صداوسیمای جمهوری اسلامی ایران
معاونت سیاسی
اداره پژوهش‌های سیاسی

اوسینت(OSINT)
و حفاظت از حریم شخصی

فرآورده‌های خبری و تولیدات پژوهشی در بخش های زیر قابل دسترس است:
ـ وب سایت خبرگزاری صداوسیما (سرویس پژوهش) http://www.iribnews.ir

پژوهشگر: یاسر بهشتی

فـهرسـت مـطالـب

عنـــــوان **صفحـــــه**

بسمه تعالی

❖ چکیده:

- در عصر حاضر به شکل حیرت انگیزی مقدار اطلاعات تولید شده توسط انواع رسانه‌ها اعم از دولتی و خصوصی مانند بنگاه‌های خبری و رادیو تلویزیون‌ها یا توسط اشخاص حقیقی در شبکه‌های اجتماعی در سرتاسر جهان دائماً در حال افزایش است و هر کدام از این منابع از ابعاد مختلفی چون، ماهیت، کمیت، اعتبار، کیفیت یا زبان مورد ا ستفاده با هم متفاوتند و به انواع خا صی از پردازش نیاز دارند.
- امروزه افراد اطلاعاتی از دارایی‌ها، تماس‌ها و ارتباطاتشان، زندگی شخصی شان، جغرافیا و محل سکونت خود را در بستر سایبر منتشر می‌کنند و این خطر از آنجایی آغاز می‌شود که در وب «همه چیز» ذخیره می‌شود.
- اوسینت یا "پایش اطلاعات آشکار "مخفف Open Source Intelligence مهارت کشف و جمع آوری اطلاعات از طریق منابع آزاد و باز اطلاعات است. در واقع اوسینت ترکیبی است از تکنیک‌های جستجوی حرفه‌ای، تحلیل منابع، داده‌کاوی، مهارت‌های حل مسئله و خلاقیت است.
- این "پایش اطلاعات" از آن جهت آ شکار نامیده می شود که به اطلاعات "غیرمحرمانه" د ست پیدا کرده و می‌توان با در کنار هم قرار دادن این اطلاعات، داده‌های خود را تکمیل نمود. منابع مر سومی که برای "پایش اطلاعات آ شکار" یا همان "اوسینت" به کار می‌رود، عبارتند از شبکه‌های مجازی، انجمن‌ها، وبسایت‌های تجاری، وبلاگ‌ها و منابع خبری. OSINT بسیار صریح و بدون پیچیدگی است و اطلاعاتی که با اوسینت جمع‌آوری می‌شود، "غیرمحرمانه" و "در دسترس" است.
- به مدد ظهور فناوری‌های نوین عرصه دیجیتال در حالی صحبت از نسل‌های دوم و سوم آن به میان آمده که از آن به دلیل کارکرد مستقیمی که در تکمیل اطلاعات طبقه‌بندی شده دارد به عنوان یک نظام اطلاعاتی و امنیتی هم یاد می‌شود.
- نکته کلیدی؛ همان قدر که اوسینت (OSINT) کردن ارزشمند است، اوسینت نشدن ضروری و حیاتی است. لذا داده‌های منبع آزاد که به صورت تک، کم‌ارزش به شمار می‌آیند اما در صورت احصاء، واجد ارزش می شوند. بنابراین هم شخص و هم سازمان باید بداند چه چیزی از خود منتشر می‌کند.
- آنچه به راهکار پیشنهادی در این ارتباط ارائه می‌شود ایجاد آشنایی عمومی با اوسینت، کمک به ارتقای سطح سواد دیجیتال عنوان در جامعه و افزایش تفکر انتقادی در مواجهه با تهدیدات سایبری است.

❖ **مقدمه:**

در عصر حاضر به شکل حیرت‌انگیزی مقدار اطلاعات تولیدشده توسط انواع رسانه‌ها اعم از دولتی و خصوصی مانند بنگاه‌های خبری و رادیو تلویزیون‌ها یا توسط اشخاص حقیقی در شبکه‌های اجتماعی در سرتاسر جهان دائماً درحال افزایش است و هر کدام از این منابع از ابعاد مختلفی چون، ماهیت، کمیت، اعتبار، کیفیت یا زبان مورد استفاده با هم متفاوتند و به انواع خاصی از پردازش نیاز دارند. در این دنیای دیجیتال، میلیاردها صفحه‌ی وب وجود دارد که هرکدام از آن‌ها صفحات حاوی اطلاعات ه ستند. ب سیاری از این اطلاعات آزادانه در دسترس عموم مردم قرار گرفته‌اند. مطالب فرم‌ها، اخبار سایت‌ها، نظرات و پیام‌های شبکه‌های اجتماعی، داد شنامه‌ها و فیلم‌ها تنها گو شه‌ای از این مجموعه‌ی ب سیار و سیع ه ستند. منابع اطلاعاتی را به شکل‌های مختلفی طبقه بندی می‌کنند یکی از مهمترین آنها، منابع باز Open Source هستند.

این اصطلاح که در توسعه نرم‌افزار و ایجاد یک روش خاص در تولید برنامه‌های کامپیوتری ریشه دارد، اساساً به چیزی اطلاق می‌شود که امکان ویرایش و اشتراک‌گذاری آن برای همه فراهم است. اهمیت پردازش و پالایش داده از آنجا مهم است که در اوسینت اگر کسی تکنیک‌های دستیابی به اطلاعات را بداند و در استفاده از این تکنیک‌ها مهارت پیدا کند، می‌تواند به راحتی و در زمانی معقول با صرف هزینه‌ی معقول در قیاس با سایر رویکردها به این اطلاعات د ستر سی پیدا کند؛ اطلاعاتی که در ظاهر برای ناشرش اهمیت چندانی ندارند اما در واقع می‌توانند در بسیاری از موارد بسیار گرانبها باشند. اینجاست که بهره‌برداری از انواع منابع به خصوص منابع باز اهمیت پیدا می‌کند.

❖ **بیان مسئله:**

جاسوسی و کاسبی محترمانه اینترنتی در کار است؟

مثال ملموس این امر گوگل ا ست. گوگل با شبکه گسترده – و البته جذّاب – محصولات خود (از سرچ و جیمیل و عکس و مپ تا یوتیوب و اندروید و محصولات سخت افزاری آن) ما را در دام خود گیر انداخته است، به‌طوریکه دیگر زندگی در دنیای اینترنت، یعنی ورود اجباری به حصار محصولات گوگل. البته این موضوع به تنهایی ایراد ندارد؛ گوگل خلّاق است، نیازها را خوب شناسایی و خوب پاسخ می‌دهد و هر کسی به محصولات آن تن می‌دهد. اما این را هم باید پذیرفت که گوگل نمی‌تواند از کنار اطلاعات کاربران بی‌شمار خود ساده عبور کند! (فقط پلتفرم اندروید گوگل در سال ۲۰۱۷، دو میلیارد کاربر فعال داشته است!)

در واقع هر بار که از محصولات و خدمات این غول دنیای تکنولوژی استفاده می‌کنیم، بایگانی اطلاعات شخصی ما بزرگ‌تر می‌شود و فرقی نمی‌کند که این ا ستفاده در وبگردی و ار سال ایمیل با شد یا ا ستفاده از برنامه‌های مختلف و ا ستفاده از گو شی هو شمند. گوگل به عکس‌ها و فیلم‌ها دسترسی دارد(Google Photos) ، ایمیل‌ها را می‌داند(Gmail) ، از تماس‌ها و ارتباطات با خبر است (Google Contacts) ، از فایل‌ها و اسناد حفاظت می‌کند(Google Drive) ، دقیقاً می‌داند که کجا از GPS استفاده و کِی کجا بودیم (Google Maps) و ... طبیعتا داشتن این حجم از اطلاعات یقیناً وسوسه کننده است!

آیا نمی شود گفت علاوه بر جا سو سی، کا سبی محترمانه هم در جریان ا ست چون گوگل، رایگان ا ست و تقریبا برای هیچ یک از مح صولات خود پولی از کاربران نمی‌گیرد! پس چرخه مالی این شرکت چطور می‌گردد؟! هرچند پا سخ رو شن ا ست. گوگل یک شرکت دنیای دیجیتال است و چرخه مالی آن نیز بر پایه اطلاعات می‌چرخد و البته چه اطلاعاتی سهل الوصول تر از اطلاعات کاربران خودش. **حال سؤال اینجاست آیا فقط گوگل این کار را می‌کند؟**

❖ تعریف اوسینت:

اوسینت نوعی پژوهش است که در آن به صورت آگاهانه منابع بسیاری بررسی می‌شود تا دید جامع‌تری نسبت به یک موضوع ایجاد شود. در عین حال در او سینت فهم علل یک پدیده مد نظر نی ست. به این معنا که بر خلاف پژوهش‌های معمول که با هدف ایجاد ابزاری برای پیش‌بینی انجام می‌شوند، در اوسینت هدف جمع‌آوری هرچه بیشتر منابع مفید و فکت‌های قابل استفاده است.

او سینت مخفف Open Source Intelligence مهارت کشف و جمع آوری اطلاعات از طریق منابع آزاد و باز اطلاعات است. در واقع اوسینت ترکیبی است از تکنیک‌های جستجوی حرفه‌ای، تحلیل منابع، داده‌کاوی، مهارت‌های حل مسئله و خلاقیت است.

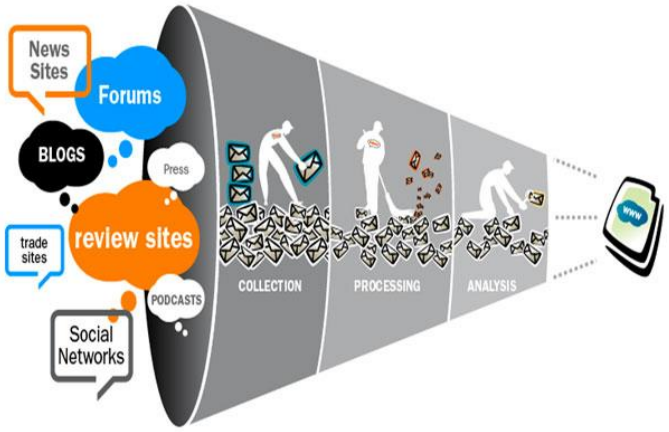
در او سینت، تنها به جستجوی اطلاعات عمومی پرداخته می شود. جستجوی اطلاعات شخصی افراد، نفوذ به شبکه‌های خصوصی، هک، استفاده از هرنوع ابزار غیرقانونی و همچنین دزدی اطلاعات، جایی در این فن ندارد. با این حال، عمده‌ی مردم به اطلاعاتی که در وب به اشـتراک می‌گذارند، توجه چندانی نشـان نمی‌دهند. به این ترتیب با اسـتفاده از این تکنیک‌ها، گاها اطلاعاتی به دسـت می‌آید که دست کمی از نفوذ به اطلاعات خصوصی مردم ندارد.

اهل فن، آن‌را به "پایش اطلاعات آ شکار" ترجمه نموده‌اند. این "پایش اطلاعات" از آن جهت آ شکار نامیده می شود که به اطلاعات "غیرمحرمانه" دسـت پیدا کرده و می‌توان با در کنار هم قرار دادن این اطلاعات، داده‌های خود را تکمیل کرد. منابع مرسـومی که برای "پایش اطلاعات آشـکار" یا همان "اوسـینت" به کار می‌رود، عبارتند از شـبکه‌های مجازی، انجمن‌ها، وبسـایت‌های تجاری، وبلاگ‌ها و منابع خبری.

OSINT بسیار صریح و بدون پیچیدگی است و اطلاعاتی که با اوسینت جمع‌آوری می‌شود، "غیرمحرمانه" و "در دسترس" است مثال‌هایی از این پایش به ترتیب ذیلند:

- جستجو کردن هر چیزی در موتورهای جستجو مانند گوگل و بینگ و ...
- تحقیق درباره یک مطلبی در انجمن ها و فروم ها و ...
- مشاهده یک ویدیو در شبکه های اجتماعی مانند یوتیوب و ...

در مجموع باید گفت می‌توان با اوسینت اطلاعاتی مانند نام کاربری، ایمیل، آدرس IP ، دامنه ها، فیلم ها، اخبار، مقالات، شبکه های اجتماعی، جستجوی مردم، شماره تلفن ها، حمل و نقل، نقشه ها، آر شیوها ، ابرداده، موتورهای جستجو، دارک وب، ارز دیجیتال، ابزار، محتوای مخرب، مستندات و غیره را به دست آورد.



❖ کارکردهای اوسینت:

- از دیدگاهی می‌توان او سینت را «کارآگاه» نامید. یعنی او سینت‌کار مثل یک کارآگاه به دنبال کشف پاسخ یک سؤال در منابع عمومی که در دسترس همه قرار دارد می‌گردد.
- علاوه بر پلیس، خبرنگاران نیز از ابزارهای اوسینتی برای پرده برداری از فسادها، حملات تروریستی، تاریخچه‌ی سیاستمداران و دیگر موضوعات مرتبط با کار خود استفاده می‌کنند و در واقع یکی از ابزارهای خبرنگاران تحقیقی برای کارهایی که انجام می‌دهند همین ابزارهای اوسینتی است
- از مهمترین کارکردهای این شیوه از پایش اطلاعات، استفاده از آن در انواع بحران‌ها ست. با توجه به اینکه زبان، نقشی حیاتی در این پردازش ایفا می‌کند و اغلب یکی از مشکلات کلیدی در فجایعی با ابعاد جهانی این است که اطلاعات فقط از منابع محلی و به زبان‌های بومی در دسترس هستند، برخی از فوری‌ترین اطلاعات در مورد یک رخداد، ممکن است توسط خبرنگاران بومیِ کم‌تجربه تولید شده باشند و سابقه‌ی اندکی از آنها موجود باشد که بتواند به‌طور مستقل مورد بررسی قرار گیرد. منابع باز، راهی ارزان، سریع و کارآمد جهت ارزیابی موقعیت آنهایی به‌دست می‌دهند که در زمان یک بحران یا فاجعه، از آن تأثیر می‌پذیرند. این منابع، اطلاعات جمع‌آوری شده توسط منابع سنتی و رسمی را تکمیل، تقویت و حتی اغلب شکار می‌کنند. در بسیاری از موارد آنها امکان نقشه‌برداری جغرافیاییِ رخدادها را فراهم می‌آورند، این مسئله به‌خصوص درمورد جمع‌آوری اطلاعاتِ با استفاده از منابع جمعی و برون‌سپاری صدق می‌کند. تعداد و تنوع منابع به سازمان‌ها کمک می‌کند تا درستی و سطح اعتبار اطلاعات فراهم‌شده را تخمین بزنند، بدین ترتیب امکان بروز پاسخ‌های هدفمندتر و چرخه‌ی تصمیم‌گیری کوتاه‌تر در شروع واکنش‌های اولیه را فراهم می‌سازند. یکی از پیش‌فرض‌های اساسی در مفهوم اطلاعات منبع باز این است که در واقع در منابعِ در دسترس عموم، موجودند و تنها کافی است جمع‌آوری شده و در اختیار اشخاص درست در زمان درست قرار گیرند.

❖ اوسینت و امنیت سایبری

این مفهوم یکی از جنبه‌های مهم در درک امنیت سایبری نیز به شمار می‌آید که امروزه اینترنت را کنترل می‌کند. این اصطلاح از چندین دهه پیش وجود دارد؛ در واقع، سازمان‌های نظامی ایالات متحده در اواخر سال ۱۹۸۰ میلادی با استفاده از آن شروع به استفاده از اطلاعات مورد نیاز در سطوح تاکتیکی در میدان های جنگ کردند سپس در سال ۱۹۹۲، اهداف اصلی جمع آوری اطلاعات شامل مفاهیمی کلیدی را انشاء کردند که از آن جمله موارد زیر است:

باید اطلاعات عینی بدون تعصب باشد.

داده ها باید در منابع عمومی و غیر عمومی در دسترس باشند.

❖ محبوب ترین تکنیک های OSINT در امنیت سایبری

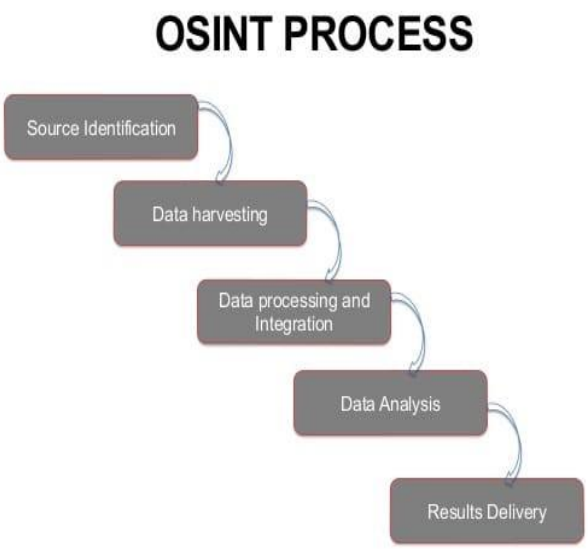
- جمع آوری اسامی کارکنان یک سازمان، نقش های کاری و همچنین نرم افزارهایی که آنها استفاده می‌کنند.
- مرور و نظارت بر اطلاعات موتورهای جستجو مانند گوگل، بینگ و ...
- نظارت بر وبلاگ شخصی و شرکتی مورد نظر، و همچنین بررسی فعالیت کاربر در انجمن ها و فروم ها
- شناسایی تمام شبکه های اجتماعی که توسط کاربر یا شرکت هدف مورد استفاده قرار می‌گیرد

- محتوای اشتراکی موجود در شبکه های اجتماعی مانند فیس بوک، توییتر یا لینکدین و ...
- اســـتفاده از ابزار جمع آوری داده ها مانند maltego ، که کمک می‌کند تا اطلاعات زیادی در مورد ســـازمان ها به دست آید
- دسترسی به داده های ذخیره شده قدیمی در Google که می‌تواند اطلاعات جالبی را نشان دهد
- بررسی نسخه‌های قدیمی وب سایت ها برای یافتن اطلاعات مهم با استفاده از سایت هایی مانند سایت آرشیو
- شناسایی شماره تلفن همراه، آدرس پست الکترونیکی از شبکه های اجتماعی یا نتایج
- جســـتجو برای عکس ها و فیلم ها در ســـایت‌های به اشـــتراک گذاری عکس مشـــترک اجتماعی مانند Google Photos و ...
- استفاده از نقشه های گوگل و دیگر منابع تصاویر ماهواره‌ای رایگان برای بازیابی تصاویر جغرافیایی کاربران
- ردیابی اطلاعات موقعیت مکانی جغرافیایی تا تصویر واضحی از مکان های فعلی کاربران به دست آید

❖ رویکرد اوسینت

رویکرد اوسینت شامل مجموعه‌ای از مهارت‌هاست که امکان دسترسی هوشمندانه به اطلاعات قابل دسترس در وب برای پاسخ به یک سؤال کاملا رو شن را فراهم می‌کند و پس از آن این اطلاعات را برای پردازش و تحلیل در اختیار متخ ص صان قرار می‌دهد. در اوسینت، فرض بر این است که غالب اطلاعات مدنظر در وب به اشتراک گذاشته شده‌اند. حال از طریق سازمان‌ها یا مردم عادی در سایت‌های ر سمی شان یا در شبکه‌های اجتماعی، از طریق هکرها در منابعی مثل ویکی‌لیکس و یا به هر روش دیگری در هرجای دیگری به جستجوی این اطلاعات می‌پردازیم.

❖ مراحل اوسینت



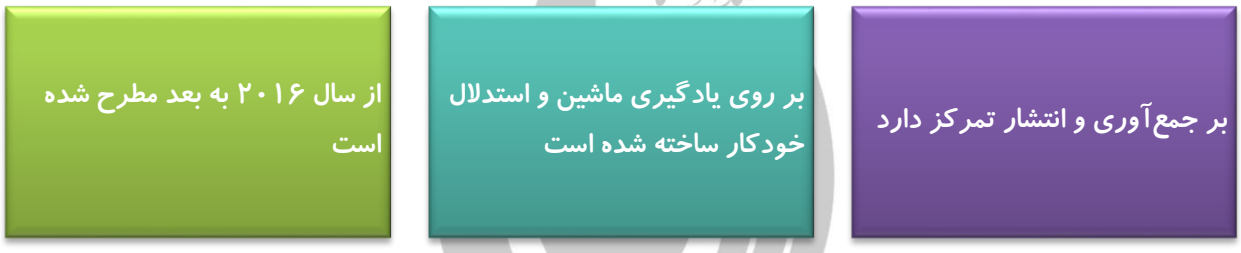
او سینت شامل مراحل مختلفی ا ست. در ابتدا منبع م شخص و داده ها جمع آوری می شود، بعد از یافتن اطلاعات، تحلیل آن فرا می‌رسد. موقع تحلیل، از هر داده‌ای می‌توانیم استفاده کنیم. اگر شخصی مهارت دستیابی به اطلاعات را بداند و در به کار بردن این تکنیک‌ها مهارت پیدا کند، می‌تواند به راحتی و در زمان کمی با صرف هزینه‌ی مناسب در مقابل با سایر روش خود به این اطلاعات دسترسی پیدا کند، برخی اطلاعات در ظاهر برای صاحبش مهم نیستند اما ممکن است برای دیگر افراد با ارزش باشند.

❖ نسل‌های مختلف اوسینت

نسل اول:

نسل دوم:

نسل سوم:



❖ جمع‌بندی و نتیجه:

ماهیت همپوشانی اوسینت با سایر رشته‌های اطلاعاتی اگرچه منحصر به فرد نیست اما از قلمداد شدن آن به عنوان یک رشته در این حوزه مانع نمی‌شود.

آنچه در چرخه اطلاعاتی او سینت (شامل جمع‌آوری، پردازش، بهره‌برداری و تولید) مهم و مفید ا ست تق سیم آن به زیرگروه‌ها به ویژه نهادی یا فردی ا ست چراکه قطعا با این روش تو صیف بهتری ارائه می شود. از طرفی د شواری درک منابع و روش‌های پویا در رسانه‌های اجتماعی نیز بدین طریق تا حد زیادی قابل حل ا ست که همانا از چالش های اوسینت نحوه محافظت از افراد و مدیریت مقادیر گسترده داده‌هاست.

از دیگر سو اوسینت امروزه از نظر منابع و روش ها به ویژه با ظهور رسانه‌های اجتماعی و اضافه شدن قابلیت‌هایی چون تولید محتوای آنلاین، بسیار پیچیده شده و طبیعتا ماهیت آن تغییر پیدا کرده است در نتیجه تلفیق قدرت رایانه و تکنیک‌های دانش داده، امکان حفظ و پردازش مقادیر انبوه داده‌های در دسترس عموم را افزایش می‌دهد.

در مجموع باید گفت اگرچه بیش از نیم قرن ا ست که جامعه اطلاعاتی درگیر این مبحث ا ست اما امروزه از نسل قدیمی آن عبور و به مدد ظهور فناوری‌های نوین عرصه دیجیتال در حالی صحبت از نسل‌های دوم و سوم آن به میان آمده که از آن به دلیل کارکرد مستقیمی که در تکمیل اطلاعات طبقه‌بندی شده دارد به عنوان یک نظام اطلاعاتی و امنیتی هم یاد می‌شود.

اما نکته کلیدی؛ همان قدر که اوسینت (OSINT) کردن ارزشمند است، اوسینت نشدن ضروری و حیاتی است.

در همین مسیر باید بدانیم چطور امنیت اکانت‌هایمان را بالا ببریم و چه کنیم تا حساب‌هایمان کاملا تحت کنترل خودمان باشد و از دست هکرها نیز در امان باشیم.

ابتدایی‌ترین کار در باب اهمیت دادن به پاد اوسینت و حفظ اطلاعات در اینترنت، مدیریت پسوردها، ساختن پسورد قوی و تعیین هویت دو مرحله‌ای، به علاوه لزوم آشنایی با هر آنچه امنیت حریم خصوصی را مورد تهدید قرار می‌دهد است؛ این که مراقب باشیم در ارتباط با دیگران چه اطلاعاتی به آنها انتقال می‌دهیم، موضوعی که ساده به نظر می‌رسد، اما امروزه کلاه‌برداری و اخاذی از این طریق به شدت شیوع یافته است

بسیار راحت امروزه افراد اطلاعاتی از دارایی‌ها، تماس‌ها و ارتباطاتشان، زندگی شخصی‌شان، جغرافیا و محل سکونت خود را در بستر سایبر منتشر می‌کنند این خطر از آنجایی می‌آید که در وب «همه چیز» ذخیره می شود. به همین دلیل باید مراقب بود. اول اینکه به «چه کسانی» اجازه‌ی ذخیره کردن اطلاعات خود را می‌دهیم. دوم اینکه این افراد اطلاعات شما را «در کجا» ذخیره می‌کنند. باید مراقب انتخاب مسیر ارسال پیام نیز بود.

لذا داده‌های منبع آزاد که به صورت تک، کم ارزش به شمار می‌آیند اما در صورت احصاء، جمعی از آنها ارز شمند می شوند. هم شخص و هم سازمان باید بداند چه چیزی از خود منتشر می‌کند.