آن فایل نوشته شوند.[155] بنابراین، هرچه فعالیت روی کامپیوتر یا رسانه ذخیره‌سازی بیشتر باشد، داده‌های جدید زودتر در محل ذخیرهٔ فایل حذف شده نوشته می‌شوند و آن فایل غیرقابل بازیابی می‌شود. بیشتر کامپیوترها دارای ابزارهای نرم‌افزاری داخلی در سیستم‌عامل خود هستند که امکان بازیابی فایل‌های حذف‌شده را فراهم می‌کنند. علاوه بر این، نرم‌افزارهای بازیابی داده نیز قابل خریداری هستند و گاهی می‌توان از آنها برای "بازگرداندن" فایل‌های حذف‌شده استفاده کرد. محققان منبع باز ممکن است نیاز داشته باشند از متخصصان فناوری اطلاعات برای دسترسی به داده‌های حذف‌شده کمک بگیرند.

[155] نگاه کنید به: شایندلین و کاپرا، «کشف الکترونیکی و شواهد دیجیتال به‌طور مختصر»، ص ۲۴.

(5) تازه سازی (بازنشانی) داده‌ها

175. تازه‌سازی (بازنشانی) شامل کپی کردن محتوا از یک رسانه ذخیره‌سازی به رسانه‌ای دیگر است. این فرآیند تنها بر منسوخ شدن رسانه تمرکز دارد و به‌عنوان یک راهبرد جامع برای حفظ داده‌ها محسوب نمی‌شود. با این حال، تازه‌سازی باید به‌عنوان بخشی اساسی از یک استراتژی بزرگ‌تر برای نگهداری در نظر گرفته شود.[156]

ث) راستی‌آزمایی

176. راستی‌آزمایی به معنای فرآیند تأیید صحت یا اعتبار اطلاعات جمع‌آوری‌شده از اینترنت است. راستی‌آزمایی اطلاعات منبع باز می‌تواند به‌عنوان بخشی از یک تحلیل همه‌جانبه – شامل اطلاعات از منابع بسته و محرمانه – یا صرفاً بر اساس منابع باز انجام شود. راستی‌آزمایی به سه بخش مجزا تقسیم می‌شود: منبع، مورد یا فایل دیجیتال، و محتوا، که باید به‌صورت جمعی آن را بررسی کرد و از نظر همخوانی مورد مقایسه قرار داد.

1- تحلیل منبع

177. تحلیل منبع فرآیند ارزیابی اعتبار و قابلیت اطمینان یک منبع است. محیط آنلاین چالش‌هایی را برای تحلیل منبع ایجاد می‌کند، زیرا بسیاری از منابع، ناشناس یا دارای نام مستعار هستند. برای تحلیل صحیح منابع اطلاعات، محققان منبع باز ابتدا باید منبع یا منابع صحیح برای تحلیل را شناسایی کنند، که به معنای نسبت دادن اطلاعات به منبع اصلی آن است. تحلیل شناسایی منبع یعنی فرآیند تعیین منبع اطلاعات دیجیتال، که ممکن است یک وب‌سایت خاص، مشترک یا کاربر یک حساب یا پلتفرم مشخص، یا هویت افرادی باشد که محتوای خاصی را نوشته، ایجاد یا بارگذاری کرده‌اند. تحلیل شناسایی منبع همیشه امکان‌پذیر نیست و ممکن است نیاز به اقدامات تحقیقی بیشتر در فضای آنلاین و دنیای واقعی یا استفاده از تکنیک‌های پیشرفته جستجو و تحلیل داشته باشد. هرچند شناسایی نویسنده مفید است، اما عدم شناسایی آن معمولاً برای اثبات اصالت یک مورد آنلاین حیاتی نیست، زیرا راه‌های دیگری برای سنجش صحت اطلاعات منبع باز وجود دارد.

(الف) منشاء

178. منشاء به خاستگاه یا اولین وجود شناخته‌شدهٔ چیزی گفته می‌شود. در مورد محتوای آنلاین، منشاء می‌تواند به اولین حضور آن در اینترنت یا نسخه اصلی آن قبل از بارگذاری در اینترنت اشاره داشته باشد. در مورد محتوای آنلاین، بهتر است به جای عبارت «اولین نسخه آنلاین»، از عبارت «اولین نسخه پیداشدهٔ آنلاین» استفاده شود، چرا که ممکن است نسخه اصلی حذف شده باشد. حتی زمانی که محققان مطمئن باشند که نسخه اولیه یک ویدیو یا اطلاعات دیگر را از منابع باز آنلاین یافته‌اند، نمی‌توانند از منشاء آن اطمینان کامل داشته باشند، زیرا کانال‌های بسته‌ای مانند ایمیل‌ها و گروه‌های

[156] نگاه کنید به: کتابخانه دانشگاه کرنل، «آموزش تصویربرداری دیجیتال» [Cornell University Library, "Digital imaging tutorial"]، قابل دسترسی در: http://preservationtutorial.library.cornell.edu/tutorial/preservation/preservation-03.html.

پیام‌رسان خصوصی ممکن است پیش از آنکه این مطلب به‌طور عمومی در فضای آنلاین ظاهر شود برای اشتراک‌گذاری آن مورد استفاده قرار گرفته باشند.[157]

(ب) اعتبار

179. تاریخچه انتشار، فعالیت آنلاین و حضور اینترنتی یک منبع ممکن است حاوی اطلاعات مرتبطی باشد که به نفع یا بر علیه اعتبار منبع است. محققان منبع باز باید حضور آنلاین و تاریخچه انتشار منبع را بررسی کنند، که ممکن است حتی به شناسایی کردنِ یک تلاش عمدی برای فریب کمک کند. برای مثال، اگر منبعی درباره رویدادهای یک کشور خاص مطلبی منتشر می‌کند، آیا پست‌های دیگرِ او نشان می‌دهد که او واقعاً در آن کشور حضور دارد؟

(پ) استقلال و بی‌طرفی

180. تحقیقات باید بی‌طرفی یک منبع را بررسی کنند. این کار می‌تواند از طریق بررسی گروه‌ها، سازمان‌ها یا وابستگی‌هایی که افراد دارند، همچنین نحوه کسب درآمد و منابع تأمین مالی آنها انجام شود. آیا ارتباطات یا روابطی با هر یک از طرف‌های دخیل در پرونده یا حادثه تحت بررسی وجود دارد؟ هنگام بررسی استقلال منابع، باید ارزیابی کرد که آیا آنها ممکن است با نهادهای مرتبط (برای مثال، طرف‌های یک درگیری) وابستگی داشته باشند یا خیر. ایدئولوژی یک منبع و هرگونه وابستگی گروهی نیز ممکن است حائز اهمیت باشد. محققان برای تمامی منابع، باید انگیزه‌ها، منافع یا دستورکارهای پنهان آنها را بررسی و آشکار کرده و میزان تأثیر این عوامل بر صحت و صداقت اطلاعات آنها را ارزیابی کنند.

(ت) میزان دقت

181. هرچه اطلاعات و ادعاها دقیق‌تر باشند، اثبات یا رد آنها آسان‌تر خواهد بود. ادعاهای کلی و مبهم معمولاً ارزیابی انتقادی را دشوارتر می‌سازند.

(ث) تضعیف

182. متونی که هم‌زمان با وقایعی که به آنها اشاره دارند نوشته شده‌اند، معمولاً قابل‌اعتمادتر از متونی در نظر گرفته می‌شوند که مدت‌ها پس از وقوع آن وقایع تهیه شده‌اند. [158]این عامل ممکن است برای محققان منبع باز چالش‌برانگیز باشد، به‌ویژه زمانی که زمان ایجاد یک متن دیجیتال مشخص نباشد.

2- تحلیل فنی

183. تحلیل فنی به تحلیل خود مورد دیجیتال گفته می‌شود، خواه یک سند، تصویر یا ویدیو باشد. برای آزمودن یکپارچگی فایل – یعنی اینکه آیا فایل به‌صورت دیجیتال تغییر، دستکاری یا اصلاح شده است –

[157] برای مثال، یک کاربر ممکن است عکسی را از طریق ایمیل برای کاربر دیگری ارسال کند، و سپس آن کاربر عکس را در رسانه‌های اجتماعی بارگذاری کند. بنابراین، منشاء عکس فرستنده ایمیل بوده، نه فردی که آن را منتشر کرده است.

[158] نگاه کنید به: مؤسسه تحقیقات کیفری بین‌المللی، راهنمای محققان [Institute for International Criminal Investigations, *Investigators Manual*]، چاپ پنجم (لاهه، ۲۰۱۲)، ص ۸۸.

محققان منبع باز ممکن است آن را تحت بررسی‌های جرم‌شناسی دیجیتال قرار دهند، که گاهی به آن تحلیل تحقیقی دیجیتال نیز گفته می‌شود. موارد زیر اجزای چنین تحلیلی هستند.

(الف) فراداده‌ها

184. فراداده‌ها (Metadata) داده‌هایی هستند که اطلاعاتی درباره داده‌های دیگر ارائه می‌دهند و آنها را توصیف می‌کنند. این فراداده‌ها می‌توانند توسط کاربری که یک مورد را ایجاد کرده است، کاربران دیگر، ارائه‌دهنده خدمات ارتباطی، یا هر دستگاهی که داده‌ها روی آن ایجاد، منتقل، دریافت یا مشاهده می‌شوند، تولید شوند. فراداده‌ها در توصیف یک مورد و شرایط ایجاد، انتشار یا تغییر آن حائز اهمیت هستند. فراداده‌ها ممکن است شامل اطلاعاتی مانند سازنده فایل، تاریخ ایجاد آن، داده‌های بارگذاری، اصلاحات، اندازه فایل و داده‌های جغرافیایی باشند. فراداده‌ها می‌توانند در یک فایل گنجانده شوند، در یک صفحه وب قابل مشاهده باشند یا در کد منبع حضور داشته باشند. برخی فراداده‌ها ممکن است قبل یا در حین بارگذاری حذف شوند یا به دلیل استفاده از برنامه‌های رسانه‌های اجتماعی از بین بروند، اما اگر در دسترس باشند، باید بررسی شوند تا مشخص شود آیا می‌توانند در اثبات اصالت کمک کنند. فراداده‌های اصلی ممکن است از بین بروند، زیرا پلتفرم‌ها اغلب رسانه‌های بارگذاری‌شده را برای بهینه‌سازی جهت نمایش آنلاین، اشتراک‌گذاری یا پخش، بازکدگذاری (transcode) می‌کنند. در چنین مواردی، فراداده بازتابی از فایل جدید خواهد بود، نه فایل اصلی. در مواردی که فراداده‌ها حذف شده‌اند، محققان منبع باز باید روش‌های دیگری را برای راستی‌آزمایِی یک مورد پیدا کنند.

(ب) داده‌های فرمت فایل تصویری قابل تبادل

185. فرمت فایل تصویری قابل تبادل نوعی فراداده است که فرمت‌های مربوط به تصاویر، صدا و برچسب‌های جانبی که توسط دوربین‌های دیجیتال، اسکنرها و سایر سیستم‌های مدیریت فایل‌های تصویری و صوتیِ ثبت‌شده توسط دوربین‌های دیجیتال استفاده می‌شوند را مشخص می‌کند.

(پ) کد منبع

186. کد منبع، برنامهٔ نوشته شده در پشت هر صفحه وب یا نرم‌افزار است. در مورد وب‌سایت‌ها، همه می‌توانند این کد را با استفاده از ابزارهای مختلف، حتی خود مرورگر وب، مشاهده کنند. کد منبع یک وب‌سایت به راحتی با استفاده از ابزارهای رایگان قابل مشاهده است. این کد ممکن است شامل فراداده، محتوای پنهان یا دستکاری‌شده باشد و ساختار لینک‌ها و لینک‌های خراب را نشان می‌دهد.

3- تحلیل محتوا

187. تحلیل محتوا فرآیندی است که طی آن اطلاعات موجود در یک ویدیو، تصویر، سند یا بیانیه از نظر اصالت و صحت ارزیابی می‌شوند. تحلیل محتوا نیز چندوجهی بوده و شامل بررسی سرنخ‌های بصری یا، برای مثال، تطبیق تصویر با فرادادهٔ آن است. ویژگی‌های محیط آنلاین مسائل متعددی را ایجاد می‌کند که می‌توانند بر اعتبار واقعی یا ادراک‌شدهٔ اطلاعات از منابع باز آنلاین تأثیر بگذارند. این مسائل شامل گزارش‌دادنِ چرخه‌ای، خارج کردن اطلاعات از بستر آن، و تفسیر نادرست هستند. داده‌های محتوا،

داده‌هایی هستند که در یک مورد دیجیتال وجود دارند، مانند ویدیو، تصویر، ضبط صوتی، سند یا متنِ بدونِ ساختار.

(الف) شناسه‌های یکتا

188. هنگامی که محققان باید صحت محتوای بصری را بررسی کنند، آنها باید بررسی را با جستجوی ویژگی‌های اختصاصی یا شناسایی‌کننده آغاز کنند. این ویژگی‌ها ممکن است شامل ساختمان‌ها، پوشش گیاهی و جانوری، افراد، نمادها و نشان‌ها باشند. هنگام تحلیل ویژگی‌های انسانی با هدف شناسایی یک فرد خاص، باید احتیاط ویژه‌ای به عمل آید.[159] روش‌های شناسایی معمولاً نیازمند مهارت‌های خاصی هستند، مانند مهارت‌هایی که با گذشت زمان و از طریق آموزش تخصصیِ یک کارشناس جرم‌شناسی به دست می‌آیند. تحلیل‌های غیرتخصصی که ممکن است توسط افراد آموزش‌ندیده انجام شوند، می‌توانند نادرست، جانبدارانه یا دارای مشکلات دیگر باشند.

(ب) اطلاعاتی که به‌صورت عینی قابل تأیید هستند

189. اغلب مفید است که با شناسایی آنچه ممکن است به عنوان «اطلاعاتِ قابل‌تأیید به‌طور عینی» شناخته شود، آغاز کنیم. برای مثال، وضعیت آب‌وهوا در یک روز مشخص، نام و رتبه یک فرمانده یا موقعیت مکانی یک ساختمان همگی می‌توانند به‌صورت عینی قابل راستی‌آزمایی باشند. ارزیابی مطالب منبع باز باید شامل بررسی محتوای آن در مقایسه با اطلاعات قابل راستی‌آزمایی به‌صورت عینی باشد.

(پ) تعیین موقعیت جغرافیایی

190. تعیین موقعیت جغرافیایی یعنی شناسایی یا تخمین موقعیت یک شیء، فعالیت یا مکانی که یک مورد از آن به وجود آمده است. برای مثال، ممکن است با استفاده از تکنیک‌های تعیین موقعیت جغرافیایی بتوان محل ضبط یک ویدیو یا عکسِ دانلودشده از اینترنت را مشخص کرد. این تکنیک‌ها برای مثال می‌توانند شامل شناسایی ویژگی‌های جغرافیایی منحصر به فرد در یک عکس و تطبیق آنها با موقعیت واقعی روی نقشه باشند.

---

[159] تحلیل جرم‌شناسی و شناسایی ویژگی‌های انسانی با استفاده از ابزارها یا تحلیل انسانی (مانند شناسایی چهره، تحلیل نحوه راه رفتن و غیره) نیازمند کارشناس جرم‌شناسی است. نگاه کنید به: نینا ام. ون ماسترایت و دیگران، «بررسی انتقادی استفاده و مبنای علمی تحلیل جرم‌شناسی نحوه راه رفتن»، تحقیقات علوم جرم‌شناسی [Nina M. van Mastrigt and others, "Critical review of the use and scientific basis of forensic gait analysis", *Forensic Sciences Research*]، جلد ۳، شماره ۳ (۲۰۱۸)، صص193-183 (قابل دسترسی در: www.tandfonline.com/doi/full/10.1080/20961790.2018.1503579؛ رویال سوسایتی و رویال سوسایتی ادینبورا، Royal Society و Royal Society of Edinburgh، «تحلیل جرم‌شناسی نحوه راه رفتن: راهنمای مقدماتی برای دادگاه‌ها»["Forensic gait analysis: a primer for courts"] (لندن، ۲۰۱۷) قابل دسترسی در: https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf؛ همچنین شبکه جرم‌شناسی اروپا [European Network of Forensic Science]، راهنمای بهترین شیوه برای مقایسه تصاویر چهره [*Best Practice Manual for Facial Image Comparison*] (۲۰۱۸) قابل دسترسی در: http://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf؛ مرکز ملی جرم شناسی سمعی و بصری [National Center for Audio and Video Forensics] ، «تحلیل ارتفاع ویدئوهای نظارتی» ["Height analysis of surveillance video"]، قابل دسترسی در: https://ncavf.com/what-we-do/forensic-height-analysis

(ت) تعیین زمان وقوع

191. زمان‌یابی، تأیید کردنِ تاریخ و زمان رخدادهای نمایش‌داده‌شده در یک موردی از اطلاعات است که معمولاً از تصاویر تشکیل شده است. برای مثال، ممکن است بتوان با بررسی طول سایه‌هایی که توسط نور خورشید ایجاد شده‌اند، همراه با سایر نشانه‌ها، زمان دقیقِ گرفتنِ یک عکس را مشخص کرد.

(ث) جامع بودن

192. یک سند یا کلیپ ویدئویی ناقص ممکن است همچنان ارزش اثباتی داشته باشد، اما وجود شکاف(ها) می‌تواند بر اهمیتی که به آن مورد نسبت داده می‌شود، تأثیر بگذارد. بنابراین، هنگام جمع‌آوری اطلاعات منبع باز، مهم است که فایل هدف به‌طور کامل ضبط شود و در صورت لزوم، زمینه‌های اطراف آن نیز ثبت گردد.

(ج) انسجام درونی

193. ارزیابی سازگاری درونی می‌تواند در رابطه با یک مورد اطلاعات از یک منبع باز آنلاین یا در رابطه با مجموعه‌ای از اطلاعات از یک منبع خاص (و/یا منابعی با منشأ یا نویسندگی مشترک) انجام شود. ارزیابی سازگاری درونی یک مورد اطلاعات آنلاین به دنبال آن است که مشخص کند آیا اطلاعات به خودی خود سازگار و منسجم است یا خیر. یک قطعه یا مجموعه اطلاعات که از نظر درونی سازگار باشد نباید با خودش تناقض داشته باشد.

(چ) همخوانی با منابع خارجی

194. هنگامی که اطلاعاتی که خارج از خود مورد دیجیتال قرار دارد با محتوای آن همخوانی داشته و در نتیجه صحت محتوای آن را تأئید می‌کند، همخوانی با منابع خارجی وجود دارد.

ج) تحلیل تحقیقی

195. تحلیل تحقیقی به فرآیند بررسی و تفسیر اطلاعات واقعی برای دستیابی به یافته‌های اساسی مرتبط با تصمیم‌گیری یا تشکیل پرونده گفته می‌شود. حجم و کیفیت متغیر اطلاعات منبع باز، داشتنِ یک رویکرد ساختارمند و منظم برای تحلیل را ضروری می‌سازد.

196. ممکن است اطلاعات منبع باز پیش از انجام برخی از انواع تحلیل، نیاز به پردازش داشته باشد. پردازش می‌تواند شامل ترجمه زبان‌های خارجی یا تشکیل دادن مجموعه داده‌های مختلف برای کمک به تحلیل رفتار افراد، مکان‌ها و اشیا، همچنین روابط یا شبکه‌ها، حرکات، فعالیت‌ها یا تراکنش‌ها باشد. این فرآیند همچنین می‌تواند شامل تغییر ماهیت یا فرمت یک مورد دیجیتال برای سازگاری با یک نرم‌افزار خاص باشد. انواع رایج پردازش داده شامل موارد زیر است:

(الف) ترجمه :اگر داده‌ها به زبانی باشند که محققان به آن مسلط نیستند یا توسط نرم‌افزار مورد نیاز برای بررسی محتوا پردازش نمی‌شوند، ممکن است لازم باشد پیش از انجام مراحل بعدی، داده‌ها ترجمه شوند.

(ب) ادغام: محققان ممکن است نیاز داشته باشند مجموعه داده‌های مختلف را در یک مجموعه داده بزرگ‌تر ادغام کنند تا بتوانند آن را تحلیل کنند.

(پ) تغییر قالب :برای آسان‌تر کردن جستجو یا بازیابی داده‌ها، محققان ممکن است نیاز داشته باشند فرمت یک مورد دیجیتال را تغییر دهند.

197. توصیه می‌شود که تنها نسخه‌های کاری یک مورد دیجیتال پردازش شوند و نه نسخه اصلی یا نسخه اثباتی. هرگونه پردازشی که روی یک مورد دیجیتال صورت می‌گیرد باید مستند شود. اگر محققان برای پردازش داده‌ها از فناوری‌های دیجیتال استفاده کنند، مثلاً تحلیل داده‌ها با استفاده از الگوریتم‌ها، از جمله پردازش زبان طبیعی و یادگیری عمیق، باید از خطر جانبداری در پردازش این داده‌ها آگاه باشند.

198. پس از پردازش، اطلاعات می‌توانند مورد تحلیل قرار گیرند. نتایج تحلیلی اطلاعات منبع باز، بسته به هدف، نوع و گسترهٔ اطلاعات پایه، جدول زمانی تولید و مخاطب آن متفاوت خواهند بود. این نتایج بر اساس نیازهای یک تحقیق ساخته می‌شوند و می‌توانند شامل نمودارها، خلاصه‌ها، واژه‌نامه‌ها، فرهنگ‌نامه‌ها و ابزارهای بصری، از جمله الگوها و تمرین‌های تحلیل الگوها باشند.[160]

199. محققان باید معیارهای موشکافانه‌ای را اعمال کنند تا از عینیت، به‌موقع بودن، مربوط بودن و دقت داده‌ها و نتیجه‌گیری‌های موجود در دستاوردهای تحلیلی اطمینان حاصل کنند و از حریم خصوصی و دیگر ملاحظات حقوق بشری به ویژه هنگام رسیدگی به اطلاعات هویتی افراد نیز محافظت نمایند. چنین اطلاعاتی باید تنها در محصولاتی گنجانده شود که محققان رضایت افراد درگیر را برای آن به دست آورده باشند و این اطلاعات مستقیماً به پیشبرد یک هدف تحقیقاتی کمک کند. همچنین باید این موضوع با در نظر گرفتن محدودیت‌های قانونی و اخلاقی مربوط به استفاده از آن مورد توجه قرار گیرد.[161]

200. بخش‌های زیر شامل انواع رایج تحلیل‌هایی است که ممکن است برای پیشبرد اهداف تحقیقاتی با استفاده از اطلاعات منبع باز به کار گرفته شوند.

1- تحلیل مقایسه‌ای تصویر/ویدئو

201. تحلیل مقایسه‌ای یا علم مقایسه، فرآیند مقایسهٔ ویژگی‌های اشیا، افراد و/یا مکان‌ها با موارد شناخته‌شده و/یا ناشناخته است، که در آن حداقل یکی از موارد مورد نظر یک تصویر باشد. این نوع تحلیل شامل بررسی محتوای تصاویر و ویدئوها، از جمله مقایسه عناصر مختلف میان موارد و ویژگی‌ها، کیفیت تصاویر و تنظیمات بصری آنها (نور، زاویهٔ دید و غیره) است. در حالی که بسیاری از افراد غیرمتخصص اکنون با اصول اولیهٔ تحلیل مقایسه‌ای تصاویر آشنا هستند، کمک گرفتن از یک کارشناس واجد شرایط و دارای گواهینامه در تحلیل ویدئوی جنایی و/یا جرم‌شناسی دیجیتال می‌تواند به ارائه تحلیل

[160] نگاه کنید به فصل ۷ در زیر درباره گزارش‌دهی یافته‌ها.
[161] نگاه کنید به فصل ۳ در بالا درباره چارچوب قانونی.

علمی، از جمله اظهار نظر کارشناسی، کمک کند. تحقیقات حقوق بشری و دیگر انواع تحقیقات نیز می‌توانند از این تخصص بهره‌مند شوند تا به یافته‌های خود اعتبار بیشتری ببخشند.

2- تحلیل تفسیری تصویر/ویدئو

202. تحلیل تفسیری تصویر/ویدئو که به تحلیل مقایسه‌ای تصویر/ویدئو مربوط است، شامل بررسی یک مورد دیجیتال برای درک محتوای بصری آن است. برای مثال، تحلیل تیراندازی‌ها، زخم‌ها، خون، وسایل نقلیه، سلاح‌ها و تجهیزات نظامی، یا تحلیل سرعت یک وسیله نقلیه در حال حرکت یا سن یک فرد، همگی بخشی از تحلیل تفسیری تصویر/ویدئو هستند. این نوع تحلیل می‌تواند توسط تحلیل‌گران برای اهداف تحقیقاتی انجام شود یا توسط کارشناسان جنایی یا متخصصان حوزهٔ موضوعی در مواردی که هدف، اثبات حقایق در دادرسی‌های قانونی یا یافته‌های حقوق بشری است، مورد استفاده قرار گیرد.

3- تحلیل فضایی

203. تحلیل فضایی یا تحلیل جغرافیایی ممکن است شامل تحلیل محتوای بصری و تحلیل فراداده برای مواردی باشد که مختصات جغرافیایی یا نام مکان‌ها را ارائه می‌دهند. تحلیل فضایی شامل بررسی اشیا و ویژگی‌های مختلف چشم‌انداز با دقت مناسب، مقایسه آنها با تصاویر ماهواره‌ای یا سایر تصاویر، داده‌های جغرافیایی و نقشه‌ها، دانش مناسب برای پرونده و زمینهٔ مربوطه، و استفاده از ابزارهای سامانه اطلاعات جغرافیایی[162] است.

4- ترسیم بازیگران

204. ترسیم بازیگران تکنیکی برای درک نقش‌آفرینان کلیدی و شناسایی روابط قدرت و کانال‌های اِعمال نفوذ است.[163] به این ترتیب، این فرآیند با شناسایی بازیگران اصلی آغاز شده و سپس روابط میان آنها ترسیم می‌شود.

5- تحلیل شبکه‌های اجتماعی

205. تحلیل شبکه‌های اجتماعی هم مانند ترسیم بازیگران، شامل ترسیم و اندازه‌گیری روابط میان افراد، گروه‌ها، سازمان‌ها، رایانه‌ها، نشانی‌های اینترنتی (URL) و دیگر نهادهای مربوط به اطلاعات/دانش است.[164] به افراد و گروه‌ها اغلب به‌عنوان گره‌ها اشاره می‌شود، به طوری که پیوندها روابط بین این گره‌ها را نشان می‌دهند. تحلیل شبکه‌های اجتماعی از ارتباطات میان رسانه‌های اجتماعی و دیگر پلتفرم‌های موبایل یا مبتنی بر وب استفاده می‌کند تا روابط میان افراد را شناسایی و درک کند. تحلیل داده‌های مربوط به ارتباطات یا پیوندها می‌تواند به‌صورت دستی توسط یک محقق یا با استفاده از نرم‌افزارهای تحلیلی انجام شود.

---

[162] سامانه اطلاعات جغرافیایی (GIS) یک پایگاه داده رایانه‌ای است که برای مدیریت و تحلیل داده‌های مکانی به کار می‌رود.

[163] نگاه کنید به: کمیساریای عالی حقوق بشر سازمان ملل متحد (OHCHR)، «راهنمای نظارت بر حقوق بشر» [*Manual on Human Rights Monitoring*]، فصل ۸ درباره تحلیل، ص. ۲۴.

[164] نگاه کنید به: Orgnet، «تحلیل شبکه‌های اجتماعی: یک مقدمه» [“Social network analysis: an introduction”]. قابل دسترسی در: www.orgnet.com/sna.html.

6- ترسیم حوادث

206. ترسیم حوادث یک تکنیک تحلیلی است که برای تعیین روابط زمانی و جغرافیایی میان حوادث مختلف استفاده می‌شود. در زمینه نقض‌های کیفری بین‌المللی و حقوق بشری، این روش می‌تواند به مکان‌یابی چنین نقض‌ها یا جرایمی، از جمله رویدادهای قبلی و بعدی، بپردازد. همچنین ممکن است شامل ترسیم رویدادهای مرتبط دیگر، مانند زمان و مکان اظهاراتِ انجام‌شده توسط مرتکبانِ احتمالی باشد.

7- تحلیل الگوهای جرم/نقض حقوق

207. در زمینه اجرای قانون در سطح ملی، یک الگوی جرم به گروهی از دو یا چند جرمِ گزارش‌شده یا کشف‌شده توسط نیروی پلیس اشاره دارد که به دلیل داشتن حداقل یک وجه مشترک در نوع جرم، از قبیل رفتار مجرمان یا قربانیان، ویژگی‌های مجرمان، قربانیان یا افرادِ هدف قرار گرفته، اموال سرقت‌شده یا مکان وقوع جرم، منحصر به فرد هستند.[165] به همین ترتیب، الگوهای جرم و نقض حقوق می‌توانند در پرونده‌های کیفری بین‌المللی و حقوق بشری بر اساس اطلاعات منبع باز شناسایی شوند.

[165] نگاه کنید به: انجمن بین‌المللی تحلیلگران جرم، «تعاریفِ الگوهای جرم برای تحلیل تاکتیکی»، راهنمای کمیته استانداردها، روش‌ها و فناوری 2011 – 01، [International Association of Crime Analysts, "Crime pattern definitions for tactical analysis", Standards, Methods and Technology Committee White Paper 2011-01]، ص 1.

7- گزارش‌دادن درباره یافته‌ها

خلاصهٔ این فصل

- یافته‌های یک تحقیق مبتنی بر منابع باز، چه مربوط به داده‌های جمع‌آوری‌شده باشد و چه نتایج حاصل از آن داده‌ها، می‌تواند به صورت شفاهی، بصری یا کتبی گزارش شود.

- محققان باید در تصمیم‌گیری درباره (الف) قالب‌های مورد استفاده و (ب) داده‌های قابل درج، در نظر بگیرند که کدام قالب‌ها برای مأموریت آنها و مخاطبان مورد نظرشان مناسب‌تر است. این تصمیم باید با توجه به عواملی مانند سواد فناوری مخاطبان، قابلیت دسترسی، عینیت، شفافیت و امنیت اتخاذ شود.

208. این فصل روش‌هایی را توصیف می‌کند که تحقیقات مبتنی بر منابع باز – از جمله روش‌شناسی، یافته‌های تحلیلی و داده‌های خام – می‌توانند ارائه یا گزارش شوند. در بسیاری از موارد، اطلاعات منبع باز همراه با اطلاعاتی که از طریق روش‌های دیگر تحقیق جمع‌آوری شده‌اند، ارائه می‌شود. این اطلاعاتِ ارائه شده می‌توانند اشکال متنوعی داشته باشند، از جمله گزارش‌های کتبی، گزارش‌های شفاهی یا گزارش‌های بصری، یا ترکیبی از این اشکال. گزارش‌ها ممکن است برای استفاده داخلی یا انتشار خارجی تهیه شوند و بسته به عوامل مختلف، به‌عنوان تخصصی یا غیرتخصصی در نظر گرفته شوند. گزارش‌ها باید عناصر زیر را تضمین کنند:

(الف) دقت: گزارش‌ها باید داده‌های جمع‌آوری‌شده را به‌طور دقیق منعکس کنند.[166] اطلاعات تبرئه‌کننده باید گنجانده شود، همان‌طور که توضیحی درباره هرگونه حذف یا نقص نیز باید ارائه شود؛

(ب) ارائهٔ منبع: گزارش‌ها باید به‌طور واضح میان محتوایی که در حوزه عمومی یا اطلاعات عمومیِ غیرمحرمانه است، اطلاعاتی که طبقه‌بندی‌شده یا به‌نوعی محدود شده است، و محتوایی که بازتاب‌دهندهٔ قضاوت یا نظر محققان و/یا دیگر متخصصان است، تمایز قائل شوند. محققان یا دیگر افرادی که درباره اطلاعات منبع باز گزارش می‌دهند، باید دقت لازم را به کار گیرند و مجوزهای مناسب را برای استفاده از محتوایی که ممکن است متعلق به دیگران باشد، به دست آورند، برای مثال کسب اطمینان از هر گونه حقوق مربوط به مالکیت فکری موردنیاز؛

(پ) کامل بودن: یافته‌ها باید نشان‌دهندهٔ میزان کامل بودن داده‌های اصلی باشند، به‌ویژه اگر داده‌ها به‌طور عمدی حذف شده باشند؛

(ت) محرمانه بودن: با وجود اینکه اطلاعات در محیط‌های منبع باز یافت شده‌اند، گزارش‌ها باید بررسی کنند که چه مواردی باید حذف یا ویرایش شوند تا محرمانگی حفظ شده و خطرات به حداقل برسند، به‌ویژه خطرات احتمالی برای منابع، شهود، قربانیان و اعضای جوامعی که با اطلاعات منبع باز به طریقی مربوط هستند.

(ث) زبان: گزارش‌ها باید از زبانی خنثی استفاده کنند و از به‌کارگیری زبان احساسی یا هیجانی پرهیز نمایند. گزارش‌ها باید بدون استفادهٔ بیش‌ازحد از صفات یا تأکید، واقعیت‌ها را به‌صورت شفاف بیان کنند. همچنین، گزارش‌ها باید با زبانی حساس به جنسیت نوشته شوند. گزارش‌های عمومی در حالت ایده‌آل، باید علاوه بر هر زبان رسمی که توسط محققان یا نهادهای تحقیقاتی استفاده می‌شود، به زبان‌های جوامع تأثیریافته نیز در دسترس قرار گیرند.

(ج) شفافیت: گزارش‌ها باید به‌وضوح بیان کنند که محققان چگونه کار خود را انجام داده‌اند و اهداف، فرآیندها و روش‌های آنها چه بوده است. این اطلاعات معمولاً در بخش روش‌شناسی گزارش گنجانده می‌شود، اما باید توصیفات در سراسر متن را نیز هدایت کند. توصیفات باید تا حد امکان شفاف باشند، بدون اینکه آسیب‌پذیری‌های امنیتی ایجاد کنند، برای مثال با افشای اطلاعات محرمانه.

الف) گزارش کتبی

[166] نگاه کنید به فصل ۲ (ب) در بالا درباره اصول روش‌شناسی.

209. یک تحقیق مبتنی بر منابع باز ممکن است به‌صورت کتبی ارائه شود که می‌تواند شامل گزارش‌های داخلی، گزارش‌ها به مشتریان و همچنین گزارش‌های عمومی باشد. یکی از روش‌های انتقالِ یافته‌های تحلیلی، گزارش کتبی است که ممکن است شامل گزارش‌های سازمان‌های غیردولتی، هیئت‌های تحقیق، کمیسیون‌های حقیقت‌یاب، سازمان ملل و گزارش‌های کارشناسی برای دادگاه‌ها یا محاکم دیگر باشد.[167] اطلاعات دیجیتال منبع باز اغلب با سایر اشکال داده‌ها و تحلیل‌های منبع باز و بسته تلفیق می‌شود. گزارش‌های کتبی باید اطلاعات جمع‌آوری‌شده را تحلیل کنند تا به نتیجه‌گیری‌های منطقی، تخمین‌ها و پیش‌بینی‌ها برسند. این گزارش‌ها باید از روش‌شناسی مستحکم برخوردار بوده و بتوانند این روش‌شناسی را به شکلی قابل‌درک برای مخاطبان مورد نظر توضیح دهند. صحت و تمامیت اطلاعات اصلیِ موجود در یک گزارش بسیار حیاتی است. داده‌های نادرست به نتایج نادرست منجر خواهند شد.[168]

210. گزارش‌های کتبی باید شامل بخش‌های زیر باشند، مگر اینکه دلیل موجه و مشخصی برای عدم گنجاندن آنها بیان شده باشد، مثل ضرورت محرمانه نگاه داشتن برخی از تکنیک‌ها، روش‌ها و منابع تحقیقاتی آنلاین:

(الف) اهداف تحقیقاتی: گزارش‌ها باید شامل اهداف تحقیقاتی و دستورالعمل‌ها یا مأموریت‌های زیربنایی از سوی مشتری باشند، از جمله سؤالات پژوهشی که به‌خوبی تعریف شده و قابل بیان باشند؛

(ب) روش‌شناسی: گزارش‌ها باید شامل روش‌های تحقیق باشند تا امکان تکرارپذیری را فراهم کرده و به مخاطبان اجازه دهند اعتبار اطلاعات و یافته‌های تحقیقات را درک و ارزیابی کنند، از جمله آنچه که در تحقیق پوشش داده شده است؛

(پ) فعالیت‌های انجام‌شده: گزارش‌ها باید شامل خلاصه‌ای از فعالیت‌هایی باشند که برای یافته‌ها یا ارزیابی کیفیت تحلیل اهمیت دارند، از جمله فعالیت‌هایی برای شناسایی داده‌های اصلی، آنچه جمع‌آوری شده و آنچه مورد تحلیل قرار گرفته است؛

(ت) داده‌ها و منابع اصلی: گزارش‌ها باید شامل توصیفی از داده‌های اصلی، از جمله منابع آنها و کیفیت این منابع باشند؛

(ث) موارد نقص یا عدم قطعیت: گزارش‌ها باید هرگونه کمبود یا عدم قطعیت در داده‌های اصلی یا تحلیل را که ممکن است بر یافته‌ها تأثیر بگذارد، شناسایی کنند؛

(ج) نتایج و توصیه‌ها: گزارش‌ها باید شامل تفسیرهای محققان از داده‌ها یا یافته‌ها بر اساس تحلیل‌های انجام‌شده بر روی آن داده‌ها باشند و محدودیت‌ها و سرنخ‌های جدید را ذکر کنند.

---

[167] برای نمونه‌ای از یک گزارش کتبی تحقیق مبتنی بر منابع باز دیجیتال، نگاه کنید به: آزمایشگاه تحقیقات حقوق بشر [Human Rights Investigations Lab]، «حملات شیمیایی به اللطامنه: ۲۵ و ۳۰ مارس ۲۰۱۷ – یک تحقیق مبتنی بر منابع باز توسط دانشجویان» [Chemical strikes on Al-Lataminah: March 25 & 30, 2017 – a student-led open source investigation] (برکلی، مرکز حقوق بشر، دانشکده حقوق دانشگاه کالیفرنیا، برکلی، ۲۰۱۸).

[168] با توجه به شرایط و الزامات محرمانگی، انجام بازبینی توسط افراد متخصص در همان زمینه توصیه می‌شود تا از صحت و کیفیت داده‌ها، همچنین تحلیل داده‌ها و یافته‌های استخراج‌شده از آنها اطمینان حاصل شود.

ب) گزارش شفاهی

211. اگر یافته‌های یک تحقیقِ مبتنی بر منابع باز به دادگاه برسد، ممکن است محققان مجبور شوند به‌عنوان شاهد شهادت دهندو تحقیقات خود را از طریق شهادت شفاهی ارائه کنند. اَشکال دیگر گزارش‌دادن شفاهی می‌تواند شامل ارائه مطالب در برابر کمیسیون‌های حقیقت‌یاب، مجامع سازمان‌های غیردولتی، دادگاه‌های مردمی یا رویدادهای رسانه‌ای باشد.

212. هر کسی که ملزم به ارائه شفاهی یافته‌های تحقیق خود که مبتنی بر منابع باز است باشد، باید بتواند کار خود را به‌طور واضح و دقیق توضیح دهد، از جمله روش‌شناسی به‌کاررفته و ابزارهای استفاده‌شده. این امر تضمین می‌کند که شهادت شفاهی و یافته‌های ارائه‌شده با دقت و اهمیت کافی مورد توجه قرار گیرند.

213. در رسیدگی‌های قضایی، اغلب سرپرست تحقیقات است که باید شهادت دهد و بتواند درباره کار تیم خود صحبت کند. این امر، البته، مستلزم آن است که این افراد از آنچه تیم‌شان انجام داده است آگاه باشند و بتوانند به سؤالاتی درباره نقش‌های انجام‌شده و دلایل تصمیم‌گیری‌های مربوط به محدوده تحقیق، روش‌ها، ابزارهای استفاده‌شده و غیره پاسخ دهند. محققان ممکن است به‌عنوان شهود متخصص یا شهود عادی عمل کنند. شهود متخصص -که به دلیل تجربه، دانش، مهارت، آموزش، تحصیلات یا مدارک مربوطهٔ خود به‌عنوان متخصص شناخته می‌شوند - می‌توانند درباره نتایجی که به آن رسیده‌اند و دیگر دستاوردهای تحلیلی شهادت دهند. شهود عادی معمولاً به ارائه شهادت درباره واقعیت‌ها محدود می‌شوند، به‌ویژه آن دسته از واقعیت‌هایی که شخصاً مشاهده کرده‌اند.

پ) گزارش بصری

214. بصری‌سازی داده‌ها به معنای نمایش تصویری اطلاعات است، برای مثال به شکل نمودارها، جدولها، نقشه‌ها و اینفوگرافیک‌ها [نمایش تصویری اطلاعات] که روشی قابل‌فهم برای مشاهده و درک روندها، نقاط غیرعادی و الگوهای داده‌ها را فراهم می‌کند.[169] این می‌تواند شامل چارت‌ها و نمایش‌های تصویری دیگری از داده‌ها در فضا و زمان؛ نمودارها (از جمله نمودارهایی که ارتباطات ریاضی، روندها یا روابط را نشان می‌دهند)؛ نمودارهای شبکه که روابط میان افراد مختلف را نمایش می‌دهند؛ و نمودارها و دیاگرام‌های آماری باشد. نقشه‌های دوبعدی و سه‌بعدی برای بصری‌سازی اشیا در فضا و زمان و بازسازی‌های سه‌بعدی از مکان‌های مختلف، از جمله صحنه‌های جرم، نیز بخشی از مجموعه ابزارهای

---

[169] نمونه‌هایی از گزارش‌دادن بصری در زمینه‌های مختلف شامل موارد زیر است: پلتفرم‌های دیجیتالی که به‌عنوان شواهد نمایشی در پرونده *دادستان علیه احمد الفقی المهدی* در دیوان کیفری بین‌المللی و پرونده *دادستان علیه سلیم جمیل عیاش و همکاران* در دادگاه ویژه لبنان مورد استفاده قرار گرفتند. «گزارشِ یافته‌های تفصیلی هیئت تحقیق مستقل بین‌المللی درباره اعتراضات در سرزمین‌های اشغالی فلسطین»، قابل دسترسی در www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP 2.pdf ؛ بی بی سی، افریکا آی، «جنایت در کامرون: پس از آنکه افریکا آی قاتل این زن را پیدا کرد، چه اتفاق افتاد»، اخبار بی بی سی [BBC Africa Eye, “Cameroon atrocity: what happened after Africa Eye found who killed this woman”, BBC News، ۳۰ مه 2019، قابل دسترسی در: www.bbc.com/news/av/world-africa-48432122/cameroon-atrocity-what-happened-after-africa-eye-found-who-killed-this-woman. همچنین، به‌طور کلی نگاه کنید به فعالیت‌های Forensic Architecture وSITU Research .

بصری‌سازی داده‌ها را تشکیل می‌دهند.[170] این ابزارها می‌توانند در درک حجم زیادی از داده‌ها، که اغلب در تحقیقات مبتنی بر منابع باز رخ می‌دهد، یا درک بهتر سناریوهای پیچیدهٔ مبتنی بر واقعیت مفید باشند.

215. انواع دیگر بصری‌سازی داده‌ها شامل موارد زیر است:

(الف) نقشه‌های ذهنی :نقشه ذهنی روشی تصویری برای نمایش ایده‌ها و مفاهیم و نحوه ارتباط آنها با یکدیگر است. نقشه‌های ذهنی اطلاعات را به شکلی سازمان‌دهی می‌کنند که تحلیل، ترکیب و درک آنها آسان‌تر شود. این نقشه‌ها اغلب شامل توضیحی درباره نحوه کشف داده‌های اصلی هستند؛

(ب) فلوچارت‌ها :فلوچارت نمایش تصویری یک رشتهٔ متوالی از رویدادها است، مانند مراحل موجود در یک الگوریتم، جریان کاری یا فرآیندهای مشابه؛

(پ) اینفوگرافیک‌ها [نمایش تصویری اطلاعات]: اینفوگرافیک یک نمایش تصویری از یک ایده یا مفهوم است که می‌تواند برای نمایش اطلاعات آماری نیز استفاده شود.

216. اطلاعات منبع باز می‌توانند به روش‌های متنوعی ارائه شوند، از نمایش صوتی-تصویری یک ویدئو یا وب‌سایت واحد گرفته تا نمایش مجموعه‌ای از اطلاعات به صورت دیجیتال، چندرسانه‌ای، و تعاملی.[171] نمایش‌ها و توضیحات بصری یا پلتفرم‌های دیجیتال ممکن است به گونه‌ای برای نمایش اطلاعات به کار روند که درک حقایق اصلی را برای مخاطبان مورد نظر آسان‌تر کند. نمونه‌هایی از این ابزارها شامل جدول‌های زمانی، عکس‌های ترکیبی (مانند نمای ۳۶۰ درجه از یک صحنه جرم) و ویدئوهای ویرایش‌شده هستند.

217. در صورت ارائه شواهد بصری‌سازی شدهٔ داده‌ها و نیز شواهد چندرسانه‌ای در دادگاه یا به دیگر مخاطبان عمومی، محققان باید درک کنند که چه مسائل فنی ممکن است پیش آید، از جمله اینکه وکلا به چه پلتفرم‌هایی نیاز دارند تا نمایش اسناد خود برای کمک به حقیقت‌یاب‌ها را تا حد امکان مؤثرتر کنند. در تصمیم‌گیری برای بهترین شکل ارائه داده‌های اصلی، یک رشته از عوامل باید در نظر گرفته شوند. این عوامل شامل مخاطبان مورد نظر، سطح آشنایی آنها با قالب‌های احتمالی و توانایی آنها در درک اطلاعاتی

---

[170] برای مثال نگاه کنید به: پلتفرم دیجیتال دیوان کیفری بین‌المللی: تیمبوکتو، مالی (تهیه شده توسط SITU Research به‌عنوان منبعی مفید برای پرونده احمد الفقی المهدی در دیوان کیفری بین‌المللی). قابل دسترسی در: http://icc-mali.situplatform.com. همچنین نگاه کنید به: مجموعه‌ای از تحقیقات آنلاین مبتنی بر منابع باز و گزارش‌های بصری آنها در Forensic Architecture. قابل دسترسی در: https://forensic-architecture.org/methodology/osint.

[171] اگرچه این توضیحات برای ارائه در دادگاه طراحی نشده‌اند، اما تیم تحقیقات بصری نیویورک تایمز تعدادی توضیحات بصری تولید کرده است که با هدف گردآوری اطلاعات منبع باز آنلاین، پشتیبانی از تحلیل حوادث پیچیده و گزارش کردنِ یافته‌ها طراحی شده‌اند. برای مثال، نیکلاس کیسی، کریستف کوتل و دبورا آکوستا در مقاله‌ای با عنوان «فیلمی که ادعای ایالات متحده مبنی بر اینکه نیکلاس مادورو کاروان کمک‌رسانی را آتش زد، نقض می‌کند» *نیویورک تایمز* [Nicholas Casey, Christoph Koettl and Deborah Acosta, “Footage contradicts U.S. claim that Nicolás Maduro burned aid convoy”]، 10 مارس ۲۰۱۹ قابل دسترسی در : www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html. ؛ مالاکی براون و دیگران در مقاله‌ای با عنوان «۱۰ دقیقه. ۱۲ انفجار تیراندازی. ۳۰ ویدئو. ترسیم کشتار لاس‌وگاس» نیویورک تایمز [Malachy Browne and others, “10 minutes. 12 gunfire bursts. 30 videos. Mapping the Las Vegas massacre”, New York Times]، ۲۱ اکتبر ۲۰۱۷ ، قابل دسترسی در : www.nytimes.com/video/us/100000005473328/las-vegas-shooting-timeline-12-bursts.html).

است که به آنها منتقل‌می‌شود.[172] در نهایت، تمام ارائه‌ها باید در راستای هدف روشن کردن حقایق مرتبط با یک پرونده عمل کنند، به شیوه‌ای که اثبات‌کننده باشد و نه جانبداری کننده، و همچنین با الزامات قانونی و اخلاقی حوزه قضایی که اطلاعات در آن ارائه می‌شود، مطابقت داشته باشند.

[172] نگاه کنید به :الکسا کینیگ، «شواهد منبع باز و پرونده‌های حقوق بشری: یک تاریخ اجتماعی مدرن»، در شاهد دیجیتال: استفاده از اطلاعات منبع باز برای تحقیقات حقوق بشر، مستندسازی وپاسخگویی، سم دوبِرلی، الکسا کینیگ و دارا موری [Alexa Koenig, "Open source evidence and human rights cases: a modern social history", in Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability, Sam Dubberley, Alexa Koenig and Daragh Murray] (آکسفورد، انتشارات دانشگاه آکسفورد، ۲۰۲۰)، صص 40-38.

8- واژه‌نامه

خلاصهٔ این فصل

- اصطلاحات و تعاریفی که در تحقیقات مبتنی بر منابع باز استفاده می‌شوند یا ممکن است در منابع مرتبط یا مشابه مطرح شوند.

218. این فصل شامل اصطلاحات و تعاریفی است که ممکن است برای محققان منابع باز مفید باشد. همه این اصطلاحات در این پروتکل استفاده نشده‌اند، اما در اینجا گنجانده شده‌اند زیرا ممکن است در منابع مرتبط یا مربوط با موضوع مطرح شوند.

شکاف هوا (Air gap): حالتی که در آن یک دستگاه دیجیتال به‌صورت مستقیم به اینترنت یا هیچ شبکه‌ای متصل نیست، و به این ترتیب امنیت اطلاعات ذخیره‌شده در آن دستگاه تأمین می‌شود.

الگوریتم (Algorithm): مراحلی مشخص و تعریف‌شده یا مجموعه‌ای از دستورالعمل‌ها که به یک رایانه امکان می‌دهد مسئله‌ای را حل کند یا به یک سناریوی از پیش تعیین‌شده پاسخ دهد.

ناشناس‌سازی (Anonymization): فرآیندی که طی آن شناسایی یک فرد مشخص غیرممکن شود.

رابط برنامه‌نویسی کاربردی (Application Programming Interface - API): کدی که امکان می‌دهد برنامه‌های نرم‌افزاری با یکدیگر ارتباط برقرار کنند.

هوش مصنوعی (Artificial Intelligence - AI): شاخه‌ای از علوم کامپیوتر که به توسعه برنامه‌نویسی برای ماشین‌ها اختصاص دارد تا بتوانند نحوه واکنش به متغیرهای ناشناخته را یاد بگیرند و خود را با محیط‌های جدید تطبیق دهند.

بیکن (Beacon): مکانیزمی برای ردیابی فعالیت‌ها و رفتار کاربران. بیکن‌ها از یک عنصر کوچک و نامحسوس (اغلب نامرئی) در یک صفحه وب تشکیل می‌شوند (به اندازه یک پیکسل شفاف) که هنگام نمایش توسط مرورگر، جزئیاتی درباره مرورگر و رایانه مورد استفاده را به یک شخص ثالث منتقل می‌کند.

داده‌های کلان (Big data): مجموعه‌های بزرگی از داده‌ها که می‌توان آنها را تحلیل کرد تا ارتباطات میان نقاط داده‌ها شناسایی و الگوهایی آشکار شوند که ممکن است به توانایی پیش‌بینی کمک‌کنند. از ویژگی‌های اصلی داده‌های کلان حجم بالا و پیچیدگی آنها است.

بلاک‌چین (Blockchain): فناوری مبتنی بر رمزنگاری که از یک دفتر کل باز و توزیع‌شده تشکیل شده است و شامل «بلوک‌ها» می‌باشد. از این فناوری می‌توان برای ثبت تراکنش‌ها بین دو طرف یا نهاد به‌صورت کارآمد، قابل تأیید و دائمی استفاده کرد.

جستجوی بولی (Boolean search): یک تکنیک جستجو در اینترنت است که به کاربران این امکان را می‌دهد تا کلمات کلیدی را با عملگرها یا اصلاح‌کننده‌هایی (مانند AND، NOT، OR) ترکیب کنند تا نتایج جستجو محدودتر شود و در نتیجه نتایج مرتبط‌تر و مشخص‌تری حاصل گردد.

کپچا (Captcha): سرواژه‌ای برای عبارت "Completely Automated Public Turing test to tell Computers and Humans Apart" (آزمون کاملاً خودکار عمومی تورینگ برای تشخیص انسان از رایانه)

است. کپچا نوعی آزمون چالشی-پاسخی در رایانه است که برای تعیین این‌که آیا کاربر انسان است یا خیر استفاده می‌شود.

اتاق گفتگو (Chat room): وب‌سایتی در اینترنت که به کاربران امکان می‌دهد به‌صورت آنلاین و بی‌درنگ با یکدیگر گفتگو کنند.

رایانش ابری (Cloud computing): مدلی عملیاتی که امکان ذخیره‌سازی، پردازش و تحلیل داده‌ها را از طریق یک شبکه داخلی (اینترانت) یا اینترنت فراهم می‌کند. رایانش ابری شامل سه نوع است: خصوصی، عمومی و ترکیبی.

کوکی (Cookie): قطعه‌ای کوچک از داده که توسط یک وب‌سایت ارسال شده و در حافظه رایانه کاربر یا روی دیسک رایانه ذخیره می‌گردد تا توسط مرورگر استفاده شود. کوکی‌ها اغلب برای عملکرد مؤثر یک وب‌سایت ضروری هستند، زیرا امکان ذخیره تنظیمات ترجیحی کاربران و جزئیات هویتی آنها را فراهم می‌کنند و نیاز به ورود مکرر اطلاعات توسط کاربران در بازدیدهای بعدی را از بین می‌برند.

امضای رمزنگاری‌شده (Cryptographic signature): یک فرآیند ریاضی برای تأیید اصالت یک مورد دیجیتال است. با استفاده از یک الگوریتم، دو کلید که به‌صورت ریاضی به یکدیگر مرتبط هستند تولید می‌شوند: یک کلید خصوصی و یک کلید عمومی. برای ایجاد یک امضای دیجیتال، نرم‌افزاری استفاده می‌شود تا از داده‌های الکترونیکی یک هش تولید کند. سپس، کلید خصوصی برای رمزگذاری این هش به کار می‌رود.

رمزنگاری (Cryptography): فرآیند کدگذاری یا رمزگشایی دیجیتالی اطلاعات.

وب تاریک (Dark web): بخشی از اینترنت که تنها از طریق نرم‌افزارهای ویژه قابل دسترسی است و به کاربران و گردانندگان وبسایت‌ها امکان می‌دهد ناشناس بمانند و ردیابی نشوند.

داده‌کاوی (Data mining): فرآیند بررسی و استخراج داده‌ها از پایگاه‌های داده برای تولید معلومات یا اطلاعات جدید.

آرشیو دیجیتال (Digital archive): مجموعه‌ای از اسناد، صفحات وب یا سوابق الکترونیکی. این اصطلاح همچنین ممکن است به یک سازمان رسمی یا غیررسمی نیز اشاره داشته باشد که مسئولیت حفظ اطلاعات و در دسترس گذاشتن آن به کاربران مجاز را بر عهده دارد.

حفاظت دیجیتال (Digital preservation): سیاست‌ها و راهبردهایی که برای مدیریت و نگهداری اطلاعات دیجیتال با ارزش ماندگار در طول زمان مورد نیاز است، به طوری که این اطلاعات دیجیتال در آینده برای کاربران مورد نظر قابل دسترسی و استفاده باشد.

نام دامنه (Domain name): برچسبی که یک دامنه شبکه را شناسایی می‌کند. در اینترنت، نام‌های دامنه بر اساس قوانین و رویه‌های سیستم نام دامنه (DNS) ایجاد می‌شوند. به طور کلی، نام دامنه نشانگر یک منبع پروتکل اینترنت (IP) است، از قبیل یک رایانه شخصی که برای دسترسی به اینترنت به کار می‌رود، سروری که میزبانی یک وب‌سایت را انجام می‌دهد، خود وب‌سایت، یا هر سرویس دیگری که از طریق اینترنت انتقال می‌یابد.

مالک نام دامنه (Domain name registrant): فرد، شرکت یا نهاد دیگری که مالک یا دارنده یک نام دامنه است.

سیستم نام دامنه (Domain Name System - DNS): سیستمی که از طریق آن تخصیص نام‌های دامنه تنظیم و مدیریت می‌شود.

درگ‌نت (Dragnet): در زمینهٔ محتوای آنلاین، به معنای یک سیستم خودکار گسترده برای جمع‌آوری یا نظارت داده‌ها است.

داده‌های جاسازی‌شده (Embedded data): داده‌هایی که در یک فایل منبع یا صفحه وب ذخیره شده‌اند.

رمزگذاری (Encryption): فرآیندی که طی آن داده‌ها بدون کلید رمزگشایی غیرقابل دسترسی می‌شوند.

هش یا کد هش (Hash or hash value): محاسباتی که می‌توان روی هر نوع فایل دیجیتال اجرا کرد تا یک رشته ثابت متشکل از حروف و اعداد تولید شود. این رشته می‌تواند به‌عنوان مدرکی مورد استفاده قرار گیرد که نشان دهد فایل دیجیتال تغییری نکرده است. این مقدار هر بار که محاسبه انجام شود، در صورتی که فایل تغییر نکرده باشد، یکسان باقی می‌ماند.

زبان نشانه‌گذاری ابرمتن (Hypertext Markup Language - HTML): یک زبان برنامه‌نویسی است که برای طراحی صفحات وب که از طریق مرورگر قابل دسترسی هستند، استفاده می‌شود.

پروتکل انتقال ابرمتن (Hypertext Transfer Protocol - HTTP): پروتکلی در بستر اینترنت که نحوه انتقال و دریافت داده‌ها را تعریف می‌کند.

مرجع واگذاری اعداد در اینترنت (Internet Assigned Numbers Authority - IANA): سازمانی که تخصیص جهانی آدرس‌های IP، اعداد سیستم خودگردان و سامانه‌های نام دامنه را مدیریت می‌کند.

آیکان - شرکت اینترنتی برای نام‌ها و اعداد واگذار شده (Internet Corporation for Assigned Names and Numbers - ICANN): سازمانی که مسئولیت تضمین عملکرد پایدار و امن اینترنت را با هماهنگی در نگهداری و ساز و کارهای چندین پایگاه دادهٔ مرتبط با فضای نام‌ها و اعداد در اینترنت بر عهده دارد.

انجمن اینترنتی (Internet forum) یا تابلوی گفتگو (Discussion board): وب‌سایتی است که کاربران می‌توانند از طریق آن پیام ارسال کنند و گفتگو داشته باشند. پیام‌های ارسال‌شده در انجمن‌ها معمولاً طولانی‌تر از پیام‌های اتاق‌های گفتگو هستند و محتوای آنها بیشتر احتمال دارد در آرشیو نگهداری شود.

نشانی پروتکل اینترنت (Internet Protocol - IP Address): هر دستگاه دیجیتالی که به اینترنت متصل می‌شود دارای یک نشانی IP است. دو نوع نشانی IP وجود دارد: IPv4 (یک عدد ۳۲ بیتی) و IPv6 (یک عدد ۱۲۸ بیتی). نشانی IP برای شناسایی رایانه‌ها و دیگر دستگاه‌ها در اینترنت استفاده می‌شود.

ارائه‌دهنده خدمات اینترنت (Internet Service Provider - ISP): نهادی که به کاربران اینترنت خدمات لازم برای دسترسی و استفاده از اینترنت را ارائه می‌دهد.

اینترانت (Intranet): یک شبکه رایانه‌ای خصوصی که از پروتکل‌های اینترنت و اتصالات شبکه برای ایجاد نسخه داخلی از اینترنت درون یک سازمان استفاده می‌کند.

شبکه محلی (Local Area Network - LAN): مجموعه‌ای از دستگاه‌های دیجیتال که در یک مکان فیزیکی مشخص به یک شبکه مشترک متصل هستند.

یادگیری ماشین (Machine Learning): نوعی از هوش مصنوعی است که از تکنیک‌های آماری استفاده می‌کند تا به رایانه‌ها توانایی «یادگیری» از داده‌ها را بدون اینکه به‌صورت آشکار برنامه‌ریزی شده باشند، می‌دهد.

بدافزار (Malware): نرم‌افزار مخربی که با هدف آسیب‌رساندن به یک دستگاه دیجیتال، شبکه، سرور یا کاربر طراحی شده است. انواع مختلف فراوانی از بدافزار وجود دارند، از جمله ویروس‌ها، اسب‌های تروا، باج‌افزار، تبلیغ‌افزار و جاسوس‌افزار.

فراداده (Metadata): داده‌هایی درباره داده‌ها هستند. آنها شامل اطلاعاتی درباره یک فایل الکترونیکی هستند که یا در فایلی جاسازی شده‌اند یا مربوط به آن هستند. فراداده‌ها اغلب شامل ویژگی‌ها و تاریخچه یک فایل، مانند نام، حجم، و تاریخ‌های ایجاد و ویرایش آن هستند. فراداده ممکن است توضیح دهد که یک فایل دیجیتال چگونه، چه زمانی، توسط چه کسی جمع‌آوری شده، به وجود آمده، دسترسی یافته، ویرایش و فرمت شده است.

فایل بومی (Native file): فایلی در قالب اصلی و اولیه خود.

فرمت متن قابل حمل – پی دی اف (Portable Document Format - PDF): یک فرمت فایل با ساختار ثابت که قالب یک متن (شامل فونت‌ها، فاصله‌ها و تصاویر) را صرف‌نظر از نرم‌افزار، سخت‌افزار یا سیستم‌عاملی که برای باز کردن و مشاهده آن استفاده می‌شود، حفظ می‌کند. تبدیل یک فایل از قالب اصلی خود به PDF فراداده‌های آن را حذف کرده و تصویری ثابت از سند ارائه می‌دهد.

نرم‌افزار پیش‌بینی‌کننده (Predictive software): نرم‌افزاری که از الگوریتم‌های پیش‌بینی و یادگیری ماشین برای تحلیل داده‌ها استفاده می‌کند تا پیش‌بینی‌هایی درباره رویدادها یا رفتارهای آینده یا ناشناخته ارائه دهد.

نام‌مستعارسازی (Pseudonymization): فرآیند پردازش داده‌های شخصی به‌گونه‌ای که اطلاعات دیگر قابل انتساب به یک فرد خاص نباشد، مگر با استفاده از اطلاعات افزوده.

داده‌کاوی (Scraping): روشی برای استخراج حجم زیادی از داده‌ها از وب‌سایت‌ها.

مهندسی اجتماعی (Social engineering): دستکاری روان‌شناختی یک فرد به‌منظور دسترسی غیرمجاز به اطلاعات. این روش مشابه هک کردن است اما به‌جای بهره‌برداری از یک ضعف فنی، از یک ضعف انسانی سوءاستفاده می‌کند. انواع مختلفی از مهندسی اجتماعی وجود دارد که از جمله آنها می‌توان به فیشینگ و فیشینگ هدفمند (Spear phishing) اشاره کرد.

حذف فراداده (Stripping): یک فرآیند فناوری برای حذف فراداده از یک فایل بدون تبدیل فایل مزبور به فرمت‌های دیگر.

داده‌های ساختاریافته (Structured data): داده‌ها یا اطلاعاتی هستند که با یک قالب ثابت و مشخص در یک مخزن (که معمولاً پایگاه داده است، اما می‌تواند مجموعه‌ای از فرم‌های پرشده نیز باشد) مطابقت می‌کنند، به‌طوری‌که عناصر آن به‌راحتی برای پردازش و تحلیل در دسترس هستند.

وب سطحی (Surface web): بخشی از اینترنت است که از طریق هر مرورگری قابل دسترسی می‌باشد و می‌توان آن را با استفاده از موتورهای جستجوی معمولی جستجو کرد.

ردیاب (Tracker): نوعی کوکی که از قابلیت مرورگر برای نگهداری سوابق صفحات بازدیدشده در وب، معیارهای جستجوی واردشده و غیره استفاده می‌کند. ردیاب‌ها معمولاً کوکی‌های پایداری هستند که یک گزارش مداوم از رفتار یک بازدیدکننده خاص را نگهداری می‌کنند.

داده‌های ترافیک (Traffic data): هرگونه داده‌ای است که برای انتقال اطلاعات در یک شبکه ارتباطات الکترونیکی یا برای صورتحساب مربوط به آن ارتباط پردازش می‌شود. این داده‌ها شامل اطلاعاتی درباره مسیریابی، زمان یا مدت‌زمان یک ارتباط هستند.

شناسه منبع یکنواخت (Uniform Resource Locator - URL): مکان یک صفحه وب در اینترنت که همان آدرس وب است.

داده‌های غیرساختاریافته (Unstructured data): داده‌ها و اطلاعاتی که به صورت‌های گوناگون وجود دارند و دارای قالب مشخص و سازمان‌یافته‌ای نیستند و بنابراین پردازش و تحلیل آنها آسان نیست. این داده‌ها معمولاً به صورت متن هستند، اما می‌توانند شامل فایل‌های تصویری، صوتی و ویدئویی نیز باشند.

ماشین مجازی (Virtual Machine): نرم‌افزاری که یک سیستم رایانه‌ای را شبیه‌سازی می‌کند.

شبکه خصوصی مجازی (Virtual Private Network - VPN): یک شبکه امن یا سیستمی از گره‌های امن که با استفاده از رمزنگاری و دیگر فرآیندهای امنیتی، دسترسی به شبکه را به کاربران مجاز محدود می‌کند. VPNها آدرس IP را پنهان کرده و از رهگیری داده‌ها جلوگیری می‌کنند.

ارائه‌دهنده خدمات مبتنی بر وب (Web-based service provider): نهادی که خدمات و محصولاتی را در اینترنت ارائه می‌دهد، مانند شرکت‌های شبکه‌های اجتماعی.

وب‌خزنده (Web crawler) که به آن عنکبوت وب یا اسپایدربات (spiderbot) نیز گفته می‌شود: برنامه‌ای که به‌صورت سیستماتیک اینترنت را طبق یک اسکریپت (کد) خودکار مرور می‌کند تا وب‌سایت‌های بازدیدشده را دانلود و فهرست‌بندی کند.

هو ایز (WHOIS): یک رکورد که بر اساس نهادی که آن نام دامنه را ثبت کرده مشخص می‌کند چه کسی مالک یک نام دامنه خاص است.. محققان منابع باز ممکن است از ابزار جستجوی WHOIS به‌عنوان بخشی از فرآیند تحلیل و راستی‌آزمایی منبع استفاده کنند.

شبکه جهانی وب (World Wide Web - WWW): فضای اطلاعات است که در آن اسناد و سایر منابع وب با استفاده از URLها شناسایی می‌شوند. URLها ممکن است از طریق ابرمتن به یکدیگر مرتبط باشند و از طریق اینترنت قابل دسترسی هستند. منابع موجود در شبکه جهانی وب می‌توانند با استفاده از یک نرم‌افزار کاربردی به نام مرورگر وب توسط کاربران قابل دسترسی شوند.

پیوست‌ها

خلاصهٔ این فصل

- الگوی برنامه‌ریزی تحقیقات آنلاین
- الگوی ارزیابی تهدیدها و ریسک‌های دیجیتال
- الگوی ارزیابی محیط دیجیتال
- فرم جمع‌آوری داده‌های آنلاین
- موارد قابل توجه برای اعتبارسنجی ابزارهای جدید

پیوست ۱

الگوی برنامه‌ریزی تحقیقات آنلاین

شماره مرجع تحقیق:

تاریخ ارزیابی:

خلاصه تحقیق: موضوع، محدوده جغرافیایی و زمانی تحقیق

۱. اهداف و فعالیت‌های برنامه‌ریزی‌شده

این بخش شامل اهداف و استراتژی تحقیق آنلاین، همچنین فعالیت‌های مشخص همراه با جدول زمانی برای اجرای آنها است.

۲. خلاصه ارزیابی محیط دیجیتال

این بخش شامل ارزیابی محیط دیجیتال در قلمرو جغرافیایی تحت تحقیق است، از قبیل شبکه‌های اجتماعی محبوب، برنامه‌های کاربردی موبایل و سایر فناوری‌ها، همچنین افرادی که به این فناوری‌ها دسترسی دارند و از آنها استفاده می‌کنند.

۳. استراتژی کاهش ریسک و اقدامات حفاظتی

این بخش شامل یافته‌های کلیدی ارزیابی تهدیدها و ریسک‌های دیجیتال، همراه با استراتژی شناسایی، مدیریت و پاسخگویی به اینگونه تهدیدها است.

۴. شناسایی و بررسی افراد و نهادهای مربوط

این بخش شامل فهرستی از این افراد است: نیروهای امداد که ممکن است محتوای آنلاین مرتبطی را جمع‌آوری کرده باشند که اکنون ناپدید شده است، ارائه‌دهندگان آرشیوهای دیجیتال و خدمات اینترنتی و مبتنی بر وب که ممکن است نسخه‌های اصلی یا فراداده‌های اضافی برای محتوای آنلاین را داشته باشند که می‌توان از طریق درخواست کمک، به دست آورد. اگرچه محققان غیرحقوقی ممکن است برای درخواست اطلاعات منبع بسته اختیارات قانونی نداشته باشند، اما ارتباط با ارائه‌دهندگان خدمات اینترنتی می‌تواند در پاسخ به سؤالات و کمک به کاربران برای پیمایش در پلتفرم‌های آنها ارزشمند باشد.

۵. نقش‌ها و مسئولیت‌ها

این بخش شامل تعیین نقش‌ها و مسئولیت‌های اعضای تیم است و باید شامل شناسایی یک هستهٔ مرکزی برای هماهنگی فعالیت‌های آنلاین باشد. این بخش همچنین ممکن است ارزیابی کند که در صورت احضار برای شهادت در دادگاه، چه کسی احتمالا این مسئولیت را خواهد داشت.

۶. منابع

این بخش شامل ارزیابی نیازهای نیروی انسانی (تعداد محققان، تنوع و فراگیر بودنِ اعضای تیم)، همچنین هرگونه آموزش تخصصی و تجهیزات مورد نیاز برای فعالیت‌های تحقیقاتی آنلاین است.

۷. مستندسازی

این بخش شامل دستورالعمل‌های مشخص در مورد نحوه و مکان مستندسازی فعالیت‌های تحقیقاتی آنلاین توسط اعضای تیم است.

پیوست ۲

الگوی ارزیابی تهدیدات و ریسک‌های دیجیتال

شماره مرجع تحقیق:
تاریخ ارزیابی:
خلاصه تحقیق: موضوع، محدوده جغرافیایی و زمانی تحقیق
اهداف تحقیقاتی:

۱. دارایی‌های شما چیست؟

افراد (تفکیک‌شده بر اساس جنسیت):
اموال ملموس:
اموال غیرملموس (مانند داده‌ها):

۲. آسیب‌پذیری‌های شما چیست؟

۳. چه نوع تهدیدهایی می‌توانند از این آسیب‌پذیری‌ها سوءاستفاده کرده و به دارایی‌های شما آسیب برسانند؟

۴. چه کسانی ممکن است عوامل تهدید بالقوه باشند؟

الف. منافع آنها چیست؟
ب. توانایی‌های آنها چیست؟
پ. احتمال وقوع یک حمله چقدر است؟

۵. چه اقداماتی برای کاهش ریسک ممکن/مناسب هستند؟ آیا نیاز به پاسخگویی به ریسک‌های متفاوتی که جنسیت‌های مختلف با آن مواجه هستند وجود دارد؟

موارد زیر باید در نظر گرفته شوند:

- آسیب‌های فیزیکی
- آسیب‌های دیجیتال
- آسیب‌های روانی

پیوست ۳

الگوی ارزیابی محیط دیجیتال

شماره مرجع تحقیق:

تاریخ ارزیابی:

خلاصه تحقیق: موضوع، محدوده جغرافیایی و زمانی تحقیق

اهداف تحقیقاتی:

علامت ستاره (*) نشان می‌دهد که محققان باید عوامل مختلفی مانند سن، جنسیت، موقعیت مکانی و سایر اطلاعات جمعیتی مربوط را در نظر بگیرند.

۱. طرف‌های مرتبط (مانند جوامع خاص، گروه‌های مسلح و غیره). مشخص کنید که آیا تفاوتی در استفاده از فناوری یا حضور آنلاین بر اساس جنسیت، سن یا معلولیت در میان هر یک از این طرف‌ها وجود دارد یا خیر.

۲. زبان‌های مرتبط (شامل اصطلاحات عامیانه و زبان‌های خاص داخلی)*

۳. موتورهای جستجویی که غالباً استفاده می‌شوند*

۴. پلتفرم‌های پرطرفدار شبکه‌های اجتماعی*

۵. وب‌سایت‌های پرطرفدار*

۶. استفاده از / نفوذ در اینترنت (تفکیک‌شده بر اساس جنسیت، سن و غیره)

۷. ترجیحات مربوط به تلفن همراه/سیستم‌عامل (تفکیک‌شده بر اساس جنسیت، سن و غیره)

۸. برنامه‌های کاربردی پرطرفدار موبایل (تفکیک‌شده بر اساس جنسیت، سن و غیره)

۹. ارائه‌دهندگان خدمات مخابراتی

۱۰. اتصال: مکان‌های وای‌فای/برج‌های مخابراتی

۱۱. قوانین مرتبط (آزادی بیان، دسترسی به اطلاعات، حریم خصوصی)

۱۲. رسانه‌ها و خبرنگاران (حضور آنلاین)

۱۳. پایگاه‌های داده باز (مانند داده‌های دولتی، داده‌های سازمان‌های غیردولتی/پژوهشگران)

۱۴. پایگاه‌های دادهٔ مشمولِ هزینه (مانند داده‌های دولتی، داده‌های شرکت‌های خصوصی/پژوهشگران)

۱۵. نمایندگی محتوای آنلاین (گروه‌های شامل‌شده در مقابل گروه‌های حذف‌شده)

پیوست ۴

فرم جمع‌آوری داده‌های آنلاین

۱. اطلاعات جمع‌آوری‌کننده

تحقیق:
جمع‌آوری‌کننده:
نشانی IP جمع‌آوری‌کننده:
شروع جمع‌آوری (تاریخ/زمان):
پایان جمع‌آوری (تاریخ/زمان):

۲. اطلاعات هدف

آدرس وب (URL):
کد منبع HTML:
تصویر صفحه (اسکرین‌شات):
داده‌های ثبت‌شده:
نشانی IP:

۳. اطلاعات بستهٔ جمع‌آوری

نام فایل بستهٔ جمع‌آوری:
فهرست هش بستهٔ جمع‌آوری:
هشِ فایلِ فهرستِ هشِ بستهٔ جمع‌آوری:

۴. خدمات استفاده‌شده

محصول(ات) نرم‌افزاری:
سرویس زمان:
سرویس IP:
سرویس WHOIS:

پیوست ۵

موارد قابل توجه برای اعتبارسنجی ابزارهای جدید

ویژگی‌ها

کد منبع باز در مقابل کد منبع بسته
رایگان در مقابل غیر رایگان
هویت مالک (فرد یا شرکت)، وابستگی‌ها یا منافع
منابع مالی (این ابزار چگونه و تا چه حد تأمین مالی شده است؟ طول عمر احتمالی محصول چقدر است؟)

سؤالات امنیتی

چه کسی مالک ابزار یا کد زیربنایی آن است؟
آیا کد زیربنایی، متعلق به منبع باز است یا منبع بسته؟
آیا ابزار به‌صورت مستقل مورد ارزیابی قرار گرفته است؟
داده‌های جمع‌آوری‌شده کجا ذخیره خواهند شد؟
چه کسانی به داده‌های جمع‌آوری‌شده دسترسی خواهند داشت؟
ساختار امنیتی ابزار چگونه است؟
کدام الزامات قانونی ممکن است بر امنیت استفاده از ابزار تأثیر بگذارد؟
اگر نقض قانون رخ دهد، آیا حقی برای غرامت وجود دارد؟

سؤالات عملیاتی

کاربرد این ابزار چیست؟
قابلیت استفاده از این ابزار چگونه است؟
ظرفیت پشتیبانی مالک، تهیه کننده یا کاربران ابزار چقدر است؟
این ابزار هر چند وقت یک‌بار به‌روزرسانی می‌شود؟
این ابزار تا چه حد با سایر سیستم‌ها سازگار است؟