EU 지침 제29조 개인정보보호작업반

0829/14/EN
WP216

익명처리 기법에 관한 의견(05/2014)

2014년 4월 10일 채택

개인정보보호작업반은 EU 지침 95/46/EC 제29조에 따라 설립되었으며 유럽의 개인정보보호 및 프라이버시에 대한 자문을 제공하는 독립적인 자문기구이다. 본 작업반의 업무는 EU 지침 95/46/EC 제30조 및 지침 2002/58/EC 제15조에 명시되어 있다.

사무국은 유럽연합 집행위원회 사법총국 소속 Directorate C(기본권 및 EU 시민권)에서 제공한다. 주소: B-1049 Brussels, Belgium, Office No MO-59 02/013.

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

1995년 10월 24일의 유럽의회 및 집행위원회 지침 95/46/EC(이하 'EU 지침')에 따라 설치된

개인정보처리 관련 개인정보보호작업반은

동 지침 제29조 및 30조와,

절차규정을 고려하여,

본 의견을 채택하였다.

요약보고서

개인정보보호작업반(WP)은 본 의견서에서 EU의 개인정보보호 관련 법률 배경으로 기존의 익명처리 기법의 효과성과 한계를 분석하고 각 기법에 내재된 식별조치의 잔존 위험을 고려하여 이들 기법을 다루기 위한 권고안을 제시한다.

WP는 특히 개인과 사회 전체적으로 '오픈 데이터'의 혜택을 향유하는 동시에 관련 개인의 위험을 완화시키기 위한 전략으로서 익명처리의 잠재가치를 인정한다. 다만, 사례연구와 연구문헌들은 업무에 필요한 기저 정보를 충분히 유지하면서 진정한 익명 데이터세트를 생성하는 것이 얼마나 어려운지를 보여주고 있다.

EU 지침 95/46/EC 및 기타 관련 EU 법적 수단에 비추어볼 때, 익명처리는 식별처리를 불가역적으로 방지하기 위해 개인정보를 처리하는 것에서 비롯된다. 그 과정에서 개인정보 처리자는 식별처리를 위해 '합리적으로 예상되는(likely reasonably)' 모든 수단(개인정보 처리자 또는 모든 제3자의 수단)과 관련된 요소를 고려해야 한다.

익명처리는 개인정보의 추가적 처리의 하나이다. 따라서 익명처리는 법적 근거 및 추가 처리의 관점에서 양립가능성의 요건을 충족해야 한다. 아울러 익명처리된 정보는 개인정보보호법의 적용을 받지 않지만, 정보주체는 여전히 다른 법률에 따라(예: 통신의비밀보호법) 보호를 받을 권리가 있을 수도 있다.

본 의견서는 주요 익명처리 기법인 무작위처리(randomization)와 일반처리(generalization)에 대해 기술한다. 특히 잡음 추가(noise addition), 치환(permutation), 차등 정보보호(differential privacy), 총계처리(aggregation), k-익명성(k-anonymity), l-다양성(l-diversity), t-근접성(t-closeness)에 대해 논의한다. 아울러 익명처리 기법의 원칙, 강점과 약점 및 각 기법의 사용에 따라 발생하기 쉬운 오류와 실패에 대해서도 기술한다.

본 의견서는 아래 세 가지 기준을 근거로 각 기법의 안전성에 대해 상술한다.

(i) 여전히 개인을 식별하는 것이 가능한가?

(ii) 여전히 개인기록부들을 서로 연결할 수 있는가?

(iii) 개인에 대한 정보를 유추할 수 있는가?

각 기법의 강점과 약점을 알면 주어진 상황에 적합한 익명처리 과정을 설계하는 데 도움이 된다.

익명처리와 관련된 몇 가지 함정과 오해를 규명하기 위해 가명처리에 대해서도 다룬다. 가명처리는 익명처리의 한 방법이 아니라, 단지 정보주체의 원래 신원과 데이터세트의 연결가능성을 줄이는 것이며 따라서 유용한 보안 조치 중의 하나이다.

본 의견서는 익명처리 기법은 프라이버시를 보장할 수 있으며 효율적인 익명처리 절차를 수립하는 데 사용될 수 있지만, 거기에는 익명처리 기법이 운용되어야 한다는 단서가 따른다. 그것은 일부 유용한 정보를 산출하는 동시에 익명처리의 목표를 달성하기 위해서는 익명처리 과정의 전제 조건(상황) 및 목적이 분명하게 제시되어야 한다는 의미이다. 최적의 해법은 사례별로 결정되어야 하며, 그 예로서는 여러 기법을 조합해서 사용하되 본 의견서에서 제시한 실용적인 권고를 참고할 수 있을 것이다.

끝으로, 개인정보 처리자는 익명처리된 데이터세트가 여전히 정보주체에게 잔존 위험을 제기한다는 점을 고려해야 한다. 실제로, 익명처리 및 재식별처리가 한편으로는 활발한 연구분야로 새로운 발견이 꾸준히 발표되고 있고, 다른 한편으로는 통계자료와 같은 익명처리정보(anonymised data)까지도 개인 프로필의 가치를 높이는 데 사용될 수도 있어 새로운 개인정보보호 문제를 제기하고 있다. 따라서 개인정보처리자는 익명처리를 일회성 활동으로 생각해서는 안 되며 수반되는 주요 위험을 정기적으로 재평가해야 한다.

1 서론

오늘날 각종 정보 기기, 센서 및 네트워크가 새로운 형태의 데이터를 대량으로 생성하고 데이터 저장 비용이 획기적으로 낮아짐에 따라 데이터 재사용에 대한 일반의 관심이 커지고 수요 또한 증가하고 있다. '오픈 데이터(open data)'는 사회, 개인, 조직에 분명한 편익을 제공하지만 이는 개인정보 및 사생활 보호에 관한 만인의 권리가 존중되는 것을 전제로 한다.

익명처리는 이러한 오픈 데이터의 편익은 유지하되, 위험은 완화시킬 수 있는 훌륭한 전략이 될 수 있다. 일단 데이터세트가 제대로 익명처리 되어 개인 식별이 불가능해지면, 유럽 개인정보보호법은 적용되지 않는다. 하지만 사례연구 및 연구문헌에 따르면 업무에 필요한 기저 정보는 최대한 보유하면서도 방대한 개인정보에서 진정으로 익명처리된 데이터세트를 생성하는 것은 결코 간단한 문제가 아니다. 예를 들어, 익명처리된 것으로 생각되는 데이터세트가 다른 데이터세트와 결합되어 개인 또는 복수의 개인이 식별될 수가 있다.

본 의견서에서 WP는 EU의 개인정보보호의 법적 배경을 토대로 기존 익명처리 기법의 효과성과 한계를 분석하고 익명처리 절차의 수립에 있어서 이들 기법을 신중하고 책임 있게 사용하기 위한 권고안을 제시한다.

2 정의 및 법률적 분석

2.1. EU의 법률적 배경에 따른 정의

EU 지침 95/46/EC는 해설전문 26항에서 익명처리정보를 개인정보보호법의 범위에서 제외한다고 명시한다.

> *"개인정보보호의 원칙은 식별되거나 식별가능한 사람에관한 정보에 적용되어야 하고, 개인이 식별가능한지를 결정하기 위해서는 개인정보 처리자 또모든 제 3자가 사용할 것으로 합리적으로 예상되는 모든 수단을 모두 고려하여야 하며, 보호의 원칙은 더 이상 정보주체를 식별할 수 없는 형태로 익명처리된 데이터에 대해서는 적용해서는 안 되며, 제27조에 규정된 행동강령은 데이터를 익명처리하여 적보주체의 식별처리가 더 이상 불가능한 형태로 보유하는 가이드라인을 제시하는*

유용한 수단이 될 수 있다." [1]

해설전문 26항을 면밀히 읽어보면 익명처리의 개념적 정의를 엿볼 수 있다. 해설전문 26항은 개인정보를 익명처리하기 위해서는 정보주체를 더 이상 식별할 수 없도록 관련 정보 요소를 충분히 제거해야 한다고 강조한다. 더 정확히 서술하면, 개인정보는 개인정보 처리자 또는 제3자가 '합리적으로 예상하는은 모든 수단'을 동원해도 더 이상 자연인의 식별에 사용될 수 없도록 처리되어야 한다. 여기서 한 가지 중요한 요소는 그러한 개인정보 처리의 불가역적(irreversible)이어야 한다는 것이다. EU 지침은 그와 같은 비식별처리 과정이 어떻게 수행되어야 하는지 또는 수행될 수 있는지에 대해서는 명시하지 않고 있다. [2] 논의의 핵심은 결과로서, 모든 예상되는 합리적인 수단을 사용해도 정보주체가 식별되지 않아야한다는 것이다. 행동강령은 정보주체의 식별처리가 '더 이상 불가능한' 형태로 데이터를 보유할 뿐아니라, 가능한 익명처리 메커니즘을 개발하는 하나의 도구이다. 따라서 EU 지침은 매우 높은 기준을 분명하게 설정하고 있다.

EU e-Privacy 지침(Directive 2002/58/EC) 또한 동일한 관점에서 '익명처리' 및 '익명처리정보'에 대해 규정하고 있다. 해설전문 26항은 다음과 같이 명시한다.

"마케팅 커뮤니케이션 서비스 또는 부가가치 서비스 제공에 사용된 교신정보는 또한 서비스 제공이 종료되면 삭제 또는 익명처리되어야 한다".

이에 따라 제6조(1항)은 다음과 같이 규정한다.

"공공 통신 네트워크 또는 대중이 이용 가능한 전자통신서비스 제공자가 처리 및 보관 중인 가입자 또는 사용자 관련 교신정보는 본 조 제2, 3, 5절 및 제15조(1)항에도 불구하고 통신의 전송 목적에 더 이상 필요하지 않게 되었을 때는 삭제하거나 익명처리 해야 한다."

아울러 제9조(1)항에 따르면,

"공공 통신 네트워크 또는 대중이 이용할 수 있는전자통신서비스 제공자의 가입자 또는 사용자와 관련된 교신정보 이외의 위치정보의 처리가 가능한 경우, 동 개인정보는 익명처리 되었을 때, 또는 사용자 또는 가입자의 동의가

---

[1] 아울러 이는 "어떤 사람이 식별가능한지를 판단할 때는 개인정보 처리자 또는 당사자의 신원을 확인할 다른 사람에 의해 합리적으로 사용이 예상되는 수단이 모두 고려되어야 한다,"고 명시한 EU 개인정보보호 규정 초안 Recital 23에서 취한 접근법임에 주목할 필요가 있다.

[2] 이 개념은 본 의견서 8 페이지에서 상술한다.

있을 때에 한해 부가가치서비스의 제공에 필요한 범위 및 기간 내에만 처리될 수 있다."

그 논거는 개인정보에 기법을 적용하여 익명처리된 결과는 현재의 기술 수준에서 삭제와 동등할 정도로 영구적이어야 하며, 다시 말하면 개인정보 처리가 불가능해야 한다는 것이다. [3]

2.2. 법률적 분석

EU의 주요 개인정보보호 규정에 언급된 익명처리 관련 표현을 분석해보면 네 가지의 주요 특징이 부각된다.

- 익명처리는 불가역적으로정보주체의 식별을 방지하기 위한 개인정보처리의 결과일 수 있다.

- 몇 가지 익명처리 기법을 상정할 수 있으나 EU 법률에 명시된 규범적인 규정은 없다.

- 상황 요소를 특히 유념해야 한다. 즉, 개인정보 처리자 또는 제3자가 사용할 것으로 합리적으로 예상되는 모든 수단을 고려하고 현재의 기술 수준에서 최근에 어떤 것이 '합리적으로 연상되는 수단이 되었는지에 대해 특별히 주의를 기울여야 한다.(이용 가능한 컴퓨터 연산능력 및 툴의 향상을 감안).

- 익명처리에 위험요인이 내재되어 있다. 익명처리 기법의 타당성을 평가할 때는 해당 기법에 의해 '익명처리된' 데이터의 위험요인을 고려해야 하고 위험의 심각성(severity)과 발생 가능성(likelihood)을 평가해야 한다.

본 의견서는 데이터를 '익명처리' 하기 위한 각종의 기술 및 관리조치와 결부된

[3] 여기서 상기해야 할 것은 익명처리가 국제표준에서도 정의되어 있다는 점이다. 예컨대 ISO 29100은 익명처리를, "개인정보 처리자 단독으로든, 아니면 제3자와의 협업에 의해서든, 개인식별정보(PII)의 주체를 더 이상 직접 또는 간접적으로 식별이 불가능하도록 불가역적으로 PII를 변경하는 프로세스"로 정의한다(ISO 29100:2011). 또한 ISO에 있어서도 직접 또는 간접적인 식별처리를 위해 개인정보에 가해지는 변경의 불가역성이 핵심이다. 이러한 관점에서 지침 95/46의 기저에 있는 원칙 및 개념과 상당한 수렴선이 존재한다. 이는 또한 비식별성에 초점을 두면서 재식별처리(D, SD)를 위한 '불균형적 노력'에 대해 명시하는 일부 국내법(예를 들어, 이탈리아, 독일, 슬로베니아)에서 볼 수 있는 정의에도 적용된다. 하지만 프랑스 개인정보보호법은 비록 정보주체의 식별처리가 매우 어렵고 재식별처리가 거의 불가능하다고 하더라도 동 정보는 여전히 개인정보로 남는다고 규정한다. 다시 말해, '합리성' 시험에 관해 언급한 조항이 없다.

재식별처리의 내재적 '잔존 위험'을 적시하기 위해 '익명성' 또는 '익명정보' 대신에 '익명처리 기법'이라는 표현을 사용한다.

2.2.1. 익명처리 과정의 적법성

첫째, 익명처리는 비식별처리의 불가역성을 달성하기 위해 개인정보에 적용되는 기법이다. 따라서 개인정보가 반드시 식별가능한 형태를 띤 개인정보의 보유를 규율하는 법률 규정에 수집 및 처리되었다고 전제한다.

이런 배경에서 익명처리과정, 즉 익명처리를 달성하기 위한 개인정보의 처리는 '추가 처리(further processing)'의 하나이다. 따라서 이러한 추가 처리는 작업반이 의견서 03/2013에서 제시한 목적 제한에 관한 지침에 따라 양립가능성 검증을 통과해야 한다. [4]

이것은 원칙적으로 익명처리의 법적 근거를 EU 지침 제 7조의 각 항(개인정보처리자의 정당한 이익 등)에서 찾을 수 있다는 뜻이다. 다만, EU 지침 제6조의 데이터 품질 요건을 충족시키는 본 작업반의 목적 제한 관련 의견서에 제시된 구체적 상황 및 제반 요소를 적절히 고려한다는 조건 또한 충족시켜야 한다. [5]

다른 한편으로, EU 지침 95/46/EC 제6조(1항)e)호와 EU e-Privacy 지침 제6조(1)항 및 9조(1)항의 규정들도 적시할 필요가 있다. 이들 조항이 개인정보를 수집 또는 추가 처리의 목적에 필요한 기간에 국한하여 '식별처리가 가능한 형태로' 보유해야 한다고 설명하고 있기 때문이다.

본질적으로 상기 조항은 적어도 개인정보는 '기본설정'이 익명처리 되어야 한다는 것을 강조한다(예컨대 교신정보에 관한 EU e-Privacy 지침에 언급된 것과 같은 다양한 법률요건을 전제로). 개인정보 처리자가 개인정보를 원래의 목적 또는 추가 처리 목적을 달성한 후에도 보유하고자 한다면, 식별처리를 불가역적으로 예방하기

---

[4] EU 지침 제29조 개인정보보호작업반의 의견서 03/2013:http://ec.europa.eu/justice/data- protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[5] 다시 구체적으로 말하자면, 아래 핵심 요인에 대해 모든 관련 상황에 비추어 실질적인 평가가 수행되어야 한다.
a) 개인정보 수집 목적과 추가 처리 목적 사이의 관계
b) 개인정보가 수집된 배경과 그 추가 사용에 대한 정보주체의 합리적인 기대
c) 개인정보의 성격 및 정보주체에 대한 추가 처리의 영향
d) 개인정보의 공정한 처리를 보장하고 정보주체에게 미치는 부당한 영향을 방지하기 위해 개인정보 처리자가 취한 안전조치

위해 익명처리 기법을 사용해야 한다.

따라서 본 작업반은 익명처리는 개인정보의 추가 처리 사례로서 원래 처리 목적과 양립한다고 볼 수 있으나, 다만 그 익명처리 과정이 본 의견서에 기술된 의미에서 익명정보를 신뢰성 있게 산출해야 한다는 조건을 충족시켜야 한다.

익명처리는 유럽사법재판소(ECJ: European Court of Justice)가 판례 Case C-553/07(College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer)를 통해 환기시킨 법적 제약을 따라야 한다는 점 또한 강조할 필요가 있다. *예컨대 정보주체의 열람권(access access rights) 보장을 위해 개인정보를 식별가능한 형태로 보유해야 할 필요가 있다는 점이다.* ECJ는, "*EU 지침 [95/46] 제12조(a)항이 회원국이 개별 개인정보 수령자 또는 개인정보 수령자 집단의 정보 및 현재는 물론 과거에 공개된 개인정보의 내용에 대한 열람권을 보장하도록의무화해야 한다고 판시했다. 이에 따라 각 회원국은 개인정보를 보관하는 기간을 결정하고 동 정보에 대한 열람권을 부여해야 한다. 여기에는 한편으로는 정보주체의 프라이버시 보호, 특히 거부권 및 소송제기권과 관련한 정보주체의 이익, 그리고 다른 한편으로는 그러한 정보 보관 의무에 따른 개인정보 처리자의제기하는 부담 사이에 공정한 균형이 이루어져야 한다.*

이는 개인정보 처리자가 익명처리와 관련하여 EU 지침 95/46 제7조(f)항을 적용할 때 특히 더 관련이 있다. 즉, 개인정보 처리자의 정당한 이익은 반드시 정보주체의 권리 및 기본적 자유와 균형을 유지해야 한다.

예를 들어, 2012-2013년 네덜란드 DPA가 4개 이동통신사업자의 심층패킷분석(DPI: Deep Packet Inspection) 기술 사용실태를 조사한 것은 교신자료의 수집 후 최단 시간 내에 동 내용의 익명처리라는 EU 지침 95/46 제7조(f)에 따른 법적 근거를 보여준 사례이다. 실제로 EU e-Privacy 지침 제6조는 공공 통신 네트워크 사업자나 공개적으로 이용 가능한 전자통신서비스 사업자가 처리 또는 보관 중인 가입자 및 사용자 관련 교신자료는 최대한 빨리 삭제하거나 익명처리하도록 규정한다. 이 사례에서 개인정보보호가 EU e-Privacy 지침 제6조에 명시되어 있으므로 그에 상응하는 데이터보호지침 제7조의 법적 근거가 존재한다. 이는 반대로 다음과 같이 말할 수도 있다. 즉, 어떤 개인정보처리 형태가 EU e-Privacy 지침 제6조에 의해 허용되지 않을 경우, 데이터보호지침 제7조의 법적 근거는 존재할 수 없다.

2.2.2. 익명정보의 잠재적 식별성

본 작업반은 개인정보에 관한 의견서 4/2007에서 EU 지침 95/46/EC 제2조(a)항에 명시된 정의의 구성요소(동 정의의 '식별된 또는 식별가능한' 부분을 포함)에 중점을 두고 개인정보의 개념에 대해 자세히 검토했다. 이런 맥락에서 우리는 "과거 식별이 가능한 사람을 지칭했으나 현재에는 더 이상 식별이 불가능한 익명처리된 개인정보는 익명정보가 된다,"고 결론을 내렸다.

따라서 본 작업반은 익명처리 과정이 충분히 견고한 것인지 여부, 다시 말해 식별처리가 '합리적으로' 불가능해졌는지 여부를 평가하려면 EU 지침이 기준으로 제안한 '합리적으로 사용될 수 있는 수단'에 대한 시험을 적용해야 한다는 입장을 밝혔다. 특정 사례의 구체적인 배경과 상황은 식별성에 직접적인 영향을 미친다. 본 의견서의 기술 부속서는 가장 타당성 있는 기법을 선택할 때의 영향을 분석한다.

앞서 강조한 바와 같이, 이 분야의 연구, 툴 및 연산능력은 계속 발전하고 있다. 따라서 식별처리가 더 이상 불가능한 상황을 빠짐 없이 열거하는 것은 가능하지도 않거니와 실효성도 떨어진다. 다만, 몇 가지 핵심 요인은 분명히 고려해야 하고 설명할 가치가 있다.

첫째, 개인정보 처리자는 익명처리 기법의 가역화에 필요한 구체적 수단, 특히 그러한 수단의 이행 및 발생 가능성과 심각도의 평가에 소요되는 비용과 노하우에 초점을 맞춰야 한다고 주장할 수 있다. 예를 들어, 개인정보 처리자는 익명처리 노력 및 비용(소요 시간과 자원 모두)과 대비하여 갈수록 더 저렴하게 이용 가능한 데이터세트 내 개인 식별 기술 수단, 공개적으로 이용 가능한 기타 데이터세트(예를 들어, '오픈 데이터' 정책에 따라 이용 가능한 데이터세트)의 증가, 그리고 정보주체에게 미치는 불리한 영향, 때로는 회복할 수 없는 피해를 수반하는 여러 불완전 익명처리 사례 사이에 균형을 유지해야 한다.[6] 식별화 위험은 시간이 흐르면서 커질 수 있으며 정보통신기술의 발전에 따라서도 영향을 받는다는 점을 주목해야 한다. 따라서 법률적 규제는, 만약 그러한 규제가 있다면, 정보기술 발전잠재력의 변화를 이상적으로 참작하여 기술적으로 중립적인 방식에 따라 제정해야 한다.[7]

---

[6] 흥미롭게도 최근 상정된(2013년 10월 21일) 유럽의회의 개인정보 보호규정 초안 개정안은 Recital 23에서 "식별처리 수단이 실제로 개인을 식별하기 위해 사용할 것이라고 합리적으로 예측되는지 확인하려면, 정보 처리 시점에 가용한 기술과 기술발전을 모두 참작하여 식별처리에 요구되는 비용과 시간 등의 목표 요인을 모두 고려해야 한다,"고 명시한다.

[7] EU 지침 제29조 개인정보보호작업반의 의견서 4/2007, 15 페이지 참조.

둘째, '어떤 개인이 식별 가능한지 여부를 결정하는 데 합리적으로 사용이 예상되는 수단'은 '개인정보 처리자 또는 기타 제3자'가 사용하게 될 수단이다. 따라서 개인정보 처리자가 이벤트 단계에서 원본(식별 가능한) 개인정보를 삭제하지 않을 때, 또한 개인정보 처리자가 해당 데이터세트의 일부를 타인에게 양도할 때(예컨대 식별 가능한 데이터를 제거 또는 마스킹한 후), 그 결과로 생기는 데이터세트는 여전히 개인정보이다. 개인정보 처리자가 더 이상 식별 불가능한 수준으로 개인 이벤트 정보를 총계처리(aggregate)한 경우에 한해 익명처리 되었다고 할 수 있다. 예를 들어, 어떤 조직이 개인의 여행경로 관련 정보를 수집한다고 가정할 때, 개인정보 처리자(또는 기타 제3자)가 여전히 원본자료에 접근이 가능하다면 비록 제3자에게 제공된 데이터세트로부터 직접적인 식별자는 제거되었다 할지라도 이 개인에 대한 이벤트 차원의 여행 패턴은 계속해서 개인정보의 성격을 유지할 것이다. 하지만 만일 개인정보 처리자가 원본자료를 삭제하고 상위레벨, 예컨대, '궤적 X에는 월요일이 화요일에 비해 여행객이 160% 더 많다'와 같은 종합통계만 제3자에게 제공할 경우, 이는 익명정보의 요건에 해당된다.

효과적인 익명처리 솔루션은 어떤 당사자도 데이터세트 내 개인을 식별하지 못하도록, 한 데이터세트 내의(또는 별도의 두 데이트세트 사이의) 두 기록을 연결하지 못하도록, 또한 동 데이터세트의 어떠한 정보도 유추할 수 없도록 방지해 준다. 따라서 일반적으로 말해 데이터세트 자체의 식별 요소를 직접 제거하는 것만으로는 완전한 정보주체 식별 불가능성을 보장하기에는 부족하다. 익명정보가 의도하는 처리의 목적과 상황에 따라서는 식별화 방지를 위해 추가조치를 취해야 하는 수가 많다.

예:
유전자 프로필 정보는 특정 프로필의 고유 특징으로 인해 만약 사용된 유일한 기법이 공여자의 신원을 제거하는 것이라면 해당 개인정보가 식별처리 위험에 처할 수 있는 사례이다. 비록 DNA가 '익명으로' 공여되었다 하더라도 공개적으로 이용 가능한 유전자 자원(예: 족보, 부고, 검색엔진 쿼리의 결과) 및 DNA 공여자의 메타데이터(공여 시간, 연령, 거주지)의 조합을 통해 특정 개인의 신원이 드러날 수 있다는 사실이 문헌[8]을 통해 알려졌다.

[8] John Bohannon, '족보 데이터베이스로 익명의 DNA 공여자 신원 확인 가능(Genealogy Databases Enable Naming of Anonymous DNA Donors), Science, Vol. 339, No. 6117 (2013년 1월 18일), p. 262.

익명처리 기법의 두 계열(데이터 무작위화와 일반화)[9] 모두 단점이 있으나, 각기 주어진 상황 및 배경에 따라서는 정보주체의 프라이버시를 해치지 않으면서 원하는 목표 달성에 부응할 수도 있다. '식별처리'는 한 개인의 이름 및/또는 주소의 식별 가능성을 의미할 뿐 아니라 식별, 연결가능성 및 추론을 통한 잠재적 식별 가능성까지 포함하는 것임이 분명하다. 더욱이 개인정보보호법을 적용할 때 식별처리는 개인정보 처리자 또는 수령자의 의도가 무엇인가 하는 것과는 무관하다. 따라서 개인정보가 식별가능한 한 개인정보보호 규정이 적용된다.

제3자가 익명처리 기법으로 처리한(원자료 처리자가 익명처리하여 배포한) 데이터세트를 가공할 경우는 원본 데이터세트의 정보주체 식별(직접 또는 간접적으로)이 불가능하다는 전제 하에 개인정보보호 요건을 고려하지 않아도 합법적으로 가공할 수 있다. 다만, 제3자는 익명처리 기법을 자신의 목적에 맞게 사용하는 방법, 특히 결합하는 방법을 결정할 때 반드시 위에서 언급한 배경 및 상황 요소(원자료 처리자가 적용한 익명처리 기법의 특징을 포함)를 고려해야 한다. 왜냐하면 해당 결과가 제3자에게 서로 다른 법적 의무를 수반하기 때문이다. 그러한 요소 및 특징으로 인해 정보주체가 수용이 불가능한 식별처리 위험이 뒤따른다면, 이 때의 정보 가공은 또 다시 개인정보보호법의 규제 대상이 된다.

위에서 말한 목록이 결코 모든 내용을 총망라하는 것은 아니고, 현재 나와 있는 여러 기법에 따라 익명처리를 거친 일정 데이터세트의 식별 가능성 평가방법에 관한 일반 지침을 제공한다는 취지이다. 상기 요소는 개인정보 처리자가 데이터세트를 익명처리할 때와 제3자가 그렇게 '익명처리된' 데이터세트를 자신의 목적에 사용할 때 따져 봐야 할 위험요인이다.

2.2.3. 익명정보 이용의 위험

개인정보 처리자는 익명처리 기법을 사용하려면 다음과 같은 위험을 고려해야 한다.

- 가명처리된 정보를 익명정보와 동일시하는 것은 분명 위험한 일이다. 가명처리된 정보는 여전히 정보주체 식별이 가능하고 다양한 데이터세트에 걸쳐 연결을 허용하므로 결코 익명정보와 동등할 수 없다는 점을 기술분석(Technical Analysis) 섹션에서 설명할 예정이다. 가명처리는 정보주체 식별을 허용할 가능성이 크므로

[9] 위 양대 익명처리 기법의 주요 특징과 차이점은 아래 섹션 3('기술분석')에서 논의한다.

개인정보보호 법률체계의 적용 범위 내에 있다. 이는 특히 과학, 통계 또는 역사적 연구의 맥락에서 관련이 있다. [10]

> 예:
> 가명처리의 오해와 관련한 대표적인 사례가 이미 잘 알려진 'AOL(America On Line) 사건'이다. 2006년, AOL 고객 65만 명의 3개월간의 검색 키워드 2천만 개가 들어 있는 데이터베이스가 일반에 공개되었는데, 여기서 프라이버시 보호 수단이라고는 AOL 사용자 ID를 숫자 속성(numeric attribute)으로 대체한 것뿐이었다. 이로써 일부 사용자의 신원과 소재지가 일반 사람들에게 공개되는 결과를 초래했다. 가명처리된 검색엔진 쿼리 문자열은 특히 그것이 IP 주소나 그 외 클라이언트 구성 매개변수 등 다른 속성과 결합되면 매우 강력한 식별 능력을 갖게 된다.

- 두 번째 실수는 무엇보다도 개인정보 이용에 다른 법률이 적용될 수도 있으므로 개인정보가 적절히 익명처리 되기만 하면 그러한 정보(위에서 언급한 조건과 기준을 모두 충족하고 의미상 EU 개인정보보호 지침의 범위에 해당되지 않는)에 대해서는 어떤 안전조치도 필요 없을 것으로 생각하는 점이다. 예컨대 EU e-Privacy 지침 제5조(3)항은 넓은 의미에서 통신비밀의 일환으로 가입자/사용자의 동의 없이는 단말장치에 있는 어떤 종류의 '정보'(비개인정보 포함)에 대해서도 보관과 접근을 금지한다.

- 세 번째 과실은 적절히 익명처리된 정보가 특정 상황 하에서, 구체적으로 말하면 프로파일링(profiling) 사례에서 개인에게 미치는 영향을 고려하지 않는 문제이다. 개인의 사생활은 ECHR 제8조 및 EU 기본권 헌장 제7조에 의해 보호된다. 따라서 비록 개인정보보호법이 적절히 익명처리된 정보에는 적용되지 않을지라도, 제3자의 사용 목적상 익명처리하여 공개된 데이터세트의 이용은 프라이버시 침해를 초래할 수도 있다. 특히 익명정보가 개인에게 영향을 미치는(비록 간접적이라 하더라도) 의사결정에 사용될 때(다른 정보와 함께)는 특별한 주의가 요구된다. 본 의견서에서 이미 지적했고, 특히 '목적 제한(의견서 03/2013) [11], 정보주체'의 개념에 관한 의견서에서 본 작업반이 분명히 밝힌 것처럼, 정보의 추가 처리에 대한 합법적 기대는 해당 상황 요소, 예컨대 정보주체와 개인정보 처리자간의 관계가 갖는 성격, 준거법상 의무, 처리작업의 투명성에 비추어 평가해야 한다.

---

[10] EU 지침 제29조 개인정보보호작업반의 의견서 4/2007, p. 18-20 참조.

[11] 참고자료: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

3 기술분석, 기술의 안전성 및 대표적인 실수

익명처리 관행과 기법은 종류도 다양하고 안전성의 정도도 다양하다. 이번 섹션은 개인정보 처리자가 익명처리 기법 적용 시 현재의 기술 수준과 아래의 3대 익명처리 리스크를 바탕으로 달성 가능한 익명처리 보장과 관련하여 유념해야 할 요점에 대해 논의한다.

- *식별*(*Singling out*): 데이터세트에서 개인이 식별되는 개인기록부의 일부 또는 전부를 분리해낼 가능성.
- *연결가능성*(*Linkability*): 동일 정보주체 또는 정보주체 그룹(동일 데이터베이스 또는 서로 다른 데이터베이스)에 대해 적어도 두 개의 개인기록부를 연결시킬 가능성. 만일 어떤 공격자가 동일한 개인 그룹에 대해 두 개의 개인기록부가 지정되었음을 밝히는 것은 가능하나 이 그룹의 개인은 식별 불가능하다고 가정하면(예: 상관분석을 통해), 그와 같은 기법은 '식별' 공격에 대해서는 내성을 가지지만 연결가능성에 대해서는 내성을 갖지 않는다.
- *추론*(*Inference*): 한 속성의 값을 유의한 확률을 근거로 다른 속성의 집합의 값으로부터 유추할 가능성.

따라서 개인정보 처리자와 제3자가 가장 합리적으로 가능성이 큰 수단으로 재식별처리를 시도할 때 이를 막는 안전한 솔루션은 상기 세 가지 위험을 제거한 솔루션이다. 이와 관련하여 본 작업반이 강조하고자 하는 것은 리스크가 없는 비식별처리 및 익명처리 기법은 현재 진행 중인 연구의 주제이며, 지금껏 단점이 없는 기법은 존재하지 않음이 많은 연구를 통해 드러났다는 사실이다. 대체로 익명처리에는 ***무작위화***(***randomization***)를 기반으로 하는 것과 ***일반화***(***generalization***)를 기반으로 하는 것, 즉 두 가지 접근법이 있다. 본 의견서는 그 밖에도 *가명처리, 차등 정보보호, l-다양성, t-근접성* 등의 개념도 다룬다.

이 섹션에서는 다음과 같은 용어를 사용한다. 즉, 데이터세트(dataset)란, 개인(정보주체)에 관한 여러 개인기록부로 구성된 것이다. 개인기록부(record)는 하나의 정보주체에 관한 것으로서 각 속성(예: 연도)에 대한 일련의 값(또는 '엔트리', 예: 2013)으로 이루어진다. 데이터세트는 개인기록부가 모인 것이며, 이 개인기록부 모음은 테이블(또는 테이블의 집합) 또는 주석이 달린/가중치 그래프의 형태를 띨 수 있는데, 최근에는 이런 추세가 증가하고 있다. 본 의견서에 제시된 예는 테이블이지만, 개인기록부의 그래픽 표현에도 적용이 가능하다. 정보주체 또는

정보주체 그룹 관련 속성의 결합을 준식별자(quasi-identifier)라고도 부른다. 경우에 따라 데이터세트는 동일한 개인에 대해 다중 개인기록부를 가질 수 있다. '공격자'는 우발적으로나 고의적으로 원본 개인기록부에 접근하는 제3자이다(즉, 개인정보 관리자도 아니요, 개인정보 처리자도 아님).

3.1. 무작위화(Randomization)

무작위화는 데이터와 개인간의 밀접한 연관성을 없애기 위해 개인정보의 정확성을 변경시키는 일련의 기법이다. 데이터가 충분히 불확실성을 갖춘다면 이 때부터 개인정보는 특정 개인과 연관 지을 수 없다. 개인기록부는 단일 정보주체로부터 파생될 수 있지만 추론 공격/위험으로부터 보호되고 일반화 기법과 결합하여 더 강력한 프라이버스 보장을 제공하기 때문에 무작위화 그 자체가 개인기록부의 특이성을 감소시키지는 않는다. 개인기록부에서 어느 한 개인이 식별되지 못하도록 추가 기법이 요구될 수도 있다.

3.1.1.잡음 추가(*Noise addition*)

잡음 추가 기법은 특히 어떤 속성이 개인에게 중대한 역효과를 미칠 때 유용하며, 데이터세트의 수정된 속성을 부정확하게 만들되 전체적인 분포도는 유지하는 방식으로 처리한다. 데이터세트를 가공할 때 관찰자는 그 값이 정확하다고 생각하겠지만 이는 어느 정도 선까지만 사실이다. 예를 들어, 어떤 사람의 키가 당초 센티미터 단위로 측정되었다면 익명처리된 데이터세트에서는 정확도를 +-10cm로 유지할 수도 있다. 이 기법이 효과적으로 적용되면 제3자는 개인을 식별할 수 없을뿐더러 개인정보의 복구가 불가능하고 수정 내역도 알아낼 수 없다.

일반적으로 잡음 추가는 명백한 속성 및 준식별자의 제거 등 여타 익명처리 기법과 결합되어야 한다. 잡음의 정도는 정보 수준의 필요성 및 보호된 속성을 공개한 결과가 개인의 프라이버시에 미치는 영향에 따라 달라진다.

3.1.1.1. 보장

- *식별:* 개인의 기록부에 대한 신뢰성이 떨어진다 하더라도 여전히 그 개인의 기록부는 식별이 가능하다(가령 비식별처리의 의미에서는).

- *연결가능성:* 동일한 개인의 기록부를 연결시킬 수 있는 가능성은 남아 있으나, 그와 같은 기록부는 신뢰성이 떨어지며, 따라서 진짜 기록부는 인위적으로 추가시킨 기록부(즉, '잡음')와 연결될 수 있다. 경우에 따라서는 잘못된 속성이 정확한 속성에 비해 더 유의하고, 심지어 더 상위레벨의 위험을 정보주체에게 노출시킬 수도 있다.
- *추론:* 추론 공격이 가능은 하지만 성공률은 더 낮으며 거짓 양성(및 거짓 음성)일 수 있다.

3.1.1.2. 흔한 실수

- 모순되는 잡음 추가: 만약 잡음이 의미론적으로 실행 가능성이 없다면(즉, 잡음이 '균형이 안 잡힌' 것이어서 데이터세트 내 속성간의 논리를 준수하지 않을 때), 데이터베이스에 접근한 공격자는 잡음을 걸러내어 경우에 따라서는 누락된 엔트리를 재생할 수 있다. 더욱이 데이터세트가 너무 희소한(sparse) 분포를 가질 경우[12], 잡음 데이터 엔트리를 외부 소스와 연결시킬 수 있다.

- 잡음 추가로 충분하다는 생각: 잡음 추가는 공격자가 개인정보를 검색하기가 더욱 어렵도록 만드는 보완조치이다. 잡음이 데이터세트에 포함된 정보에 비해 더 크지 않은 이상, 잡음 추가가 익명처리를 위한 독립형 솔루션이라고 추정해서는 안 된다.

3.1.1.3. 잡음 추가 실패

매우 유명한 재식별처리 실험 가운데 온라인 영상물 대여서비스업체인 넷플릭스의 고객 데이터베이스를 상대로 수행한 실험이 있다. 연구자들이 넷플릭스 데이터베이스의 기하학적 특성을 분석하였는데, 당시 넷플릭스가 이용자 약 50만 명이 18,000편의 영화에 대해 1~5점까지 점수를 매긴 기록 1억 개를 사내 프라이버시 정책에 따라 평점과 점수를 매긴 날짜만 제외하고 모든 고객의 식별정보를 삭제하는 방법으로 '익명'처리한 뒤 일반에 공개했다. 점수가 약간 증가 또는 감소하는 데 따라 잡음이 추가되었다.

그런 조치에도 불구하고, 평점 8개 및 점수를 매긴 날짜(오차 14일)를 선정기준으로 사용했을 때는 데이터세트의 개인기록부에서 사용자의 99%를 정확히 식별해내고, 더 낮은 선정기준(평점 2개 및 점수를 매긴 날짜 오차

[12] 이 개념은 부속서, p. 30에서 상술한다

3일)이라 하더라도 68%를 식별해낼 수 있는 것으로 나타났다. [13]

3.1.2. 치환(Permutation)

치환은 일부 속성의 값이 인위적으로 서로 다른 정보주체들과 연결되게끔 속성값의 위치를 바꾸는 것으로, 데이터세트 내 각 속성의 정확한 분포를 유지할 필요가 있을 때는 이 기법이 유용하다.

치환은 특수한 형태의 잡음 추가라고 할 수 있다. 고전적인 잡음 기법에서는 랜덤값을 사용하여 속성을 수정한다. 일관된 잡음 생성은 어려운 작업일 수 있으며 속성값을 수정함으로써 충분한 프라이버시를 노출하지 않을 수도 있다. 또 다른 대안으로는, 치환기법을 통해 단순히 개인기록부를 서로 교환하여 데이터세트의 값을 변경하는 수도 있다. 이러한 교환으로 속성값의 범위와 분포는 동일하되 그 값과 개인간의 상관관계는 사라지게 할 수 있다. 둘 이상의 속성이 논리적 관계 또는 통계적 상관관계가 있는데 독립적으로 치환되었다면 그러한 관계는 파괴되고 만다. 따라서 논리적 관계가 깨지지 않도록 관련이 있는 속성 집합을 치환하는 것이 중요하다. 그렇지 않으면 공격자가 치환된 속성을 식별하여 치환을 되돌릴 수 있다.

예를 들어, 만약 우리가 '입원/증상/담당부서 등의 이유로' 의료 데이터세트 내에서 속성의 부분집합을 생각해 볼 때, 대개의 경우 밀접한 논리적 관계는 속성의 값을 연결하게 될 것이고, 한 개의 값만 치환되었다면 이는 제3자에 의해 탐지되고 심지어 치환이 원상 복귀될 수도 있다.

잡음 추가와 마찬가지로, 치환이 그 자체적으로는 익명화를 제공할 수 없을 수도 있으므로 명백한 속성/준식별자의 제거가 병행되어야 한다.

3.1.2.1. 보장

- *식별:* 잡음 추가와 마찬가지로, 치환도 개인의 기록부를 식별해낼 수 있지만 기록부의 신뢰성은 떨어진다.

[13] Narayanan, A., & Shmatikov, V. (2008년 5월). 대규모 스파스 데이터세트의 안전 비익명처리(Robust De-anonymization of Large Sparse Datasets). *보안 및 개인정보보호(Security and Privacy), 2008. SP 2008. IEEE Symposium on* (pp. 111-125). IEEE.

- *연결가능성:* 만약 치환이 속성과 준식별자에 영향을 미친다면, 내부적으로든 외부적으로든 속성이 데이터세트와 '정확한' 연결이 되지 않도록 예방할 수 있지만, 진짜 엔트리가 다른 정보주체와 연상될 수 있기 때문에 '부정확한' 연결가능성이 상존한다.
- *추론:* 속성이 상관관계가 있다거나 논리적 관계가 밀접할 경우에는 데이터세트에서 추론이 가능하다. 하지만 어떤 속성이 치환되었는지 모르는 상황이기 때문에 공격자는 자신의 추론이 틀린 가설에 근거한 것으로 생각해야 하며, 따라서 단지 확률적인 추론만이 가능할 뿐이다.

3.1.2.2. 흔한 실수

- 틀린 속성 선택: 민감하지 않은 속성 또는 위험하지 않은 속성의 치환은 개인정보보호의 측면에서 유의한 이득을 얻을 수 없다. 실제로 만약 민감/위험한 속성이 여전히 원래 속성과 연관성이 있다면, 공격자는 개인의 민감한 정보를 추출할 수 있을 것이다.
- 속성의 무작위 치환: 두 속성이 밀접한 상관관계가 있다면 속성의 무작위 치환은 확실한 보장책을 제시하지 않는다. 이와 같은 흔한 실수는 표 1에 나와 있다.
- 치환으로 충분하다는 생각: 잡음 추가와 마찬가지로, 치환 그 자체가 익명성을 보장하지는 않으므로 명백한 속성의 제거 등 기타 기법이 병행되어야 한다.

3.1.2.3. 치환의 실패:

다음의 예는 서로 다른 속성간에 논리적 연결성이 존재하지 않을 때 어떻게 속성의 무작위 치환이 열악한 프라이버시 보호로 이어지는지 잘 보여준다. 익명화 시도가 있은 후에 개인의 직업별(생년별) 소득을 추정하는 것은 간단한 일이다. 예컨대, 개인정보의 직접 검사를 통해 다음과 같이 말할 수 있다. 즉, 표에 나타난 CEO는 1957년생이고 급여를 가장 많이 받을 가능성이 매우 높은 반면, 실업자는 1964년생이고 소득이 가장 낮을 확률이 크다.

연도	성별	직업	소득(치환됨)
1957	M	엔지니어	70k
1957	M	CEO	5k
1957	M	실업자	43k
1964	M	엔지니어	100k
1964	M	관리자	45k

표 1. 상관관계가 있는 속성의 치환을 통한 비효과적인 익명화 사례

3.1.3.차등 정보보호(Differential privacy)

차등 정보보호[14]는 여러 접근법이 있는 무작위화 계열의 기법에 속한다. 실제로 잡음 추가는 데이터세트가 공개되기 전에 미리 개입되며, 개인정보 처리자가 익명처리된 데이터세트의 관점을 생성하면서도 원본 데이터의 사본은 유지하고자 할 때는 차등 정보보호 기법을 사용할 수 있다. 그와 같이 익명처리된 관점은 일반적으로 특정 제3자에 대한 쿼리의 부분집합을 통해 생성된다. 사후에 의도적으로 추가한 무작위 잡음이 이 부분집합에 주입된다. 차등 정보보호는 필요한 정도의 프라이버시 보장을 위해 개인정보 처리자가 추가해야 할 잡음이 어느 정도인지, 또한 어떤 형태라야 하는지를 알려주는 기법이다.[15] 이 때 쿼리 결과 세트 내의 개인이 식별될 가능성에 대한 지속적인 모니터링이 매우 중요하다(적어도 새로운 쿼리가 나타날 때마다). 다만, 차등 정보보호 기법은 원자료를 변경하지 않으므로 그 원자료가 남아 있는 한 개인정보 처리자에 의해 합리적으로 사용이 예상되는 가능한 모든 수단을 고려하여 차등 정보보호 쿼리의 결과에서 개인을 식별할 수 있다는 점을 명확히 할 필요가 있다. 그 결과 역시 개인정보라고 봐야 한다.

차등 정보보호에 바탕을 둔 접근법의 이점 중 하나는, 데이터세트가 인가된 제3자에게 제공되며 이것이 단일 데이터세트의 공개를 통해서가 아니라 특정 쿼리에 대한 응답을 통해 이뤄진다는 점이다. 개인정보 처리자는 검사에 도움이 되기 위해 모든 쿼리 및 요청의 목록을 계속 보유함으로써 인가 받지 않은 제3자의 개인정보 접근을 방지할 수 있다. 쿼리 또한 잡음 추가나 프라이버시 보호 강화를 위한 대체와 같은 익명처리 과정을 거칠 수 있다. 어떤 질문에 대해서도 비교적 정확하게 답변할 능력(즉, 잡음을 적게 추가하는 방식)과 프라이버시 보호 능력을 동시에 갖춘 훌륭한

---

[14] Dwork, C. (2006). 차등 정보보호(Differential privacy). *오토마타, 언어 및 프로그래밍(Automata, languages and programming)* (pp. 1-12). Springer Berlin Heidelberg

[15] Cf. Ed Felten (2012) 잡음 추가에 의한 프라이버시 보호(Protecting privacy by adding noise). URL:https://techatftc.wordpress.com/2012/06/21/protecting-privacy-by-adding-noise/.

상호작용적 쿼리-응답 메커니즘을 찾는 것은 여전히 일반에 문호가 개방된 연구 주제이다.

추론 및 연결가능성 공격을 제한하려면 개체가 실행한 쿼리를 지속적으로 추적하고 정보주체에 대해 취득한 정보를 관찰할 필요가 있다. 따라서 '차등 정보보호' 데이터베이스를 쿼리 실행 개체에 대한 추적이 불가능한 공개 검색엔진상에 구축해서는 안 된다.

3.1.3.1 보장

- *식별:* 통계가 단지 산출물에 지나지 않고 데이터세트에 적용될 규칙을 잘 선택한다면 응답을 사용하여 개인을 가려내는 것은 불가능하다.
- *연결가능성:* 다중 요청을 사용함으로써 두 응답 사이의 특정 개인과 관련된 엔트리를 연결하는 것이 가능할 수도 있다.
- *추론:* 다중 요청을 사용하면 개인 또는 집단의 정보를 추론할 수 있다.

3.1.3.2. 흔한 실수

- 충분한 잡음을 추가하지 않음: 개인정보가 배경지식과 연결되지 않도록 예방할 때의 힘든 점은 특정 정보주체 또는 정보주체 그룹이 해당 데이터세트 생성에 기여했는지 여부에 대해 최소한의 증거만 제공하는 문제이다. 개인정보보호의 관점에서 큰 난관은 공개된 응답의 효용은 유지하는 동시에 개인의 프라이버시 보호를 위해 올바른 대답에 추가시킬 정확한 분량의 잡음을 생성하는 능력이다.

3.1.3.3 차등 정보보호의 실패

각 쿼리를 독립적으로 취급: 쿼리를 조합할 경우, 비밀로 하려는 정보가 공개되는 결과를 초래할 수 있다. 쿼리 이력을 보관하지 않을 경우, 공격자는 '차등 정보보호' 데이터베이스를 상대로 단일 정보주체의 구체적 특징이 결정적으로 드러나거나, 아니면 해당 주체일 가능성이 매우 높을 때까지 산출된 표본의 진폭을 계속 줄여나가는 다중 질문을 설계할 수도 있다. 한 가지 더 경고한다면, 합리적으로 예상되는 모든 수단을 고려할 때 개인정보 처리자가 원본 데이터베이스에서 여전히 정보주체 식별이 가능한데도 제3자의 관점에서 해당

개인정보가 익명정보일 것으로 생각하는 오류를 범하지 말라는 것이다.

3.2. 일반화(Generalization)

일반화는 익명처리 기법 중 두 번째 방법이다. 이 접근법은 축척 또는 자릿수를 수정함으로써(즉, 도시 대신에 지역, 일주일 대신에 한달 등) 정보주체의 속성을 일반화 또는 희석하는 것이다. 일반화가 개인을 식별해내는 것을 방지하는 데는 효과적이지만, 항상 실질적인 익명처리를 가능하게 하지는 않는다. 특히 일반화는 연결가능성과 추론을 예방할 수 있는 구체적이고 정교한 정량적 접근법을 필요로 한다.

3.2.1.총계처리와 k-익명성

총계처리와 k-익명성 기법은 동일한 속성을 가진 정보주체가 적어도 k번 나타나게 함으로써 정보주체가 식별되지 않도록 하는 것을 그 목적으로 한다. 이를 위해 각 개인이 공통된 값을 가지도록 속성값을 일반화시킨다. 예를 들어, 장소의 단위를 도시에서 국가로 바꿈으로써 더 많은 정보주체가 포함되도록 만드는 식이다. 생년월일은 날짜 범위로 일반화시키거나 월별 또는 연도별로 그룹을 만들 수 있다. 그 외 숫자 속성(예: 급여, 체중, 키, 약 복용량)은 간격값으로 일반화시킬 수 있다(예: €20,000 – €30,000). 정확한 속성값의 상관관계가 준식별자를 생성할 가능성이 있을 때는 이런 방법이 사용된다.

3.2.1.1. 보장

- *식별:* 이제 동일한 속성을 공유하는 사용자가 k명이므로 사용자 k명으로 구성된 그룹 내의 한 개인을 식별하는 것은 불가능하다.
- *연결가능성:* 연결가능성은 제한적이지만 k명의 사용자로 구성된 그룹별로 개인기록부를 연결하는 것은 여전히 가능하다. 그 때 이 그룹 내에서 두 개인기록부가 동일한 준식별자와 일치할 확률은 1/k이다(이는 동 엔트리가 연결 불가능할 확률에 비해 매우 유의하게 높다).
- *추론:* k-익명성 모델의 주요 단점은 어떤 형태의 추론 공격도 예방하지 못한다는 데 있다. 실제로 k명의 개인이 모두 같은 그룹에 들어 있다고 가정하고, 이 때 한 개인이 어느 그룹에 속하는지 알려진다면, 이 속성값을 검색하는 것은 간단한 일이다.

3.2.1.2. 흔한 실수

- 일부 준식별자의 누락: k-익명성을 고려할 때 결정적인 매개변수는 k의 기준치이다. k의 값이 높으면 높을수록 프라이버시는 더 철저히 보호된다. 이 때 흔한 실수가 원래 고려한 준식별자 집합을 줄여 인위적으로 k값을 높이는 것이다. 준식별자 축소는 다른 속성과 연관된 본원적인 식별처리 능력 때문에(특히 매우 희소한 속성의 사례에서 보는 것처럼, 일부가 민감한 속성이거나 엔트로피가 대단히 높은 속성일 경우) k-사용자의 클러스터 구축을 더 쉽게 해준다. 일반화를 위해 속성을 선택할 때 모든 준식별자를 다 고려하지 않는 것은 치명적인 실수이다. 만일 k명으로 구성된 클러스터에서 개인을 식별하는 데 몇몇 속성이 이용된다면 그러한 일반화는 일부 개인에 대해서는 보호에 실패한다(표 2의 예 참조).
- k값이 작은 경우: 마찬가지로 문제가 되는 것이 k값의 목표를 작게 잡는 것이다. k값이 너무 작을 경우, 한 클러스터 내에서 어떤 개인이든 비중이 너무 커지고 추론 공격의 성공률이 더 높아진다. 예를 들어, k=2이라면 그 때 두 사람이 같은 속성을 공유할 확률은 k>10일 때보다 더 높다.
- 개인을 동일한 비중의 그룹으로 만들지 않음: 개인의 집합을 불균등한 속성 분포로 그룹화하는 것도 문제가 된다. 개인의 기록부가 데이터세트에 미치는 영향은 같지 않다. 어떤 것은 엔트리의 큰 몫을 차지하는 반면, 그 외 기록부의 분포는 별로 유의하지 않을 것이다. 따라서 어떤 개인도 클러스터 내에서 너무 큰 비중을 차지하지 않도록 k가 높은 값이 되도록 하는 것이 중요하다.

3.1.3.3. k-익명성의 실패:

k-익명성의 주요 쟁점은 이 기법이 추론 공격을 막지 못한다는 것이다. 다음의 예에서, 만약 공격자가 특정 개인이 데이터세트 내에 있고 1964년생이라는 사실을 안다고 가정하면, 이 공격자는 해당 개인이 심근경색 병력이 있다는 사실도 알게 된다. 뿐만 아니라, 만약 우리가 이 데이터세트는 프랑스 기관에서 입수된 것이라는 사실을 안다면, 우편번호 앞 3자리(750*)가 파리를 의미하므로 해당 개인은 모두 파리에 거주하고 있다는 사실도 알 수 있다.

연도	성별	우편번호	진단
1957	M	750*	심근경색
1957	M	750*	콜레스테롤
1957	M	750*	콜레스테롤
1964	M	750*	심근경색
1964	M	750*	심근경색

표 2. 잘못 설계된 k-익명처리 사례

3.2.2.l-다양성/t-근접성

l-다양성은 각 동질 집합 내에서 모든 속성이 적어도 서로 다른 l개의 값을 갖도록 함으로써 결정적 추론 공격이 불가능하도록 k-익명성을 확대한다.

기본적인 목표는 속성 가변성이 낮은 동질 집합의 출현을 제한함으로써 특정 정보주체에 대한 배경지식을 가진 공격자가 항상 유의한 불확실성에 직면하게 만드는 것이다.

l-다양성은 속성값이 양호하게 분포되었을 때 추론 공격으로부터 개인정보를 보호하는 데 유용하다. 다만, 이 기법은 어떤 파티션(partition) 내의 속성이 불균일하게 분포되었거나 좁은 범위의 값 또는 의미론적 의미를 가질 경우는 정보 유출을 막을 수 없다는 점을 강조할 필요가 있다. 결국 l-다양성은 확률론적 추론 공격의 대상이 된다.

t-근접성은 테이블 내에서 속성의 초기 분포를 닮은 동질 집합을 생성함으로써 l-다양성을 개선한 것이다. 이 기법은 개인정보를 최대한 원자료와 가깝게 유지할 필요가 있을 때 유용하며, 그 목적을 달성하기 위해 동질 집합에 추가적인 제약을 가한다. 즉, 각 동질 집합에 적어도 l개의 상이한 값이 존재해야 할 뿐 아니라 각 속성의 초기 분포를 반영할 수 있도록 각 값이 가능한 한 자주 표현되어야 한다.

3.2.2.1. 보장

- *식별:* k-익명성과 마찬가지로 l-다양성과 t-근접성은 데이터베이스에서 개인 관련 기록부가 식별되지 않도록 할 수 있다.
- *연결가능성:* l-다양성과 t-근접성은 연결 불가능성의 관점에서 k-익명성을 개선한 것이 아니다. 이 문제는 모든 클러스터에서도 마찬가지이다. 즉, 같은

엔트리가 동일한 정보주체에 속할 확률은 1/N보다 더 크다(여기서 N은 데이터베이스 내 정보주체의 수).

- *추론:* k-익명성과 비교할 때 l-다양성과 t-근접성의 주요 개선점은, l-다양성 또는 t-근접성 데이터베이스를 상대로 100% 확신을 갖고 추론 공격을 감행하는 것이 더 이상 불가능하다는 점이다.

3.2.2.2. 흔한 실수

- 민감한 속성값에 그 이외의 민감한 속성을 혼합하는 방법으로 민감한 속성값을 보호: 프라이버시 보호를 위해 클러스터 내에서 하나의 속성에 대해 두 개의 값을 갖는 것으로는 충분치 못하다. 실제로 각 클러스터 내 민감한 속성값의 분포는 전체 모집단 내 민감한 속성값의 분포와 닮거나, 그렇지 않으면 적어도 클러스터 전체에 걸쳐 균일성을 가져야 한다.

3.2.2.3. l-다양성의 실패:

아래 표에서, '진단'이라는 속성에 대해 l-다양성이 부여되어 있다. 하지만 1964년에 출생한 어떤 개인이 이 표에 있다는 사실을 안다면 그 사람이 심근경색 병력을 가졌을 확률이 매우 높다고 가정할 수 있다.

연도	성별	우편번호	진단
1957	M	750*	**심근경색**
1957	M	750*	**콜레스테롤**
1957	M	750*	**콜레스테롤**
1957	M	750*	**콜레스테롤**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**
1964	M	750*	**콜레스테롤**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**
1964	M	750*	**심근경색**

표 3. '진단' 속성값이 균일하게 분포되지 않은 l-다양성 표

이름	생년	성별
Smith	1964	M
Rossi	1964	M
Dupont	1964	M
Jansen	1964	M
Garcia	1964	M

표 4. 이 사람들이 표 3에 있다는 사실을 안다면, 공격자는 그들이 심근경색 병력이 있다는 것을 추론할 수 있다.

4. 가명처리(Pseudonymisation)

가명처리는 개인기록부 내에 있는 어떤 속성(일반적으로 고유 속성)을 다른 속성으로 교체하는 것이다. 그러므로 자연인은 여전히 간접적으로 식별될 가능성이 있다. 따라서 가명처리가 단독으로 사용되었을 때는 데이터세트의 익명화를 달성할 수 없다. 그럼에도 불구하고 가명처리 기법 이용을 둘러싼 오해와 실수가 있기 때문에 본 의견서는 가명처리에 대해 논의한다.

가명처리는 데이터세트를 정보주체의 원래 신원과 연결시킬 가능성을 낮춘다. 그래서 가명처리가 유용한 보안 조치이긴 하나, 익명처리의 한 방법은 아니다.

가명처리의 결과는 초기값과는 독립적이거나(개인정보 처리자가 생성한 난수 또는 정보주체가 선택한 성씨의 경우와 같이), 아니면 속성 또는 속성의 집합의 원래 값에서 도출된 값, 예컨대 해시 함수(hash function) 또는 암호화 기법이 될 수 있다

가장 널리 사용되는 가명처리 기법은 다음과 같다.

- 비밀키(Secret Key) 암호화 기법: 이 경우 비록 암호화된 형태이지만 여전히 데이터세트 내에 개인정보가 들어 있기 때문에 비밀키 소유자는 각 정보주체를 간단히 재식별할 수 있다. 첨단 암호화 기법이 적용되었다고 가정한다면 키에 사용된 암호를 알고 있어야만 복호화가 가능하다.
- 해시 함수: 이는 임의의 크기를 가진 데이터를 입력 받아서(입력은 단일 속성 또는 속성의 집합이 될 수 있음) 고정된 크기의 결과값을 출력함으로써 다시 원래의 값으로 되돌릴 수 없는 함수이다. 따라서 암호화와 관련하여 원래의 값으로 되돌릴 위험이 더 이상 존재하지 않는다. 다만, 해시 함수의 입력값의 범위가 알려질 경우, 특정 개인기록부에 대한 정확한 값을 추출하기 위해 해시 함수를 통해 그 입력값이 재전송될 수 있다. 예를 들어, 어떤 데이터세트가 국가식별번호 해싱을 통해 가명처리되었다면, 이 데이터세트는 가능한 모든 입력값을 해싱하여 그 결과값을 데이터세트 내의 값과 비교함으로써 간단히 추출될 수 있다. 일반적으로 해시 함수는 비교적 신속한 계산이 가능하도록 설계되므로 무차별 대입(brute force) 공격의 대상이 된다.[16] 사전 계산 테이블(pre-computed table)을 생성하여 대량 해시값을 한꺼번에 되돌릴

[16] 무차별 대입 공격이란 상응하는 테이블을 생성하기 위해 가능한 입력값을 모두 시도하는 것이다.

수도 있다.

솔트 해시 함수(해싱할 때 '솔트'라고 하는 랜덤값을 속성에 추가)를 사용하면 입력값 추출의 가능성을 낮출 수 있다. 하지만 타당한 수단을 이용한다면 솔트 해시 함수의 결과 뒤에 숨은 원래 속성값 계산은 여전히 실현 가능한 일이다.[17]

- 저장된 키를 사용하는 키 해시 함수: 이것은 비밀키를 추가 입력으로 사용하는 특별한 해시 함수이다(대개 솔트는 비밀이 아니므로 솔트 해시 함수와는 다름). 개인정보 처리자는 비밀키를 사용하여 속성 관련 키 해시 함수를 재전송할 수는 있으나, 테스트해야 할 경우의 수가 너무 많아 실용성이 떨어지므로 키를 모르고서는 함수를 재전송하기가 훨씬 더 어렵다.
- 키 삭제를 통한 결정적 암호화 또는 키 해시 함수: 이 기법은 데이터베이스 내 각 속성에 대한 가명으로서 난수를 선택한 뒤에 상응하는 테이블을 삭제하는 것과 같다. 이 솔루션은 데이터세트 내 개인정보와 또 다른 데이터세트 내에서 가명이 사용된 동일인물 관련 개인정보 사이의 연결 위험을 줄여준다. [18] 첨단 알고리즘을 고려할 때, 공격자는 키를 구할 수 없어 가능한 모든 키를 테스트해야 하기 때문에 함수를 복호화하거나 재전송하기란 계산상 어려운 일이다.
- 토큰화(Tokenization): 일반적으로 이 기법은 금융부문에서 카드 ID 번호를 공격자에게 유용하지 않은 값으로 대체하기 위해 사용한다. 토큰화 기술은 단방향 암호화 기법 또는 원자료로부터 수학적으로 도출되지 않은 일련번호 또는 난수를 인덱스 함수를 통해 지정하는 어플리케이션에 기반한 예전의 기술을 모체로 개발된 것이다.

4.1. 보장

- *식별:* 개인은 여전히 가명처리 함수의 결과값인 고유 속성(가명처리된 속성)에 의해 식별될 수 있기 때문에 개인의 기록부를 식별하는 것이 여전히 가능하다.
- *연결가능성:* 동일한 개인을 나타내기 위해 동일한 가명 속성을 사용하는 기록부들은 그 연결성을 간단히 알아낼 수 있다. 설사 동일한 정보주체에 대해 상이한 가명 속성을 사용했다 하더라도 그 외 속성을 수단으로 하여 여전히 연결이 가능하다. 데이터세트 내 다른 어떤 속성도 정보주체 식별에 사용되지 않을 경우에 한해, 또한 원래 속성과 가명처리된 속성 사이의 연결성이 완전히

[17] 특히 속성의 유형이 알려져 있을 경우(이름, 사회보장번호, 생일, 등). 계산 요건을 추가할 때는 계산된 값이 짧은 솔트로 여러 차례 해싱되는 키 유도 해시 함수가 사용될 수 있다.

[18] 데이터세트 내 다른 속성 및 원자료 삭제 여부에 따라 달라짐.

제거되었을 때라야(원자료 삭제를 포함하여), 상이한 가명 속성을 사용하는 두 데이터세트간에 명백한 교차 추론은 불가능해질 것이다.

- *추론:* 개인에 대해 동일한 가명 속성을 사용하는 데이터세트 내에서나 서로 다른 데이터베이스 전반에 걸쳐서, 또는 가명이 자명하고 정보주체의 원래 신원을 제대로 마스킹하지 않는다면 정보주체의 진짜 신원에 대한 추론 공격이 가능하다.

4.2. 흔한 실수

- 가명처리된 데이터세트가 익명처리되었다고 믿는 일: 개인정보 처리자는 흔히 하나 이상의 속성만 제거 또는 교체하면 데이터세트 익명처리에 충분하다고 생각한다. 하지만 그렇지 않음이 많은 사례에서 입증되었다. 단지 ID만 바꾸는 것은 만일 준식별자가 데이터세트에 남아 있다거나 다른 속성값이 개인 식별을 가능하게 한다면 정보주체가 식별되는 것을 방지할 수 없다. 가명처리된 데이터세트에서 개인을 식별하는 것이 원자료에서 개인을 식별하는 것만큼 쉬운 경우가 허다하다. 데이터세트가 익명처리되었다고 판단하기 위해서는 속성 제거와 일반화, 또는 원자료 삭제, 혹은 적어도 원자료를 고차원의 총계처리 정보로 바꾸는 등의 추가 조치를 취해야 한다.
- 연결가능성 감소 기법으로서 가명처리를 사용할 때의 일반적 실수:
    - 상이한 데이터베이스에 동일한 키를 사용: 상이한 데이터세트의 연결가능성을 제거하는 것은 키 알고리즘 및 한 사람의 개인이 다양한 맥락의 여러 가명 속성에 해당한다는 사실에 크게 달라진다. 따라서 연결가능성을 낮추려면 서로 다른 데이터베이스에 동일한 키 사용을 피하는 것이 중요하다.
    - 서로 다른 사용자에 대해 상이한 키('회전 키')를 사용: 서로 다른 사용자에 대해 상이한 키를 사용하고 일정한 사용 기준으로(예를 들어, 같은 사용자에 대해 기록부 10 엔트리마다 동일한 키를 사용) 키를 바꾸고 싶은 유혹을 느낄 수도 있다. 하지만 그러한 방식을 제대로 설계하지 않을 경우 패턴을 발생시킴으로써 의도된 이점이 부분적으로 줄어들 수 있다. 예를 들어, 특정 개인에 대해 특정 규칙을 사용하는 방식으로 키 회전을 적용하면 어떤 개인에 상응하는 엔트리의 연결가능성이 커진다. 아울러 새 가명 정보가 나타날 때 데이터베이스 내에서 반복되는 가명 정보가 사라진다면, 이는 두 기록부가 같은 자연인을 지칭한다는 신호가 될 수 있다.

○ 키 보관: 만일 비밀키가 가명처리된 정보와 함께 보관되고 이 개인정보가 공격을 당할 경우, 공격자는 가명 정보와 그 원래 속성을 간단히 연결할 수 있을 것이다. 키가 개인정보와는 별도로 보관되나 안전하게 보관되지 않는다면, 이 때도 마찬가지 위험이 적용된다.

4.3. 가명처리의 단점

- *의료*

1. **이름, 주소,** **생년월일**	2. **특별지원수당 기간**	3. **체질량지수**	6. **연구 코호트 참조** **번호**
[redacted]	< 2년	15	QA5FRD4
	> 5년	14	2B48HFG
	< 2년	16	RC3URPQ
	> 5년	18	SD289K9
	< 2년	20	5E1FL7Q

표 5. 쉽게 되돌릴 수 있는 해싱(이름, 주소, 생년월일)에 의한 가명처리의 예

개인의 체중과 특별지원수당 지급금 수령과의 관계를 조사하기 위해 데이터세트를 만들었다. 원본 데이터세트에는 정보주체의 이름, 주소, 생년월일이 들어 있으나 표에서는 삭제되었다. 해시 함수를 사용하여 삭제된 데이터에서 연구 코호트 참조번호를 생성했다. 표에서 비록 이름, 주소, 생년월일은 삭제되었지만, 만일 정보주체의 이름, 주소, 생년월일이 알려져 있고 그 뿐만 아니라 사용된 해시 함수까지 안다면, 연구 코호트 참조번호를 계산하기는 어렵지 않다.

- *소셜네트워크*

특정 개인에 대한 민감한 정보가 '가명처리' 기법을 적용했음에도 불구하고 소셜네트워크 그래프에서 추출될 수 있음이 알려졌다.[19] 한 소셜네트워크 서비스제공업체가 마케팅 및 홍보 목적으로 개인정보를 다른 기업에 판매한 뒤, 식별처리 방지에 충분할 정도로 가명처리가 안전하게 수행된 것으로 잘못 생각했다. 서비스제공업체는 실명 대신에 별명을 사용했으나, 서로 다른 개인

[19] A. Narayanan and V. Shmatikov, '소셜네트워크 역익명화(De-anonymizing social networks),' 제30회 IEEE 보안 및 개인정보보호 심포지엄, 2009년.

사이의 관계가 유일무이하고 또한 식별자로 사용될 수 있기 때문에 이는 사용자 프로필을 익명화하기에 불충분했다.

- *위치*

최근 MIT 연구원들이 150만 명의 반경 100km 영역에 대한 15개월 동안의 시공간 이동성 좌표로 구성된 가명처리된 데이터세트를 분석했다.[20] 이 분석에 의하면, 4개의 위치 지점만으로 모집단의 95%를 식별할 수 있고, 2개의 위치 지점(위치 지점 중 하나는 알려져 있으며, '집' 또는 '회사'일 가능성이 매우 큼)으로도 정보주체의 50%는 식별이 가능하며, 비록 개인의 신원은 진짜 속성을 다른 라벨로 교체하여 가명처리했다 하더라도 프라이버시 보호를 위한 공간이 매우 제한적인 것으로 나타났다.

5. 결론 및 권고

5.1. 결론

비식별처리 및 익명처리 기법은 집중적인 연구의 주제이며, 본 의견서는 각 기법이 저마다의 장점과 단점이 있음을 일관되게 제시한다. 대부분의 경우 각 데이터세트는 사례별로 고려할 필요가 있기 때문에 최소한의 파라미터에 대한 권고안을 제시하기란 불가능하다.

익명처리된 데이터세트가 여전히 정보주체에게 잔존 위험을 제기하는 수가 많다. 실제로 비록 개인 기록부의 정확한 검색은 불가능하다 하더라도 이미 나와 있는 다른 정보 소스(일반에 공개된 정보 또는 그렇지 않은 정보)의 도움을 받아 개인에 관한 정보를 모으는 것은 여전히 가능하다. 열악한 익명처리 과정의 결과가 정보주체에 미친 직접적인 영향(알지도 못하는 사이에, 또는 사전 동의도 받지 않고 클러스터에 포함됨으로 인한 성가심, 시간 소모 및 자제력을 잃는 느낌) 외에도, 익명 정보 처리의 결과로서, 특히 공격자의 의도가 악의적일 때는 일부 공격자에 의해 정보주체가 표적에 잘못 포함될 때마다 간접적인 부작용이 발생할 수 있음을 강조할 필요가 있다. 따라서 본 작업반은 익명처리 기법이 프라이버시를 보장할 수 있지만, 그것은 익명처리 기법 적용이 적절하게 이뤄질 때에 한하는 것이며, 다시 말해,

[20] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen and V. Blondel, '군중의 고유성: 인간 이동성의 프라이버시 경계(Unique in the Crowd: The privacy bounds of human mobility),' Nature, no. 1376, 2013

목표로 하는 익명처리 수준을 달성하려면 익명처리 과정의 전제 조건(상황) 및 목적이 분명하게 명시되어야 함을 강조하는 바이다.

5.2. 권고안

- 일부 익명처리 기법은 본원적인 한계를 노출한다. 개인정보 처리자가 익명처리 과정을 설계할 때는 이러한 한계를 심각히 고려해야 한다. 개인정보 처리자는 익명처리를 통해 데이터세트를 공표할 때나 어떤 정보가 데이터세트에서 검색되도록 허용할 때는 개인의 프라이버시 보호 등의 목적이 달성될 수 있도록 유념해야 한다.
- 본 의견서에 기술된 기법들은 효과적인 익명처리의 기준(즉, 개인이 식별되지 않도록 할 것, 개인 관련 기록부 사이에 연결가능성이 없을 것, 개인에 대한 추론이 불가능할 것)을 확실히 충족하지는 못한다. 하지만 이들 위험 중 일부는 본고에서 소개한 기법을 통해 전체적으로든 부분적으로든 충족될 수도 있으므로, 개별 기법을 특정 상황에 적용하는 방법을 고안하거나 결과의 안전성을 제고하기 위해 여러 기법을 결합하여 적용할 때는 주도면밀한 설계가 필요하다.

아래 표는 전술한 세 가지 기본요건의 관점에 따라 본고에서 고찰한 기법의 강점과 약점을 정리한 것이다.

	개인이 식별될 위험이 상존하는가?	**연결가능성의 위험이 상존하는가?**	**추론의 위험이 상존하는가**
가명처리	그렇다	그렇다	그렇다
잡음 추가	그렇다	그렇지 않을 수도 있다.	그렇지 않을 수도 있다.
대체	그렇다	그렇다	그렇지 않을 수도 있다.
총계처리와 k-익명성	아니다	그렇다	그렇다
l-다양성	아니다	그렇다	그렇지 않을 수도 있다.
차등 정보보호	그렇지 않을 수도 있다.	그렇지 않을 수도 있다.	그렇지 않을 수도 있다.
해싱/토큰화	그렇다	그렇다	그렇지 않을 수도 있다.

표 6. 본고에서 고찰한 기법의 강점과 약점

- 최적의 해법은 사례별로 결정해야 한다. 따라서 상기 세 가지 기준을 충족하는 솔루션(즉, 완전한 익명처리 과정)이야말로 개인정보 처리자와 제3자가 가장 합리적으로 가능성이 큰 수단을 통해 재식별처리를 시도할 때 이를 막는 안전한 솔루션이 될 것이다.

- 만약 어떤 제안이 위 기준 중에서 한 가지를 충족하지 못한다면, 그 때마다 식별처리 위험에 대한 철저한 평가가 수행되어야 한다. 익명처리 과정의 평가 또는 인가가 당국의 소관사항이라고 국내법에 규정되어 있다면, 그러한 평가는 관련 당국이 제공해야 할 것이다.

식별처리 위험을 줄이기 위해서는 다음과 같은 모범관행을 고려해야 한다.

<u>모범적인 익명처리 관행</u>

일반적으로:

- '공개 후 망각'과 같은 접근법에 기대지 않는다. 개인정보 처리자는 식별처리의 잔존 위험을 감안하여 다음 사항에 유념해야 한다.
    - 1. 신규 위험을 파악하고 잔존 위험을 정기적으로 재평가한다.
    - 2. 식별된 위험에 대한 관리가 충분한지 평가하고 그에 맞춰 조정한다. 그와 동시에,
    - 3. 위험을 감시, 통제한다.
- 이러한 잔존 위험의 일부로서 데이터세트의 비익명처리 부분(만약 있다면)이 익명처리 부분과 결합했을 때의 식별 가능성 및 속성간의 상관관계(예: 지리적 위치와 보유 재산 자료)에 의한 식별 가능성에 주의한다.

상황 요소:

- 식별처리 위험을 판단할 때는 익명처리된 데이터세트로 달성해야 할 목적이 핵심적인 역할을 하므로 이에 대해 분명히 규정해야 한다.
- 익명처리의 목적은 관련 상황 요소, 예를 들면, 원자료의 성격, 구축된 통제장치(데이터세트 접근을 제한하는 보안 조치를 포함), 샘플 사이즈(정량적 도구), 공공정보자원의 가용성(정보 수령자가 의존하게 됨), 제3자에 대한 개인정보 개방계획(예: 인터넷 등에서 제한, 비제한 등)과 같은 고려사항과 밀접한 연관이 있다.
- 표적공격을 유발할 수 있는 데이터의 매력을 염두에 두고 공격자에 대비해야 한다(이 때에도 정보의 민감성과 데이터의 성격이 핵심 요소가 됨).

기술적 요소:

- 개인정보 처리자는 개인정보를 공개할 때, 특히 익명처리된 데이터세트를 공개할 계획이 있을 경우, 현재 적용 중인 익명처리 기법(또는 기법의 결합)을 고지해야 한다.

- 명백한(예: 희소) 속성/준식별자는 데이터세트에서 제거해야 한다.

- 잡음 추가 기법이 사용될 경우(무작위화에서), 개인기록부에 추가되는 잡음 수준은 속성값, 보호되어야 할 속성의 정보주체에 미치는 영향 및/또는 데이터세트의 희박성에 대한 함수로서 결정해야 한다(다시 말해, 균형이 맞지 않는 잡음을 주입해서는 안 됨).

- 차등 정보보호를 적용할 경우에는(무작위화에서) 쿼리의 침입성은 누적되므로 프라이버시 침해 쿼리 탐지를 위해 지속적인 쿼리 추적의 필요성을 고려해야 한다.

- 일반화 기법이 적용된 경우, 개인정보 처리자가 심지어 동일한 속성에 대해서도 하나의 일반화 기준에만 국한되지 않는 것이 매우 중요하다. 그 말은, 서로 다른 위치 단위 또는 시간 간격을 선택해야 한다는 뜻이다. 적용 기준의 선택은 해당 모집단 내 속성값의 분포에 따라 결정되어야 한다. 모든 분포가 다 일반화에 적합한 것은 아니다. 즉, 일반화 기법에서는 획일적 접근법을 따라서는 안 된다. 동질 집합 내 가변성을 보장해야 한다. 예를 들어, 위에서 언급한 '상황 요소'(샘플 사이즈, 등)에 따라 구체적 기준치를 선택해야 하며, 만일 그 기준치에 도달하지 못한다면 해당 샘플은 폐기해야 한다(또는 그와는 다른 일반화 기준을 수립해야 함).

부속서

익명처리 기법 지침서

A.1. 서론

익명성에 대한 해석은 EU 국가별로 차이가 난다. 어떤 국가에서는 계산적 익명성(즉, 개인정보 처리자가 비록 제3자와 협력한다 하더라도 직접적으로든 간접적으로든 정보주체를 식별하는 것이 계산적으로 매우 어려움)을, 또 어떤 국가에서는 완전 익명성(즉, 개인정보 처리자가 비록 제3자와 협력한다 하더라도 직접적으로든 간접적으로든 정보주체를 식별하는 것이 불가능함)을 의미한다. 하지만 어느 경우든 '익명처리'가 개인을 식별할 수 없도록 한다는 점에는 이견이 없다. 차이가 나는 대목은 재식별처리의 위험 수준을 어느 선까지 허용하느냐이다.

익명정보의 사용 예(use case)는 사회조사나 통계분석에서부터 신제품, 서비스 개발에 이르기까지 다양하게 예상해 볼 수 있다. 그것이 비록 일반적 용도의 활동이라 하더라도 때로는 가공된 개인정보의 익명성을 무력화시켜 정보주체에게 영향을 미칠 수가 있는데, 실제로 표적 마케팅 계획에서부터 사용자 프로파일링, 행동, 이동성 패턴에 기초한 공공정책 시행에 이르기까지 그 사례가 적지 않다.[21]

애석하게도 개인정보 처리 후 재식별처리에 소요되는 시간이나 노력을 사전에 평가하고자 할 때, 또는 공개된 데이터베이스가 정보주체의 식별된 데이터세트를 지칭할 확률을 낮추고자 할 때, 이런 경우 최적의 절차 선택에 사용될 수 있는 정립된 지표는 존재하지 않는다. 단지 일반적인 설명만 있을 뿐이다.

과학문헌에 자주 언급되는 이른바 '익명처리 기술'은 아직 초기단계에 있는 새로운 과학분야[22]이며, 데이터세트 식별처리 능력을 무력화시킬 관행은 많이 존재한다. 하지만 그 중 대다수는 가공된 개인정보와 정보주체의 연결을 방지할 수 없음을 분명히 밝혀 두고자 한다. 상황에 따라서는 익명처리된 것으로 알았던 데이터세트가 매우 성공적으로 식별되는 것으로 드러났으며, 또 어떤 상황에서는 거짓 양성(false positive)도 발생했다.

익명처리에는 대체로 속성 일반화와 무작위화의 두 가지 접근법이 있다. 이 두 접근법의 세부 요소를 자세히 살펴보면 개인정보 식별처리 능력에 대한 식견을

---

21 예컨대 네덜란드의 TomTom GPS 데이터 사용 사건을 들 수 있다(단락 2.2.3에서 설명한 예 참조).

22 Jun Gu,Yuexian Chen,Junning Fu,HuanchunPeng,Xiaojun Ye, '합성: 익명처리 기술, 데이터베이스 및 전문가시스템 어플리케이션-컴퓨터공학과 강의노트(Synthesizing:Art of Anonymization, Database and Expert Systems Applications Lecture Notes in Computer Science)' –Springer- Volume 6261, 2010, pp 385- 399

넓히고 개인정보의 개념에 대해 새로운 이해를 얻을 수 있을 것이다.

A.2. 무작위화에 의한 '익명처리'

익명처리의 한 방법은 익명정보와 원래 값 사이의 연결 방지를 위해 실제 값을 수정하는 것이다. 이 목표는 잡음 추가에서부터 개인정보 교환(치환)에 이르기까지 다양한 방법을 사용하여 달성이 가능하다. 속성을 제거하는 것은 그 속성을 극단적인 형태로 무작위화하는 것과 마찬가지라는 점 또한 강조할 필요가 있다(속성이 잡음에 의해 완전히 가려짐).

상황에 따라서는 대체적인 개인정보 처리의 목표가 무작위화된 데이터세트를 공개하는 것이 아니라 쿼리를 통한 개인정보 접근을 허용하는 것이다. 이 경우, 정보주체가 받는 위험은 개인정보 처리자가 모르는 사이에 공격자가 일련의 쿼리를 통해 정보를 빼가는 데서 비롯된다. 데이터세트 내 개인의 익명성을 보장하려면 해당 정보주체가 데이터세트에 기여한 것으로 결론짓지 못하게 함으로써 공격자가 보유하고 있을지도 모르는 배경정보와의 연결을 완전히 차단해야 한다.

쿼리 응답에 적절한 잡음을 추가하면 재식별화 위험을 더 낮출 수 있다. 연구문헌에서 차등 정보보호[23]라고 칭하는 이 접근법은 일반 공개와 비교할 때 개인정보 발표자에게 데이터 접근권한을 더 많이 부여한다는 점에서 앞서 설명한 기법들과는 구분된다. 잡음 추가의 목적은 첫째, 데이터세트 내 정보주체의 프라이버시 보호, 둘째 공개된 정보의 효용 유지이다. 특히 잡음의 크기는 쿼리의 수준과 비례해야 한다(정확히 응답해야 할 쿼리가 너무 많으면 해당 개인이 식별될 위험이 커진다). 오늘날 개인정보 처리자가 데이터세트를 무작위화했는데도 정보주체의 속성(데이터세트에 포함되었는지 여부와는 무관하게)이 극히 간단한 방법으로 유출되는 기법이 제시되지 않게끔 무작위화를 성공적으로 적용하는 방안을 사례별로 검토해야 한다.

이 때 익명처리 수단으로서의 무작위화가 실패할 가능성이 있는 사례를 논의하는 것이 도움이 될 것이다. 예를 들어, 상호작용적 접근(interactive access)의 맥락에서, 프라이버시 친화적인 쿼리는 정보주체에게 위험을 제기할 수 있다. 실제로 만약 공격자가 개인들의 하부집단(S)이 모집단(P)의 속성(A) 발생빈도 관련 정보가 있는

[23] Cynthia Dwork, '차등 정보보호, 국제 오토마타, 언어 및 프로그래밍(ICALP) 학술대회(Differential Privacy, International Colloquium on Automata, Languages and Programming) 2006, p. 1–12

데이터세트 내에 있다는 사실을 안다면, "모집단 P에서 속성 A를 갖는 개인은 몇 명인가?"와 "하부집단 S에 속하면서 속성 A를 갖는 개인을 제외하고, 모집단 P 안에는 몇 명의 개인이 있는가?"라는 두 가지 질의만 하면 결정론적으로든, 아니면 확률 추론에 의해서든 하부집단 S 안에 들어 있는 개인(실제로 속성 A를 보유)의 수를 알아낼 수도 있다. 어떤 경우든 하부집단 S 내에 있는 개인들의 프라이버시는 심각하게 위협받을 수 있으며, 특히 속성 A의 성격에 크게 좌우된다.

만일 어떤 정보주체가 데이터세트 내에 들어 있지는 않지만 해당 정보주체와 데이터세트 내 개인정보와의 관계가 알려졌다면, 그 때 개인정보의 공개는 해당 개인의 프라이버시에 위험을 제기한다고 생각할 수도 있다. 예를 들어, 만약 "표적의 속성 A의 값은 수량 X에 의해 모집단의 평균값과는 달라진다"가 알려졌다면, 속성 A의 평균값을 추출하는 프라이버시 친화적인 작업을 수행하도록 데이터베이스 큐레이터에게 요청하는 것만으로 공격자는 특정 정보주체와 관련된 개인정보를 추론할 수도 있다.

데이터베이스 내 실제값에 상대적 부정확성을 추가하는 것도 제대로 된 설계가 필요한 작업이다. 프라이버시가 보호될 정도로 잡음이 충분해야 할 뿐 아니라, 데이터 유용성이 확보될 정도로 잡음이 많지 않아야 한다. 예를 들어, 고유 속성을 갖는 정보주체의 수가 너무 작거나 속성의 민감도가 높을 경우, 실제 숫자를 알리는 대신 예컨대, "몇 안 되는 사례, 제로(0)일 수도 있음"과 같이 어떤 범위 또는 일반적인 문장으로 표시하는 것이 더 낫다. 이런 방식을 쓰면, 비록 잡음이 추가된 공개 메커니즘이 사전에 알려진다 하더라도 어느 정도의 부정확도가 유지되기 때문에 정보주체의 프라이버시가 보호된다. 정보 유용성의 측면에서 볼 때, 적절하게 부정확성을 설계한다면 그 결과는 통계나 의사결정의 목적으로 여전히 효용가치가 있다.

데이터베이스 무작위화 및 차등 정보보호 접근은 심도 있는 검토를 필요로 한다. 첫째, 정확한 왜곡량은 상황에 따라(쿼리의 종류, 데이터베이스 내 모집단의 크기, 속성의 특징 및 속성의 내재적 식별능력) 크게 달라질 수 있으며 결코 '*어디에나 통하는* ' 솔루션을 바랄 수는 없다. 더욱이, 시간이 흐르면 상황이 바뀔 수 있으므로 상호작용적 메커니즘 역시 그에 맞게 수정해야 한다. 잡음을 수정하기 위해서는 상호작용적 메커니즘이 정보주체에게 제기할 수 있는 누적 프라이버시 위험을 추적해야 한다. '프라이버시 비용(privacy cost)'이 예산에 도달하여 새로운 쿼리가 실행되면 정보주체가 위험에 노출되는 문제에 대비하여 개인정보 접근

메커니즘(data access mechanism)에 경보장치를 탑재함으로써 개인정보 처리자가 수시로 실제 개인정보에 잡음을 추가하기 위한 적정 왜곡 수준을 결정할 수 있게 도움을 주어야 한다.

다른 한편으로는, 속성값이 삭제(또는 수정)되는 경우도 생각해봐야 한다. 비정형(atypical) 속성값을 다루기 위한 일반적인 솔루션이 비정형 개인 관련 데이터 또는 비정형 값의 세트를 제거하는 방법이다. 후자의 경우, 비정형 값을 없앤 그 자체가 정보주체 식별을 위한 요소가 되지 않도록 하는 것이 중요하다.

이제부터는 속성 대체에 의한 무작위화에 대해 논의하기로 한다. 익명화를 다룰 때의 큰 오해는 익명처리 기법을 암호화나 키 코딩(key-coding)과 같은 것으로 생각하는 점이다. 그러한 오해가 나오는 이유는, a) 데이터베이스 내에서 개인기록부의 어떤 속성(예: 이름, 주소, 생일)에 암호화를 적용하거나, 아니면 키를 혼합한 해시 함수와 같은 키 코딩 작업의 결과로 이 속성을 무작위화된 스트링으로 대체하면 그 개인기록부는 '익명처리된' 것이다. b) 키의 길이가 충분하고 암호화 알고리즘이 최신 기술을 사용한 것이라면 익명처리가 더 효과적일 것이라는 가정 때문이다. 즉, 개인정보 처리자 사이에 이런 오해가 확산되어 있기 때문에 이 문제는 제대로 밝힐 필요가 있으며, 이는 가명처리가 위험도가 덜하다는 주장과도 연관된다.

먼저, 위에서 말하는 기법은 전혀 같은 것이 아니다. 암호화는 도청 또는 의도하지 않은 공개를 막기 위한 보안 관행의 일환으로서 식별된 당사자(사람, 장치, 소프트웨어/하드웨어)간 통신 채널의 비밀성을 제공하는 것이 그 목적이다. 키 코딩은 비밀키에 따라 개인정보를 의미론적으로 변환시키는 것이다. 한편, 익명처리의 목적은 은연 중에 정보주체의 속성이 연결되지 못하도록 하는 개인 식별 방지책이다.

암호화도 키 코딩도 그 자체만으로는 정보주체의 비식별처리에 적합하지 않다. 적어도 원자료가 정보관리자의 수중에 있는 한, 개인정보는 여전히 입수 또는 추정이 가능하다. 키 코딩에서 발생하는 것처럼, 개인정보의 의미론적 변환만 수행하는 것은 반대방향으로 알고리즘을 적용하거나, 아니면 공격 계획의 성격에 따라 무차별 대입 공격을 통하거나 또는 데이터 유출로 인해 개인정보를 원래 구조로 재생할 가능성을 완전히 없애지는 못한다. 첨단 암호화 기법은 복호화 키를 무시하는 개체에 대해서는 정보 식별이 불가능하게 함으로써 한층 더 높은 수준의 개인정보보호를 보장할 수는 있지만 반드시 익명처리로 귀결되는 것은 아니다. 그 이유는, 키 또는 원자료를 구할

수 있는 한(보안키 에스크로 서비스를 제공하기로 계약에 묶여 있는 신뢰할 만한 제3자의 경우라 하더라도), 정보주체 식별 가능성을 배제할 수는 없다. .

암호화 메커니즘 또는 해시 함수의 종합적인 보안에는 여러 기술적, 조직적 요인이 영향을 미치므로, 데이터세트 '익명처리' 수준의 척도로서 암호화 메커니즘의 안전성에만 중점을 두는 것은 판단을 그르칠 수 있다. 키 보관의 취약점을 노린다든가(예: 보안 등급이 낮은 디폴트 모드의 존재) 기타 인적 요인(예: 키 복구 패스워드 취약) 때문에 알고리즘을 완전히 우회함으로써 공격에 성공한 사례가 문헌을 통해 많이 보고되었다. 끝으로, 일정 키 사이즈의 암호화 기법을 선택하면 일정 기간(현재의 키는 대부분 2020년경에 사이즈를 조정해야 함)에 대한 비밀성을 보장하도록 설계되어 있는 반면, 익명처리 과정에는 시간제약이 없어야 한다.

이번에는 최근 발생한 무작위화를 통한 익명처리의 나쁜 예와 그러한 실패의 이유를 살펴보고 속성 무작위화(또는 대체 및 제거)의 제한에 대해 상술할 필요가 있다.

이와 관련하여 잘 알려진 사례가 익명처리 수준이 미흡한 개인정보를 공개한 넷플릭스 프라이즈(Netflix Prize) 행사이다.[24] 정보주체 관련 속성들을 무작위화한 데이터베이스 내 범용 개인기록부를 분석하면 각 기록부를 {randomized attribute, clear attribute}라는 두 개의 하부 기록부로 분할이 가능하며, 여기서 'clear attribute'는 어떤 비개인정보의 조합도 될 수 있다. Netflix Prize 데이터세트는 각 기록부가 다차원 공간의 점으로 표현될 수 있음을 염두에 두고(이 때 각 'clear attribute'는 좌표) 구체적으로 관찰이 가능하다. 이 기법을 사용하면 모든 데이터세트를 다차원 공간 내 점의 집합으로 생각할 수 있는데, 공간의 희박성이 크기 때문에 각 점은 서로 멀리 떨어져 있다고 볼 수 있다. 실제로 점의 거리가 너무 멀기 때문에 공간을 넓은 영역으로 분할하면 각 영역에는 단 하나의 기록부만 남는다. 잡음을 추가하더라도 동일한 다차원 공간 영역을 공유할 정도로 충분히 가까이 있는 기록부가 되지 못한다. 예를 들어, 넷플릭스 실험에서는 14일이라는 간격 이내에서 영화 8편에 대한 평점만으로 이루어진 고유 기록부가 사용되었다. 평점과 날짜 모두 잡음을 추가한 후에는 영역 중첩이 관찰되지 않았다. 다시 말해, 단지 평점을 매긴 영화 8편을 선택한 것 그 자체가 데이터베이스 내 두 정보주체간에 공유되지 않는, 즉 이용자가 매긴 등급의 지문 역할을 했다. 이와 같은 기하학적 관찰을 바탕으로 연구자들은 익명처리된 것으로 알려진 넷플릭스 데이터세트를 다른

[24] Arvind Narayanan, Vitaly Shmatikov: 대규모 스파스 데이터세트의 안전 비익명처리(Robust De-anonymization of Large Sparse Datasets). 2008 IEEE 보안 및 개인정보보호 심포지엄(IEEE Symposium on Security and Privacy 2008): 111-125

공개 데이터베이스(IMDB)와 연결시켜 같은 시간대에 같은 영화에 대해 평점을 매긴 사용자들을 찾아냈다. 대부분의 사용자가 1:1 대응관계를 나타냈기 때문에 IMDB 데이터베이스에서 검색한 부가정보를 넷플릭스 데이터세트로 임포트(import)하는 방법으로 익명처리된 것으로 알려진 신원을 모두 확인할 수 있었다.

넷플릭스 개인기록부에서 익명처리된 것은 일반 속성인 점을 강조할 필요가 있다. 즉, '무작위화된' 데이터베이스의 나머지 부분은 잔존 속성의 결합의 희귀성에 따라 여전히 매우 높은 식별처리 능력을 보유한다. 이는 개인정보 처리자가 익명화라는 목표 달성을 위해 무작위화를 선택할 때 항상 유념해야 할 경고이다.

그 후에 이런 형태의 재식별처리 실험에서도 두 데이터베이스를 하나의 하부 공간에 투사하는 유사한 접근법이 시도되었다. 이는 매우 강력한 재식별처리 방법으로 최근 다양한 분야에서 응용되고 있다. 예를 들어, 한 소셜네트워크[25]를 대상으로 수행한 식별처리 실험에서는 꼬리표(label)를 수단으로 하여 가명처리된 사용자들의 소셜 그래프(social graph)가 활용되었다. 이 경우, 두 개인 사이에 주소록이 같을 확률은 매우 낮은 것으로 나타났기 때문에 식별처리에 사용된 속성은 각 사용자의 주소록이었다. 이처럼 직관적인 가정을 바탕으로 숫자가 매우 제한적인 노드의 내부 연결에 대한 하부 그래프는 네트워크에 숨은 데이터 추출을 위한 위상학적인 지문 역할을 하며, 한 번 하부 네트워크가 식별된 후에는 전체 소셜네트워크의 상당한 범위가 식별이 가능한 것으로 나타났다.

유사한 공격 수행과 관련된 수치를 제시하자면, 10개 이하의 노드(매우 다양한 서브네트워크 설정이 가능하며, 각 설정은 위상학적 지문 역할을 하는)만 사용하면 가명처리된 노드 400만 개 및 링크 7천만 개로 이루어진 소셜네트워크가 재식별처리 공격에 쉽게 노출될 수 있으며, 수많은 사람의 프라이버시가 위협받을 수 있는 것으로 나타났다. 이와 같은 재식별처리 접근법은 특정 소셜네트워크 상황에 특화된 것이 아니라 사용자간의 관계가 기록되어 있는(전화번호부, 이메일 연락처, 데이트 장소 등) 다른 데이터베이스에 맞게 개조될 가능성이 있는 일반적인 접근법이란 사실을 강조할 필요가 있다.

익명처리된 것으로 알려진 개인기록부를 식별하는 데는 저자가 사용하는 문체를 기반으로 한 분석방법이 있다(문체분석).[26] 특정 단어 사용 빈도, 문법 패턴 등장,

---

[25] L. Backstrom, C. Dwork, and J. M. Kleinberg. '그대는 왜 r3579x인가?: 익명처리된 소셜네트워크, 은닉 패턴, 구조적 스테가노그라피(Wherefore art thou r3579x?:anonymized social networks, hidden patterns, and structural steganography)', 제16차 국제 월드와이드웹 회의 WWW'07, page 181-190. (2007)

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

구두점 형태 등, 파스 텍스트(parsed text)로부터 지표를 추출하는 알고리즘이 이미 몇 가지 개발되었다. 이런 속성은 모두 익명처리된 것으로 알려진 텍스트와 식별된 저자의 문체를 연결하는 데 사용된다. 연구자들은 10만 개가 넘는 블로그에서 저자의 문체를 복원해 냈으며, 현재 블로그 포스트의 저자를 약 80%의 정확도로 자동 식별할 수 있는데, 텍스트에 나와 있는 위치, 기타 메타데이터 등의 신호를 이용하여 이 기법의 정확도는 더 높아질 것으로 예상된다.

개인기록부의 의미론을 이용한 식별처리 능력(즉, 개인기록부의 무작위화되지 않은 잔존 부분)은 연구계와 기업의 심층적 검토가 필요한 이슈이다. 최근의 DNA 공여자 신원 식별 사건(2013)[27] 에 비추어 볼 때, 사용자 65만 명의 3개월간 키워드 검색 정보 2천만 건이 들어 있는 데이터베이스를 공개한 유명한 AOL 사건(2006) 이후에도 식별처리 능력에 관한 한 별 진전이 없음을 보여주고 있다. 앞서의 AOL 사건은 많은 이용자의 신원과 거주지가 파악되는 결과로 이어진 바 있다.

정보주체의 신원을 제거하거나 일부 속성의 부분적 암호화만으로는 익명처리가 거의 불가능한 또 한 가지 개인정보가 위치정보이다. 사람의 이동성 패턴은 고유성이 높기 때문에 다른 속성은 모르더라도 위치정보의 의미론적 부분만으로(특정 시간에 정보주체가 있었던 장소) 정보주체의 궤적을 노출시킬 수 있다.[28] 이는 대표적인 학문분야의 연구를 통해 여러 차례 증명되었다.[29]

그 점과 관련하여, 신원 또는 속성 누출로부터 정보주체를 보호하기 위한 적절한 방법으로서의 가명 사용은 지양하도록 경고할 필요가 있다. 만약 정보주체의 신원을 다른 고유 코드로 대체하는 방식으로 가명화를 수행했다면, 이로써 안전한 비식별처리가 되었다고 추정하는 것은 순진한 발상이며 식별처리 방법론의 복잡성 및 그러한 방법이 적용되는 다채로운 상황들을 고려하지 않은 처사이다.

---

27 유전자 데이터는 민감한 개인정보를 '익명처리'하는 데 사용될 유일한 메커니즘이 DNA 공여자의 신원을 제거하는 것일 때 재식별처리의 위험이 있음을 보여주는 유의한 예이다. 위 단락 2.2.2에 인용된 예 참조. John Bohannon, '족보 데이터베이스로 익명의 DNA 공여자 신원 확인 가능(Genealogy Databases Enable Naming of Anonymous DNA Donors), Science, Vol. 339, No. 6117 (2013년 1월 18일), p. 262 참조.

28 상기 쟁점은 몇몇 국내법에서 다룬 바 있다. 예를 들어, 프랑스에서는 위치에 대한 통계를 발표할 때 일반화 및 치환을 통해 정보를 익명처리한다. 따라서 프랑스 통계청(INSEE)은 통계자료 발표 시 모든 개인 위치정보를 면적 4만m^2 로 총계처리하여 일반화시킨다. 데이터세트의 단위는 개인정보의 효용을 유지하기에 충분하며, 치환을 통해 스파스 영역에 대한 역익명화(de-anonymisation) 공격을 예방한다. 전체적으로 볼 때, 이러한 개인정보의 총계처리 및 치환은 추론 공격과 역익명화 공격에 대한 보안성을 크게 향상시킨다 (http://www.insee.fr/en/).

29 de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. 크라우드의 고유성: 인간의 이동성과 프라이버시의 한계(Unique in the Crowd: The privacy bounds of human mobility) Nature. 3, 1376 (2013)

A.3. 일반화에 의한 '익명처리'

속성 일반화에 기초한 접근법을 간단한 예를 통해 알아본다.

개인정보 처리자가 간단한 표를 공개하는 경우를 생각해보자. 표에 나타난 정보/속성은 세 가지로, 첫째, 각 개인기록부마다 고유한 식별번호, 둘째, 정보주체와 그가 사는 거주지를 연결하는 위치 ID, 셋째, 정보주체가 가진 속성을 나타내는 속성 ID이다. 이 때 속성 ID는 {P1, P2}로 구분되는 두 개의 값을 갖는다고 가정한다.

식별번호	위치 ID	속성
#1	로마	P1
#2	마드리드	P1
#3	런던	P2
#4	파리	P1
#5	바르셀로나	P1
#6	밀라노	P2
#7	뉴욕	P2
#8	베를린	P1

표 A1. 위치 및 속성 P1, P2로 수집된 정보주체 샘플

어떤 공격자가 밀라노에 거주하는 특정 정보주체(표적)가 표 A1에 들어 있다는 사실을 미리 알고 있다면, 이 표를 조사한 후에 공격자는 밀라노라는 위치 ID를 가진 정보주체는 #6뿐이므로 #6이 속성 P2를 가졌다는 사실도 알 수 있다.

이 기본적인 예는 추정상의 익명처리 과정을 거친 개인정보 세트에 적용된 식별처리 절차의 핵심 요소를 잘 보여준다. 다시 말해, 여기 공격자가 있고, 그는 데이터세트 내 전부 또는 일부 정보주체에 대한 배경지식을 갖고 있다(우연이든 의도적이든). 공격자는 정보주체들의 특정을 정확히 파악하기 위해 이 배경지식을 공개된 데이터세트 내 개인정보와 연결시키고자 한다.

배경지식을 이용한 데이터 연결의 효과 및 적시성을 최소화시키려면, 개인정보 처리자는 위치 ID에 신경을 써서 정보주체가 거주하는 도시를 국가와 같이 좀 더 넓은 구역단위로 대체하면 된다. 그런 방법으로 위 표를 아래와 같이 바꿀 수 있다.

식별번호	위치 ID	속성
#1	이탈리아	P1
#2	스페인	P1
#3	영국	P2
#4	프랑스	P1
#5	스페인	P1
#6	이탈리아	P2
#7	미국	P2
#8	독일	P1

표 A2. 표 A1을 국가별로 일반화한 표

이처럼 개인정보를 총계처리하면, 식별되는 정보주체에 대한 공격자의 배경지식(말하자면, "표적은 로마에 거주하며, 그는 이 표 안에 들어 있다")으로는 표적의 속성에 관해 명백한 결론을 도출하기 어렵다. 표의 이탈리아인 두 사람이 각각 서로 다른 속성 P1과 P2를 갖고 있기 때문이다. 공격자는 표적 개체의 속성에 대해 50%의 불확도를 갖게 된 것이다. 이 간단한 예는 일반화가 익명처리 관행에 미치는 효과를 잘 보여준다. 실제로 이러한 일반화가 이탈리아인 표적을 식별할 확률을 1/2로 줄이는 데는 효과적일지 모르나, 다른 지역 출신의 표적의 경우에는(예: 미국) 효과가 없다.

더욱이 공격자는 여전히 스페인 표적에 관한 정보를 알아낼 수도 있다. 만약 배경지식이 "표적은 마드리드에 거주하며, 그는 이 표 안에 들어 있다", 또는 "표적은 바르셀로나에 거주하며, 그는 이 표 안에 들어 있다"라고 한다면, 공격자는 표적이 속성 P1을 보유하고 있다는 사실을 100% 확신을 갖고 추론이 가능하다. 따라서 일반화는 데이터세트 내 전체 모집단에 대한 추론 공격으로부터 같은 수준의 프라이버시 또는 내성을 보장하지는 않는다.

이런 추리를 바탕으로, 예컨대 대륙별 일반화 등의 방법을 통한 더 강도 높은 일반화가 모든 형태의 연결을 방지하는 데 도움이 되는 것으로 결론지을 수도 있다. 그런 방법으로 위 표를 아래와 같이 바꿀 수 있다.

식별번호	위치 ID	속성
#1	유럽	P1
#2	유럽	P1
#3	유럽	P2
#4	유럽	P1
#5	유럽	P1
#6	유럽	P2
#7	북미	P2
#8	유럽	P1

표 A3. 표 A1을 대륙별로 일반화한 표

이처럼 개인정보를 총계처리하면, 미국에 거주하는 한 사람을 제외하고 표에 들어 있는 모든 정보주체는 연결 및 식별처리 공격으로부터 보호되며, "표적은 마드리드에 거주하며, 그는 이 표 안에 들어 있다", 또는 "표적은 바르셀로나에 거주하며, 그는 이 표 안에 들어 있다"라는 배경지식은 직접적인 연결이 아니라, 주어진 정보주체에 속성을 적용할 수 있는 일정 수준의 가능성(P1일 확률은 71.4%, P2일 확률은 28.6%)으로 귀결될 것이다. 아울러 이러한 추가 일반화는 반대급부로 명백하고 근본적인 정보의 상실을 요구한다. 따라서 정보주체의 위치가 속성 P1과 P2의 모집단 범위 내 절대적 발생 확률(우리의 예에서 각각 62.5%와 37.5%) 및 대륙 내 절대적 발생 확률(마찬가지로 유럽에서 각각 71.4%와 28.6%, 북미에서 100%와 0%), 다시 말해 소위 '한계(marginal)' 분포를 나타낼 뿐이기 때문에, 속성과 위치 사이의 잠재적 상관관계, 즉 특정 위치가 두 속성 중 하나를 밝혀낼 수 있는지 여부를 알 수 없게 만든다.

이 예 또한 일반화 관행이 개인정보의 실질적 효용에 미치는 영향을 잘 보여준다. 오늘날 공개 데이터의 효용을 지나치게 떨어뜨리지 않으면서도 표에 포함된 정보주체의 식별처리 위험을 줄여보고자 적절한 속성 일반화 수준을 사전에 결정하는(즉, 데이터세트를 공개하기 전에) 설계 도구가 몇 가지 나와 있다.

k-익명성

속성 일반화를 기반으로 한 연결 공격을 방지하는 기법이 k-익명성이다. 이 관행의 유래는 미국의 한 의료분야 민간기업이 소위 익명처리된 데이터세트를 일반에 공개하여 1990년대 후반에 수행한 재식별처리 실험이다. 이 익명처리 사례에서는

데이터세트에서 정보주체의 이름은 제거했으나 건강정보를 비롯하여 우편번호 코드(정보주체가 거주하는 위치 ID), 성별, 생년월일 등의 속성은 남겨 두었다.

공개적으로 이용 가능한 명부(예: 유권자 명단)에도 마찬가지로 3대 속성{우편번호 코드, 성별, 생년월일}이 공개되었으므로, 학계의 연구자들은 그 공개된 데이터세트의 속성을 이용하여 특정 정보주체의 신원과 연결시킬 수 있었다. 공격자(연구자)가 가진 배경지식은 다음과 같다. 즉, "나는 유권자 명단에 있는 사람 중에서 3대 속성{우편번호 코드, 성별, 생년월일}이 유일무이한 정보주체를 알고 있다. 공개한 데이터세트에 이 3대 속성을 가진 개인기록부가 존재한다". 이 연구 실험에 사용된 공개 명부에 포함된 대다수(80% 이상) 정보주체는 한결같이 특정 3대 속성과 연관성이 있어 식별이 가능하다는 것이 실증적으로 관찰되었다.[30] 따라서 이 경우는 개인정보가 제대로 익명처리된 것이 아니었다.

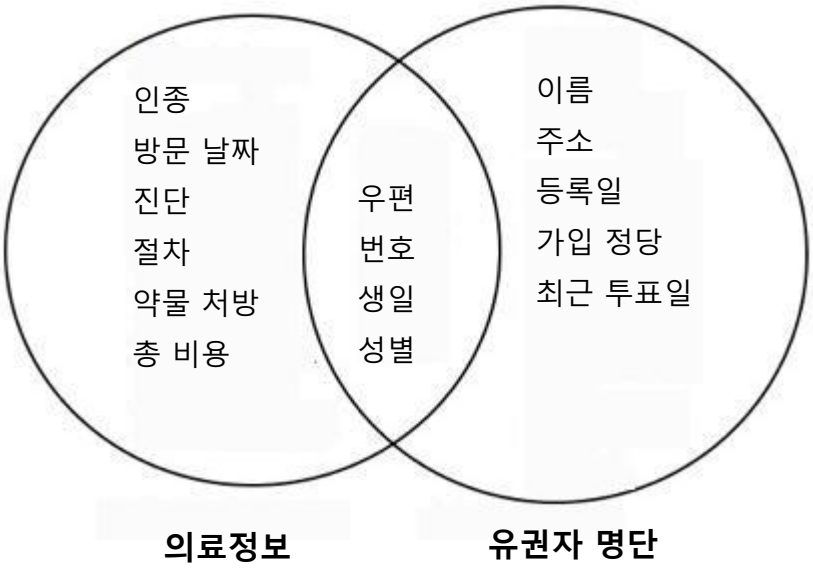

그림 A1. 데이터 연결에 의한 재식별처리

유사한 연결 공격의 효과를 최소화하기 위해서는 개인정보 처리자가 다음과 같은 조치를 취해야 한다는 주장이 제기되어 왔다. 즉, 먼저 데이터세트를 검사한 다음, 공격자가 공개된 표와 기타 보조 정보원을 연결하는 데 합리적으로 사용이 예상되는 속성을 그룹으로 나누는 한편, 각 그룹은 일반화된 동일 속성을 적어도 k개 포함(즉, 각 그룹은 속성의 동질 집합을 표현해야 함)하도록 만든다. 이 때 데이터세트는 그와 같이 동질적인 그룹으로 분할한 후에 공개해야 한다. 연구 문헌에서는 일반화를 위해 선정된 속성을 준식별자라 칭한다. 준식별자를 분명히 알면 정보주체를 즉시 식별할

[30] L. Sweeney. 비밀성 유지를 위한 기술과 정책의 통합(Weaving Technology and Policy Together to Maintain Confidentiality). Journal of Law, Medicine &Ethics, 25, nos. 2&3 (1997):98-110

수 있기 때문이다.

이 밖에도 미흡하게 설계된 k-익명성 표의 약점이 많은 식별처리 실험을 통해 드러났다. 예를 들어 동질 집합 내 여타 속성이 동일하거나(표 A2의 스페인 정보주체의 동질 집합에서 발생한 것처럼), 동질 집합 내 개인기록부 개수가 아주 적어 특정 속성이 크게 확산됨으로 인해 속성간의 분포가 매우 불균형을 이룬다면, 두 경우 모두 가능성 기반 추론을 허용하게 되고, 또한 동질 집합에서 익명처리된 속성 사이에 유의한 '의미론적' 차이가 존재하지 않기 때문에(예: 해당 속성의 정량적 측정은 실제로 다를 수가 있으나 수치적으로는 매우 근접하거나, 또는 예를 들면 동일한 신용위험, 동일한 가족력 등과 같이 의미적으로 유사한 속성의 범위에 속함) 연결 공격으로 인해 데이터세트에서 정보주체의 정보 중 상당 부분이 여전히 누출될 가능성이 있다면 이는 그 표에 약점이 있는 것이다.[31] 여기서 한 가지 중요한 요소를 지적하자면, 데이터 분포가 희박하면 희박할수록(예: 어떤 지리적 영역에서는 특정 속성의 발생건수가 거의 없을 때), 또한 첫 번째 종합처리에서 상이한 속성의 충분한 발생건수로 데이터 분류가 잘 안 되면 안 될수록(예: 극소수 속성의 극소수 발생건수를 여전히 어떤 지리적 영역에 배치할 때) 목표로 하는 익명화를 달성하기 위해서는 추가적인 속성 종합처리가 필요하다.

l-다양성

위와 같은 관찰 끝에 변형된 k-익명성 기법이 최근 수년에 걸쳐 제시되었고, 연결 공격의 위험 최소화를 목표로 일반화에 의한 익명처리 관행을 강화하기 위한 설계 기준이 개발되었다. 이는 데이터세트의 확률론적 속성에 근거한다. 구체적으로 말해, 동질 집합의 각 속성이 적어도 *l*회 등장하도록 더 까다로운 제약을 추가함으로써 공격자는 설사 정보주체에 대한 배경지식이 있다 하더라도 속성에 대해 반드시 유의한 불확도를 떠안게 될 수밖에 없도록 만들었다. 따라서 선정된 하나의 속성은 데이터세트(또는 파티션) 내에서 반드시 최소한의 회수만큼 발생해야 하기 때문에, 이런 요령으로 재식별처리 위험을 낮출 수도 있다. 바로 이것이 l-다양성 익명처리 관행의 목표이다. 이 관행의 예가 표 A4(원자료)와 A5(데이터 가공 결과)에 제시되어 있다. 아래에서 분명히 알 수 있듯이, 표 A4에 포함된 개인의 위치 ID와 나이를

[31] 일단 데이터 개인기록부를 속성별로 분류한 후에는 상관관계도 구축이 가능하다는 점을 강조할 필요가 있다. 개인정보처리자가 자신이 검증을 원하는 상관관계 유형을 알고 있을 때는 가장 연관성이 높은 속성을 선택할 수 있다. 예를 들어, PEW 조사 결과는 정교한 추론 공격에 취약성을 드러내지 않으면서도 인구 집단과 그 관심사 사이의 상관관계를 파악하는 데도 매우 유용하다 (http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx)

적절히 가공함으로써 이 설문조사에서 속성 일반화는 모든 정보주체의 실제 속성에 대한 불확도가 대폭 커지는 결과로 나타난다. 예를 들어, 비록 공격자가 어떤 정보주체는 첫 번째 동질 집합에 속한다는 사실을 알고 있다 하더라도, 해당 집합에(또한 다른 동질 집합에) 그런 속성을 나타내는 개인기록부가 적어도 하나는 존재하기 때문에 공격자는 이 정보주체가 속성 X, Y 또는 Z 중에서 어떤 속성을 가졌는지 더 이상 확인할 수 없다.

일련번호	위치 ID	나이	속성
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

표 A4. 개인을 위치, 나이, 3개 속성(X, Y, Z)별로 분류한 표

일련번호	위치 ID	나이	속성
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

표 A5. 표 A4의 l-다양성 버전의 예

t-근접성:

어떤 파티션 내의 속성이 불균일하게 분포되었거나 좁은 범위의 값 또는 의미론적 의미를 가질 때의 문제를 해결하는 것이 t-근접성이라는 이름으로 알려진 접근법이다. t-근접성 기법은 일반화에 의한 익명처리를 한 단계 더 발전시킨 것으로, 가능한 한 원자료 내에 있는 속성의 초기 분포를 반영한 동질 집합이 되도록 개인정보를 배열하는 방법이다. 다음의 예와 같이 두 단계의 절차를 이용하여 설명할 수 있다. 표 A6은 정보주체가 익명처리된 개인기록부가 수록된 원본 데이터베이스로, 각 개인기록부는 위치, 나이, 급여 및 각각 (X1, X2, X3)와 (Y1, Y2, Y3)라는 의미론적으로 유사한 속성의 두 계열(예: 비슷한 신용위험 등급, 유사 질병)로 분류되어 있다. 먼저 표에서 개인기록부를 의미론적으로 유사한 동질 집합 및 미흡한 익명처리 타겟으로 분류하여 *l*=1로 *l-다양성* 기법을 적용했다(표 A7). 다음으로 t-근접성을 얻고 각 파티션 내 가변성을 높이기 위해 이 표를 가공하였다(표 A8). 실은 두 번째 단계에서 각 동질 집합은 두 속성 계열의 개인기록부를 모두 포함한다. 각 가공 단계별로 위치 ID와 나이의 단위가 다른 점을 주목할 필요가 있다. 이는 목표로 하는 익명처리를 위해서는 각 속성이 서로 다른 일반화처리 기준이 요구되며, 결국은 개인정보 처리자의 구체적 설계 능력 및 적당한 계산상의 부담이 요구된다는 의미이다.

일련번호	위치 ID	나이	급여	속성
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

표 A6. 위치, 나이, 급여 및 두 속성 계열로 분류된 개인에 대한 표

일련번호	위치 ID	나이	급여	속성
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

표 A7. 표 A6의 l-다양성 버전

일련번호	위치 ID	나이	급여	속성
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

표 A8. 표 A6의 t-근접성 버전

이런 기법에 따라 정보주체의 속성을 일반화하는 목표는 전부가 아닌 몇 개의 개인기록부만으로 달성 가능한 수가 많다. 각 동질 집합에 많은 숫자의 개인이 포함됨으로써 일체 추론 공격이 불가능하도록 모범적인 관행이 수립되어야 한다. 어떤 경우든 이 접근법을 채택하려면 개인정보 처리자는 여러 대안의 조합 가능성을 검토함과 동시에(예를 들어, 다양한 진폭 범위, 다양한 위치 또는 나이 단위 등) 가용 데이터에 대한 심층적인 평가가 선행되어야 한다. 다시 말해, 일반화에 의한 익명처리란 결코 개인기록부 내 범위별 속성 분석값을 대체한다는 명목으로 우선 개략적으로 시도한다고 해서 얻어지는 결과물이 아니라, 예컨대 각 파티션 내 속성 엔트로피의 평가, 원본의 속성 분포와 각 동질 집합 내 분포간의 거리 측정과 같은 보다 더 구체적이고 정량적인 접근법을 필요로 하기 때문이다.