ARTIKEL 29-ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER

0829/14/EN
WP216

Yttrande 05/2014 om avidentifieringsmetoder

Antaget den 10 april 2014

Arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet.Dess uppgifter beskrivs i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

Gruppens sekretariat finns hos direktorat C (Grundläggande rättigheter och unionsmedborgarskap) på Europeiska kommissionen, Generaldirektoratet för rättsliga frågor, BE-1049 Bryssel, Belgien, kontor MO-59 02/013.

Webbplats:http://ec.europa.eu/justice/data-protection/index_en.htm

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLING AV PERSONUPPGIFTER HAR ANTAGIT DETTA YTTRANDE

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995,

med beaktande av artiklarna 29 och 30 i det direktivet, och

med beaktande av dess arbetsordning.

SAMMANFATTNING

I detta yttrande analyserar arbetsgruppen befintliga avidentifieringsmetoders effektivitet och begränsningar mot bakgrund av EU:s bestämmelser om uppgiftsskydd. Arbetsgruppen lämnar rekommendationer om hur dessa metoder bör hanteras genom att beakta den kvarstående risken för identifiering i samband med var och en av dem.

Arbetsgruppen är medveten om det potentiella värdet av avidentifiering, särskilt som en strategi för att låta enskilda och samhället i stort dra nytta av ”öppna data”, om man samtidigt minskar riskerna för de berörda personerna. Fallstudier och forskningsrapporter har dock visat hur svårt det är att skapa helt anonyma dataset och samtidigt behålla så mycket av den underliggande informationen som krävs för ändamålet.

Enligt direktiv 95/46/EG och andra relevanta EU-rättsakter är avidentifiering resultatet av behandling av personuppgifter för att oåterkalleligen förhindra identifiering. När detta utförs bör den registeransvarige beakta flera aspekter beträffande alla hjälpmedel som ”rimligen” kan komma att användas för identifieringen (antingen av den registeransvarige eller av någon annan person).

Avidentifiering utgör en senare behandling av personuppgifter och måste som sådan uppfylla förenlighetskraven genom att man beaktar de rättsliga grunderna och omständigheterna för den senare behandlingen. Avidentifierade uppgifter omfattas dessutom inte längre av lagstiftningen om skydd av personuppgifter, men registrerade kan fortfarande ha rätt till skydd enligt andra bestämmelser (t.ex. bestämmelser om skydd av konfidentialiteten vid kommunikation).

I yttrandet beskrivs de viktigaste avidentifieringsmetoderna, nämligen randomisering och generalisering. Tillägg av brus, permutation, differentiell integritet, aggregering, *k*-anonymitet, *l*-diversitet och *t*-närhet diskuteras särskilt. Principerna för dessa metoder förklaras liksom deras starka och svaga sidor samt ofta förekommande misstag och försummelser i samband med användningen av respektive metod.

I yttrandet behandlas tillförlitligheten hos respektive metod utifrån tre kriterier:

(i) Går det fortfarande att särskilja en person?

(ii) Går det fortfarande att länka till registerposter som rör en enskild person?

(iii) Går det att sluta sig till uppgifter om en enskild person?

Om man känner till varje metods viktigaste starka och svaga sidor är det lättare att välja hur en lämplig avidentifieringsprocess ska utformas i ett visst sammanhang.

Pseudonymisering tas också upp för att klargöra vissa fallgropar och missuppfattningar: Pseudonymisering är inte en metod för avidentifiering. Den minskar endast möjligheten att länka ett dataset till den registrerades ursprungliga identitet och är därför en användbar säkerhetsåtgärd.

Slutsatsen i yttrandet är att avidentifieringsmetoder kan ge integritetsgarantier och kan användas för att skapa effektiva avidentifieringsprocesser, men endast om tillämpningen av dem är utformad på lämpligt sätt. Det innebär att förutsättningarna (sammanhanget) och målet eller målen för avidentifieringsprocessen måste fastställas tydligt så att den avsedda

avidentifieringen uppnås samtidigt som användbara uppgifter produceras. Vad som är den bästa möjliga lösningen bör bestämmas från fall till fall, eventuellt med hjälp av en kombination av olika metoder, samtidigt som man tar hänsyn till de praktiska rekommendationerna i detta yttrande.

Slutligen bör den registeransvarige tänka på att ett avidentifierat dataset fortfarande kan innebära kvarstående risker för de registrerade. Avidentifiering och återidentifiering är aktiva forskningsområden och nya upptäckter offentliggörs regelbundet, men även avidentifierade uppgifter, som t.ex. statistik, kan användas för att utöka enskilda personers befintliga profiler och därigenom skapa nya problem beträffande skyddet av personuppgifter. Avidentifiering bör därför inte betraktas som en engångsåtgärd, och de registeransvariga bör regelbundet ompröva riskerna med deltagandet.

1 Inledning

I takt med att komponenter, sensorer och nätverk skapar stora datavolymer och nya typer av uppgifter, och kostnaderna för lagring av uppgifter blir alltmer försumbar, finns det ett växande allmänt intresse för och efterfrågan på återanvändning av dessa uppgifter. ”Öppna uppgifter” kan vara till klar fördel för samhället, enskilda och organisationer, men endast om allas rätt till skydd av sina personuppgifter och sitt privatliv respekteras.

Avidentifiering kan vara en bra strategi för att behålla fördelarna och minska riskerna. När ett dataset är helt avidentifierat och enskilda personer inte längre kan identifieras är EU-lagstiftningen om uppgiftsskydd inte längre tillämplig. Det framgår emellertid tydligt av fallstudier och forskningspublikationer att det inte är en enkel uppgift att skapa ett helt avidentifierat dataset från ett en innehållsrik samling av personuppgifter och samtidigt behålla så mycket av den underliggande informationen som krävs för ändamålet. Exempelvis kan ett dataset som anses vara avidentifierat kombineras med andra dataset på ett sådant sätt att en eller flera personer kan identifieras.

I detta yttrande analyserar arbetsgruppen befintliga avidentifieringsmetoders effektivitet och begränsningar mot bakgrund av EU:s rättsliga uppgiftsskydd och lämnar rekommendationer om en försiktig och ansvarsfull användning av dessa metoder för att bygga upp en avidentifieringsprocess.

2 Definitioner och rättslig analys

2.1. Definitioner i EU:s rättsliga sammanhang

I direktiv 95/46/EG hänvisas till avidentifiering i skäl 26 för att undanta avidentifierade uppgifter från tillämpningsområdet för lagstiftningen om skydd av personuppgifter:

> *”Principerna för skyddet måste gälla all information som rör en identifierad eller identifierbar person, för att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person att identifiera vederbörande. Skyddsprinciperna gäller inte för uppgifter som gjorts anonyma på ett sådant sätt att den registrerade inte längre är identifierbar. En sådan uppförandekodex som avses i artikel 27 kan vara ett användbart redskap för att ge vägledning om hur uppgifter kan göras anonyma och behållas i en form som identifiering av den registrerade inte längre är möjligt.”*[1]

En noggrann läsning av skäl 26 ger en begreppsmässig definition av avidentifiering. Skäl 26 innebär att man för att avidentifiera uppgifter måste avlägsna tillräckligt med beståndsdelar från dem så att den registrerade inte längre kan identifieras. Uppgifterna ska med andra ord behandlas på ett sådant sätt att de inte längre kan användas för att identifiera en fysisk person med hjälp av ”alla hjälpmedel som rimligen kan komma att användas” antingen av den

[1] Det bör också noteras att denna uppläggning också följs i förslaget till en EU-förordning om uppgiftsskydd i skäl 23: ”För att avgöra om en person är identifierbar bör härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av en registeransvarig eller av någon annan person.”

registeransvarige eller av någon annan person. En viktig faktor är att behandlingen måste vara oåterkallelig. I direktivet klargörs inte hur en sådan avidentifieringsprocess bör eller kan utföras.[2] Tyngdpunkten ligger på resultatet: att uppgifterna ska vara sådana att det inte går att identifiera den registrerade via ”alla” hjälpmedel som är ”troliga” och ”rimliga”. Det hänvisas till uppförandekodex som ett redskap för att utforma tänkbara avidentifieringsmekanismer och för att behålla uppgifterna i en form som ”gör det omöjligt” att identifiera den registrerade. I direktivet fastställs således helt klart en mycket hög standard.

I direktivet om integritet och elektronisk kommunikation (direktiv 2002/58/EG) hänvisas också till ”avidentifiering” och ”anonyma uppgifter” i stort sett i samma avseende. I skäl 26 anges följande:

> *”Trafikuppgifter som används för marknadsföring av kommunikationstjänster eller för tillhandahållande av mervärdestjänster bör också utplånas eller avidentifieras efter det att tjänsten tillhandahållits.”*

I artikel 6.1 anges därför följande:

> *”Trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst skall utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation, utan att det påverkar tillämpningen av punkterna 2, 3 och 5 i den här artikeln samt artikel 15.1.”*

Enligt artikel 9.1 gäller dessutom följande:

> *”Om andra lokaliseringsuppgifter än trafikuppgifter som rör användare eller abonnenter av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster kan behandlas, får dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna givit sitt samtycke, i den utsträckning och för den tid som krävs för tillhandahållandet av en mervärdestjänst.”*

Den bakomliggande motiveringen är att resultatet av att tillämpa avidentifiering som metod på personuppgifter bör vara lika permanent med dagens teknik som radering, dvs. göra det omöjligt att behandla personuppgifter.[3]

2.2. Rättslig bedömning

En analys av formuleringarna om avidentifiering i de viktigaste EU-instrumenten för skydd av personuppgifter gör det möjligt att lyfta fram fyra centrala drag:

- Avidentifiering kan vara resultatet av behandling av personuppgifter i syfte att oåterkalleligen förhindra identifiering av den registrerade.

[2] Detta begrepp diskuteras närmare på sidan 8 i detta yttrande.

[3] Det bör här erinras om att avidentifiering även definieras i internationella standarder som t.ex. ISO 29100 – som den ”process varigenom uppgifter om identifierbara personer (PII) oåterkalleligen ändras på ett sådant sätt att en den PII-berörda inte längre kan identifieras direkt eller indirekt, antingen av den PII-ansvarige ensam eller i samarbete med någon annan” (ISO 29100:2011). Oåterkalleligheten hos den ändring som personuppgifterna genomgått för att omöjliggöra direkt eller indirekt identifiering är viktig också för ISO. Från denna synpunkt råder det betydande överensstämmelse med de principer och begrepp som ligger till grund för direktiv 95/46/EG. Detta gäller även definitionerna i vissa nationella lagar (t.ex. i Italien, Tyskland och Slovenien), där tyngdpunkten ligger på icke-identifierbarhet och där man hänvisar till en ”oproportionerlig insats” för att återidentifiera (Tyskland, Slovenien). I den franska lagen om skydd av personuppgifter föreskrivs dock att uppgifter ska förbli personuppgifter även om det är ytterst svårt och osannolikt att den registrerade återidentifieras – det finns alltså ingen bestämmelse som hänvisar till ”rimlighetstestet”.

- Flera avidentifieringsmetoder kan övervägas. Det finns ingen föreskriven standard i EU-lagstiftningen.

- Uppmärksamhet bör fästas vid omständigheterna: Hänsyn måste tas till ”alla” hjälpmedel som den registeransvarige och andra ”rimligen” kan komma att använda för identifiering, med särskild uppmärksamhet vid vad som på senare tid på teknikens nuvarande nivå har blivit ”rimligen” (med hänsyn till ökningen av databehandlingskraften och de hjälpmedel som är tillgängliga).

- Avidentifiering medför en inneboende riskfaktor: Denna riskfaktor måste beaktas vid bedömning av värdet av en avidentifieringsmetod, inklusive tänkbara användningar av uppgifter som är ”avidentifierade” med hjälp av metoden, och riskens allvarlighetsgrad och sannolikhet måste bedömas.

I detta yttrande används benämningen ”avidentifieringsmetod” hellre än ”anonymitet” eller ”anonyma uppgifter” för att framhålla den kvarstående och inneboende risken för återidentifiering som är förknippad med en teknisk-organisatorisk åtgärd i syfte att göra uppgifter ”anonyma”.

2.2.1. Avidentifieringsprocessens laglighet

Avidentifiering är för det första en metod som tillämpas på personuppgifter i syfte att åstadkomma oåterkallelig avidentifiering. Ett utgångsantagande är därför att personuppgifterna måste ha samlats in och behandlats i enlighet med gällande lagstiftning om bevarande av uppgifter i en identifierbar form.

I detta sammanhang är avidentifieringsprocessen, som innebär att personuppgifterna behandlas för att avidentifiera dem, ett fall av ”senare behandling” eller ”ytterligare behandling”. I den egenskapen måste behandlingen överensstämma med förenlighetstestet i enlighet med riktlinjerna från arbetsgruppen i dess yttrande 03/2013 om ändamålsbegränsning[4].

Detta innebär i princip att den rättsliga grunden för avidentifieringen kan återfinnas bland någon av dem som nämns i artikel 7 (inklusive den registeransvariges berättigade intresse) förutsatt att kraven på uppgifternas kvalitet i artikel 6 i direktivet också uppfylls och med vederbörlig hänsyn till de särskilda omständigheterna och alla faktorer som nämns i arbetsgruppens yttrande om ändamålsbegränsning[5].

Å andra sidan bör bestämmelserna i artikel 6.1 e i direktiv 95/46/EG (men också i artiklarna 6.1 och 9.1 i direktivet om integritet och elektronisk kommunikation) framhållas eftersom de anger att personuppgifter inte ska förvaras på ett sätt som medger identifiering under längre tid än vad som behövs för insamling eller senare behandling.

---

[4] Yttrande 03/2013 från den arbetsgrupp som inrättats enligt artikel 29, som är tillgängligt på: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[5] Detta innebär i synnerhet att en materiell prövning behöver utföras mot bakgrund av alla relevanta omständigheter och särskilt följande huvudfaktorer:
a) Sambandet mellan de ändamål för vilka personuppgifter har samlats in och ändamålen med senare behandling.
b) Det sammanhang i vilket personuppgifterna har samlats in och de registrerades rimliga förväntningar om uppgifternas framtida användning.
c) Personuppgifternas beskaffenhet och konsekvenserna för de registrerade av senare behandling.
d) De säkerhetsåtgärder som den registeransvarige vidtar för att garantera en korrekt behandling och förhindra negativa effekter för de registrerade.

Denna bestämmelse i sig innebär ett starkt krav på att personuppgifter ska avidentifieras som standard (med förbehåll för andra rättsliga krav, såsom de som anges i direktivet om integritet och elektronisk kommunikation i fråga om trafikuppgifter). Om den registeransvarige vill behålla personuppgifter när ändamålet för den ursprungliga eller senare behandlingen har uppnåtts, ska avidentifieringsmetoder användas för att oåterkalleligen förhindra identifiering.

Arbetsgruppen anser följaktligen att avidentifiering som ett fall av senare behandling av personuppgifter kan anses vara förenlig med det ursprungliga ändamålet med behandlingen men endast på villkor att avidentifieringsprocessen på ett tillförlitligt sätt producerar avidentifierade uppgifter i den mening som beskrivs i detta dokument.

Det bör också betonas att avidentifiering måste ske i enlighet med de rättsliga begränsningar som EU-domstolens åberopade i sitt avgörande i mål C-553/07 (College van burgemeester en wethouders van Rotterdam, mot M.E.E. Rijkeboer) avseende behovet av att behålla uppgifterna i en identifierbar form som gör det möjligt exempelvis för de registrerade att utöva sin rätt till tillgång. EU-domstolen fastslog följande: *”Medlemsstaterna är, enligt artikel 12 a i direktivet [95/46/EG] skyldiga att föreskriva en rätt att få tillgång till information om de mottagare eller mottagarkategorier till vilka uppgifterna lämnas ut och om innehållet i de uppgifter som lämnas ut, vilken avser inte enbart nutid, utan även förfluten tid. Det ankommer på medlemsstaterna att fastställa den tid under vilken denna information ska lagras och att fastställa en motsvarande rätt att få tillgång till denna information, vilket innebär en lämplig avvägning mellan den registrerades intresse av att skydda sitt privatliv, bland annat genom den rätt att göra invändningar och att föra talan som föreskrivs i direktivet, och den börda som skyldigheten att lagra denna information utgör för den registeransvarige.”*

Detta är särskilt betydelsefullt om artikel 7 f i direktiv 95/46/EG åberopas av en registeransvarig avseende avidentifiering: Den registeransvariges berättigade intresse ska alltid avvägas mot de registrerades rättigheter och grundläggande friheter.

I exempelvis en undersökning som genomfördes av den nederländska dataskyddsmyndigheten 2012–2013 om fyra mobiloperatörers användning av s.k. DPI-tekniker (Deep Packet Inspection, djup paketinspektion) påvisades en rättslig grund enligt artikel 7 f i direktiv 95/46/EG för avidentifiering av innehållet i trafikuppgifter så snart som möjligt efter insamlingen av uppgifterna. I artikel 6 i direktivet om integritet och elektronisk kommunikation föreskrivs att trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska utplånas eller avidentifieras så snart som möjligt. Eftersom det i det här fallet är tillåtet enligt artikel 6 i direktivet om integritet och elektronisk kommunikation finns en motsvarande rättslig grund i artikel 7 i direktivet om skydd av personuppgifter. Det skulle också kunna presenteras som det motsatta förhållandet: Om en typ av databehandling inte är tillåten enligt artikel 6 i direktivet om integritet och elektronisk kommunikation, kan det inte finnas en rättslig grund i artikel 7 i direktivet om skydd av personuppgifter.

2.2.2. Potentiell identifierbarhet hos avidentifierade uppgifter

Arbetsgruppen har behandlat begreppet personuppgifter i detalj i yttrande 4/2007 om personuppgifter, med inriktning på byggstenarna i definitionen i artikel 2 a i direktiv 95/46/EG, inklusive ”identifierad eller identifierbar” i den definitionen. I detta sammanhang har arbetsgruppen också konstaterat att ”avidentifierade uppgifter därför är

anonyma uppgifter som tidigare hänvisade till en identifierbar person men där denna identifiering inte längre är möjlig".

Arbetsgruppen har följaktligen redan klargjort att testet av "hjälpmedel … som rimligen kan komma att användas" anges i direktivet som ett kriterium som ska tillämpas för att bedöma om avidentifieringsprocessen är tillräckligt stark, dvs. om identifiering har blivit "rimligen" omöjlig. Det särskilda sammanhanget och omständigheterna i ett visst fall har direkt inverkan på identifierbarheten. I den tekniska bilagan till detta yttrande analyseras konsekvensen av att välja den mest lämpliga metoden.

Som tidigare betonats utvecklas forskning, verktyg och databehandlingskraft. Därför är det varken möjligt eller till nytta att tillhandahålla en uttömmande förteckning över de omständigheter då identifiering inte längre är möjlig. Vissa nyckelfaktorer förtjänar dock att beaktas och exemplifieras.

För det första kan det hävdas att de registeransvariga bör inrikta sig på de konkreta hjälpmedel som skulle krävas för att omkasta avidentifieringsmetoden, särskilt avseende kostnaden och det kunnande som krävs för att införa hjälpmedlen och en bedömning av deras sannolikhet och allvarlighetsgrad. De bör exempelvis avväga sin insats och kostnad för avidentifieringen (både vad gäller tid och nödvändiga resurser) mot tillgängliga billiga tekniska hjälpmedel för att identifiera enskilda personer i dataset, den ökande allmänna tillgången på andra dataset (t.ex. sådana som görs tillgängliga enligt principen om "öppna data"), och de många exemplen på ofullständig avidentifiering med därefter följande negativa och ibland oavhjälpliga effekter för de registrerade.[6] Det bör noteras att identifieringsrisken kan öka med tiden och även är beroende av informations- och kommunikationsteknikens utveckling. I förekommande fall måste därför rättsliga bestämmelser formuleras på ett teknikneutralt sätt och helst ta hänsyn till förändringarna i informationsteknikens utvecklingspotential.[7]

För det andra, de "hjälpmedel som rimligen kan komma att användas för att avgöra om en person är identifierbar" är de som ska användas "av den registeransvarige eller av någon annan person". Det är därför viktigt att förstå att när en registeransvarig inte utplånar de ursprungliga (identifierbara) uppgifterna på händelsenivå och överlämnar en del av detta dataset (t.ex. efter avlägsnande eller maskering av identifierbara uppgifter) är det dataset som blir följden fortfarande personuppgifter. Endast om den registeransvarige aggregerar uppgifterna till en nivå där de enskilda händelserna inte längre kan identifieras kan det dataset som blir följden anses vara anonymt. Exempel: Om en organisation samlar in uppgifter om enskilda personers resor utgör de individuella resemönstren på händelsenivå fortfarande personuppgifter för varje part, så länge som den registeransvarige (eller någon annan part) fortfarande har tillgång till ursprungliga rådata, även om direkta identifierare har avlägsnats från det dataset som tillhandahålls till tredje parter. Men om den registeransvarige utplånar rådata och endast tillhandahåller statistik som aggregerats på hög nivå till tredje parter, såsom "på måndagar är det 160 % fler passagerare på reseträcka X än på tisdagar", kan detta räknas som anonyma uppgifter.

[6] Det är intressant att notera att Europaparlamentets i sina nyligen (21 oktober 2013) framlagda ändringsförslag till förslaget om en allmän förordning om uppgiftsskydd i skäl 23 särskilt nämner följande: "För att fastställa om hjälpmedel rimligen kan komma att användas för att identifiera vederbörande bör man ta i beaktande samtliga objektiva faktorer som kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen."

[7] Se yttrande 4/2007 från den arbetsgrupp som inrättats enligt artikel 29, s. 15.

En effektiv avidentifieringslösning gör det omöjligt för alla parter att särskilja en person i ett dataset, förhindrar att två poster inom ett dataset länkas (eller att länkningar görs mellan två separata dataset) och förhindrar att det går att sluta sig till information från detta dataset. Därför räcker det i allmänhet inte att enbart se till att direkt identifierande element avlägsnas för att garantera att identifiering av den registrerade inte längre är möjlig. Det är ofta nödvändigt att vidta ytterligare åtgärder för att förhindra identifiering, som återigen är beroende av sammanhanget och ändamålen med den behandling för vilken de avidentifierade uppgifterna är avsedda.

EXEMPEL:
Genetiska profiler är på grund av vissa profilers unika beskaffenhet ett exempel på personuppgifter som kan riskera att identifieras om den enda metod som används är att avlägsna givarens identitet. Det har redan visats i litteraturen[8] att kombinationen av offentligt tillgängliga genetiska resurser (t.ex. släktforskningsregister, dödsrunor, resultat av sökmotorfrågor) och metadata om DNA-givare (tidpunkt för donationen, ålder, bostadsort) kan avslöja vissa personers identitet trots att DNA donerades ”anonymt”.

Båda typerna av avidentifieringsmetoder – randomisering och generalisering[9] – har brister, men vardera metoden kan vara lämplig under givna omständigheter och en given situation för att uppnå det önskade ändamålet utan att äventyra de registrerades integritet. Det måste stå klart att ”identifiering” inte bara innebär möjlighet att få fram en persons namn och/eller adress, utan även potentiell identifierbarhet genom att särskilja, länka och dra slutsatser. För att lagstiftningen om uppgiftsskydd ska vara tillämplig spelar det heller ingen roll vilka avsikter den registeransvarige eller mottagaren har. Så länge som uppgifterna är identifierbara är bestämmelserna om uppgiftsskydd tillämpliga.

Om en tredje part bearbetar ett dataset som behandlats med en avidentifieringsmetod (som avidentifierats och gjorts tillgänglig av den ursprunglige registeransvarige) kan den tredje parten göra detta lagligen utan att behöva ta hänsyn till krav på skydd av personuppgifter under förutsättning att den parten inte (direkt eller indirekt) kan identifiera de registrerade i det ursprungliga datasetet. Tredje parter är dock skyldiga att beakta alla ovannämnda faktorer rörande sammanhanget och omständigheterna (inklusive särdragen hos de avidentifieringsmetoder som tillämpats av den ursprungliga registeransvarige) när de beslutar hur de ska använda och, framför allt, kombinera sådana avidentifierade uppgifter för sina egna ändamål, eftersom de konsekvenser som kan bli följden bland annat är olika former av skadeståndsansvar från deras sida. Om dessa faktorer och egenskaper medför en oacceptabel risk för att de registrerade identifieras, ingår behandlingen återigen i tillämpningsområdet för lagstiftningen om skydd av personuppgifter.

Ovanstående förteckning är inte på något vis avsedd att vara uttömmande, utan snarare att ge allmän vägledning om hur man går till väga för att bedöma ett visst datasets potentiella identifierbarhet som genomgår avidentifiering enligt de olika tillgängliga metoderna. Alla ovannämnda faktorer kan anses vara lika många riskfaktorer som ska avvägas av såväl de registeransvariga vid avidentifiering av dataset som av tredje parter som använder dessa avidentifierade dataset för sina egna ändamål.

[8] Se John Bohannon, Genealogy Databases Enable Naming of Anonymous DNA Donors, *Science*, Vol. 339, nr 6117 (18 januari 2013), s. 262.
[9] Huvudfunktionerna och skillnaderna mellan dessa båda avidentifieringsmetoder beskrivs i avsnitt 3 (Teknisk analys) nedan.

2.2.3. Risker med användningen av avidentifierade uppgifter

När de registeransvariga överväger att använda avidentifieringsmetoder måste de beakta följande risker:

- En särskild fallgrop är att betrakta pseudonymiserade uppgifter som likvärdiga med avidentifierade uppgifter. I avsnittet Teknisk analys förklaras att pseudonymiserade uppgifter inte kan likställas med avidentifierade uppgifter eftersom det även fortsättningsvis går att särskilja enskilda registrerade och uppgifter kan länkas mellan olika dataset. Pseudonymitet tillåter troligen identifierbarhet och ingår därför fortfarande i tillämpningsområdet för rättsordningen för skydd av personuppgifter. Detta är särskilt relevant när det gäller vetenskaplig, statistisk eller historisk forskning.[10]

EXEMPEL:
Ett typiskt exempel på de missuppfattningar som omgärdar pseudonymisering är den välkända AOL-incidenten (America On Line, AOL): År 2006 gjordes en databas som innehöll 20 miljoner söknyckelord för över 650 000 användare under en 3-månadersperiod tillgänglig, och den enda åtgärden för att skydda den personliga integriteten bestod i att ersätta AOL-användarnamnet med ett numeriskt attribut. Detta ledde till offentlig identifiering och lokalisering av vissa av dem. Pseudonymiserade frågesträngar för sökmotorer, särskilt i kombination med andra attribut, t.ex. IP-adresser eller andra kundkonfigurationsparametrar, har en mycket hög identifieringsbarhet.

- Ett andra misstag är att anse att korrekt avidentifierade uppgifter (efter att alla ovanstående villkor och kriterier uppfyllts och vilka per definition inte omfattas av direktivet om skydd av personuppgifter) innebär att de enskilda personerna berövas alla skyddsåtgärder, först och främst eftersom andra rättsakter kan vara tillämpliga på användningen av dessa uppgifter. Exempelvis förhindrar artikel 5.3 i direktivet om integritet och elektronisk kommunikation lagring av och tillgång till information av något slag (inklusive uppgifter utan personanknytning) på terminalutrustning utan abonnentens/användarens samtycke, vilket utgör en del av den bredare principen om konfidentialitet vid kommunikation.

- En tredje försumlighet kan också uppkomma av att inte beakta vilka konsekvenser ordentligt avidentifierade uppgifter under vissa omständigheter kan få för de enskilda personerna, särskilt när det gäller profilering. Den enskilda personens privatliv skyddas i sig enligt artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och artikel 7 i EU-stadgan om de grundläggande rättigheterna. Även om lagstiftningen om skydd av personuppgifter inte längre är tillämplig på denna typ av uppgifter kan utnyttjandet av dataset som avidentifierats och gjorts tillgängliga för tredje parter att använda leda till integritetsförlust. Speciell försiktighet krävs vid hantering av avidentifierade uppgifter, särskilt när sådana uppgifter används (ofta i kombination med andra uppgifter) för att fatta beslut som har konsekvenser (även om det bara är indirekt) för enskilda individer. Som redan påpekats i detta yttrande och som arbetsgruppen förtydligat framför allt i yttrandet om begreppet ”ändamålsbegränsning” (yttrande 03/2013)[11], bör de registrerades berättigade förväntningar om senare behandling av deras personuppgifter bedömas mot bakgrund av relevanta faktorer i sammanhanget, t.ex. karaktären hos relationen mellan de registrerade och de registeransvariga, tillämpliga rättsliga skyldigheter, insyn i behandlingen.

[10] Se även yttrande 4/2007 från den arbetsgrupp som inrättats enligt artikel 29, s. 18–20.
[11] Tillgänglig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

3 Teknisk analys, metodernas stabilitet och vanliga misstag

Det finns olika avidentifieringsmetoder och -tekniker med varierande grad av stabilitet. I detta avsnitt behandlas de huvudpunkter som registeransvariga bör beakta, särskilt med avseende på de garantier som kan uppnås med en viss metod med dagens teknik och tre risker som är väsentliga för avidentifiering:

- *Särskiljbarhet*, som motsvarar möjligheten att isolera en del eller alla poster som identifierar en enskild person i datasetet.
- *Länkbarhet*, som är förmågan att länka samman åtminstone två poster för samma registrerad eller en grupp av registrerade (antingen i samma databas eller i två olika databaser). Om en angripare kan fastställa (t.ex. genom korrelationsanalys) att två poster hänför sig till en och samma grupp av enskilda personer, men inte kan särskilja enskilda personer i denna grupp, ger metoden skydd mot särskiljbarhet men inte mot länkbarhet.
- *Inferens*, som är möjligheten att med signifikant sannolikhet sluta sig till värdet av ett attribut från värdet av en rad andra attribut.

En lösning som skyddar mot dessa tre risker ska således vara motståndskraftig mot återidentifiering som utförs med de mest sannolika och rimliga verktyg som den registeransvarige och eventuell annan person kan utnyttja. Arbetsgruppen betonar i detta avseende att det pågår forskning om metoder för avidentifiering och anonymisering och att forskningen ständigt visat att ingen metod är utan brister i sig. I stort sett finns det två olika metoder för avidentifiering: Den första bygger på ***randomisering*** och den andra på ***generalisering***. I yttrandet behandlas även andra begrepp som *pseudonymisering*, *differentiell integritet*, *l-diversitet*, *t-närhet*.

Följande terminologi används i detta avsnitt av yttrandet: Ett dataset består av olika poster som är relaterade till enskilda personer (de registrerade). Varje post är relaterad till en registrerad och består av en uppsättning värden (t.ex. 2013) för varje attribut (t.ex. år). Ett dataset är en samling poster som kan ha formen av en tabell (eller en uppsättning tabeller) eller ett annoterat/viktat diagram, vilket blir allt vanligare i dag. Exemplen i yttrandet avser tabeller, men rekommendationerna är tillämpliga också på andra grafiska representationer av poster. Kombinationer av attribut som rör en registrerad person eller en grupp av registrerade kan kallas kvasi-identifierare. I vissa fall kan ett dataset ha flera poster om en och samma individ. En ”angripare” är en tredje part (dvs. varken den registeransvarige eller registerföraren) som oavsiktligt eller avsiktligt får åtkomst till de ursprungliga posterna.

3.1. Randomisering

Randomisering är en samling metoder som påverkar sanningsenligheten i uppgifterna i syfte att avlägsna den starka kopplingen mellan uppgifterna och den enskilda personen. Om uppgifterna är tillräckligt osäkra kan de inte längre hänföras till en viss enskild person. Randomiseringen i sig minskar inte varje posts singularitet eftersom varje post fortfarande härleds från en enda registrerad men kan skydda mot inferensattacker och inferensrisker, och randomisering kan kombineras med generaliseringsmetoder för att skapa starkare integritetsskydd. Ytterligare metoder kan krävas för att se till att en post inte kan identifiera en enskild person.

3.1.1. Brustillägg

Metoden med brustillägg är särskilt användbar när attribut kan ha en betydande negativ inverkan på enskilda individer. Den består av att ändra attribut i datasetet så att de blir mindre exakta samtidigt som den övergripande fördelningen bevaras. Vid behandling av ett dataset antar en observatör att värdena är korrekta, men detta stämmer bara i en viss grad. Ett exempel: Om en persons längd ursprungligen angavs avrundat till närmaste centimeter kan det avidentifierade datasetet innehålla en längduppgift med endast noggrannheten ± 10 cm. Om denna metod tillämpas effektivt kommer en tredje part inte att kunna identifiera en enskild person och inte heller kunna reparera uppgifterna eller på annat sätt upptäcka hur uppgifterna har ändrats.

Brustillägg brukar behöva kombineras med andra avidentifieringsmetoder, t.ex. avlägsnande av uppenbara attribut och kvasi-identifierare. Brusnivån bör vara beroende av den erforderliga informationsnivån och konsekvenserna för enskilda personers integritet om de skyddade attributen avslöjas.

3.1.1.1. Garantier

- *Särskiljbarhet:* Det går fortfarande att särskilja en enskild persons poster (eventuellt på ett icke identifierbart sätt) även om posterna är mindre tillförlitliga.
- *Länkbarhet:* Det går fortfarande att länka poster som rör samma enskilda person, men posterna är mindre tillförlitliga och en verklig post kan således länkas till en artificiell post (dvs. ”brus”). I vissa fall kan en felaktig tillskrivning utsätta en registrerad för betydande och ännu högre risk än en korrekt tillskrivning.
- *Inferens:* Inferensattacker kan vara möjliga, men framgångsfrekvensen blir lägre och vissa falskt positiva resultat (och falskt negativa) är troliga.

3.1.1.2. Vanliga misstag

- Tillägg av inkonsekvent brus: Om brus inte är semantiskt gångbart (dvs. oproportionerligt och inte följer logiken mellan attributen i ett set) kan en angripare med åtkomst till databasen filtrera bort bruset och i vissa fall generera om de uppgifter som saknas. Om datasetet är alltför glest[12] kan det fortfarande att vara möjligt att länka brusuppgifter till en extern källa.
- Om vi antar att bruset är tillräckligt: Brustillägget är en kompletterande åtgärd som gör det svårare för en angripare att hämta personuppgifter. Om bruset är högre än uppgifterna i datasetet ska man inte anta att brustillägget utgör en fristående lösning för avidentifiering.

3.1.1.3. Misslyckanden med brustillägg

Ett mycket berömt experiment med återidentifiering utfördes på Netflix-videoleverantörens kunddatabas. Forskare har analyserat de geometriska egenskaperna hos den databasen som består av mer än 100 miljoner omdömen på skalan 1–5 om över 18 000 filmer, som lämnats av nästan 500 000 användare. Företaget offentliggjorde databasen efter att den hade avidentifierats enligt en intern integritetspolicy, som innebar att all kundidentifierande information avlägsnades utom omdömen och datum. Brus lades till genom att öka eller minska omdömena en aning.

[12] Begreppet utvecklas närmare i bilagan, s. 30.

Trots detta konstaterade man att 99 % av användarposterna i datasetet kunde identifieras unikt med hjälp av åtta omdömen och datum med 14 dagars fel som urvalskriterier. Om urvalskriterierna sänktes (två omdömen och tre dagars fel) kunde fortfarande 68 % av användarna identifieras.[13]

3.1.2. Permutation

Denna metod består i att blanda om värdena för attribut i en tabell på så sätt att vissa av dem artificiellt länkas till andra registrerade. Metoden är användbar när det är viktigt att bevara den exakta fördelningen av varje attribut i datasetet.

Permutation kan betraktas som en särskild form av brustillägg. I en klassisk brusmetod ändras attribut med randomiserade värden. Det kan vara en svår uppgift att generera konsekvent brus och att ändra attributvärden en aning kanske inte ger tillräckligt integritetsskydd. Som alternativ ändrar permutationsmetoder värdena i datasetet genom att endast byta dem från en post till en annan. Ett sådant byte säkerställer att värdenas variationsbredd och fördelning blir oförändrade men att korrelationerna mellan värden och enskilda personer förändras. Om två eller flera attribut har en logisk relation eller en statistisk korrelation försvinner den relationen om de permuteras oberoende av varandra. Det kan därför vara viktigt att permutera en uppsättning relaterade attribut för att inte bryta den logiska relationen, annars kan en angripare identifiera de permuterade attributen och omkasta permutationen.

Om vi exempelvis har en undergrupp av attribut i ett medicinskt dataset, t.ex. ”anledning till sjukhusvistelse/symtom/ansvarig avdelning”, finns det i de flesta fall en stark logisk relation mellan värdena, och om endast ett av värdena permuteras skulle detta därför upptäckas och till och med kunna omkastas.

På samma sätt som för brustillägg kanske permutation inte ensam ger avidentifiering utan alltid bör kombineras med avlägsnande av uppenbara attribut/kvasi-identifierare.

3.1.2.1. Garantier

- *Särskiljbarhet:* Precis som med brustillägg går det fortfarande att särskilja en enskild persons poster, men posterna är mindre tillförlitliga.
- *Länkbarhet:* Om permutation berör attribut och kvasi-identifierare kan detta förhindra att attribut ”korrekt” länkas till ett dataset både internt och externt men tillåter fortfarande ”felaktig” länkning, eftersom en verklig uppgift kan tillskrivas en annan registrerad.
- *Inferens:* Slutsatser kan fortfarande dras från datasetet, särskilt om attributen är korrelerade eller har starka logiska relationer. Eftersom angriparen inte vet vilka attribut som har permuterats måste han eller hon beakta att inferensen bygger på en felaktig hypotes och att därför endast probabilistisk inferens fortfarande är möjlig.

3.1.2.2. Vanliga misstag

- Att välja fel attribut: Att permutera de minst känsliga eller icke-riskabla attributen skulle inte leda till någon betydande vinst när det gäller skydd av personuppgifter. Om de känsliga/riskabla attributen fortfarande är knutna till det ursprungliga attributet, kan en angripare fortfarande extrahera känslig information om enskilda personer.

[13] Narayanan, A., och Shmatikov, V. (maj 2008), Robust de-anonymization of large sparse datasets. I *Security and Privacy, 2008. SP 2008. IEEE Symposium on* (s. 111–125). IEEE.

- Att permutera attribut slumpmässigt: Om två attribut är starkt korrelerade ger slumpmässig permutation inte några starka garantier. Detta vanliga misstag illustreras i tabell 1.
- Att anta att permutation är tillräckligt: Precis som brustillägg ger permutation inte anonymitet i sig själv och bör kombineras med andra metoder som att avlägsna uppenbara attribut.

3.1.2.3. Misslyckanden med permutation

Detta exempel visar hur slumpmässig permutation av attribut leder till dåliga integritetsgarantier när det finns vid logiska relationer mellan olika attribut. Efter avidentifieringsförsöket är det en lätt sak att härleda varje enskild persons inkomst med utgångspunkt från arbetet (och födelseåret). Utifrån en direkt inspektion av uppgifterna i tabellen kan man t.ex. hävda att vd i tabellen troligen är född 1957 och har den högsta lönen, medan de arbetslösa är födda 1964 och har de lägsta inkomsterna.

År	Kön	Arbete	Inkomst (permuterad)
1957	M	Ingenjör	70k
1957	M	Vd	5k
1957	M	Arbetslös	43k
1964	M	Ingenjör	100k
1964	M	Mellanchef	45k

Tabell 1. Ett ineffektivt exempel på avidentifiering genom permutation av korrelerade attribut.

3.1.3. Differentiell integritet

Differentiell integritet[14] hör till gruppen randomiseringsmetoder, men tillvägagångssättet är ett annat: Brustillägg används i förväg när ett dataset ska göras tillgängligt. Differentiell integritet kan däremot användas när den registeransvarige genererar avidentifierade vyer av ett dataset och samtidigt bevarar en kopia av ursprungliga data. Sådana avidentifierade vyer brukar genereras med hjälp av en delmängd av frågor för en viss tredje part. I delmängden ingår visst slumpmässigt brus som avsiktligt har lagts till i efterhand. Differentiell integritet ger den dataansvarige information om hur mycket brus som behöver läggas till, och i vilken form, för att få de nödvändiga integritetsgarantierna.[15] I detta sammanhang är det särskilt viktigt att fortlöpande övervaka (minst för varje ny sökfråga) om det finns möjlighet att identifiera en enskild person i frågeresultatet. Det måste dock förtydligas att metoder för differentiell integritet inte ändrar de ursprungliga uppgifterna, och därmed kan den registeransvarige så länge som de ursprungliga uppgifterna finns kvar identifiera enskilda personer i resultaten av differentiella integritetsfrågor med beaktande av alla hjälpmedel som rimligen kan komma att användas. Sådana resultat måste alltså anses utgöra personuppgifter.

En fördel med ett tillvägagångssätt som bygger på differentiell integritet är att dataset tillhandahålls till behöriga tredje parter som svar på en särskild sökfråga, i stället för att ett enstaka dataset görs tillgängligt. Som hjälp vid kontrollen kan den registeransvarige föra en

[14] Dwork, C. (2006). Differential privacy. I *Automata, languages and programming* (s. 1–12). Springer Berlin Heidelberg.
[15] Jfr Ed Felten (2012), *Protecting privacy by adding noise*. URL: https://techatftc.wordpress.com/2012/06/21/protecting-privacy-by-adding-noise/.

förteckning över alla frågor och begäranden för att se till att tredje parter inte får åtkomst till uppgifter som de inte har behörighet till. En sökfråga kan också genomgå avidentifieringsprocesser, inklusive tillägg av brus eller ersättning för att ytterligare skydda integriteten. Det är fortfarande ett olöst forskningsproblem att hitta en bra interaktiv sökmekanism som klarar att besvara sökfrågor någorlunda korrekt (dvs. med mindre brus), samtidigt som integritetsskyddet bevaras.

För att begränsa inferens- och länkbarhetsattacker är det nödvändigt att följa upp de sökfrågor som skickas från en enhet och observera den information som erhålls om de registrerade. Databaser med differentiell integritet bör därför inte driftsättas i öppet tillgängliga sökmotorer som inte erbjuder någon möjlighet att spåra de enheter som gör sökningarna.

3.1.3.1 Garantier

- *Särskiljbarhet:* Om endast statistik produceras och de regler som tillämpas på datasetet är välvalda ska det inte vara möjligt att använda svaren för att särskilja en enskild person.
- *Länkbarhet:* Genom att använda flera begäranden kan det gå att länka uppgifter som rör en enskild person mellan två svar.
- *Inferens:* Det är möjligt att sluta sig till information om enskilda personer eller grupper med hjälp av flera begäranden.

3.1.3.2. Vanliga misstag

- Att inte infoga tillräckligt med brus: Svårigheten ligger i att tillhandahålla så lite spår som möjligt om huruvida en viss registrerad eller grupp av registrerade bidragit till datasetet för att förhindra länkning med bakgrundskunskap. Den största svårigheten i fråga om uppgiftsskydd är att kunna generera rätt mängd brus som läggs till i de verkliga svaren så att enskilda personers integritet skyddas samtidigt som de lämnade svaren fortsätter att vara användbara.

3.1.3.3 Misslyckanden med differentiell integritet

Att behandla varje sökfråga för sig: En kombination av sökresultat kan göra det möjligt att avslöja information som var avsedd att vara hemlig. Om frågehistoriken inte bevaras, kan en angripare konstruera flera sökfrågor mot en databas med differentiell integritet för att successivt minska storleken på det producerade urvalet tills det med säkerhet eller med hög sannolikhet dyker upp ett visst kännetecken för en enskild registrerad person eller grupp av registrerade. En ytterligare varning är att undvika misstaget att tänka att uppgifterna är anonyma för den tredje parten, medan den registeransvarige fortfarande kan identifiera den registrerade i den ursprungliga databasen med beaktande av alla hjälpmedel som rimligen kan komma att användas.

3.2. Generalisering

Generalisering är den andra gruppen av avidentifieringsmetoder. Detta tillvägagångssätt består i att generalisera, eller späda ut, de registrerades attribut genom att ändra den relativa storleksordningen (t.ex. en region i stället för en stad, en månad i stället för en vecka). Generalisering kan vara effektivt för att förhindra särskiljning, men det tillåter inte effektiv avidentifiering i samtliga fall. Det kräver särskilda och sofistikerade kvantitativa metoder för att förhindra länkbarhet och interferens.

3.2.1. Aggregering och *k*-anonymitet

Aggregerings- och *k*-anonymitetsmetoder syftar till att förhindra att registrerade särskiljs genom att gruppera dem med minst k andra personer. För att uppnå detta generaliseras attributvärdena så att varje enskild person har samma värde. Genom att t.ex. sänka detaljrikedomen (granulariteten) för en plats från en stad till ett land kan ett större antal registrerade inbegripas. Enskilda födelsedatum kan generaliseras till ett datumintervall eller grupperas per månad eller år. Andra numeriska attribut (t.ex. löner, vikt, längd eller dos av ett läkemedel) kan generaliseras genom intervallvärden (t.ex. lön 20 000–30 000 euro). Dessa metoder kan användas när korrelationen av punktvärden kan skapa kvasi-identifierare.

3.2.1.1. Garantier

- *Särskiljbarhet:* Eftersom samma attribut nu delas av k användare ska det inte längre vara möjligt att särskilja enskilda personer inom en grupp av k användare.
- *Länkbarhet:* Länkbarheten är visserligen begränsad, men det går fortfarande att länka poster för grupper om k användare. Inom denna grupp är sannolikheten att två poster motsvarar samma pseudo-identifierare 1/k (vilket kan vara betydligt högre än sannolikheten för att sådana uppgifter inte är länkbara).
- *Inferens:* Den största bristen hos *k*-anonymitetsmodellen är att den inte förhindrar någon typ av inferensattack. Om alla k enskilda personer ingår i samma grupp och det är känt vilken grupp en enskild person tillhör är det en lätt sak att ta fram värdet för denna egenskap.

3.2.1.2. Vanliga misstag

- Att missa vissa kvasi-identifierare: En viktig parameter när man överväger *k*-anonymitet är tröskeln för k. Ju högre värdet är för k, desto starkare är integritetsgarantierna. Ett vanligt misstag är att artificiellt höja värdet k genom att minska den aktuella uppsättningen kvasi-identifierare. Minskningen av kvasi-identifierare gör det enklare att bygga upp kluster av *k*-användare på grund av andra attributs inneboende identifieringsförmåga (särskilt om en del av dem är känsliga eller har en mycket hög entropi, så som är fallet för mycket sällsynta attribut). Det är ett allvarligt misstag att inte beakta alla kvasi-identifierare vid valet av attribut som ska generaliseras. Om vissa attribut kan användas för att särskilja en enskild person i ett kluster av k, kan inte generaliseringen skydda vissa enskilda personer (se exempel i tabell 2).
- Att använda för små *k*-värden: Det leder till liknande problem om man siktar på ett för litet *k*-värde. Om k är för litet blir varje enskild persons vikt i ett kluster för signifikant, och inferensattacker får en större framgångsfrekvens. Om exempelvis k = 2 är sannolikheten för att de båda enskilda personerna har samma egenskap högre än för k > 10.
- Att inte gruppera enskilda personer med samma vikt: Det kan också leda till problem om en uppsättning enskilda personer med ojämn fördelning av attribut grupperas. Inverkan av en enskild persons post på ett dataset kommer att variera: Somliga kommer att representera en signifikant fraktion för egenskaperna medan andras bidrag förblir ganska obetydligt. Det är därför viktigt att se till att k är tillräckligt högt så att inga enskilda personer representerar en alltför stor fraktion av uppgifterna i ett kluster.

3.1.3.3. Misslyckanden med *k*-anonymitet

Det främsta problemet med *k*-anonymitet är att det inte förhindrar inferensattacker. Om angriparen vet att en viss person i följande exempel finns i datasetet och är född 1964 vet angriparen också att personen i fråga har haft en hjärtattack. Om vi vet att datasetet erhållits från en fransk organisation, då är varje enskild person bosatt i Paris eftersom de tre första siffrorna i postkoderna för Paris är 750*).

År	Kön	Postnr	Diagnos
1957	M	750*	Hjärtattack
1957	M	750*	Kolesterol
1957	M	750*	Kolesterol
1964	M	750*	Hjärtattack
1964	M	750*	Hjärtattack

Tabell 2. Ett exempel på en dåligt utformad *k*-avidentifiering.

3.2.2. *L*-diversitet/*t*-närhet

L-diversitet utvidgar *k*-anonymitet för att säkerställa att deterministiska inferensattacker inte längre är möjliga genom att se till att varje attribut i varje ekvivalensklass har minst *l* olika värden.

Ett grundläggande mål att uppnå är att begränsa förekomsten av ekivivalensklasser med dålig attributvariabilitet, så att en angripare med bakgrundskunskaper om en viss registrerad alltid lämnas med en betydande ovisshet.

L-diversitet är lämpligt för att skydda uppgifter mot inferensattacker när attributvärdena är väl fördelade. Det måste understrykas att denna teknik dock inte kan förhindra läckage av information om attributen inom en partition är ojämnt fördelade eller tillhör ett litet intervall av värden eller semantiska betydelser. Till sist är *l*-diversitet utsatt för probabilistiska inferensattacker.

T-närhet är en förfining av *l*-diversitet, eftersom syftet är att skapa ekvivalensklasser som liknar den ursprungliga fördelningen av attribut i tabellen. Metoden är användbar när det är viktigt att bevara uppgifterna så nära de ursprungliga som möjligt. I detta syfte används ytterligare en begränsningsregel på ekvivalensklassen, nämligen inte bara att det ska finnas minst *l* olika värden inom varje ekvivalensklass, utan också att varje värde representeras så många gånger som krävs för att avspegla varje attributs ursprungliga fördelning.

3.2.2.1. Garantier

- *Särskiljbarhet:* Precis som *k*-anonymitet kan *l*-diversitet och *t*-närhet säkerställa att poster som rör en enskild person inte kan särskiljas i databasen.
- *Länkbarhet:* *L*-diversitet och *t*-närhet är inte en förbättring jämfört med *k*-anonymitet när det gäller avsaknad av länkbarhet. Problemet är detsamma som med varje kluster: Sannolikheten för att samma uppgifter tillhör samma registrerad är högre än 1/N (där N är antalet registrerade i databasen).

- *Inferens:* Den viktigaste förbättringen som *l*-diversitet och *t*-närhet ger jämfört med *k*-anonymitet är att det inte längre är möjligt att konfigurera en inferensattack mot en databas som är ”*l*-diversifierad” eller ”*t*-nära” med 100 % konfidens.

3.2.2.2. Vanliga misstag

- Att skydda känsliga attributvärden genom att blanda dem med andra känsliga attribut: Det räcker inte att ha två värden för ett attribut i ett kluster för att ge integritetsgarantier. Fördelningen av känsliga värden i varje kluster ska påminna om värdenas fördelning i hela populationen, eller åtminstone vara enhetlig inom hela klustret.

3.2.2.3. Misslyckanden med *l*-diversitet

I tabellen nedan tilldelas *l*-diversitet för attributet ”Diagnos”. Om man känner till att en person som är född 1964 finns i tabellen är det dock fortfarande möjligt att med hög sannolikhet anta att han har haft en hjärtattack.

År	Kön	Postnr	Diagnos
1957	M	750*	**Hjärtattack**
1957	M	750*	**Kolesterol**
1957	M	750*	**Kolesterol**
1957	M	750*	**Kolesterol**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Kolesterol**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**
1964	M	750*	**Hjärtattack**

Tabell 3. En *l*-diversitetstabell där värdena för ”Diagnos” inte är jämnt fördelade.

Namn	Födelsedatum	Kön
Smith	1964	M
Rossi	1964	M
Dupont	1964	M
Jansen	1964	M
Garcia	1964	M

Tabell 4. En angripare som känner till att dessa personer finns i tabell 3 kan sluta sig till att de har haft en hjärtattack.

4. Pseudonymisering

Pseudonymisering består i att ersätta ett attribut (oftast ett unikt attribut) i en post med ett annat. Det är därför fortfarande troligt att den fysiska personen kan identifieras indirekt. Om pseudonymisering används ensamt blir resultatet följaktligen inte ett avidentifierat dataset. Metoden diskuteras ändå i detta yttrande på grund av de många missuppfattningar och misstag som omger dess användning.

Pseudonymisering minskar ett datasets länkbarhet med den registrerades ursprungliga identitet. I det avseendet är det en användbar säkerhetsåtgärd men inte en metod för avidentifiering.

Resultatet av pseudonymisering kan vara oberoende av det ursprungliga värdet (så som är fallet för ett slumptal som genererats av den registeransvarige eller ett efternamn som valts av den registrerade) eller kan härledas från de ursprungliga värdena för ett attribut eller en uppsättning attribut, t.ex. en hashfunktion eller ett krypteringsschema.

De mest använda pseudonymiseringsmetoderna är följande:

- Kryptering med hemlig nyckel: I detta fall kan innehavaren av nyckeln lätt återidentifiera varje registrerad genom att dekryptera datasetet, eftersom personuppgifterna finns kvar i datasetet, om än i krypterad form. Om vi antar att ett modernt krypteringsschema tillämpas är dekryptering endast möjlig om man känner till nyckeln.
- Hashfunktion: Detta är en funktion som returnerar utdata med en fast storlek från indata av valfri storlek (indata kan vara ett enda attribut eller en uppsättning attribut) som inte kan återföras. Det innebär att risken för återföring som vid kryptering inte längre finns. Om intervallet med indatavärden för hashfunktionen är känt kan värdena köras genom hashfunktionen på nytt för att härleda det korrekta värdet för en viss post. Om ett dataset till exempel har pseudonymiserats genom en hashfunktion på personnummer, kan dessa enkelt härledas genom att tillämpa hashfunktionen på alla möjliga indatavärden och sedan jämföra resultatet med värdena i datasetet. Hashfunktioner brukar utformas för att vara relativt snabba att beräkna och är utsatta för attacker med ren råstyrka.[16] Förberäknade tabeller kan också skapas för att möjliggöra återföring i bulk av en stor uppsättning med hashvärden.

[16] Sådana angrepp går ut på att prova alla troliga indata för att bygga jämförelsetabeller.

Användning av en saltad hashfunktion (där ett slumpvärde kallat ”salt” läggs till i det attribut som hashas) kan minska sannolikheten att indatavärdet ska kunna härledas, men det kan fortfarande vara möjligt att med rimliga hjälpmedel beräkna det ursprungliga attributvärdet som döljs bakom resultatet av en saltad hashfunktion.[17]

- Nyckelbaserad hashfunktion med lagrad nyckel: Detta är en särskild hashfunktion där man använder en hemlig nyckel som ytterligare indata (detta skiljer sig från en saltad hashfunktion eftersom saltet inte brukar vara hemligt). En registeransvarig kan upprepa funktionen på attributet genom att använda den hemliga nyckeln, men det är mycket svårare för en angripare att upprepa funktionen utan att känna till nyckeln eftersom antalet möjligheter som måste testas är tillräckligt stort för att vara ogenomförbart.
- Deterministisk kryptering eller nyckelbaserad hashfunktion med radering av nyckeln: Denna metod kan likställas med att välja ett slumptal som pseudonym för varje attribut i databasen och sedan radera jämförelsetabellen. Denna lösning gör det möjligt[18] att minska risken för länkbarhet mellan personuppgifterna i datasetet och uppgifter som rör samma person i ett annat dataset där en annan pseudonym används. Med en modern algoritm blir det beräkningsmässigt svårt för en angripare att dekryptera eller upprepa funktionen, eftersom det skulle kräva att varje tänkbar nyckel måste provas, förutsatt att nyckeln inte är tillgänglig.
- Tokenisering: Denna metod brukar ofta tillämpas i finanssektorn (men är inte begränsad till den sektorn) för att ersätta kort-id-nummer med värden som är mindre användbara för en angripare. Metoden har utvecklats från de tidigare nämnda och brukar bygga på mekanismer för envägskryptering eller en indexfunktion som tilldelar ett ordningsnummer eller ett slumptal som inte är matematiskt härlett från ursprungliga data.

4.1. Garantier

- *Särskiljbarhet:* Det går fortfarande att särskilja en enskild persons post eftersom personen fortfarande identifieras med ett unikt attribut som är resultatet av pseudonymiseringsfunktionen (= det pseudonymiserade attributet).
- *Länkbarhet:* Länkning är fortfarande enkelt mellan poster som använder samma pseudonymiserade attribut för att hänvisa till en och samma person. Även om olika pseudonymiserade attribut används för samma registrerade person kan länkning fortfarande vara möjlig med hjälp av andra attribut. Endast om inget annat attribut i datasetet kan användas för att identifiera den registrerade och om varje länk mellan det ursprungliga attributet och det pseudonymiserade attributet har tagits bort (inklusive genom att utplåna de ursprungliga uppgifterna), kommer det inte att finnas någon uppenbar korshänvisning mellan två dataset som använder olika pseudonymiserade attribut.
- *Inferens:* Inferensattacker mot den registrerades verkliga identitet är möjliga inom datasetet eller inom flera olika databaser som använder samma pseudonymiserade attribut för en enskild person, eller om pseudonymer är självförklarande och inte döljer den registrerades ursprungliga identitet ordentligt.

[17] Särskilt om attributets typ är känt (namn, personnummer, födelsedatum osv.). För att lägga till beräkningskrav kan man använda en hashfunktion för nyckelhärledning, där det beräknade värdet hashas flera gånger med ett kort salt.
[18] Beroende på övriga attribut i datasetet och på utplåning av de ursprungliga uppgifterna.

4.2. Vanliga misstag

- Att tro att ett pseudonymiserat dataset är avidentifierat: Registeransvariga tror ofta att det räcker att ta bort eller ersätta ett eller flera attribut för att göra datasetet anonymt. Många exempel har visat att så inte är fallet. Att bara ändra id förhindrar inte att någon identifierar en registrerad om kvasi-identifierare finns kvar i datasetet, eller om värdena för andra attribut fortfarande kan identifiera en person. I många fall kan det vara lika lätt att identifiera en person i ett pseudonymiserat dataset som med de ursprungliga uppgifterna. Extra åtgärder bör vidtas för att datasetet ska kunna anses som avidentifierat, bland annat att ta bort och generalisera attribut eller utplåna de ursprungliga uppgifterna eller åtminstone överföra dem till en starkt aggregerad nivå.
- Vanliga misstag vid användning av pseudonymisering som metod för att minska länkbarheten:
    - Att använda samma nyckel i olika databaser: Undanröjandet av olika datasets länkbarhet är starkt beroende av användningen av en nyckelbaserad algoritm och att en enskild person motsvarar olika pseudonymiserade attribut i olika sammanhang. För att minska länkbarheten är det därför viktigt att inte använda samma nyckel i olika databaser.
    - Att använda olika nycklar (”roterande nycklar”) för olika användare: Det kan vara frestande att använda olika nycklar för olika grupper av användare och ändra nyckel per användning (t.ex. att använda samma nyckel för att registrera 10 uppgifter om samma användare). Om denna åtgärd inte har rätt utformning kan den leda till återkommande mönster, vilket delvis minskar de avsedda fördelarna. Att t.ex. rotera nyckeln enligt särskilda regler för olika personer gör det lättare att länka uppgifterna för en viss person. Att återkommande pseudonymiserade uppgifter försvinner ur databasen samtidigt som en ny uppgift tillkommer kan signalera att båda posterna avser samma fysiska person.
    - Att behålla nyckeln: Om en hemlig nyckel lagras tillsammans med pseudonymiserade uppgifter, och uppgifterna läcker ut, kanske angriparen lätt kan länka de pseudonymiserade uppgifterna till deras ursprungliga attribut. Detsamma gäller om nyckeln lagras skilt från uppgifterna men inte på ett säkert sätt.

4.3. Brister med pseudonymisering

- *Hälsoskydd*

1. **Namn, adress, födelsedatum**	**2.** **Period med särskilt stöd**	**3.** **BMI**	**6.** **Kohortreferensnr**
[redacted]	< 2 år	15	QA5FRD4
	> 5 år	14	2B48HFG
	< 2 år	16	RC3URPQ
	> 5 år	18	SD289K9
	< 2 år	20	5E1FL7Q

Tabell 5. Ett exempel på pseudonymisering genom hashfunktion (namn, adress, födelsedatum) som lätt kan återföras.

Ett dataset har skapats för att undersöka sambandet mellan en persons vikt och mottagandet av ett särskilt stödbidrag. I det ursprungliga datasetet ingick den registrerades namn, adress och födelsedatum, men dessa uppgifter har utplånats. Kohortreferensnumret för forskningen genererades från de utplånade uppgifterna med hjälp av en hashfunktion. Trots att namn, adress och födelsedatum utplånades i tabellen är det lätt att beräkna kohortreferensnumren om man känner till en registrerads namn, adress och födelsedatum och den hashfunktion som användes.

- *Sociala nätverk*

  Det har visats[19] att känslig information om enskilda individer kan extraheras ur diagram över sociala nätverk, trots de pseudonymiseringsmetoder som tillämpats på sådana uppgifter. En leverantör av ett socialt nätverk antog felaktigt att pseudonymisering var tillförlitligt för att förhindra identifiering efter försäljning av uppgifter till andra företag för marknadsförings- och reklamändamål. I stället för verkliga namn, använde leverantören kortnamn, men detta var helt klart inte tillräckligt för att avidentifiera användarprofiler, eftersom relationerna mellan olika personer är unika och kan användas som en identifierare.

- *Platser*

  Forskare vid MIT[20] analyserade nyligen ett pseudonymiserat dataset bestående av 15 månaders koordinater för rumslig-temporal rörlighet för 1,5 miljoner människor inom ett område med en radie på 100 km. De visade att 95 % av befolkningen kunde särskiljas med hjälp av fyra lokaliseringspunkter och att det räckte med endast två punkter för att särskilja över 50 % av de registrerade (en av dessa punkter är känd och är högst sannolikt ”hem” eller ”kontor”) med mycket lite utrymme för integritetsskydd, trots att personernas identiteter pseudonymiserades genom att ersätta deras verkliga attribut […] med andra etiketter.

5. Slutsatser och rekommendationer

5.1. Slutsatser

Metoder för avidentifiering och anonymisering är föremål för intensiv forskning, och denna rapport har genomgående visat att varje metod har sina fördelar och nackdelar. För det mesta är det inte möjligt att ge minimirekommendationer om vilka parametrar som bör användas eftersom varje dataset måste bedömas från fall till fall.

I många fall innebär ett avidentifierat dataset fortfarande en kvarstående risk för de registrerade. Även när det inte längre är möjligt att exakt hämta posten för en enskild person, är det fortfarande möjligt att plocka ihop uppgifter om den personen med hjälp av andra informationskällor som är tillgängliga (offentliga eller inte). Det måste betonas att utöver den direkta effekten på registrerade som blir följden av en dålig avidentifieringsprocess (irritation, tidsförbrukning och känslan av att ha förlorat kontrollen genom att ingå i ett kluster utan att veta om det eller ha gett sitt samtycke), kan andra indirekta bieffekter av dålig avidentifiering förekomma när en registrerad felaktigt tas med i en målgrupp av en angripare vid behandling

[19] A. Narayanan och V. Shmatikov, ”De-anonymizing social networks”, i *30th IEEE Symposium on Security and Privacy*, 2009.
[20] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen och V. Blondel, ”Unique in the Crowd: The privacy bounds of human mobility”, *Nature*, nr 1376, 2013.

av avidentifierade uppgifter, särskilt om angriparens avsikt är att skada. Arbetsgruppen betonar därför att avidentifieringsmetoder kan ge integritetsgarantier, men endast om tillämpningen av dem är utformad på lämpligt sätt, vilket innebär att förutsättningarna (sammanhanget) och målet eller målen för avidentifieringsprocessen måste vara klart fastställda för att åstadkomma önskad avidentifieringsnivå.

5.2. Rekommendationer

- Vissa avidentifieringsmetoder har inneboende begränsningar. Dessa begränsningar måste övervägas ordentligt innan registeransvariga använder en viss metod för att utforma en avidentifieringsprocess. De måste ta hänsyn till ändamål som ska uppnås genom avidentifieringen, t.ex. att skydda enskilda personers integritet när ett dataset offentliggörs eller tillåta att en viss uppgift hämtas från ett dataset.
- Ingen av de metoder som beskrivs i detta dokument uppfyller med säkerhet kriterierna för effektiv avidentifiering (dvs. ingen enskild person ska kunna särskiljas, ingen länkbarhet mellan poster som rör en enskild person och ingen möjlighet att dra slutsatser om en enskild person). En del av dessa risker kan dock mötas helt eller delvis av en viss metod. Det krävs därför omsorgsfull utformning av tillämpningen av en viss metod på den specifika situationen och tillämpningen av en kombination av metoderna som ett sätt att göra resultatet mer tillförlitligt.

I nedanstående tabell ges en översikt över metodernas starka och svaga sidor i fråga om de tre grundkraven:

	Är särskiljbarhet fortfarande en risk?	**Är länkbarhet fortfarande en risk?**	**Är inferens fortfarande en risk?**
Pseudonymisering	Ja	Ja	Ja
Brustillägg	Ja	Går inte	Går inte
Substitution	Ja	Ja	Går inte
Aggregering eller *k*-anonymitet	Nej	Ja	Ja
L-diversitet	Nej	Ja	Går inte
Differentiell integritet	Går inte	Går inte	Går inte
Hashfunktion/tokenisering	Ja	Ja	Går inte

Tabell 6. De diskuterade metodernas starka och svaga sidor.

- Den optimala lösningen bör bestämmas från fall till fall. En lösning (dvs. en fullständig avidentifieringsprocess) som uppfyller de tre kriterierna är motståndskraftig mot identifiering som utförs med de mest rimliga hjälpmedel som den registeransvarige eller någon annan person kan tänkas utnyttja.
- Om ett förslag inte uppfyller något av kriterierna bör en grundlig utvärdering av identifieringsriskerna utföras. Utvärderingen bör överlämnas till tillsynsmyndigheten om det i nationell lagstiftning krävs att myndigheten ska bedöma eller ge tillstånd till avidentifieringsprocessen.

För att minska identifieringsriskerna bör följande goda praxis beaktas:

<u>God avidentifieringspraxis</u>

Som allmän regel:

- Man bör inte förlita sig på strategin ”gör tillgängligt och glöm bort”. Med tanke på den kvarstående identifieringsrisken bör den registeransvarige
    - 1. identifiera nya risker och regelbundet göra en ny utvärdering av den kvarstående risken,
    - 2. bedöma om kontrollerna för identifierade risker är tillräckliga och annars justera dem, och
    - 3. övervaka och kontrollera riskerna.
- Ta hänsyn till identifieringspotentialen hos eventuell icke-avidentifierad del av ett dataset, särskilt om denna del kombineras med den avidentifierade delen, plus eventuella korrelationer mellan attribut (t.ex. mellan geografisk plats och uppgifter om förmögenhetsnivå) vid bedömningen av kvarvarande risker.

Sammanhangsaspekter:

- De ändamål som ska uppnås med det avidentifierade datasetet bör tydligt anges eftersom de spelar en viktig roll vid fastställandet av identifieringsrisken.
- Detta går hand i hand med att beakta alla relevanta omständigheter i sammanhanget, t.ex. vilken beskaffenhet de ursprungliga uppgifterna har, införda kontrollmekanismer (inklusive säkerhetsåtgärder för att begränsa tillgången till dataset), sampelstorleken (kvantitativa egenskaper), tillgång till offentliga informationsresurser (som mottagarna kan utnyttja, planerat överlämnande av uppgifter till tredje parter (begränsat, obegränsat t.ex. på internet osv.).
- Tänkbara angripare bör övervägas genom att beakta om uppgifterna är lockande för målinriktade attacker (även i detta avseende är uppgifternas känslighet och beskaffenhet viktiga faktorer).

Tekniska aspekter:

- Registeransvariga bör upplysa om den avidentifieringsmetod eller den blandning av metoder som införs, särskilt om de planerar att offentliggöra eller överföra det avidentifierade datsetet.
- Uppenbara (t.ex. ovanliga) attribut/kvasi-identifierare bör avlägsnas från datasetet.
- Om brustilläggsmetoder används (i randomisering), bör den brusnivå som läggs till i posterna fastställas som en funktion av värdet för ett attribut (dvs. oproportionerligt brus bör inte infogas), liksom konsekvensen för de registrerade av de attribut som ska skyddas och/eller datasetets gleshet.
- Om differentiell integritet används (i randomisering) bör hänsyn tas till behovet av att följa upp sökfrågor för att upptäcka frågor som gör intrång i integriteten eftersom frågornas intrång är ackumulerande.
- Om generaliseringsmetoder införs är det viktigt att de registeransvariga inte begränsar sig till ett generaliseringskriterium ens för samma attribut, dvs. man bör välja olika granularitet eller olika tidsintervall. Valet av kriterium som ska tillämpas måste styras av attributvärdenas fördelning i den berörda populationen. Alla fördelningar är inte lämpliga att generaliseras, dvs. det finns ingen universalmetod som kan följas vid generalisering. Variabiliteten inom ekvivalensklasser bör säkerställas. Exempelvis bör en specifik tröskel väljas beroende på de ovannämnda sammanhangsaspekterna (sampelstorlek m.m.), och om den tröskeln inte uppnås bör detta sampel kasseras (eller ett annat generaliseringskriterium fastställas).

BILAGA
En introduktion till avidentifieringsmetoder

A.1. Inledning

Anonymitet tolkas på olika sätt i EU. I en del länder betyder det datorrelaterad anonymitet (dvs. det bör vara datatekniskt svårt, även för den registeransvarige i samarbete med någon annan part, att direkt eller indirekt identifiera någon av de registrerade). I andra länder betyder det total anonymitet (dvs. det bör vara omöjligt, även för den registeransvarige i samarbete med någon annan part, att direkt eller indirekt identifiera någon av de registrerade). I båda fallen innebär dock ”avidentifiering” den process genom vilken uppgifter görs anonyma. Skillnaden beror på vad som betraktas som en godtagbar nivå för risken för återidentifiering.

Olika användningsområden kan planeras för avidentifierade uppgifter, bland annat sociala undersökningar, statistiska analyser, utveckling av en ny tjänst eller produkt. Ibland kan även sådana verksamheter för allmänna ändamål ha konsekvenser för vissa registrerade personer och omintetgöra de behandlade uppgifternas förmodade anonyma beskaffenhet. Många exempel kan ges, alltifrån inledandet av målinriktade marknadsföringsinitiativ till genomförandet av offentliga åtgärder som grundas på användarprofilering, användarbeteenden eller rörlighetsmönster[21].

Förutom allmänna uttalanden finns det ingen mogen mätmetod för att i förväg utvärdera vilken tid eller insats som krävs för återidentifiering efter behandlingen, eller alternativt att välja att införa det lämpligaste förfarandet om man vill minska sannolikheten för att en tillgängliggjord databas refererar till en identifierad uppsättning registrerade personer.

”Avidentifieringskonsten”, som dessa metoder ibland kallas i den vetenskapliga litteraturen[22], är ett nytt forskningsfält som fortfarande befinner sig i sin linda, och det finns många metoder för att minska datasets identifieringsförmåga. Det måste dock sägas tydligt att de flesta av dessa metoder inte förhindrar att behandlade uppgifter länkas till registrerade personer. Under vissa omständigheter har man med framgång identifierat dataset som ansågs vara anonyma, och i andra fall har falska positiva identifieringar förekommit.

Generellt kan man säga att det finns två olika typer av metoder: Den ena bygger på attributgeneralisering, den andra på randomisering. Genom att gå igenom detaljerna och nyanserna för dessa metoder får vi en ny insikt om möjligheterna att identifiera uppgifter, och det kastar samtidigt nytt ljus på själva begreppet personuppgifter.

A.2. Avidentifiering genom randomisering

Ett alternativ för avidentifiering består av att ändra de faktiska värdena för att förhindra länkning mellan de avidentifierade uppgifterna och de ursprungliga värdena. Detta mål kan uppnås genom en rad olika metoder, allt från tillägg av brus till uppgiftsväxling (permutation). Det måste betonas att borttagningen av ett attribut motsvarar en extrem form av randomisering av detta attribut (attributet täcks helt av brus).

Under vissa omständigheter är målet med hela förfarandet inte i första hand att göra ett randomiserat dataset tillgängligt utan snarare att ge åtkomst till uppgifterna med hjälp av

[21] Ett exempel är TomTom-fallet i Nederländerna (se det exempel som förklaras i avsnitt 2.2.3).

[22] Jun Gu, Yuexian Chen, Junning Fu, Huanchun Peng, Xiaojun Ye, Synthesizing: Art of Anonymization, Database and Expert Systems Applications, Lecture Notes in Computer Science – *Springer*, vol. 6261, 2010, s. 385–389.

sökfrågor. Risken för den registrerade uppkommer i det här fallet från sannolikheten för att en angripare kan extrahera information från en rad olika sökfrågor utan den registeransvariges kännedom. För att garantera anonymiteten för de registrerade i datasetet får det inte vara möjlighet att sluta sig till att en registrerad bidragit till datasetet, dvs. man måste bryta länken till alla slags bakgrundsinformation som en angripare kan ha.

Genom att lägga till lämpligt brus i svaret på sökfrågan kan man ytterligare minska risken för återidentifiering. Detta tillvägagångssätt, som även kallas differentiell integritet[23], skiljer sig från de ovan beskrivna metoderna genom att uppgiftspublicerare ges större kontroll över åtkomsten till uppgifterna än vid offentliggörande. Tillägget av brus har följande två huvudsyften: för det första att skydda de registrerades integritet, och för det andra att bevara de tillgängliggjorda uppgifternas användbarhet. Brusets omfattning måste stå i proportion till frågenivån (alltför många sökfrågor om enskilda som ska besvaras alltför korrekt ökar sannolikheten för identifiering). I dag måste frågan om vad som är en lämplig tillämpning av randomisering bedömas från fall till fall eftersom ingen teknik erbjuder en idiotsäker metod. Det finns exempel på informationsläckor om en registrerad persons attribut (oavsett om attributet ingår i datasetet eller inte) även när den registeransvarige betraktat datasetet som randomiserat.

Det kan vara värdefullt att diskutera konkreta exempel för att klargöra potentiella misslyckanden med randomisering som medel att åstadkomma avidentifiering. Exempelvis i samband med interaktiv åtkomst kan sökfrågor som anses icke-integritetskänsliga utgöra en risk för de registrerade. Låt oss tänka oss att angriparen känner till att en personundergrupp S finns i det dataset som innehåller information om förekomsten av attributet A i en population P. Då kan angriparen helt enkelt söka med de två frågorna: ”Hur många personer i population P har attributet A?” och ”Hur många personer i population P, utom de som tillhör undergrupp S, har attribut A?” Därefter kan det vara möjligt för angriparen att bestämma hur många personer i S som faktiskt har attribut A (skillnaden) – antingen deterministiskt eller genom sannolikhetsinferens. Under alla omständigheter kan integriteten för personerna i undergrupp S vara allvarligt hotad, särskilt beroende på beskaffenheten av attribut A.

Om en registrerad inte finns i datasetet men den registrerades relation till uppgifterna i datasetet är känd kan det också anses att tillgängliggörandet av datasetet utgör en risk för den registrerades integritet. Om det t.ex. är känt att ”målpersonens värde för attribut A skiljer sig med kvantiteten X från populationens medelvärde” kan angriparen genom att helt enkelt be databasförvaltaren att utföra den icke-integritetskänsliga åtgärden att extrahera medelvärdet för attributet A exakt sluta sig till en personuppgift som rör en viss registrerad person.

Infogande av vissa relativa felaktigheter i de verkliga värdena i en databas är en åtgärd som måste utformas omsorgsfullt. Tillräckligt men inte för mycket brus måste läggas till för att skydda integriteten och samtidigt bevara uppgifternas användbarhet. Om det till exempel är mycket få registrerade som har ett märkligt attribut eller om attributet är känsligt kan det vara bättre att redovisa ett intervall eller lämna en allmän beskrivning som ”ett fåtal fall, troligen t.o.m. noll”, i stället för att redovisa det faktiska antalet. På så sätt bevaras den registrerades integritet eftersom en viss ovisshet kvarstår även om brusmekanismen är känd i förväg. Från användbarhetssynpunkt är resultaten fortfarande användbara för statistikändamål eller beslutsfattande om felaktigheten har utformats på rätt sätt.

[23] Cynthia Dwork, Differential Privacy, International Colloquium on Automata, Languages and Programming (ICALP) 2006, s. 1–12.

Databasrandomisering och differentiell integritet kräver ytterligare eftertanke. För det första kan vad som är lagom mycket förvrängning variera betydligt beroende på sammanhanget (typen av sökfråga, populationsstorleken i databasen, attributets beskaffenhet och dess inneboende identifierbarhet), och ingen lösning kan utpekas som den bästa. Dessutom kan omständigheterna förändras över tiden, och den interaktiva mekanismen bör ändras i enlighet med detta. För att kalibrera bruset måste man följa upp de ackumulerade risker som en interaktiv mekanism medför för de registrerade. Mekanismen för åtkomst till uppgifterna bör sedan förses med varningar när en budget för ”integritetskostnader” har uppnåtts och de registrerade kan vara utsatta för specifika risker om en ny sökfråga skickas. Det hjälper den registeransvarige att bestämma vilken brusnivå som det är lämpligt att tillfoga i de faktiska personuppgifterna i det aktuella fallet.

Vi bör också överväga fall då attributvärdena har utplånats (eller ändrats). En ofta använd lösning för att hantera vissa atypiska attributvärden är att utplåna antingen de uppgifter som är relaterade till de atypiska personerna eller utplåna de atypiska värdena. I det senare fallet är det viktigt att se till att avsaknaden av värde inte i sig blir ett element som gör att en registrerad kan identifieras.

Låt oss nu titta på randomisering genom attributersättning. En vanlig missuppfattning i samband med avidentifiering är att likställa det med kryptering eller nyckelbaserad kodning. Detta misstag beror på två antaganden, nämligen a) att när kryptering tillämpas på vissa attribut för en post i en databas (t.ex. namn, adress, födelsedatum), eller när dessa attribut ersätts med en till synes randomiserad sträng som resultat av en nyckelbaserad kodningsoperation som t.ex. en hashfunktion, blir den posten avidentifierad, och b) att avidentifieringen blir effektivare om nyckeln är tillräckligt lång och en modern krypteringsalgoritm används. Denna missuppfattning är vanligt förekommande bland registeransvariga och förtjänar ett klargörande, vilket också är fallet för pseudonymisering och dess påstått lägre risker.

För det första har dessa tekniker helt olika syften: Kryptering är ett säkerhetsförfarande som syftar till att göra en kommunikationskanal mellan identifierade parter (människor, enheter eller programvaru- eller maskinvarukomponenter) konfidentiell för att undvika tjuvlyssnande eller oavsiktliga avslöjanden. Nyckelbaserad kodning är en semantisk översättning av uppgifter enligt en hemlig nyckel. Syftet med avidentifiering är däremot att undvika att enskilda personer identifieras genom att förhindra att attribut länkas till en registrerad person.

Varken kryptering eller nyckelbaserad kodning är i sig lämpad för syftet att göra en registrerad oidentifierbar: De ursprungliga uppgifterna är fortfarande tillgängliga eller härledbara, åtminstone för den registeransvarige. Att enbart genomföra en semantisk översättning av personuppgifter, som vid nyckelbaserad kodning, undanröjer inte möjligheten att återställa uppgifterna i deras ursprungliga struktur genom att tillämpa algoritmen i motsatt riktning, eller genom attacker med ren råstyrka, beroende på systemens beskaffenhet eller till följd av ett personuppgiftsbrott. Modern kryptering kan säkerställa att uppgifterna är i hög grad skyddade, dvs. uppgifterna är obegripliga för enheter som inte känner till dekrypteringsnyckeln, men detta leder inte nödvändigtvis till avidentifiering. Så länge som nyckeln eller de ursprungliga uppgifterna är tillgängliga har möjligheten att identifiera den registrerade inte undanröjts. (Detta gäller även om det finns en betrodd tredje part som har en avtalsmässig skyldighet att tillhandahålla nyckeldeponeringstjänster.) .

Att enbart uppmärksamma krypteringsmekanismens robusthet som ett mått på graden av avidentifiering av ett dataset är missledande eftersom många andra tekniska och organisatoriska faktorer påverkar en krypteringsmekanisms eller hashfunktions totala

säkerhet. Många framgångsrika angrepp har rapporterats i litteraturen som helt kringgår algoritmen, antingen därför att de utnyttjar en svaghet i förvaret av nycklarna (t.ex. att det finns ett mindre säkert standardläge) eller andra mänskliga faktorer (t.ex. svaga lösenord för nyckelåterskapande). Ett visst krypteringsschema med en viss nyckelstorlek är utformat för att garantera konfidentialiteten under en viss period (storleken på de flesta av dagens nycklar kommer att behöva ändras omkring 2020), men en avidentifieringsprocess får inte vara tidsbegränsad.

Det är värt att nu fundera över begränsningarna hos attributrandomisering (eller ersättning och borttagning) och beakta olika dåliga exempel på avidentifiering genom randomisering på senare år och orsakerna till dessa misslyckanden.

Netflix-priset[24] är ett välkänt fall av offentliggörande av ett dåligt avidentifierat dataset. Om man tittar på en allmän post i en databas där ett antal attribut som rör en registrerad person randomiserats kan varje post fortfarande vara uppdelad i två underposter på följande sätt: {randomiserade attribut, attribut i klartext}, där attributen i klartext fortfarande kan vara vilken kombination som helst av vad som antas vara uppgifter som inte är personuppgifter. Ett konstaterande som kan göras från Netflix Prize-datasetet är att varje post kan representeras av en punkt i en flerdimensionell rymd, där varje attribut i klartext är en koordinat. Genom denna teknik kan varje dataset ses som en sammanställning av punkter i en sådan flerdimensionell rymd, som kan vara mycket glest, dvs. att punkterna ligger långt ifrån varandra. De kan faktiskt ligga så långt ifrån varandra att varje region endast innehåller en post när rymden har delats upp i breda regioner. Även om brus tillförs kommer posterna inte att vara tillräckligt nära varandra för att dela en gemensam flerdimensionell rymd. I Netflix-experimentet var posterna tillräckligt unika med endast åtta filmomdömen avgivna med 14 dagars avstånd. Efter tillägg av brus till både omdömen och datum kunde ingen överlappning av regioner observeras. Med andra ord utgjorde just detta urval med endast åtta bedömda filmer ett fingeravtryck för de uttryckta omdömena, som inte delades av två olika registrerade i databasen. Utifrån denna geometriska observation matchade forskarna det enligt uppgift avidentifierade Netflix-datasetet med andra offentligt tillgängliga databaser med filmomdömen (IMDb), och hittade på så sätt användare som hade lämnat omdömen om samma filmer inom samma tidsintervall. Eftersom majoriteten av användarna uppvisade en ett-till-ett-överensstämmelse kunde extrainformationen i IMDb-databasen importeras till det tillgängliggjorda Netflix-datasetet för att därigenom berika dessa enligt förmodan avidentifierade poster med identiteter.

Det är viktigt att betona att detta är en allmän egenskap: Den resterande delen av en randomiserad databas har fortfarande en mycket hög identifieringsförmåga, därför att kombinationen av restattribut är sällsynt. Detta är en varning som registeransvariga alltid bör hålla i minnet när de väljer randomisering som sitt sätt att uppnå riktad avidentifiering.

Många återidentifieringsexperiment av detta slag har följt en liknande uppläggning där man projicerat två databaser på samma delrymd. Detta är en mycket kraftfull återidentifieringsmetod, som nyligen har fått många tillämpningar på olika områden. Som exempel kan nämnas ett identifieringsexperiment som utfördes mot ett socialt nätverk[25], där den sociala grafen utnyttjades för användare som pseudonymiserats med hjälp av etiketter. I

[24] Arvind Narayanan, Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, *IEEE Symposium on Security and Privacy 2008*, s. 111–125.

[25] L. Backstrom, C. Dwork och J. M. Kleinberg, Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography, *Proceedings of the 16th International Conference on World Wide Web WWW'07*, s. 181–190 (2007).

detta fall var de attribut som användes för identifieringen varje användares kontaktlista, eftersom det visade sig att det var mycket osannolikt att två personer hade identiska kontaktlistor. Utifrån detta intuitiva antagande upptäckte man att en delgraf över de interna förbindelserna mellan ett mycket begränsat antal noder bildade ett topologiskt fingeravtryck, dolt i nätverket, som kunde hämtas fram och att en stor andel av hela det sociala nätverket kan identifieras så snart detta delnätverk har identifierats. Här följer lite uppgifter om en liknande attack. Det har visats att man genom att använda färre än tio noder (som kan ge upphov till miljontals olika delnätskonfigurationer, som var och en potentiellt utgör ett topologiskt fingeravtryck) kan utsätta ett socialt nätverk med över 4 miljoner pseudonymiserade noder och 70 miljoner länkar för återidentifieringsattacker, och att integriteten för ett stort antal förbindelser kan äventyras. Det måste betonas att denna återidentifieringsmetod inte är skräddarsydd för just sociala nätverk, utan är tillräckligt generell för att kunna anpassas till andra databaser där relationerna mellan användare registreras (t.ex. telefonkontakter, e-postkorrespondens, nätdejtningswebbplatser m.m.).

Ett annat sätt att identifiera en förmodat avidentifierad post bygger på stilistisk analys av texter (stylometry).[26] En rad algoritmer har redan utvecklats för att extrahera mätvärden från analyserad text, bland annat frekvensen av särskilda ordval, förekomsten av vissa grammatiska mönster och användningen av skiljetecken. Alla dessa egenskaper kan användas för att förankra en påstått anonym text till en identifierad författares skrivsätt. Forskare har undersökt skrivsättet i fler än 100 000 bloggar och kan i dag automatiskt identifiera författaren av ett inlägg med en precision som redan närmar sig 80 %. Teknikens precision förväntas öka ytterligare när man även utnyttjar andra signaler, t.ex. platsuppgifter eller andra metadata i texten.

Möjligheten till identifiering genom att använda semantiska särdrag i en post (dvs. den kvarvarande icke-randomiserade delen av en post) är en fråga som förtjänar större uppmärksamhet från forskarvärlden och näringslivet. Återföringen nyligen av DNA-givares identiteter (2013)[27] visar att mycket lite framsteg har gjorts sedan den välkända AOL-incidenten (2006) – då en databas som innehöll tjugo miljoner söknyckelord för över 650 000 användare under en 3-månadersperiod offentliggjordes. Detta ledde till identifiering och positionering av ett antal AOL-användare.

En annan grupp av uppgifter som sällan avidentifieras enbart genom att ta bort de registrerades identiteter eller genom att delvis kryptera vissa attribut är lokaliseringsdata. Människors rörlighetsmönster kanske kan vara tillräckligt unika för att den semantiska delen av lokaliseringsdata (de platser där den registrerade personen befann sig vid en viss tidpunkt), även utan andra attribut, ska klara att avslöja många av den registrerades särdrag.[28] Detta har bevisats många gånger i representativa vetenskapliga studier.[29]

---

[26] http://33bits.org/2012/02/20/is-writing-style-sufficient-to-deanonymize-material-posted-online/

[27] Genetiska uppgifter är ett särskilt viktigt exempel på känsliga data som riskerar att återidentifieras om den enda mekanismen för avidentifiering är att givarnas identitet tas bort. Se det exempel som citerades i avsnitt 2.2.2 ovan. Se även John Bohannon, Genealogy Databases Enable Naming of Anonymous DNA Donors, *Science*, Vol. 339, nr 6117 (18 januari 2013), s. 262.

[28] Detta problem har tagits upp i vissa nationella lagstiftningar. I exempelvis Frankrike avidentifieras offentliggjord lokaliseringsstatistik genom generalisering och permutation. INSEE publicerar således statistik som är generaliserad genom aggregering av alla uppgifter till en 40 000 kvadratmeter stor yta. Datasetets granularitet är tillräckligt för att bevara uppgifternas användbarhet och permutationer förhindrar återidentifieringsattacker i glesa områden. Aggregeringen och permutationen av uppgifter av detta slag ger starka garantier mot inferens- och återidentifieringsattacker (http://www.insee.fr/en/).

[29] de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. *Nature*. 3, 1376 (2013).

Här är det nödvändigt att varna för användningen av pseudonymer som ett sätt att ge de registrerade tillräckligt skydd mot identitets- eller attributläckor. Om pseudonymiseringen bygger på att ersätta en identitet med en annan unik kod är antagandet att detta utgör en robust avidentifiering naiv, och man tar inte hänsyn till mängden olika identifieringsmetoder och de många olika sammanhang där dessa kan tillämpas.

A.3. Avidentifiering genom generalisering

Ett enkelt exempel kan hjälpa till att förklara det tillvägagångssätt som bygger på attributgeneralisering.

Låt oss ta fallet där en registeransvarig bestämmer sig för att tillgängliggöra en enkel tabell som innehåller tre uppgifter eller attribut: ett identifieringsnummer, som är unikt för varje post, en platsidentifiering, som länkar den registrerade till dennes bostadsort och en egenskapsidentifiering, som visar den registrerades egenskap. Låt oss vidare anta att denna egenskap har två distinkta värden, generellt angivna genom {P1, P2}:

Löpnr	**Plats-id**	**Egenskap**
#1	Rom	P1
#2	Madrid	P1
#3	London	P2
#4	Paris	P1
#5	Barcelona	P1
#6	Milano	P2
#7	New York	P2
#8	Berlin	P1

Tabell A1. Urval av registrerade som grupperats efter plats och egenskaperna P1 och P2.

Om en angripare på förhand vet att en viss registrerad person (målet) som bor i Milano ingår i tabellen, vet angriparen också efter att ha studerat tabellen att den registrerade har egenskapen P2, eftersom nr 6 är den enda registrerade som har detta plats-id.

Detta mycket enkla exempel visar huvudelementen i varje identifieringsförfarande som tillämpas på ett dataset som har genomgått vad som förmodas vara en avidentifieringsprocess. Det vill säga att det finns en angripare som (av en tillfällighet eller avsiktligt) hade bakgrundskunskaper om vissa eller alla registrerade i ett dataset. Angriparen försöker länka denna bakgrundskunskap till uppgifterna i det tillgängliggjorda datasetet för att få en tydligare bild av de registrerades egenskaper.

För att göra det mindre effektivt eller mindre omedelbart att länka uppgifter till någon form av bakgrundskunskap fokuserar den registeransvarige på plats-id och ersätter staden där de registrerade bor med ett större område som t.ex. landet. Då kommer tabellen att se ut på följande sätt.

Löpnr	Plats-id	Egenskap
#1	Italien	P1
#2	Spanien	P1
#3	UK	P2
#4	Frankrike	P1
#5	Spanien	P1
#6	Italien	P2
#7	USA	P2
#8	Tyskland	P1

Tabell A2. Generalisering av tabell A1 efter nationalitet.

Med denna nya uppgiftsaggregering tillåter angriparens bakgrundskunskap om en identifierad registrerad (t.ex. ”målet bor i Rom och han finns i tabellen”) inte att angriparen drar några tydliga slutsatser om den registrerades egenskap: Detta beror på att de båda italienarna i tabellen har olika egenskaper, P1 respektive P2. Angriparen lämnas med 50 % osäkerhet om målpersonens egendom. Detta enkla exempel visar effekten av generalisering på avidentifieringsförfarandet. Även om detta generaliseringstrick kan vara effektivt för att halvera sannolikheten för att identifiera en italiensk målperson, är det inte effektivt när personen i fråga kommer från andra länder (t.ex. USA).

En angripare kan fortfarande få fram information om en spanjor. Om bakgrundskunskapen är av typen ”målpersonen bor i Madrid och han finns i tabellen” eller ”målpersonen bor i Barcelona och han finns i tabellen”, kan angriparen alltså med 100 % säkerhet dra slutsatsen att målpersonen har egenskapen P1. Generalisering ger därför inte samma nivå av integritetsskydd eller motståndskraft mot interferensattacker mot hela populationen i datasetet.

Enligt detta resonemang kan man frestas att dra slutsatsen att starkare generalisering kan bidra till att förhindra länkning, t.ex. en generalisering efter kontinent. Då kommer tabellen att se ut på följande sätt:

Löpnr	Plats-id	Egenskap
#1	Europa	P1
#2	Europa	P1
#3	Europa	P2
#4	Europa	P1
#5	Europa	P1
#6	Europa	P2
#7	Nordamerika	P2
#8	Europa	P1

Tabell A3. Generalisering av tabell A1 efter kontinent.

Med en aggregering av detta slag skulle alla registrerade i tabellen, utom den person som bor i USA, skyddas mot länknings- och identifieringsangrepp. All bakgrundsinformation av typen ”målpersonen bor i Madrid och han finns i tabellen” eller ”målpersonen bor i Milano och han finns i tabellen” leder till samma nivå av sannolikhet om den egenskap som är tillämplig på en viss registrerad (P1 med sannolikhet 71,4 % och P2 med sannolikhet 28,6 %), i stället för med

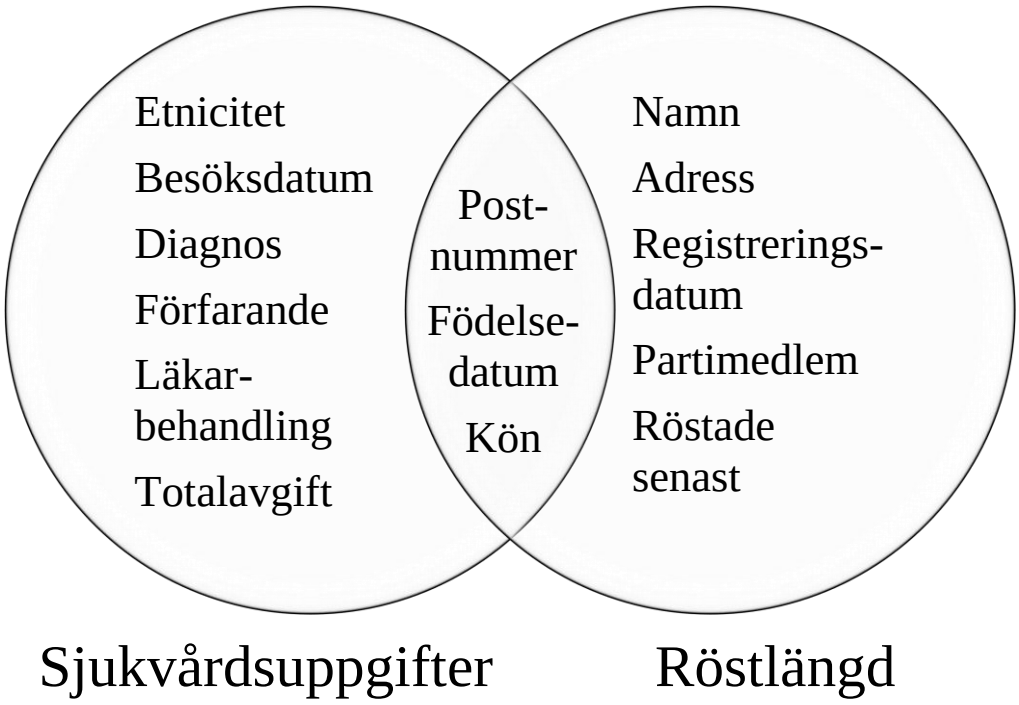
direkt länkning. Denna ytterligare generalisering sker också på bekostnad av en uppenbar och radikal förlust av information: Tabellen gör det inte möjligt att upptäcka potentiella korrelationer mellan egenskaperna och platsen, nämligen om en viss plats kan utlösa någon av de båda egenskaperna med högre sannolikhet, eftersom den endast ger s.k. marginella fördelningar, det vill säga den absoluta sannolikheten att egenskapen P1 och P2 förekommer i populationen (62,5 % respektive 37,5 % i vårt exempel) och inom respektive kontinent (71,4 % och 28,6 % i Europa respektive 100 % och 0 % i Nordamerika).

Exemplet visar också att generalisering påverkar uppgifternas praktiska användbarhet. Det finns i dag vissa tekniska verktyg för att i förväg (dvs. innan ett dataset görs tillgängligt) avgöra den lämpligaste nivån av attributgeneralisering för att minska risken att registrerade i tabellen identifieras utan att i onödigt hög grad påverka användbarheten hos de tillgängliga uppgifterna.

k-anonymitet

Ett försök att förhindra länkningsattacker som kallas *k*-anonymitet bygger på generalisering av attribut. Metoden härrör från ett experiment med återidentifiering som utfördes i slutet av 1990-talet, då ett privat amerikanskt företag som var verksamt inom hälso- och sjukvårdssektorn gjorde ett förmodat avidentifierat dataset allmänt tillgängligt. Denna avidentifiering bestod av att ta bort de registrerades namn, men datasetet innehöll fortfarande hälsouppgifter och andra egenskaper såsom postnummer (id för den plats där de bodde), kön och det fullständiga födelsedatumet. Samma triplett {postnummer, kön, fullständigt födelsedatum} ingick även i andra offentligt tillgängliga register (t.ex. röstlängden) och kunde därmed användas av en forskare för att länka enskilda registrerade personers identitet till attributen i det tillgängliga datasetet. De bakgrundskunskaper som angriparen (forskaren) har kan vara följande: ”Jag vet att den registrerade i röstlängden med en viss triplett {postnummer, kön, fullständigt födelsedatum} är unik. Det finns en post i det offentliggjorda datasetet med den tripletten”. Det har empiriskt konstaterats[30] att den stora majoriteten (över 80 %) av de registrerade i det offentliga register som användes i detta forskningsexperiment var entydigt associerade till en viss triplett, vilket gjorde identifieringen möjlig. Följaktligen var uppgifterna inte ordentligt avidentifierade i detta fall.

[30] L. Sweeney, Weaving Technology and Policy Together to Maintain Confidentiality, *Journal of Law, Medicine & Ethics*, 25, nr 2 och 3 (1997), s. 98–110.



Figur A1. Återidentifieringen genom sammanlänkning av uppgifter.

Det har hävdats att den registeransvarige för att minska effektiviteten hos liknande länkningsattacker först bör inspektera datasetet och gruppera de attribut som en angripare rimligen kan använda för att länka den tillgängliggjorda tabellen till en extra källa. Varje grupp bör innehålla minst *k* identiska kombinationer av generaliserade attribut (dvs. den ska representera en ekvivalensklass av attribut). Dataset bör sedan tillgängliggöras först efter att det partitionerats i sådana homogena grupper. De attribut som väljs för generalisering kallas i litteraturen kvasi-identifierare, eftersom den som känner till dem i klartext omedelbart kan identifiera de registrerade.

Många identifieringsexperiment har visat svagheten i dåligt utformade *k*-avidentifieringstabeller. Detta kan exempelvis inträffa därför att attributen i en ekvivalensklass är identiska (så som för ekvivalensklassen spanska registrerade i exemplet i tabell A2) eller därför att deras fördelning är mycket obalanserad med hög prevalens för ett visst attribut, eller därför att antalet poster i en ekvivalensklass är mycket litet. I båda fallen ger detta möjlighet till sannolikhetsinferens. Det kan också bero på det inte finns någon signifikant semantisk skillnad mellan attributen i klartext i ekvivalensklasserna (t.ex. kan det kvantitativa måttet för sådana attribut vara olika men numeriskt mycket nära, eller de kan tillhöra ett intervall av semantiskt likartade attribut, t.ex. samma intervall av kreditrisk eller samma patologigrupp), så att datasetet fortfarande kan läcka en stor mängd information om de registrerade för länkningsattacker.[31] En viktig punkt här är att om datasetet är glest (t.ex. att det finns färre förekomster av en viss egenskap i ett geografiskt område) och man med en första aggregering inte lyckas gruppera uppgifter med ett tillräckligt antal förekomster av olika egenskaper (det finns t.ex. fortfarande ett litet antal förekomster för några få egenskaper i ett geografiskt område), krävs ytterligare attributaggregering för att uppnå den önskade avidentifieringen.

[31] Det måste framhållas att korrelationer också kan fastställas efter att dataposterna har grupperats efter attribut. När den registeransvarige känner till vilka typer av korreleringar han vill verifiera, kan han välja de attribut som är mest relevanta. I PEW-undersökningsresultaten är de registrerade inte utsatta för finkorniga inferensattacker,

l-diversitet

Med utgångspunkt från dessa observationer har varianter av *k*-anonymitet föreslagits under årens lopp, och vissa utformningskriterier för att förbättra avidentifieringsförfarandet genom generalisering har utvecklats i syfte att minska riskerna för länkningsattacker. De bygger på de probabilistiska egenskaperna hos dataset. En ytterligare begränsning läggs därför till, nämligen att varje attribut i en ekvivalensklass förekommer minst *l* gånger så att angriparen alltid har en betydande kvarvarande ovisshet om attributen även om angriparen har bakgrundskunskap om en viss registrerad person. Detta är detsamma som att ett dataset (eller en partition) ska ha ett visst minimiantal förekomster av en vald egenskap: Detta trick kan begränsa risken för återidentifiering. Det är detta som är målet med avidentifieringsmetoden *l*-diversitet. Ett exempel på denna metod finns i tabellerna A4 (de ursprungliga uppgifterna) och A5 (resultatet av behandlingen). Genom att utforma plats-id och personernas åldrar på lämpligt sätt i tabell A4 leder generaliseringen av attributen till en betydande ökning av ovissheten om de verkliga attributen för varje registrerad person i undersökningen. Även om angriparen exempelvis vet att en registrerad tillhör den första ekvivalensklassen, kan han inte ytterligare förvissa sig om huruvida en person har egenskapen X, Y eller Z, eftersom det finns minst en post i den klassen (och i alla andra ekvivalensklasser) som har sådana egenskaper.

Löpnr	Plats-id	Ålder	Egenskap
1	111	38	X
2	122	39	X
3	122	31	Y
4	111	33	Y
5	231	60	Z
6	231	65	X
7	233	57	Y
8	233	59	Y
9	111	41	Z
10	111	47	Z
11	122	46	Z
12	122	45	Z

Tabell A4. En tabell med enskilda personer grupperade efter plats, ålder och tre egenskaper X, Y och Z.

och uppgifterna är fortfarande användbara för att hitta korrelationer mellan demografiska uppgifter och intressen (http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx).

Löpnr	Plats-id	Ålder	Egenskap
1	11*	< 50	X
4	11*	< 50	Y
9	11*	< 50	Z
10	11*	< 50	Z
5	23*	> 50	Z
6	23*	> 50	X
7	23*	> 50	Y
8	23*	> 50	Y
2	12*	< 50	X
3	12*	< 50	Y
11	12*	< 50	Z
12	12*	< 50	Z

Tabell A5. Ett exempel på en 1-diversitetsversion av tabell A4.

t-närhet:

Specialfallet med attribut inom en partition som är ojämnt fördelade eller tillhör ett litet värdeintervall eller intervall av semantiska betydelser åtgärdas med den metod som kallas för *t*-närhet. Den är en ytterligare förbättring av avidentifieringen genom generalisering och består av att ordna uppgifter för att uppnå ekvivalensklasser som speglar den ursprungliga fördelningen av attributen i det ursprungliga datasetet så mycket som möjligt. För detta ändamål används ett tvåstegsförfarande på ungefär följande sätt. Tabell A6 är den ursprungliga databasen inklusive poster i klartext för de registrerade, som grupperats efter plats, ålder, lön och två grupper med semantiskt likartade egenskaper, (X1, X2, X3) respektive (Y1, Y2, Y3) (t.ex. likartade kreditklasser, likartade sjukdomar). Först *l-diversifieras* tabellen med $l = 1$ (tabell A7) genom att gruppera posterna i semantiskt likvärdiga ekvivalensklasser och dåligt inriktad avidentifiering. Därefter behandlas tabellen för att uppnå *t*-närhet (tabell A8) och högre variabilitet inom varje partition. Med det andra steget innehåller varje ekvivalensklass faktiskt poster från båda egenskapsgrupperna. Det är värt att notera att plats-id och ålder har olika granularitet i de olika stegen i processen: Det innebär att varje attribut kan kräva olika generaliseringskriterier för att uppnå önskad avidentifiering, och detta kräver i sin tur särskild utformning och tillräcklig behandlingsinsats av de registeransvariga.

Löpnr	Plats-id	Ålder	Lön	Egenskap
1	1127	29	30K	X1
2	1112	22	32K	X2
3	1128	27	35K	X3
4	1215	43	50K	X2
5	1219	52	120K	Y1
6	1216	47	60K	Y2
7	1115	30	55K	Y2
8	1123	36	100K	Y3
9	1117	32	110K	X3

Tabell A6. En tabell med enskilda personer grupperade efter plats, ålder, löner och två egenskapsgrupper.

Löpnr	Plats-id	Ålder	Lön	Egenskap
1	11**	2*	30K	X1
2	11**	2*	32K	X2
3	11**	2*	35K	X3
4	121*	> 40	50K	X2
5	121*	> 40	120K	Y1
6	121*	> 40	60K	Y2
7	11**	3*	55K	Y2
8	11**	3*	100K	Y3
9	11**	3*	110K	X3

Tabell A7. En *l*-diversitetsversion av tabell A6.

Löpnr	Plats-id	Ålder	Lön	Egenskap
1	112*	< 40	30K	X1
3	112*	< 40	35K	X3
8	112*	< 40	100K	Y3
4	121*	> 40	50K	X2
5	121*	> 40	120K	Y1
6	121*	> 40	60K	Y2
2	111*	< 40	32K	X2
7	111*	< 40	55K	Y2
9	111*	< 40	110K	X3

Tabell A8. En *t*-närhetsversion av tabell A6.

Det måste tydligt anges att målet med generalisering av de registrerades attribut på sådana upplysta sätt ibland kan uppnås endast för ett begränsat antal poster, inte för samtliga. Genom god praxis bör man se till att varje ekvivalensklass innehåller flera personer och att ingen inferensattack fortfarande är möjlig. Detta tillvägagångssätt kräver under alla omständigheter att de registeransvariga gör en djupgående bedömning av de tillgängliga uppgifterna och en utvärdering av kombinationer av olika alternativ (t.ex. olika intervallstorlekar, olika plats- eller åldersgranularitet osv.). Med andra ord kan avidentifiering genom generalisering inte uppnås genom ett grovt första försök från de registeransvarigas sida att ersätta analysvärdena för attribut i en post efter intervall, eftersom det behövs mer specifika kvantitativa metoder – t.ex. att utvärdera attributens entropi inom varje partition, eller mäta avståndet mellan de ursprungliga attributfördelningarna och fördelningen inom varje ekvivalensklass.