법학석사학위논문

개인정보의 개념에 관한 연구

식별가능성에 관한 유럽 및 일본의 논의를 중심으로

2017년 2월

서울대학교 대학원

법 학 과

채 성 희

개인정보의 개념에 관한 연구

식별가능성에 관한 유럽 및 일본의 논의를 중심으로

지도교수 정 상 조

이 논문을 석사 학위논문으로 제출함.

2016년 11월

서울대학교 대학원

법 학 과

채 성 희

채성희의 석사 학위논문을 인준함.

2016년 12월

위 원 장 _____ (인)

부위원장 _____ (인)

위 원 _____ (인)

국문초록

개인정보의 개념에 관한 연구

식별가능성에 관한 유럽 및 일본의 논의를 중심으로

개인정보보호법 등 개인정보 보호 관련 법률의 가장 핵심적인 개념은 '개인정보'이다. 개인정보는 "살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다"로 정의된다. 현실에서 어떤 정보가 개인정보인지 확정하는 것은 매우 어려운 문제이다. 우리나라에서는 이 문제에 관하여 확립된 판례가 존재하지 않고, 학설 또한 분분하나 깊이 있는 이론적 접근은 발견되지 아니한다.

이에 본고에서는 개인정보 개념 특히 '식별가능성' 개념을 중심으로, 개인정보 보호법제가 정비되어 있는 유럽연합 특히 독일 및 영국과, 일본의 법제를 참고하여 검토하였다. 구체적으로, '식별가능성' 개념을 이를 처리하는 주체에 따라 상대적으로 판단할 것인지 여부와, 개인정보처리자가 자신에게는 개인정보인 어떤 정보를, 정보 자체로 개인식별이 어려운 형태로 가공하여 제공하는 경우 그러한 정보가 개인정보의 제공에 해당하는지 여부가 이 논문의 핵심 주제이다.

비교법적으로, 전자의 쟁점에 관하여 유럽연합, 독일, 영국, 일본 모두 개인정보 개념은 이를 처리하는 주체에 따라 상대적으로 판단되어야 하는 입장이 우세한 것으로 보인다. 후자의 쟁점에 관하여는, 유럽연합의 경우 개별 회원국 간에 통일된 견해가 존재하지 아니하는 것으로 보이나, 적어도 제29조 작업반(Article 29 Working Party)은 개인정보의 제공을 인정하여야 한다는 입장인 것으로 보이고, 일본 또한 비슷한 태도이다. 그러나 영국은 이와 반대로 개인정보의 제공을 부정한다.

우리나라의 경우, 전자의 쟁점에 대해서는 대체로 상대설이 우선하는 것으로 보인다. 후자의 쟁점에 관하여 학설 및 정부의 태도에서는 영국의 경우와 유사하게 해석하려는 경향이 감지되나, 이는 현행법의 해석상 적절치 않다. 필자의 견해로는, 개인정보보호법 하에서 개인정보 개념은

그 처리자를 기준으로 상대적으로 해석하여야 하며, 제공행위의 맥락에서 굳이 제공받는 자의 입장을 고려할 필요가 없다는 해석이 타당하다. 만일 정보주체의 동의 등 제17조 제1항 각호가 규정하는 법률적 근거 없이 개인정보를 제공하고 싶다면, 개인정보보호법 제18조 제2항 각호의 요건을 갖추어야 한다. 특히 '개인을 알아볼 수 없도록' 하는 처리 즉 비식별처리를 하는 경우라면 통계 목적 또는 학술적 목적이 있는 경우에 한하여 제18조 제2항 제4호에 의하여 제공을 정당화할 수 있을 것이다.

주요어: 개인정보 개념, 식별가능성, 익명화, 비식별화, 개인정보보호법, 유럽연합, 독일, 영국, 일본

학 번:2013-23342

목 차

I. 서론

1. 문제의 제기

개인정보는 정보화사회에서 매우 중요한 경제적 자원으로, “정보화 사회의 원유”[1]라고도 불린다. 그러나 무분별한 활용이 이루어질 경우 개인의 권리와 이익이 침해될 것이 우려된다. 그러므로 개인정보의 활용과 개인의 권익보호의 조화가 무엇보다도 중요하다.

우리나라는 개인정보보호법, 정보통신망의 이용촉진 및 정보보호 등에 관한 법률(이하 ‘정보통신망법’), 신용정보의 이용 및 보호에 관한 법률(이하 ‘신용정보법’) 등 개인정보 보호에 관한 여러 가지 법률들이 있다. 어떤 정보가 이들 법률상의 보호규범의 적용을 받기 위하여서는 ‘개인정보’에 해당하여야 하므로, ‘개인정보’는 이 법률들의 가장 핵심적인 개념이다.

개인정보보호법 제2조 제1호는 개인정보 개념에 관하여, “살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다”고 정의하고 있으며, 정보통신망법 제2조 제1호 제6호도 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다”고 함으로써

[1] Meglena Kuneva, Keynote Speech in Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 2009. (2016. 10. 9. 방문) <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>

거의 동일한 개념을 채택하고 있다.

문제는 어떤 정보가 이러한 '개인정보'에 해당하는지를, 현실에서 쉽게 구별할 수 없다는 데에 있다. 예컨대 유동 IP주소, 단말기 ID(IMEI, MAC Address 등), 앱 ID, 쿠키 정보 같은 것은 개인정보인가? 암호화가 되어 나는 (복호화 또는 내가 보유하고 있는 다른 정보와의 대조를 통하여) 문제의 개인을 알아볼 수 있으나 다른 사람은 알아볼 수 없는 정보는 그 다른 사람의 손에서 개인정보인가? 이러한 질문들에 대한 명확한 답이 아직 존재하지 않는 것은 물론, 구체적인 사안에서 무엇이 개인정보인지 판단하는 것은 쉽지 않으며, 여기에 대한 확립된 판단 기준조차 존재하지 않는 실정이다.

이에 본고는 개인정보 개념에 관한 국내외 법령 및 해석론을 비교법적으로 검토해 보고, 이를 바탕으로 개인정보 개념에 대한 목적론적·체계적 해석을 시도하는 것을 목표로 한다. 특히, 개인정보 개념의 성립 요소 중 가장 많은 논쟁을 불러일으키는 '식별가능성' 개념을 중심으로, 개인정보 보호법제가 정비되어 있는 유럽연합 특히 독일 및 영국과, 일부 논자들이 개인정보 개념에 대한 완화된 해석의 근거로 즐겨 인용하는 일본의 법제를 참고하기로 한다. 한편, 국내 법령 중에서는, 개인정보 보호에 관한 여러 법률 중 일반법인 개인정보보호법을 중심으로 검토하기로 하고, 필요한 범위 하에서 정보통신망법을 언급하기로 한다. 신용정보법 또한 개인정보보호법제에서 매우 중요한 위치를 차지하고 있으나, 신용정보의 보호 못지 않게 그 이용에 비중을 두고 있다는 특수성이 있으므로, 본고에서는 직접적으로 논의하지 않기로 한다.

2. 논문의 구성

본고에서는 먼저 우리나라에서 개인정보 개념을 둘러싼 논의 현황을 검토해 보기로 한다. 이러한 검토에 있어, 개인정보자기결정권에 관하여도 간단히 살펴본다. 개인정보자기결정권은 개인정보보호법의 이념적 기초로서, 개인정보 개념의 해석에 있어 지도원리가 되어야 하기 때문이다.

다음으로, 유럽의 개인정보 개념에 관하여 검토한다. 먼저, 유럽연합 개인정보보호지침상 개인정보 개념에 관하여 본다. 동 지침은 우리나라 개인정보보호법에 상당한 영향을 미친 것으로 알려져 있을 뿐 아니라[2], 실제로 우리나라 실무에서도 동 지침 및 동 지침과 관련한 유럽사법재판소의 판결, 유럽 규제기관의 해석은 개인정보보호법의 해석과 관련하여 자주 원용되고 있기 때문이다.

그런데 유럽연합 개인정보보호지침은 어디까지나 지침(Directive)으로, 그 내용은 각국의 실제 입법에 의하여 현실적·구체적으로 규정된다. 따라서 유럽연합 각 회원국들의 실제 규정을 살펴 보는 것이 필수적이다. 본고에서는 (아마도 언어상의 이유로) 우리나라에서 가장 많이 인용되는 영국법과 함께, 우리와 법체계와 법학방법론이 상당 부분 유사한 독일법상의 논의들을 검토해 보기로 한다. 특히 독일에서는 유동 IP주소의 개인정보성 여부와 관련하여 개인정보 개념에 관한 풍부한 논의가 존재하는바, 우리법의 해석에도 상당히 참고가 될 수 있을 것으로 생각된다.

일본법상 논의도 검토할 가치가 있다. 일본의 개인정보 개념도 기본적으로 우리와 유사하다. 그러나 일본 개인정보보호법은 유럽이나 우리나라와는 달리, 민간부문과 공공부문의 개인정보

[2] 박준석, “저작재산권법에서 바라본 개인정보 보호”, 개인정보보호의 법과 정책, 박영사, 2014, 114면

보호에 관하여 별개의 규정을 두고 있고, 실제로 이 점이 개인정보 개념의 해석에도 영향을 미치고 있으므로 일본의 개인정보 개념을 우리 법의 해석에 도입할 때에는 주의할 필요가 있다. 한편 일본은 최근 개인정보보호법의 개정을 통하여 개인정보 개념의 명확화와 함께 '익명가공정보'라는, 개인정보와 개인정보 아닌 정보 사이의 중간적 개념을 도입함으로써 정보의 보호와 활용이라는 두 가지 가치를 조화하려는 시도를 하고 있고, 그 과정에서 다양한 논의가 이루어지고 있다. 이것이 우리법의 해석에 어떠한 시사점을 줄 수 있는지 정확히 검토하는 것 또한 의미가 있을 것이다.

마지막으로, 이러한 검토 내용을 바탕으로, 개인정보 개념에 대한 필자 나름의 해석론을 전개해 보고자 한다.

II. 개인정보 개념에 관한 우리나라에서의 논의 현황

1. 개요

아직 개인정보 개념에 관한 판례나 실무례가 충분히 축적되어 있지 않은 것이 우리나라의 현실이다. 그러나 학설을 통하여 어느 정도 다양한 논의가 이루어지고 있으므로, 이를 통하여 살펴보기로 한다. 먼저, 개인정보 개념에 관한 논의의 전제가 되는, 개인정보 자기결정권의 내용에 관하여 간략히 살펴 본다.

2. 개인정보 자기결정권과 개인정보보호법

가. 개인정보보호법의 헌법적 근거로서의 개인정보자기결정권

현행 개인정보보호법 제1조는 "이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다"고 규정하고 있고, 구 개인정보보호법(2014. 3. 24. 법률 제12504호로 개정되기 이전의 것) 제1조는 "이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다"고 규정하고 있다. 여기서의 '개인의 자유와 권리' 및 '사생활의 자유 등'에는 개인의 여러 가지 인격적·재산적 이익이 광범위하게 포함될 수 있겠지만, 개인정보 자기결정권의 보호가 가장 중요한 헌법상 근거라는 점은 판례 및 학설의 거의 일치된 입장인 것으로 보인다[34].

---

[3] 헌법재판소 2005. 5. 26. 선고 99헌마513 결정; 헌법재판소 2005. 7. 21. 선고 2003헌마282 결정; 대법원 1998. 7. 24. 선고 96다42789 판결; 대법원 2001. 9. 2. 선고 2008다42430 판결 등. 성낙인, 헌법학(제15판), 법문사, 2015,

이러한 개인정보 자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 통제하고 결정할 수 있는 권리로 정의된다[5]. 정보통신기술의 발달로 인하여 국가가 개인의 정보를 수집하고 처리할 능력이 증대됨에 따라 개인의 사생활 침해의 위험이 증가하고, 아울러 감시에 대한 두려움으로 인하여 개인의 결정의 자유가 침해당하며, 나아가 자유민주체제의 근간이 흔들리는 것을 방지하기 위하여 인정되는 권리라고 한다[6].

1228면; 권건보, 개인정보보호와 자기정보통제권, 서울대 법학연구총서 3, 경인문화사, 2006, 94면 이하; 권건보, "개인정보보호의 헌법적 기초와 과제", 저스티스 통권 제144호, 2014, 7면 이하; 한편, 김진환, "개인정보보호의 규범적 의의와 한계-사법 영역에서의 두 가지 주요 쟁점을 중심으로", 저스티스 통권 제144호, 2014, 43면 이하는 개인정보보호를 통하여 달성하고자 하는 "법익"이 개인정보자기결정권 뿐만이 아니며, 사생활의 자유나 재산권적 측면도 고려하여야 한다고 주장하고 있으나, 이는 개인정보보호법의 위반이 있더라도 바로 정보주체의 인격권, 재산권 등 구체적인 사적 법익이 침해되는 것은 아니라는 취지이고, 절차적, 형식적 위험규제를 목적으로 한 정보자기결정권이 개인정보보호법의 각종 예방적 규정들의 근거가 되고 있다는 점은 긍정하고 있는바, 개인정보보호법의 헌법적 근거 내지 1차적 보호법익이 정보자기결정권의 보호라는 점 자체를 부정하는 것은 아니라고 생각된다.

[4] 학설 중에서는 '자기정보통제권'이라는 용어를 사용하는 견해도 있다. 권건보(주3, 2006) 88~93면에 따르면 '자기정보통제권'이 '정보자기결정권'보다 한 단계 더 진전하여 개인의 정보에 대한 적극적 통제권이라는 측면을 부각시킬 수 있으므로 이러한 용어의 사용이 바람직하다고 한다. 그러나 이러한 견해에 따르더라도 개인정보 자기결정권과 자기정보통제권 사이에 내용상 차이는 크지 않다고 하므로(같은 책 92면), 본고에서는 헌법재판소와 대법원이 사용하는 '개인정보 자기결정권'이라는 용어를 사용하기로 한다.

[5] 헌법재판소 2005. 5. 26. 선고 99헌마513 결정; 성낙인(주3), 1227면

[6] 성낙인(주3), 1227면; 권건보(주3, 2006)94~96면; 권건보(주3, 2014), 12~14면

나. 개인정보 자기결정권의 헌법적 근거

개인정보 자기결정권의 헌법적 근거에 관하여는 헌법 제10조설[7], 헌법 제17조설[8], 헌법 제10조 및 국민주권과 민주주의 원리설[9] 등 학설이 대립하고 있다. 그러나 최근 헌법학계의 논의에서는 이러한 다툼이 크게 부각되지 않는 듯 하며, 이러한 차이가 실제에 있어 어떠한 다른 결과를 가져올 수 있는지에 관하여 언급한 문헌도 없는 것으로 보인다[10].

헌법재판소는 주민등록법 제17조의8등 위헌확인 등 사건에서 "개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권주의와 민주주의 원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고

---

[7] 정태호, "현행 인구주택총조사의 위헌성-독일의 인구조사판결(BVerGE65, 1)의 법리분석과 우리의 관련법제에 대한 반성-", 법률행정논총 제12집, 2000

[8] 성낙인(주3), 1229면; 권건보(주3, 2006), 113~115면

[9] 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론", 인터넷 법률 제4호, 2001, 43면 이하; 이창민, 개인정보자기결정권 연구-개인정보처리의 자유와의 충돌 해결을 중심으로-, 서울대학교 법학석사논문, 2009, 16면에서 재인용.

[10] 김철수, 헌법학신론(제21전정신판), 박영사, 2013, 716~722면; 허영, 한국헌법론(전정10판), 박영사(2014), pp.405~406; 정종섭, 헌법과 기본권, 박영사, 2010 등. 특히 김철수는 한때 제10조설을 주장하였으나(권건보(주3, 2006), 100면 참고), 현재는 이러한 견해를 주장하고 있지 않은 것으로 보인다.

보아야 할 것이다"라고 함으로써 헌법에 명시되지 않은 독자적 기본권설을 취하였으나[11] 이후 교육행정정보시스템과 관련한 개인정보수집 등 위헌확인 사건에서 "헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장"되는 권리라고 판시하였다[12].

대법원 또한 1998. 7. 24. 선고 96다42789 판결에서 구 국군보안사령부가 법령에 규정된 직무범위를 벗어나 민간인들을 대상으로 평소의 동향을 감시·파악할 목적으로 지속적으로 개인의 집회·결사에 관한 활동이나 사생활에 관한 정보를 미행, 망원 활용, 탐문채집 등의 방법으로 비밀리에 수집·관리한 사안에서, 헌법 제10조의 행복추구권과 제17조의 사생활의 비밀과 자유 규정을 근거로 "개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리" 즉 개인정보자기결정권의 존재를 도출한 바 있다. 이후에도 대법원은, 변호사 정보 제공 웹사이트 운영자가 변호사들의 개인신상정보를 기반으로 변호사들의 '인맥지수'를 산출하여 공개한 사안에서 인격권 침해 여부를 검토하면서[13], 위 96다42789 판결을 인용한 바 있다[14].

---

[11] 헌법재판소 2005. 5. 26. 선고 99헌마513·2004헌마190 결정

[12] 헌법재판소 2005. 7. 21. 선고 2003헌마282 결정; 헌법재판소 2014. 8. 28. 선고 2011헌마28 등 결정.

[13] 대법원 2011. 9. 2. 선고 2008다42430 판결

[14] 채성희, "검색엔진에 대한 자기정보삭제권 행사의 범위와 한계-유럽사법재판소의 이른바 '잊혀질 권리' 판결을 중심으로", LAW & TECHNOLOGY 제10권 제4호, 2014, 58~81면

다. 개인정보 자기결정권이 적용되는 정보

개인정보 자기결정권은 개인정보의 수집이나 활용으로 인한 각종 위험으로부터 개인을 보호하기 위하여 인정되는 권리이다. 그렇다면 그 수집 또는 활용으로 인하여 개인에게 위험이 발생할 수 있는 정보와 관련하여서만 인정된다고 보아야 한다. 그러므로 모든 정보에 대하여 인정되는 것이 아니고, 개인의 동일성을 식별할 수 있게 하는 정보에 한하여 관련성을 가진다고 본다[15]. 개인의 동일성을 식별할 수 없는 정보라면 개인의 사생활 보호, 행복추구권의 보호 등에 저촉될 여지가 없기 때문에 이는 당연한 것이라 생각된다. 개인의 동일성을 식별할 수 있게 하는 정보는, 반드시 그 정보 자체만으로 특정 개인을 식별할 수 있는 것에 국한되지 아니하고, 다른 정보와 쉽게 결합하여 당해 개인을 식별할 수 있는 정보까지도 포함한다. 헌법재판소는 여기에 따라, 그 자체로는 개인의 신원 확인이 불가능한 정보인, 디엔에이신원확인정보의 이용 및 보호에 관한 법률상의 디엔에이신원확인정보도 개인정보에 해당한다고 판시한 바 있다[16]. 여기에 따르면, 헌법상 개인정보 정보자기결정권과 개인정보 개념은 서로 일치하는 것으로 판단된다[17].

한편 보호의 대상이 되는 개인정보는 반드시 개인의 내밀한 영역이나 사사의 영역에 속하는 것 뿐 아니라 공적 생활에서

---

[15] 권건보(주3, 2014), 16면

[16] 헌법재판소 2014. 8. 28. 선고 2011헌마28등 결정

[17] 여기에 대하여, 개인정보보호법상 개인정보 개념과 개인정보자기결정권에서 문제되는 개인정보 개념이 그 자체로 개인식별이 불가능하지만 다른 정보와 결합하여 개인을 식별하게 하는 정보를 포함하는지 여부의 문제에 있어 서로 다르다고 하는 견해가 있다. 백윤철 · 김상겸 · 이준복, 인터넷과 개인정보보호법, 한국학술정보(주), 2012, 115면. 그러나 이는 특별한 근거가 없을 뿐 아니라, 헌법재판소의 위와 같은 명시적 판시에도 반하는 것이다.

형성되었거나 이미 공개된 것까지 포함된다[18]. 이로써 개인정보 자기결정권의 보호 영역이 '홀로 있을 권리(the right to be left alone)'라는 전통적인 프라이버시권의 영역을 초월한다는 점을 알 수 있다[19].

그러나 모든 정보를 동일한 정도로 보호하여야 하는 것은 아니다. 최근 헌법재판소는 "일반적으로 볼 때, 종교적 신조, 육체적·정신적 결함, 성생활에 대한 정보와 같이 인간의 존엄성이나 인격의 내적 핵심, 내밀한 사적 영역에 근접하는 민감한 개인정보들에 대하여는 그 제한의 허용성이 엄격히 검증되어야 할 것이다. 반면, 성명, 직명과 같이 인간이 공동체에서 어울려 살아가는 한 다른 사람들과의 사이에서 식별되고 전달되는 것이 필요한 기초정보들은 사회생활 영역에서 노출되는 것이 자연스러운 정보이고, 국가가 그 기능을 제대로 수행하기 위해서 일정 부분 축적·이용하지 않을 수 없는 정보이다. 이러한 정보들은 다른 위험스런 정보에 접근하기 위한 식별자 역할을 하거나, 다른 개인정보들과 결합함으로써 개인의 전체적·부분적 인격상을 추출해 내는 데 사용되지 않는 한 그 자체로 언제나 엄격한 보호의 대상이 된다고 하기 어렵다"고 판시함으로써, '내밀한 영역이나 사사의 영역'에 관한 개인정보와 '기초정보' 및 '공개된 정보'는 보호의 정도가 달라질 수 있다는 판시를 한 바 있다[20].

---

[18] 헌법재판소 2005. 5. 26. 선고 99헌마513·2004헌마190 결정

[19] 이와 달리, 박경신, "사생활의 비밀의 절차적 보호규범으로서의 개인정보보호법리", 공법연구 제40집 제1호, 한국공법학회, 2011는 개인정보보호법의 보호법익은 전통적 의미의 프라이버시권, 특히 그 중에서도 프롯서(Prosser)가 제안한 프라이버시 4유형 중 제개인이 비밀로 하고 싶어하는 사적 사실의 공표 및 사적인 공간에의 침입에 국한하므로, 개인정보보호법의 보호 범위 또한 프라이버시권 침해의 우려가 있는 정보로 한정되어야 한다고 주장한다. 그러나 이와 같이 보아야 하는 근거가 분명하지는 않다.

[20] 헌법재판소 2014. 8. 28. 선고 2011헌마28등 결정

라. 개인정보 자기결정권의 내용

앞서 살펴본 바와 같이 개인정보 자기결정권은 '언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 통제하고 결정할 수 있는 권리'이다. 그러므로 정보주체가 자신에 관한 정보의 수집, 이용, 제3자에 대한 제공 등 처리에 관하여 동의할 권리, 이를 철회할 권리, 정보에 대한 열람·정정·삭제·처리정지 등을 요구할 권리가 여기에 포함된다[21]. 따라서 국가가 개인정보를 조사·수집·보관·처리·이용하는 행위는 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다[22].

마. 개인정보자기결정권에 대한 제한

개인정보자기결정권 또한 절대적 권리가 아니므로 제한 가능하다. 일반적인 다른 권리들과 마찬가지로, 법률유보원칙, 명확성의 원칙, 비례원칙에 의한 제한이 가능하다[23].

헌법재판소는 헌법재판소 2005. 5. 26. 선고 99헌마513•2004헌마190 결정에서 "기본권은 헌법 제37조 제2항에 의하여 국가안전보장•질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 이를 제한할 수 있으나, 그 제한의 방법은 원칙적으로 법률로써만 가능하고 제한의 정도도 기본권의 본질적 내용을 침해할 수 없고 필요한 최소한도에 그쳐야 한다"는 법리를 개인정보자기결정권의 제한에도 그대로 적용하였다.

또한, 헌법재판소에 따르면 개인정보자기결정권의 제한은 명확성의 원칙에 따라야 하며, 그 정도는 "개인정보의 종류와 성격,

[21] 권건보(주3, 2014), 17~19면; 김진환(주3), 이창민(주9), 29~32면

[22] 헌법재판소 2005. 7. 21. 선고 2003헌마282 결정 등

[23] 헌법재판소 2005. 5. 26. 선고 99헌마513 결정 등

정보처리의 방식과 내용 등에 따라" 달라지며, "일반적으로 볼 때 개인의 인격에 밀접히 연관된 민감한 정보일수록 규범명확성의 요청은 더 강해진다"고 한다[24].

3. 개인정보 개념에 관한 해석론

가. 일반론

개인정보보호법 제2조 제1호는 개인정보 개념을 "살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)"이라고 정의하고 있고, 정보통신망법 제2조 제1항 제6호는 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다"고 함으로써 개인정보보호법과 동일하게 정의하고 있다.

이러한 개인정보의 개념 요소는 일반적으로 1)정보의 임의성, 2)살아있는 개인, 3)특정 개인과의 관련성, 4)식별가능성으로 분설된다[25]. 이 중 '정보의 임의성'은 정보의 종류와 형식에 제한이 없음을 나타내는 개념이므로[26], 보다 정확히는 '정보일 것'이 개념을 구성하는 요건이고, '정보의 임의성' 즉 '정보이기만 하면 그 종류와 형식에는 제한이 없다'는 것은

---

[24] 헌법재판소 2005. 7. 21.자 2003헌마282·425(병합) 결정

[25] 이창범, 개인정보보호법, 법문사, 2012, 15면. 그 외 다수의 문헌들이 동일한 용어를 사용하여 개인정보의 해당 요건을 설명하고 있다.

[26] 이창범(주25), 15면

‘정보’라는 요건을 설명하는 하나의 명제로 취급함이 상당하다 생각된다. 이렇게 볼 때 ‘정보’ 요건과 ‘살아 있는 개인’은 그 의미가 비교적 분명하여 다툼이 발생할 여지는 많지 않아 보인다.

다음으로, 관련성 요건에 대하여 살펴보면, 방송통신위원회는 “현행 정보통신망법은 개인정보에 관한 구체적이고 세부적인 기준이나 요건을 규정하고 있지 않으므로 특정 개인과 관련된 모든 정보는 개인정보에 해당된다”는 입장[27]으로 관련성에 관하여 큰 의미를 부여하고 있지 않다. 학설 또한 유럽연합 규제기관의 일반론을 답습하여 정보의 내용, 처리목적, 정보의 처리 결과 중 하나가 개인과 관련되면 관련성을 인정한다고 보는 데 그치고 있고[28], 그 결과 “매우 광의로 해석되고 있기 때문에 강학상, 이론상의 논의에 불과한 면이 적지 않아 현실적인 구분 표지로서의 역할을 수행하기에는 뚜렷한 한계를 지닌다”[29]는 주장에서도 볼 수 있듯이 관련성 요건에는 그다지 큰 의미를 두지 않는 것이 일반적인 태도인 것으로 보인다. 뒤에서 살펴보게 될 것이지만, 유럽연합과 영국에서 관련성 의미에 관한 실제적인 논의가 비교적 활발하게 진행되고 있는 것과는 대조되는 상황이라 할 수 있다. 다만, 국내의 일부 학설은 개인정보 개념을 무제한적으로 확장시켜서는 안되고 일정한 범위에서의 제한이 필요하다는 전제 하에, 영국의 판례를 원용하며, 관련성을 인정하기 위해서는 개인에 ‘관한’ 정보를 표시하고 있는 것만으로는 충분하지 않고, 특정 개인과 직접 ‘관련한’ 것이어야 한다고 주장하고 있으나[30],

---

[27] 방송통신위원회·한국인터넷진흥원, 정보통신서비스 제공자를 위한 개인정보보호 가이드, 2012, 5면

[28] 이창범(주25), 18면

[29] 김진환, “개인정보 보호법의 해석 원칙을 위한 제언과 시론:개인정보에 대한 정의 규정의 해석을 중심으로”, 법학평론 제3권, 2012, 18면; 同旨, 주민철, 개인정보보호조치 위반의 형사적 책임, 서울대학교 석사학위논문, 2015, 20면

[30] 윤주희 등, 개인정보보호위원회, 개인정보의 범위에 관한 연구, 2014; 同旨, 박유

‘관한’ 것과 ‘직접 관련한’ 것의 차이가 무엇인지 주장 내용이 불분명할 뿐 아니라 인용된 영국 판례[31]의 취지와도 맞지 않는 것으로 보인다.

나. 식별가능성 개념

개인정보의 성립요건 중 국내에서 가장 중요하게 취급되고 있으며, 대부분의 논의가 집중되는 부분은 식별가능성 개념이라 할 수 있다. 이하에서 규제기관, 학설, 판례의 태도를 중심으로 우리나라에서의 식별가능성 논의에 관하여 살펴 보도록 한다.

(1) 정부의 입장

행정자치부는 식별가능성의 ‘식별’이란 특정 개인을 다른 사람과 구분하거나 구별할 수 있다는 것을 의미한다고 보고 있다[32]. 식별가능성이란 이러한 구분 및 구별의 가능성인데, 반드시 문제의 정보 자체로 식별이 가능할 필요는 없고, 개인정보보호법 제2조 제1호의 취지상 그 정보와 다른 정보가 쉽게 결합하여 식별 가능하게 되는 경우 그 정보에 대하여도 식별가능성을 인정할 수 있다[33]. 여기서의 ‘쉽게’ 결합할 수 있다는 것은 ‘합리적으로’ 결합 가능하다는 것을 의미하는데, 합리적 결합 가능성을 인정하기 위해서는 물리적·과학적 결합가능성이 존재하는 것만으로는 불충분하고, 합리적인 시간, 노력, 비용으로 결합할 수 있는 수단과 방법까지 존재하여야 한다고 한다[34].

영, 개인정보 보호범위에 관한 헌법적 연구-민간부문에서의 개인정보 보호범위를 중심으로, 서울대학교 법학석사학위논문, 2015, 54~55면

[31] Michael John Durant v. Financial Service Authority [2003] EWCA Civ 1946

[32] 행정안전부, 개인정보 보호법령 및 지침·고시 해설, 2011, 8면

[33] 행정안전부, 전게서, 8면

[34] 행정안전부, 전게서, 9면

방송통신위원회 및 한국인터넷진흥원이 발간한 해설서 등에서는 위와 같이 식별, 식별가능성 그리고 식별가능성의 판단 기준 중 하나인 '쉽게 결합하여'의 의미에 관하여 명확한 일반론을 제시한 것은 보이지 아니한다. 그러나 '위치정보의 보호 및 이용 등에 관한 법률 해설서'에서, 위치정보의 보호 및 이용 등에 관한 법률(이하 '위치정보법') 제2조 제2호의 '개인위치정보'의 구성요건인 '용이하게 결합하여'의 의미에 관하여, "결합할 수 있는 정보들이 반드시 하나의 DB 또는 시스템에 함께 있어야 함을 의미하지 않는다. 회사 내의 여러 DB로 분산되어 있거나 제휴회사에서 별도로 보유하고 있더라도 위치정보 관련 서비스를 제공하기 위해 상호 결합될 가능성이 많은 경우도 포함한다"고 서술한 것이 발견된다[35]. 위치정보법상 개인위치정보는 개인정보보호법과 정보통신망법상 개인정보에 대응하는 개념이고, 여기서의 '용이하게 결합하여'는 '쉽게 결합하여'와 거의 유사한 개념이므로, '용이하게 결합하여'에 대한 위 서술은 '쉽게 결합하여'에 대한 방송통신위원회의 이해를 반영하고 있었다고 읽어도 무방할 것이다.

한편, 2016. 6. 30. 행정자치부와 방송통신위원회를 비롯한 개인정보보호 유관 정부부처들은 합동으로[36] "개인정보 비식별조치 가이드라인"[37](이하 '비식별조치 가이드라인')을 발표하고, 그 부록으로 "-개인정보의 범위 명확화 및 비식별 정보의 안전한 활용을 위한- 개인정보 보호 관련 법령 통합 해설서"를 발간하였다. 이 '해설서'에 따르면, 개인을 식별할 수 있다는

---

[35] 방송통신위원회·한국인터넷진흥원, 위치정보의 보호 및 이용 등에 관한 법률 해설서, 2010, 21면

[36] 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부, 국무조정실

[37] 행정자치부 등, 개인정보 비식별 조치 가이드라인 - 비식별 조치 기준 및 지원·관리체계 안내-, 2016

것은 “해당 정보를 ‘처리하는 자’ 및 ‘제공 등에 따라 향후 처리가 예정된 자’의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다”는 것을 의미한다. 그리고 어떤 정보가 그 자체로는 개인을 알아볼 수 없으나 다른 추가적 정보와 ‘쉽게 결합하여’ 개인을 알아볼 수 있는 경우, ‘쉽게 결합’의 의미에 관하여, ‘쉽게 결합’이란 추가적 정보의 입수가능성 및 추가적 정보와 보유 정보의 결합 가능성을 의미한다고 전제한 후, ‘입수가능성’은 합법적인 방법의 정보 입수만을 의미하고, ‘결합 가능성’은 현재의 기술 수준에 비추어 결합이 가능한 경우와 결합하는 데 비합리적인 수준의 비용이나 노력이 수반되지 않는 경우를 말한다는 취지로 해석하고 있다[38].

(2) 판례

식별가능성 개념에 대하여 명시적으로 판결한 판례 중 확정된 것으로는 하급심 판결인 이른바 ‘증권통 사건’과 ‘전화번호 뒷 4자리 사건’이 있다.

(가) 증권통 사건(서울중앙지방법원 2011. 2. 23. 선고 2010고단5343 판결)

A 개발사는 B 금융사의 위탁을 받아 스마트폰용 증권시세 검색 앱을 개발하였다. 이 앱은 사용자가 설치할 때 사용자의 스마트폰으로부터 IMEI(국제 모바일 단말기 인증번호)와 USIM 일련번호, 휴대전화 번호 등의 정보를 수집하여 A 개발사 및 B 금융사의 서버에 저장하였다. 그 목적은 사용자가 앱에 재접속할 경우 사용자의 동일성을 식별하여 별도 로그인 없이도 그 사용자가 등록해 놓은 관심 종목을 보여 주기 위한 것이었다. B 금융사는 이와 관련하여 사용자들로부터 정보통신망법에 따른 개인정보의

[38] 행정자치부 등(주37), 55면

수집 및 이용에 관한 고지를 하지 아니하였고, 동의 또한 받지 아니하였다.

이러한 사실관계 하에, 법원은 IMEI와 USIM 번호에 관하여 개인정보성을 긍정하였다. 먼저 식별가능성이란 “당해 정보와 결합 가능한 다른 정보가 모두 동일인에게 보유되고 있는 것을 전제로 하지는 아니하고, 여기서 쉽게 결합하여 알아볼 수 있다는 것은 쉽게 다른 정보를 구한다는 의미이기보다는 구하기 쉬운지 어려운지와는 상관 없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다”고 판시하였다.

구체적 판단에 있어서는, “IMEI나 USIM 일련번호는 그 값 자체만으로는 사용자 정보를 확인하는 것이 불가능하나 권한 있는 자가 정보를 조합하여 사용자정보를 확인할 수 있는 점, 피고인들이 사용자의 접속의 편의를 위하여 ID 대용으로 위 일련번호 내지 휴대전화번호를 수집하여 보관한 점, 피고인들은 당초에는 사용자의 IMEI만을 수집하다가 IMEI 하나만 취득하는 경우 사용자들의 휴대폰이 바뀌었을 때 전에 사용한 사람의 증권 관심종목이 표시되는 등의 문제가 발견되어 개인사용자를 분명하게 인식하게 하기 위하여 IMEI와 더불어 USIM 일련번호를 취득하되, USIM 일련번호가 있으나 읽을 수 없는 경우에는 USIM 일련번호 대신 개인 휴대전화번호를 취득한 점, 현재 통신사에서 휴대폰 개통시 작성하는 가입신청서에 위 일련번호가 기재되어 있고, 통신사 데이터베이스에 기록되어 관리되는 점, 위 일련번호를 아는 경우 통신사의 시스템 등을 통해 구체적인 개인정보 확인이 가능한 점, 위 일련번호와 개인에 관한 정보가 통신사별로 접근을 엄격히 통제하고 있으나, 제3자에 의하여 획득될 가능성이 없는 것으로는 보이지 않는 점” 등을 고려하여 이들 정보의 개인정보성을 인정하였다.

식별 개념에 관하여, 위의 “IMEI나 USIM 일련번호는 그 값 자체만으로는 사용자 정보를 확인하는 것이 불가능하나 권한 있는 자가 정보를 조합하여 사용자정보를 확인할 수 있는 점”이라고 판시하고 있는 점을 보면, 위 판결은 일응 통신사업자가 보유하고 있는 사용자의 성명, 주민등록번호 등의 정보와 결합하여야만 식별이 된 것으로 보고 있는 것 같다.

그러나 재판부는 위와 같은 판시에 이어 i) 피고인들이 비록 통신사가 보유하는 구체적 사용자정보에 접근하지는 못하더라도 사용자 동일성 식별을 위한 ID 대용으로 문제의 정보들을 수집하여 휴대폰이 바뀌더라도 동일한 사용자에 대해서는 기존 관심 종목이 보이도록 하였다는 점을 강조하였고, ii) “IMEI나 USIM 일련번호는 모두 특정 개인의 소유로 귀속되기 전까지는 기기나 특정 카드에 부여된 고유번호로서 그 자체로는 당해 개인을 알아볼 수 있는 정보라 보기는 어렵다 하더라도 위 번호정보를 가지는 휴대폰이 어느 개인의 소유로 귀속되는 순간부터 위 각 번호는 ‘기기나 특정카드에 부여된 고유번호’라는 의미 외에 ‘특정 개인 누가 소유하는 휴대폰의 기기번호 및 USIM카드의 일련번호’라는 의미를 함께 지니게 된다”고도 판시하였다. 이로부터 처리자가 식별의 목적을 가지고 특정의 식별자를 수집하고, 이를 중심으로 동일한 사용자에 관한 구체적 사실이 계속적으로 집적되고, 여기에 기반한 정보가 다시 그 사용자에게 전달된 경우에는, 성명 등의 구체적 사용자정보 없어도 식별을 인정한 것이라고 볼 여지도 있어 보인다.

즉, 이 판결에는 식별의 개념에 관하여, IMEI, USIM이 이 사건의 맥락에서는 그 자체로 개인식별을 가능케 하는 정보라는 관점과, 이러한 정보들은 그 자체로는 식별이 불가능하고 통신사업자가 보유하고 있는 사용자 정보가 결합되어야만 비로소 식별이 가능해진다는 정보라는 상호 모순된 관점이 혼재되어 있는 것으로

보인다. 그런데 통신사가 보유하는 구체적 사용자정보에 접근하지 못하였더라도 식별가능성을 인정하는 취지의 기재가 있는 것으로 보아, 우선 IMEI 등은 다른 정보와 결합하여야 개인식별이 가능하나, 예비적으로 그러한 결합이 없이도 동일한 사용자에 연결될 수 있는 상황이 있다면 식별가능성이 인정될 수 있다는 것이 위 판결의 입장이라고 이해할 수도 있다고 생각된다.

물론 '쉽게 결합하여'의 의미에 관해서는, "쉽게 결합하여 알아볼 수 있다는 것은 쉽게 다른 정보를 구한다는 의미이기보다는 구하기 쉬운지 어려운지와는 상관 없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다"라는 것이 법원이 명시적으로 취한 태도이다. 뒤에서 언급하다시피, 위 판결을 평가함에 있어 후자의 쟁점에만 주목하는 것이 학설의 일반적인 태도이기도 하다.

(나) 전화번호 뒷 네자리 사건(대전지방법원 논산지원 2013. 8. 9. 선고 2013고단17 판결)

경찰공무원인 A는 B로부터 "지금 모처에서 도박하는 사람들이 있으니 단속해달라"는 휴대전화 신고를 받고 현장으로 출동하여 C를 검거하였다. C는 훈방된 후 A에게 신고자 전화번호를 알려 달라고 하였고, A는 B의 휴대전화번호 뒷자리 4개를 C에게 알려 주었다. C는 이 정보와 자기 휴대전화에 저장된 통화내역을 결합하여 신고자가 B였음을 알게 되었다.

법원은 이 사안에서 휴대전화 뒷자리 네 개가 개인정보에 해당한다고 판시하였다. 그 근거는, 휴대전화 4자리에 개인정체성이 담기는 경우가 많아지고 있으므로 이것만으로도 사용자가 누구인지 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더더욱 그러할 가능성이 높으며, 설령 휴대전화번호 뒷자리 4자만으로는 그 전화번호 사용자를

식별하지 못한다 하더라도 기존 통화내역을 포함한 다른 정보(기존 통화내역 포함)와 쉽게 결합하여 사용자를 알아볼 수 있다는 취지로 판시하였다.

(3) 학설

(가) 식별 개념에 대한 이해

먼저, '식별'의 개념에 관하여 명시적으로 논하고 있는 문헌은 많지 않다. 그러나 '식별' 개념은 식별가능성 논의의 전제가 되는 것이고, 일부 문헌에서 이를 언급 내지 암시하고 있는 것이 있으므로 간단히 살펴 본다.

식별 개념에 관하여 언급하고 있는 문헌들은 대체로 행정자치부와 유사하게 구별 내지 구분이라는 관점에서 접근하는 것으로 보인다[39]. 그러나 구별 내지 구분이 무슨 의미인지에 관한 구체적이고 명시적인 설명은 거의 찾아보기 어렵다.

이와 관련하여, 행태기반서비스와 같이 하드웨어 고유번호, IP주소, 쿠키 등의 식별자를 통하여 개인에 관한 정보가 집적·처리되는 서비스의 맥락에서, 위와 같은 식별자만으로는 식별되었다고 볼 수 없고, 식별은 개인식별정보(PII)와 결합된 이후에야 비로소 가능하다 보는 견해가 있다[40]. 그런데 이 견해에서 말하는 PII는 개인정보와 같은 개념인지 다른 개념인지, PII라고 볼 수 있는 특정한 부류의 정보들이 존재하는 것인지가 불분명하다. 특히, PII라는 용어가 비교적 빈번하게 사용되는 미국에서도 PII 개념을

---

[39] 이창범(주25), 18면; 경정익, 스마트시대 개인정보보호 이해와 해설, 부연사, 2015, 94면

[40] 박상철, "행태기반서비스(위치기반서비스 포함) 관련 법령 정비 방안", 개인정보보호법제 개선을 위한 정책연구보고서, 프라이버시 정책 연구 포럼, 2013, 120면

명확히 정의하기 어렵다는 점을 감안하면[41] 더욱 그러하다. 즉, 이 견해는 결국 식별이 무엇인지에 대한 답이 없이 '개인을 식별할 수 있는 정보와 결합하여야 개인이 식별가능하다' 라는 순환논법에 의존하고 있는 것으로 보인다. 따라서 그 논리적 완결성이 불충분해 보이기는 하나, 이 견해는, 위에서 열거된 하드웨어 고유번호(흔히 단말 ID라고 부르는 것)나 쿠키 같은 식별자들의 존재만으로는 개인이 식별되었다고 보지 않고, 여기에 더하여 개인과 보다 긴밀한 관련이 있는 정보가 존재하여야만 식별을 인정할 수 있다고 보는 것만은 분명한 듯 하다. 왜냐하면 쿠키나 단말 ID의 경우 이로써 정보주체의 신원을 정확히 알 수는 없으나 적어도 그 정보에 의하여 지칭되는 자를 다른 주체와 '구분' 내지 '구별' 하게 함으로써 그 자에게 도달할 수 있게 해 주는데(바로 그러하기 때문에 이러한 정보들이 행태기반서비스를 위하여 사용되는 것이다), 이러한 정보들만으로는 식별성을 인정할 수 없다고 한다면, 결국 식별 개념에 관하여 '구별' 내지 '구분' 이라는 개념표지와 '도달' 이라는 추가적 요소 이상의 것을 요구하는 것, 아마도 현실적인 개인의 신원 확인까지를 요구하는 것에 다름 아니기 때문이다.

인터넷 홈페이지 운영자가 개인의 성명, 주소, 전화번호 등 개인 식별을 용이하게 하는 다른 정보 없이 이용자의 ID와 비밀번호만을 수집하는 경우를 예로 들어, ID와 비밀번호에 관한 정보만 보유하고 있는 경우라면 이는 '어느' 개인이 그러한 ID와 비밀번호를 사용한다는 의미에 불과하여 개인을 특정할 개연성이 없으므로 개인식별성이 없지만, 만일 해당 인터넷 홈페이지를 이용한 정보와 결합되면 '특정한' 개인을 식별할 수 있는 가능성이 발생할 수

[41] Paul Schwarz and Daniel Solove, THE PII PROBLEM: PRIVACY AND A NEW CONCEPT OF PERSONALLY IDENTIFIABLE INFORMATION, 86 N.Y.U.L. Rev. 1814 2011, pp.1828

있을 것이라고 하는 견해 또한 위 견해와 비슷한 전제 하에 서 있는 것으로 보인다[42].

한편, i) 성명, 주민등록번호, 영상 등의 고유식별자가 담겨 있는 정보라면 개인정보에 해당하고, ii) 고유식별자가 담겨 있지 않더라도 그 정보에 포함된 다른 요소정보를 종합적으로 고려하여 개인을 식별할 수 있다고 보는 견해도 있다[43]. 그러나 이 견해는 정작 '식별'이 무엇인지는 정확히 정의하고 있지 않은 듯 하다.

여기에 대하여는, 성명, 주민등록번호, 영상이 고유식별자이기는 하지만 그 정보만으로는 실제적으로 개인식별이 되지 않기 때문에, 이들 정보가 바로 개인정보라고 보기는 어렵고 다만 다른 정보와 쉽게 결합하여 개인을 식별할 수 있게 하는 정보라고 보아야 한다는 반론이 있다[44]. 이 견해 또한 '식별'을 '실제 신원 확인' 내지 '현실적 지목 가능성'으로 이해하는 것으로 보인다.

(나) 결합의 용이성을 누구를 기준으로 판단할 것인가

'쉽게 결합'의 의미에 관하여, '용이성'이 '합리성'이고, '합리성'이 식별에 투입되는 시간, 노력, 비용의 과다 여부를 의미한다는 원칙론에 관해서는 거의 이론이 없어 보인다.

그러나 이를 누구를 기준으로 판단할 것인지에 관하여는 대립이 존재한다. 즉 그 자체만으로 개인식별이 불가능하나 다른 추가적 정보(Zusatzwissen)와 쉽게 결합한 경우 개인식별이 가능해지는 정보의 개인정보 해당성과 관련하여, i) 추가적 정보가 이미

---

[42] 장주봉, "개인정보의 의미와 규제범위", 개인정보보호의 법과 정책, 박영사, 2014, 78면

[43] 이인호, "「개인정보 보호법」상의 '개인정보' 개념에 대한 해석론", 정보법학 제19권 제1호, 2015, 76~77면

[44] 주민철(주29), 22~23면

어딘가에 존재하면 족하다고 전제한 후 문제가 되는 정보와 추가적 정보가 결합하는 데 객관적으로 소요되는 시간, 노력, 비용만 검토하면 되는 것인지 ii) 아니면 문제의 정보를 처리하는 자를 기준으로 그 자가 추가적 정보를 입수하는 데 드는 시간, 노력, 비용을 검토해야 하는 것인지가 다투어지고 있다.

정보의 식별가능성은, 첫번째 견해에 따르면 정보처리자가 추가적 정보를 입수하는 것이 용이한지 여부와 무관하게 언제나 객관적•통일적으로 정해질 수 있을 것이고, 두번째 견해에 따르면 정보처리자가 누구이며 그가 처한 상황이 어떠한지에 따라 달라질 수 있을 것이다. 한편 식별가능성 개념을 획일적으로 정립하는 것을 거부하고 사안별로 판단한다는 견해도 있다. 편의상 이들 학설들을 각각 '객관설', '상대설', '절충설'로 명명하여 살펴 보겠다.

한편, 위 쟁점과 별도로, 결합 용이성의 정도 즉 추가적 정보의 입수 및 결합이 얼마나 용이하여야 하는지에 관한 문제도 있을 수 있다. 아직 이 부분에 관하여 뚜렷한 견해 대립을 찾아볼 수는 없으나, 상대설을 주장하는 일부 학자 및 실무가들이 이 부분에 관한 의견을 밝힌 바 있으므로, 함께 검토해 보기로 한다.

1) 객관설

이 설에 따르면[45] '결합의 용이성' 내지 '합리성'은 개인정보처리자나 개개의 사정에 따라 달라져서는 안되고, 객관적 기준에 따라 통일적으로 평가하여야 한다고 한다. 구체적으로, 문제되는 정보 자체의 성격에 주목하여, 그 정보가 그 자체로는 개인을 식별할 수 없더라도 다른 정보와 결합하여 식별을 용이하게

[45] 주민철(주29), 28~30면; 박혁수, "빅데이터 시대에 개인정보 개념의 재검토", Law & Technology 제10권 제1호(2014), 16면; 함인선, "개인정보 처리와 관련한 법적 문제-우리나라 「개인정보 보호법」과 EU의 '2012년 규칙안'을 중심으로 하여-", 경제규제와 법 제6권 제1호, 2013, 150면 이하

하는 것인지, 그 정보가 개인식별을 위하여 고안되고, 실제 그러한 목적으로 사용되고 있는 것인지 등을 합리적으로 판단한다는 것이다. 그리하여 증권통 판결의 식별가능성에 대한 논증 및 결론을 지지한다. 이 학설이 주장하는 근거는 다음과 같다.

첫째, 개인정보 개념이 처리 주체에 따라 달라진다면 개인정보보호법 적용 여부에 대한 예측가능성이 떨어지므로 법적 안정성을 저해하게 된다는 것이다.

둘째, 정보주체의 권리 보호에 소홀해질 수 있다는 점이다. 예컨대 개인정보처리자가 보유하고 있는 개인정보를 불법으로 제3자에게 제공하고, 그 제3자가 제공받은 정보 중 개인식별이 가능한 부분만을 삭제한 후 스팸 메일 발송 등의 방식으로 임의로 사용할 경우, 위의 상대설에 따르면 제3자가 자신의 정보는 개인정보가 아니라고 주장할 수 있게 되는데, 수사기관 입장에서는 그러한 주장을 반박할 증거를 발견하기가 현실적으로 어려우므로, 결국 정보주체의 권리 보호가 어려워진다는 것이다[46].

셋째, 헌법재판소가 디엔에이신원확인정보의 이용 및 보호에 관한 법률에 대한 헌법소원 사건 결정(2014. 8. 28. 선고 2011헌마28등)에서 객관설을 지지하고 있다고 한다. 즉 위 법률상 디엔에이신원확인정보는 단순한 숫자에 불과하고 이로부터 유전정보를 확인할 수 없어 그 자체로는 개인식별이 불가능하고 개인의 인적사항 및 식별코드와 결합하여야만 개인식별이 가능한 정보인데, 여기에 대하여 개인정보성을 인정하였다는 것이다[47][48].

---

[46] 주민철(주29), 28~32면

[47] 주민철(주29), 28~32면

[48] 그러나 디엔에이신원확인정보와 인적사항 및 식별코드가 각각 디엔에이신원확인정보담당자와 디엔에이인적관리자에 의하여 별도 관리되고는 있지만, 결국 일정한 요건을 갖춘 경우에는 법원, 검찰, 경찰에 의하여 인적 사항 및 식별코드와 결합되

넷째, 그 자체로는 식별가능성이 없는 정보가 유출된 경우 그 정보를 처리하는 자에게 정보 유출에 대한 책임(정보 관리체계의 개선책임 등)을 부여할 필요가 있으므로 식별성과 결합의 용이성을 상대적으로 결정하여서는 아니된다는 것[49]이 있다. '처리자의 손에서 식별가능성이 없는 개인관련성 있는 정보가 유출되어 불특정 다수의 손에 들어갈 수 있는 상황이 발생하면 누군가는 그 정보를 이용하여 개인을 식별할 수 있는 가능성이 있다. 그런데 처리자 기준설에 따르면 그 정보는 개인정보가 아니다. 따라서, 처리자로서는 그 정보가 자기의 손에 있는 동안 개인정보보호법상 요구되는 기술적 관리적 보호조치를 취할 의무가 없고, 정보 유출에 대한 통지의무를 지는지 여부도 불투명하다. 그러나 유출의 경우를 생각하면 이러한 정보에 대해서도 처리자에게 보호 의무를 부과하여야 하므로, 상대적 접근은 바람직하지 않다'는 취지로 생각된다.

2) 상대설

상대설은, 개인식별성 없는 개인관련 정보는, 정보처리자가 스스로 보유하고 있거나 접근권한을 가진 추가적 정보와 용이하게 결합하여 개인식별이 가능해지는 경우에 한하여 식별가능성이 있다고 본다. 즉, 정보처리자의 입장에서 추가적 정보의 입수 및 결합이 용이한지 여부를 결합용이성 판단의 기준으로 삼는다[50][51].

어 개인식별을 가능케 하는 것을 전제로 하고 있다는 점에서(위 법률 제11조 참고) 위 헌법재판소 결정이 객관설의 근거가 되기는 어렵다고 생각된다.

[49] 장주봉, "개인정보의 의미와 보호범위", 법학평론 제3권, 2012, 43면

[50] 김주영 · 손형섭, 개인정보 보호법의 이해-이론 · 판례와 해설, 법문사, 2012, 160면; 정상조, "위치기반서비스 규제에 관한 연구", 2015 Naver Privacy White Paper, 2015, 57~58면; 구태언, "개인정보 보호법의 제문제", 법학평론 제3권, 2012, 88면; 권영준, "개인정보 자기결정권과 동의제도에 관한 고찰", 2015 Naver Privacy White Paper, 99면; 김진환(주29), 25면; 김진환(주3),

64~66면; 문재완, “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 한국공법학회, 2014, 63면(여기서는 처리자 기준설이 타당하다고 명시되어 있지는 않으나, 증권통 판결에 대한 평석에서 피고인을 기준으로 결합가능성을 판단하고 있기 때문에 처리자 기준설로 분류한다); 박상철(주40), 122~126면; 이대희, “개인정보 개념의 해석 및 범위에 관한 연구”, 고려법학 제79호, 2015, 199면; 이인호(주43), 80~82면; 전응준, “위치정보법의 규제 및 개선방안에 관한 연구”, 정보법학 제18권 제1호, 2014, 216~219면 등 참고. 이창범(주25)의 경우 분명하지는 않으나, “‘쉽게’라는 단어는 과학적 가능성보다는 수단·방법의 합리성에 무게가 있다. 과학적으로 정보주체의 식별이 가능하다고 하더라도 식별을 위해 불합리할 정도의 시간, 노력, 비용이 투입되어야 한다면 그런 ‘단편적인 정보들’은 식별성이 있다고 할 수 없다”고 서술하고 있는 것으로 보아, 상대설에 가까운 것이 아닌가 생각된다.

[51] 김진환(주3), 66면, 전응준(주50), 218~219면은, 여기에 관하여 ‘**개인정보처리자**’를 기준으로 판단한다고 서술하고 있다. 그러나 이는 정확하지 않은 용어 사용이라고 생각된다. 왜냐하면 개인정보보호법 제2조 제5호의 ‘개인정보처리자’는 “업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등”이다. 즉, ‘개인정보처리자’는 그자가 개인정보를 다루고 있다는 점을 전제하는 개념이므로, 개인정보처리자를 기준으로 개인정보성을 판단한다는 명제는 개인정보를 다루는 자를 기준으로 개인정보성을 판단한다는 것으로, 일종의 순환논법이 된다. 더욱이, 위 용어를 사용하는 분들은 예컨대 암호화된 정보를 복호화 키 없이 전송받은 정보 수신자가 그 정보로부터 개인을 식별할 수 없는 경우, 그 수신자에게는 그 정보가 개인정보가 아니라는 입장을 취하고 있다. 여기에 따르면 그 수신자는 개인정보처리자가 아니라 할 것인데, 개인정보성은 개인정보처리자를 기준으로 판단되어야 하기 때문에 그 수신자가 전송받은 정보가 개인정보가 아니라고 한다면, 이는 일종의 논리적 모순에 이르게 되는 것이다. 한편 권영준(주50), 99면은 결합용이성 판단 기준이 되는 주체를 ‘정**보를 재식별하고자 하는 주체**’로 명명하고 있다. 그러나 어떤 정보의 개인정보 해당성 내지 식별가능성은 그 정보를 처리하는 자의 주관적 식별 의도보다는, 그 자가 객관적으로 그 정보를 식별할 수 있는 상황에 있는지를 기준으로 판단되어야 할 것이므로 이러한 용어 또한 정확하지 않다고 생각한다. 따라서 본고에서는 위 논문들의 ‘개인정보처리자’ 또는 ‘식별하고자 하는 자’라는 용어를, 적어도 그 자가 취급하는 정보가 개인정보인지 여부가 문제되고 있는 한에서는, ‘정보를 처리하거나 처리할 자’로 선해하고, ‘정보처리자 기준’ 또는 ‘처리자 기준’이라는 용어

이들 견해는 거의 예외 없이 증권통 판결의 의의를 단지 객관설을 명시한 데에서 찾고 있으며, 비판적인 태도를 취하고 있다.

이 견해에 따르면, 예컨대 임상 시험 기관이 시험 데이터 중 환자의 실명 등 환자를 식별할 수 있는 표지를 제거한 후 제약회사 등에 제공하였을 경우, 제약회사 측이 그 정보로부터 환자 개인을 식별할 수 없다면 그 정보는 그 제약회사에 대하여는 개인정보가 아니므로, 그러한 제공행위는 개인정보의 제공에 해당하지 않는다고 본다.

이러한 견해의 근거는 다음과 같이 정리될 수 있다.

첫째, 정보통신기술의 발달로 인하여 다양한 방식의 정보처리가 가능해지고 정보의 상호 결합 가능성 또한 높아졌기 때문에, 객관설에 따를 경우 개인정보의 범주가 사실상 무한히 확장되고, 사실상 모든 정보에 개인정보보호법이 적용되는 결과가 발생한다는 것이다[52]. 이 경우 개인의 권리가 침해당할 염려가 없는 경우에까지 기계적으로 개인정보보호법이 적용되는 반면 통계, 가명화된 정보의 활용 등 정보를 활용한 산업활동 전반이 위축되는 결과가 야기된다고 한다.

둘째, 외국의 입법례에 비추어 보더라도 정보처리자의 입장을 기준으로 보는 것이 옳다고 한다. 구체적으로, 영국 개인정보보호법(Data Protection Act 1998) 제1조 제1항 (b)가 개인정보 개념을 "그 정보(those information)와, 정보통제자(data controller)가 점유하고 있거나 그의 점유에 들어올 가능성이 있는(likely to come into) 다른 정보(other information)로부터 식별될 수 있는 생존하는 개인에 관한

를 사용하기로 한다.

[52] 구태언, 개인정보 정의조항, 동의제도 및 형사처벌의 합리화에 관한 연구, 고려대학교 정보보호대학원 석사학위논문, 2013, 98면; 김진환(주29), 64~66면; 권영준(주50), 99면; 전응준(주50), 219면; 정상조(주50), 57~58면 등.

정보”로 정의함으로써 개인정보처리자를 기준으로 결합의 용이성을 판단하고 있으며, 우리 개인정보보호법 제2조 제1호와 거의 동일한 법문을 가지고 있는 일본법의 통설적 해석 또한 결합용이성에 관하여 ‘정보처리자가 통상적인 업무 과정에서 쉽게 입수할 수 있는 다른 정보와 결합이 용이할 것’으로 보고 있기 때문에 우리 개인정보보호법도 여기에 준하여 해석하여야 한다는 것이다[53].

셋째, 앞서 살펴본 바와 같이 객관설은 해킹 사고에 대한 우려를 근거로 상대설을 비판하나, 실제로 그러한 사고는 처벌 규정으로 단속할 수 있으며[54], 정보가 수집·생성되거나 이전되는 경우의 법률적 위험은 기존 개인정보 처리 현황을 넘어 그러한 정보를 새로이 수집·생성하거나 이전받는 상황에서 비로소 발생한다고 보아야 하므로 상대설을 취하더라도 정보주체 보호와 관련하여 사각지대가 발생할 우려는 많지 않다고 한다[55].

넷째, 결합용이성 판단을 위하여 개인정보처리자 이외의 제3자의 시점까지 고려해야 한다고 보면, 수범자인 개인정보처리자가 개인정보성 여부를 판단하는 것이 사실상 불가능해지므로 부당할 뿐 아니라[56], 개인정보성의 유무를 처리자가 행위 당시 인식할 수 없었던 사정을 기초로 사후적으로 고찰하게 되므로 사실상 개인정보의 범위를 무한히 확대하는 결과가 발생할 수 있다고 한다[57]. 또한, 우리나라 개인정보보호법이 형사처벌 조항을 두고 있으므로, 죄형법정주의 및 명확성의 원칙에 반하게 된다고도

---

[53] 구태언(주52), 73면, 88면; 김진환(주29), 65면; 박상철(주40), 124면; 전응준(주50), 218면; 정상조(주50), 57~58면 등.

[54] 박상철(주40), 215면

[55] 김진환(주3), 65면

[56] 김진환(주3), 66면

[57] 전응준(주50), 219면

한다[58]. 요컨대, '결합용이성'의 요건으로서의 기능이 사실상 무의미해지며[59], 정보처리자의 이익이 과도하게 침해될 우려가 있다는 것이다.

3) 절충설

문제되는 상황의 다양한 측면을 고려하여, 정보주체의 자기정보결정권이나 사생활의 자유와 비밀을 침해할 우려가 있는지 여부에 따라 개인정보에 해당하는지 여부를 개별·구체적으로 결정하자는 입장이다[60]. 이 견해는, 객관설과 같이 문제되는 정보와 추가적 정보 사이의 객관적 결합가능성을 고려하는 입장은 사실상 모든 정보를 개인정보화하는 결과를 가져오므로 바람직하지 않다고 보고, 정보를 처리하는 자가 추가 정보를 쉽게 입수하여 결합할 수 있는지를 중요하게 고려하여야 한다고 보는 점에서는 상대설과 맥락을 같이 한다. 그러나 그 밖에도, (1) 문제가 된 정보와 관련된 행위의 유형(처리자 스스로 수집·사용하는 것인지 또는 제공·유출하는 것인지), (2) 해당 정보와 관련된 행위의 주체들 및 그들이 부담하는 주의의무의 정도(처리자가 보유하는 정보의 양, 상업적 목적의 유무, 정보가 민감한 성질의 것인지 여부, 공공기관인지 여부 등에 따라 주의의무의 정도를 판단하고, 이를 식별성 여부 판단에 고려), (3) 문제가 된 정보의 유형(사생활의 비밀 침해 가능성의 고저), (4) 개별 상황에서 문제가 된 정보가 식별성을 가질 경우 발생할 수 있는 정보주체에 대한 불이익 또는 위험의 정도 등 다양한 요소도 종합적으로 고려하여야 한다고 보는 점에서, 상대설과 구별되는 측면이 있어 보인다.

한편, 기타 처리자를 우선 고려하되 제3자의 관점을 배제할 필요가

---

[58] 구태언(주52), 93~94면

[59] 구태언(주52), 72면

[60] 장주봉(주42), 78~87면

없다는 설[61], 제3자를 기준으로 하여야 한다는 설[62]도 존재한다. 이들 학설의 경우 고려되어야 하는 제3자는 누구인지, 처리자를 우선으로 하되 제3자의 관점도 고려한다고 할 때 제3자의 관점이 보충적으로 사용되는 조건과 그 정도는 어떠한지가 불명확한 부분이 있다. 다만, 제3자의 관점을 폭넓게 고려하게 되면, 사실상 객관설과 같은 결론에 도달할 가능성이 높다고 생각된다.

(다) 식별가능성을 인정하기 위하여 추가적 정보의 입수는 얼마나 용이하여야 하는가

"구하기 쉬운지 어려운지와는 상관 없이"라는 증권통 판결의 판시대로, 이 쟁점은 객관설을 취하는 경우에는 거의 의미가 없다. 상대설을 취할 경우 비로소 의미가 있는 쟁점이다.

그 의미에 관하여, 용이하게 입수할 수 있는 정보란 "예컨대 서비스모델에 비추어 사업수행 과정에서 향후 추가로 정보입수가 예정된 경우라거나 또는 제휴관계나 접근권한을 가지고 다른 개인정보처리자로부터 추가로 정보를 입수할 수 있는 경우와 같이 합리적이고 당사자들이 예측가능한 범위 내의 정보"라는 설명이 있다[63]. 이와 관련하여, 이러한 '합리적이고 예측가능한 범위 내의 정보'에 오로지 통상적인 업무 과정상 입수 가능한 정보만 포함될 것인지, 불법적인 방법으로 수집된 정보가 포함될 수 있는지가 문제된다.

1) 통상적인 업무 과정상 입수 가능한 정보만 고려할 것인지

통상적인 업무 과정상 입수 가능한 정보만 고려하여야 한다는 설은, 일본 개인정보보호법의 통설적 해석을 근거로, "정보처리자가

[61] 임규철, "개인정보의 보호범위", 한독법학 제17호, 2012, 241면

[62] 윤주희 등(주30), 185면

[63] 정상조(주50), 58면

통상적인 업무과정에서 쉽게 입수할 수 있는 다른 정보”만이 용이하게 결합될 수 있는 추가정보라고 주장한다[64].

구체적으로, 일본의 ‘개인정보보호법에 대한 경제산업 분야를 대상으로 한 가이드라인’은 照合의 용이성에 관하여 “통상의 작업범위에서 개인정보데이터베이스에 접근해서 조합할 수 있는 상태를 말하며, 다른 사업자에게 조회해야 하는 경우 또는 당해 사업자 내부에서도 취급 부문이 다른 경우 등 조합이 곤란한 상태를 제외한다”고 규정하고 있으며[65], 일본의 우가 카츠야 교수의 개인정보보호법 축조해설서에 따르면 “다른 사업자에게 통상의 업무에서는 행하지 않는 특별한 조회를 요청하고 해당 다른 사업자가 상당한 조사를 한 때에 비로소 회답이 가능하게 되는 경우, 내부조직 사이에서도 시스템의 차이 때문에 기술적으로 조합이 곤란한 경우, 조합을 위하여 특별한 소프트를 구입하여 인스톨할 필요가 있는 경우”[66] 용이성이 부인되는바, 이를 우리법의 해석에도 참작하여야 한다는 것이다. 이러한 해석에 따르면 심지어 동일한 처리자가 보유하고 있는 추가적 정보라도, 현실적인 제약이 있으면 결합용이성이 부인될 수 있다.

그러나 동일한 처리자가 보유하고 있는 추가정보의 경우 결합용이성을 인정하여야 한다는 견해도 있다[67].

2) 불법적인 추가정보 입수 가능성을 고려할 것인지

위와 같이 ‘통상적인 업무 과정에서만 입수 가능한 정보’에 대해서만 결합용이성을 인정하게 된다면, 불법적인 경로로만 입수 가능한 정보는 결합용이성 판단에 고려하여서는 안된다는 결론이

64 구태언(주52), 88면, 92면; 이인호(주43), 81면

65 이인호(주43), 81면에서 재인용

66 구태언(주52), 88면

67 박상철(주40), 94~95면

도출될 것이다[68]. 앞에서 언급한, 동일한 처리자가 보유하고 있는 추가정보와 관련하여 결합용이성을 인정하는 견해도, 위법하게 입수 가능한 정보를 명시적으로 배제한다는 점에서는 위 견해와 일치한다[69].

4. 소결론

이상에서 살펴본 바와 같이, 우리나라에서는 '식별' 개념에 대하여는 구체적인 논의 자체가 존재하지 않으며, '식별가능성' 개념에 대해서는 객관설과 상대설, 절충설이 대립하고 있다. 판례의 경우 일견 객관설을 취하는 것으로 보이나, 학설 대립과 상관 없이 IMEI가 결론적으로 개인정보에 해당하는 것으로 인정될 만한 사안이었기 때문에, 특별히 어떤 견해를 취하고 있다고 단정하기 어려워 보인다. 이러한 상황에서 최근 정부가 비식별조치 가이드라인을 통하여 상대설(특히 처리자 및 제공받는 자 모두의 입장을 고려)을 취한다고 밝혔는바, 이후 실무의 전개가 기대된다. 한편 '입수가능성'과 관련하여 불법한 수단으로 식별에 필요한 추가적 정보를 입수하는 경우도 고려할 것인지 여부도 하나의 쟁점을 이루는 것이 관찰된다.

---

[68] 구태언(주52), 92면

[69] 박상철(주40), 94~95면

III 비교법적 검토

1. 개요

유럽연합은 유럽연합 개인정보보호지침(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 이른바 Data Protection Directive)을 통하여 각국이 법률로 규정하여야 할 개인정보보호의 최소 수준을 규정하고, 구체적인 내용은 각국의 입법에 맡기는 구조를 취하고 있다. 그러므로 이 지침은 비록 실제적인 규율은 아니지만, 유럽연합 전체의 개인정보보호 체계를 관통하는 기본 원리로서 중대한 의미가 있다. 또한, 지침의 해석과 관련하여 유럽사법재판소의 판례가 상당히 축적되어 있고, 규제기관의 상세한 의견서 또한 다수 존재하는바, 이들은 유럽연합 개인정보보호지침의 영향을 받은 우리법의 해석과 관련하여서도 참고자료로서의 가치가 높다. 한편, 최근 유럽연합 개인정보보호지침을 대체할 개인정보보호 규칙(Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, “General Data Protection Regulation”, 이하 “일반 개인정보보호 규칙” 또는 “GDPR”)이 확정되었고, 2018년 4월경부터 시행될 예정이다. 이 규칙은 지침과는 달리 유럽연합 각국에 대하여 직접효를 가진다. 이하에서는 지침을 위주로 검토해 보되, 일반 개인정보보호 규칙에 관하여도 간단히 살펴보기로 한다.

이와 같은 유럽연합법에 대한 이해를 바탕으로, 현재 사인에 대하여 구체적, 직접적으로 적용되고 있는 대표적인 두 가지 법제 즉

독일과 영국의 그것을 검토한다. 먼저 독일은 가장 먼저 근대적 개인정보보호법제를 완비한 국가 중 하나로, 유럽 내에서도 개인정보 보호가 엄격한 편이다. 현재 일반법으로 연방 개인정보보호법(Bundesdatenschutzgesetz, BDSG)이 있고, 정보통신서비스 분야에서 텔레미디어법(Telemediengesetz, TMG) 및 텔레커뮤니케이션법(Telekommunikationsgesetz, TKG)이 특별법으로 적용되고 있다. 유동 IP주소의 개인정보성을 둘러싸고 개인정보 개념에 관한 치열한 논의가 이루어지고 있다.

이와 대조적으로 영국은 아일랜드와 더불어 유럽에서 개인정보보호가 가장 완화되어 있는 곳으로, 유럽에서는 영국법의 태도가 매우 특수한 것으로 받아들여지고 있다[70]. 그러나 언어적 접근가능성이 높은 관계로 우리나라에서는 매우 흔히 참고되고 있는 점, 유럽 대륙과는 다른 새로운 관점을 보여줄 수 있다는 점에서 검토의 가치가 있다고 생각된다. 개인정보 개념은 물론, 암호화된 정보의 개인정보 제공의 적법성에 관하여 비교적 활발한 논의가 있는 편이다.

일본의 경우 유럽에 비하여 개인정보보호에 관한 논의가 덜 활발해 보이지만, 최근 정보통신기술의 발달 및 개인정보 활용의 중요성에 대한 인식을 바탕으로, 개인정보개념에 관하여 불명확한 부분을 명확히 하고 정보의 활용 및 이용자 보호라는 두 가지 목표를 동시에 달성한다는 취지에서 개인정보보호법이 전면 개정되었다. 일본의 전통적 개인정보 개념이 개정법과, 개정을 위한 논의 과정에서 어떻게 해석 내지 재해석되고 있는지를 검토하여 본다.

---

[70] Richard Cumbley and Peter Church, “EU-What is personal data?”, Linklaters Technology Media And Telecommunication Newsletter, October 2008, (2016. 10. 9. 방문) <http://www.linklaters.com/Insights/Publication1403Newsletter/PublicationIssue20081001/Pages/PublicationIssueItem3513.aspx>

2. 유럽연합

가. 유럽연합 개인정보보호지침

(1) 개인정보 개념의 정의

개인정보보호지침 제2조 (a)는 개인정보(personal data)의 개념에 대하여 다음과 같이 정의하고 있다:

'개인정보'는 식별된 또는 식별 가능한(identified or identifiable) 자연인('정보주체')에 관한 모든 정보를 말한다. 식별 가능한 사람이란 특히 식별 번호(identification number)나 그의 육체적, 생리학적, 정신적, 경제적 또는 사회적 동일성에 특유한 하나 또는 그 이상의 요소들을 언급함으로써 직접적으로 또는 간접적으로 식별 가능한 사람이다.

이러한 지침 규정의 해석에 참고하여야 할 부분이 지침 전문 부분의 고려이유(Recital, Erwägungsgrund)인데, 고려이유 26은 식별가능성(identifiability) 개념에 관하여 다음과 같이 설명하고 있다:

보호의 원칙들이 식별된 또는 식별 가능한 사람에 관한 모든 정보에 적용되어야 한다. 어떤 사람이 식별가능한지를 결정하기 위하여, 통제자(controller) [71] 나 제3자에 의하여 그 사람을 식별하기 위하여 합리적으로 사용될 수 있는 모든 수단(all the means likely reasonably to be used)을 고려하여야 한다. 보호의 원칙은 정보주체가 더 이상 식별 가능하지 않도록 익명화된 정보(data rendered anonymous)에 대해서는 적용되어서는 아니된다. 제27조의 의미에서의 행동 규칙(code of conducts)이 정보가 익명화되고 정보주체의 식별이 더 이상 가능하지 않은 형태로 보존되는 방법에 관한 가이드를 제공하기 위한 유용한 도구가

[71] Data controller. 우리나라의 '개인정보처리자'와 유사한 개념이다. 본고에서는 data controller나 controller는 우리말로 '정보통제자' 또는 '통제자'로 번역하기로 한다.

될 수 있다.

즉, 개인정보는 식별된 또는 식별 가능한 사람에 관한 모든 정보를 말하며, 여기서의 식별가능성 유무를 판단함에 있어서는 개인정보를 가지고 이를 처리하는 자 즉 통제자(controller) 자신 뿐만 아니라 다른 제3자의 관점이 고려되고, 이들이 식별을 위하여 합리적으로 사용할 수 있는 모든 수단을 고려한다. 즉, 문언상으로는 정보를 저장하고 사용하고 있는 자 이외의 제3자가 식별을 시도하는 경우도 고려되어 있는 것으로 보인다[72].

(2) 익명화 개념과의 관계

위 고려이유 26에 따르면 식별가능성이 없는 경우 '익명화(anonymisation)'가 된 것으로 보며, 익명화가 된 경우 지침의 개인정보보호 원칙이 적용되지 않는다. 그러므로 지침에 따르면 익명화된 정보는 개인정보가 아니라고 할 수 있다. 그러나 지침은 어떤 경우 익명화가 되었다고 볼 수 있는지에 관하여 구체적인 규정을 두고 있지 아니하다.

(3) 개인정보 개념에 관한 제29조 정보보호 작업반의 해석

유럽연합 각국의 개인정보보호 관청으로 구성된 제29조 정보보호 작업반(Article 29 Data Protection Working Party, 이하 'WP29')은, 2007년 '개인정보의 개념에 관하여'[73]라는 제목의 의견서에서 지침의 개인정보 개념의 해석 기준을 제시한 바 있다.

---

[72] European Union Agency of Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Publications Office of the EU, 2014, p.41

[73] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data(WP136), 2007

여기에 따르면, 지침상의 개인정보는 i)정보, ii)개인과의 관련성(relating to an individual), iii)식별 또는 식별가능성(identified or identified), iv)자연인에 관한 정보를 개념요소로 한다.

이 중 i), iv)와 관련하여서는 특별히 문제될 것이 없으나, ii) 개인과의 관련성 유무는 예컨대 자동차 번호판이나 기기의 ID와 같이 개인 자체가 아니라 특정한 사물이나 대상에 관한 정보가 개인정보인지 여부 그리고 여러 사람에 관한 기록 중 특정 개인에 관한 사항이 포함된 경우 그 기록 전체가 그 한 개인에 관한 것이라고 볼 수 있는지, 특정 개인과 관련 있는 기록이기만 하면 전부 그 개인에 관한 것이라고 볼 수 있는지 등이 문제될 수 있다. WP29는 이에 대하여 내용, 목적 또는 결과라는 세 가지 판단 기준을 제시한다. 즉, 어떤 정보가 내용(content)에 있어 개인에 관한 것인 경우 즉 개인의 신원(identity), 특성 또는 행동을 언급하거나 그러한 정보가 그 사람이 취급되거나 평가되는 방법을 결정함으로써 결과(result)에 있어 그에게 영향을 미치거나, 또는 정보의 취급 목적(purpose)이 위와 같은 것이라면 개인과의 관련성을 인정할 수 있다는 것이다[74].

다음으로 iii) '식별 또는 식별 가능' 요건에 관하여, WP29는 먼저 식별 개념을 "한 그룹의 사람 중에서 어떤 한 사람이 그 그룹의 나머지 다른 구성원들과 구별(distinguished)되는 상태"라고 정의한다[75]. 이와 같이 식별 개념의 본질을 타인과의 구별가능성에서 찾는다면, 식별 여부는 문제가 되는 그룹의 성격, 그룹에 속하는 개인에 관하여 존재하는 정보들이라는 구체적인 상황의 맥락에 따라 판단되어야 하며, 반드시 특정한 식별자가 존재하여야만 개인이 식별되었다고 볼 수 있는 것은 아니며, 어떤

[74] WP 29(주73), pp.10~12
[75] WP 29(주73), p.12

식별자가 개인을 식별 가능하게 하는가도 절대적으로 정하여져 있는 것이 아니고 개별 맥락에 따라 달라질 수 있는 것이 아닌가 생각해 볼 수 있을 것이다.

WP29 또한 이러한 입장을 명시적으로 확인하고 있다. 예컨대, 컴퓨터 파일링 시스템에서 개인들을 그 성명이 아니라 고유한 ID를 사용하여 구별하는 경우, 또는 개인이 사용하는 특정 단말의 ID만을 보유하고 있는 경우, 관련 개인의 성명이나 주소에 관한 정보가 없어도 그를 다른 사람과 구별할 수 있고, 그를 범주화하여 그에게 영향을 미치는 어떤 결정을 할 수 있다. 그러므로 이러한 경우에도 개인의 식별을 인정해야 한다는 것이다[7677].

한편 '식별가능'하다는 것은 어떤 정보만으로는 식별이 불가능하지만, 다른 정보와 결합할 경우 식별이 가능해질 수 있는 상태를 의미한다[78].

식별에 사용될 수 있는 수단과 관련하여, WP 29는 앞서 언급한

---

[76] WP 29(주73), pp.13~14

[77] 반면, 여기서 WP 29가 '개인에게 영향을 미치는 결정' 내지 '개인과의 연결점(individual's contact point)'을 언급하고 있다는 점에 주목할 만하다고 생각되는데, 뒤에서 언급하는 키 코드화된(key-coded) 정보의 경우, 키 코드화된 개인의 집단 속에서 각각의 개인은 각자에게 서로 다르게 부여된 키 코드에 의하여 상호 구별 가능할 것이지만, WP 29는 그것만으로 그 개인이 식별되었다고 보지는 않을 것으로 생각된다. 예컨대 임상시험 대상인 환자 집단에서 환자의 인적 사항이 가명으로 치환된 경우, 각각의 가명을 가진 환자들은 서로 구별 가능하더라도, 이 가명을 환자의 실제 동일성과 연결시킬 수 있는 상황에서만 식별가능성을 인정하고 있는 것이다(WP 29(주73) p.20). 이는 앞서 제시한 식별 개념과는 모순되는 주장으로 보인다. 그렇다면 WP 29는 단지 그룹 내에서 개인이 다른 개인과 구별된다고 해서 식별 가능성을 인정하는 것은 아니고, 현실세계의 개인과 각각의 키 코드로 표상되는 개인을 연결할 수 있는 가능성이 존재하여야만 식별 가능성을 인정하는 것이라고 보아야 하는 것은 아닐까?

[78] WP 29(주73), p.13

지침 고려이유 26의 통제자 또는 제3자가 합리적으로 사용할 수 있는 모든 수단을 고려하여야 한다고 한다. 구체적으로, “식별에 드는 비용, 정보처리 목적, 정보처리가 짜여진 구조, 통제자가 예상하는 이점, 그 개인들과 관련하여 문제되는 이익들, 조직의 기능 장애(organzational dysfunction, 예컨대 정보유출과 같은 사태) 가능성, 정보처리에서 통제자가 추구하는 목적, (개인 식별이라는 목적이 없는 경우) 식별을 방지하기 위하여 취해진 기술적 보호조치의 유무” 등을 고려 요소로 꼽고 있다[79].

이러한 수단 중 불법한 수단도 포함될 수 있는지가 문제될 수 있는데, 이 점과 관련하여 WP 29는, 키 코드화된(key-coded) 정보와 이를 풀기 위한 키(key)를 각각 다른 주체가 가지고 있는 경우, 외부 해킹 위험, 정보를 전송하는 조직 내에 있는 누군가가 직업적 비밀유지의무에도 불구하고 키 코드화된 정보를 전송받은 자에게 키까지 제공할 가능성을 고려하여야 한다고 함으로써, 불법적인 수단도 경우에 따라서는 ‘합리적’ 수단의 범위에 포함될 수 있다는 입장에 있는 것으로 보인다.

이와 같은 일반론은 임상시험을 위하여 가명화(pseudonymization)된 환자 정보와 IP주소라는 두 가지 경우에 다음과 같이 적용될 수 있다:

(가) 임상시험을 위하여 가명화된 환자 정보의 경우

의료기관 또는 연구기관은 임상시험을 위하여, 각 환자의 인적 사항과 병증, 적용된 치료방법 내지 의약품 내역이 기재된 자료를 보유하는데, 이 때 환자들의 보호를 위하여 개별 환자를 식별할 수 없도록 관련 정보를 키 코드화하는 한편, 적용된 의약품 등에 의한 부작용이 발생하는 경우 해당 환자를 찾아내어 치료를 진행할 수

[79] WP 29(주73), pp.15~16

있도록, 환자의 재식별을 가능케 하는 키 또한 함께 보유한다. 의료기관은 키를 제외한 코드화된 환자 정보만을 제약회사 등에게 제공한다. 이 경우 제약회사와의 관계에서 코드화된 환자 정보를 개인정보로 취급하여야 하는가?

WP 29는 오로지 제약회사가 키를 입수할 가능성이 없고, 환자를 재식별할 수 없으며, 이를 막기 위한 적절한 기술적 조치가 취해진 경우에 한하여 제약회사와의 관계에서 개인정보성을 부정할 수 있으며, 제약회사도 재식별 가능성을 전제로 키를 보유하고 있는 의료기관과의 관계를 설정한 경우에는 개인정보성을 인정하여야 한다는 입장인 것으로 보인다[80].

그러나 최근 발표한 '익명화 기술에 관한 의견' 에서 WP29는, 정보 통제자가 정보로부터 식별자(identifier)를 제거함으로써 정보를 그 자체로 식별 불가능한 형태로 변환한 후 이를 제3자에게 제공한 경우, 제공한 통제자 스스로가 제공된 정보와 결합하여 개인을 식별할 수 있게 하는 다른 정보를 보유하고 있다면, 비록 그 제3자가 그 정보로부터 개인을 식별할 수 없다고 하더라도, 총계화된(aggregated) 정보가 아닌 한 그 정보를 개인정보로 본다는 의견을 명확히 밝힌 바 있다[81].

(나) IP주소의 경우

이 부분 논의를 본격적으로 들어가기 전에, 먼저 그 배경에 관하여

---

[80] WP 29(주73) pp.18~21. 유럽연합 집행위원회도 결정(Decision) 2000/520/EC of 26.07.2000-O.J.L 215/7 of 25.08.2000.에서 같은 취지로 결정하였다고 한다. Patrik Lundevall-Unger&Tommy Tranvik, "IP Address - Just a Number?", International Journal of Law and Information Technology Vol. 19 No. 1, Oxford University Press, 2010, p.67에서 재인용.

[81] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 2014, p.9

간단히 설명하기로 한다.

일반적으로 IP주소의 개인정보성의 문제는, 인터넷 접속 서비스 제공자(internet service provider, “ISP”)가 아닌 일반 웹사이트 운영자(contents provider, “CP”)에게 유동 IP주소가 개인정보인가라는 쟁점을 둘러싸고 다투어지고 있다. 우선 고정 IP주소가 개인정보에 해당한다는 점에 관하여는 거의 이견이 없다. 고정 IP주소는 즉 한 개인 내지 하나의 단말기에 고정적으로 할당되고, 개인 식별에 필요한 추가 정보 또한 손쉽게 구할 수 있기 때문이다.

다만 유동 IP주소의 경우 접속 세션마다 새로운 주소가 할당되므로 CP가 이것으로부터 개인을 식별하기 위하여서는 다른 추가적인 정보가 필요하다. 그러한 추가 정보는 컨텐츠 제공 과정에서 CP 스스로 수집한 이용자에 관한 다른 정보일 수도 있지만, 그러한 정보가 존재하지 않는 경우에는 ISP가 보유 중인 접속 기록이 필요하다. 후자의 경우, ISP 입장에서는 유동 IP주소가 개인정보일 수 있는데, 과연 ISP에게 추가 정보가 존재한다는 이유로 CP의 입장에서도 그렇게 볼 수 있는가라는 문제가 발생하는 것이다.

WP29는, “인터넷에서의 프라이버시에 관한 작업 문서 – 온라인 정보보호에 관한EU의 통합적 접근”이라는 문서에서, i) ISP 아닌 CP 중 유니크 ID를 포함하는 쿠키와 같이 유동 IP와 결합하여 개인을 식별할 수 있는 정보를 보유한 자에 대하여는 유동 IP가 개인정보에 해당할 수 있고, ii) 저작권자가 온라인에서 발생하는 저작권 침해(예컨대 무단 복제 파일의 전송)를 단속하기 위하여 침해자의 IP주소를 보유하고 있는 경우, 저작권자는 민사소송 등으로 인터넷 접속 서비스 제공자에 대하여 특정 시간에 해당 IP를 사용한 개인의 신원을 알 수 있기 때문에[82] 이러한 경우

[82] 저작권자가 인터넷 접속 서비스 제공자에 대한 민사소송에서 특정 IP 사용자의

CP라도 개인을 식별할 수 있는 합리적 수단을 보유하고 있는 것으로 볼 수 있으나(사법 기관이나 국가의 정보기관의 경우에도 마찬가지다) iii) 인터넷 카페에서 불특정 다수의 사용자가 실명을 공개하지 않고 사용할 수 있는 PC의 IP 주소에 대해서는 개인정보성을 부정하여야 한다고 보았다[83].

그러나 WP29는 ISP 아닌 CP들에 대하여도, ISP가 유동 IP를 이용하여 개인을 식별할 수 있다는 이유로 유동 IP를 개인정보로 보아야 하는지에 대하여는 명확한 답을 하고 있지 않았다. 다만 현실적으로 CP는 유동 IP 뿐 아니라 비교적 개인식별이 용이한 고정 IP도 함께 보유하고 있는 점, 기타 다른 정보들과 유동 IP가 결합하여 개인식별이 가능할 수 있는 점 등을 감안하여 CP가 보유하고 있는 IP주소 중 개인식별이 가능한 것과 아닌 것을 명백히 구분할 수 있는 경우가 아니라면 모든 IP주소를 개인정보로 취급하는 것이 바람직하다고 하였을 뿐이다[84].

위에서 살펴본 WP 29의 '합리성' 기준을 감안하면, CP가 ISP가 보유하고 있는 정보를 입수할 합리적 가능성이 없다면 개인정보성을 부정할 수도 있을 것으로 보인다. 그러나 한편으로는 WP 29가 이해하는 '식별'이 어떤 그룹의 사람들 중 특정인을 구별할 수 있는 것에 지나지 않는다고 본다면, IP 주소는 그 자체로 동시간대에 인터넷에 접속한 수많은 유저 중 특정인을 구별해낼 수

신원을 공개하도록 청구하는 것이 EU법상 허용되는지 여부에 관하여, 유럽 사법재판소는 2008. 1.29.자 Promusicae v. Telefónica de España SAU 사건 판결(C-275/06)에서 이를 긍정한 바 있다.

[83] WP 29(주73) p. 21; WP 29, Working Document Privacy on the Internet - An integrated EU approach to On-line Data Protection-(WP37), 2000, pp. 16~17; WP 29, Opinion 1/2008 on Data Protection Issues related to Search Engines(WP 148), 2008

[84] WP 29(주73), p.17

있는 징표가 되므로 식별을 가능케 하는 정보라고 볼 여지도 없지는 않을 것이다. 그렇더라도, 구체적인 경우에서는, 앞서 살펴본 '내용, 목적, 결과' 라는 관련성의 3요건 유무에 따라 IP주소의 개인정보성을 인정할 수도, 부정할 수도 있을 것이다[85].

나. 유럽 사법재판소의 판례들

(1) 개인정보 개념 해석의 기초- *Lindqvist* 판결

유럽 사법재판소의 판례 중 개인정보 개념에 관하여 인용되는 대표적인 판례는 2003. 11. 6. 선고된 *Lindqvist* 사건의 판결[86]이다. 이 사건의 쟁점 중에서는 '사람을 이름이나, 이름과 전화번호 등으로 인터넷 홈페이지에서 언급하는 것이 유럽 개인정보지침상의 개인정보 처리행위에 해당하는지 여부' 가 포함되어 있었는데, 유럽 사법재판소는 여기에 대하여, '인터넷 페이지에서 여러 사람들을 언급하고 그들을 이름이나 다른 수단에 의하여, 예컨대 전화번호나 근로조건과 취미를 제공함으로써, 식별(identify)하는 것' 은 개인정보의 처리에 해당한다고 판시하였다. 즉, 이름 뿐 아니라 다른 수단에 의해서도 개인이 식별될 수 있다고 한다.

(2) *YS* 판결

2014. 7. 17. 선고된 *YS* 사건 판결[87] 또한 개인정보 개념에 관하여 매우 중요한 판시를 담고 있다. 즉 외국인이 네덜란드 이민청에 거주 허가(residency permit)를 신청하였다가 거절당하자,

---

[85] Robinson et al, Review of the European Data Protection Directive, Rand Corporation, 2009, p.27

[86] CJEU Case C-101/01 Lindqvist (2003)

[87] CJEU Joined Cases C-141/12 and C-372/12 YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S(2014)

네덜란드 개인정보보호법(개인정보보호지침 제12조에 상응함)상 접근권에 근거하여 거절의 근거가 된 법률분석 내용을 담은 내부 문서의 제공을 요구하였는데, 그러한 법률분석 내용이 신청인에 '관한' 정보로서 개인정보보호지침상 개인정보에 해당하는지 여부, 즉 개인정보 정의 중 개인과의 관련성의 내용이 문제된 사안이다. 여기에 관하여 유럽사법재판소는 법률분석 문서에 담겨 있는 신청인에 관한 정보들 즉 신청인의 성명, 생년월일, 국적, 성별, 인종 등의 정보는 개인정보에 해당하지만, 법률분석 자체는 비록 신청인의 개인정보에 근거하여 도출된 것이기는 하나 신청인에 '관한' 정보가 아니라고 판시하였다[88].

그 근거는, 개인정보보호지침이 지침의 목적으로 삼고 있는 개인의 사생활 존중에 관한 기본권의 보호는 그 개인이 그에 관한 개인정보가 정확하고, 적법하게 처리된다는 것을 의미하며, 정보주체의 개인정보에 대한 접근권은 정보주체가 이 점을 점검(check)할 수 있도록 하는 데 취지가 있는데, 법률적 분석은 그러한 점검의 대상이 아니고, 따라서 지침상 개인정보 보호라는 취지와 무관하다는 점이다[89].

이러한 판결은, 개인정보의 개념은 정보주체의 사생활 보호 등에 관한 기본권을 실현하는 범위 내로 제한하여 해석되어야 하고, 구체적으로 정보주체가 정보의 정확성 및 정보 처리의 적법성 여부를 확인할 수 있게 하는 성질의 것이어야 함을 시사한다는

---

[88] CJEU, Joined Cases C-141/12 and C-372/12 YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S(2014), para. 40

[89] CJEU, Joined Cases C-141/12 and C-372/12 YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S(2014), para. 41~48

점에서[90], 비단 관련성 요건에만 관계되었다기보다는 개인정보 개념에 대한 해석원칙 일반을 도출함에 있어 고려할 가치가 있다고 생각된다. 더욱이 WP 29가 관련성에 관하여 제시한 세 가지의 심사 기준(test) 즉 내용-목적-결과 기준에 따를 때, 문제의 법률 분석은 정보주체와 내용적으로 관련되어 있고, 정보주체에 대한 처분을 도출하기 위한 것이므로 내용, 목적 또는 결과 기준을 충족한다고 할 것이지만 유럽사법재판소가 이를 거부하였다는 점에서, WP 29의 기준에 비하여 제한된 해석기준을 제시하였다고 볼 여지가 있다[91].

(3) IP 주소의 개인정보성: *Breyer* 사건에 이르기까지의 판결들

한편 IP주소의 개인정보성에 관하여, 유럽 사법재판소는 일찌기 *Promusicae* 사건[92]에서, ISP가 보유하고 있는 유동 IP주소와 그 사용자를 매칭하는 데 필요한 정보는 개인정보에 해당함을 긍정한 바 있다.

이어 *Scarlet Extended* 사건[93]에서도 유동 IP주소가 개인정보에 해당한다고 판시하였으나, 사실관계상 ISP가 보유하고 있는 유동 IP의 개인정보성이 문제된 것이었기 때문에 유동 IP주소가 언제나 개인정보에 해당한다는 취지로 보기에는 다소 무리가 있었던 것이 사실이다.

---

[90] 同旨, Peter Church, "EU-What is personal data? Just the facts..." , Linklaters Technology Media And Telecommunication Newsletter, December 2014. (2016. 10. 9. 확인) <http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-8-December-2014/Pages/EU-What-is-personal-data.aspx>

[91] Church(주90)

[92] CJEU Case C-275/06 Promusicae(2008)

[93] CJEU Case C-70/10 Scarlet Extended(2011)

ISP가 아닌 CP에 대하여, 그에게 유동 IP와 이용자를 매칭하는 정보가 없는 경우라 할지라도 유동 IP가 개인정보에 해당하는지 여부는 2014. 10. 28. 독일 연방 대법원이 유럽 사법재판소에 대하여 선결적 판단(preliminary ruling)을 요청하였고, 2016. 10. 19. 유럽사법재판소의 판결이 선고되었다(CJEU C-582/14 Patrik Breyer v. Deutschland)[94].

이 판결에 따르면 CP가 유동 IP주소와 함께 접속을 시도한 웹페이지 또는 파일의 이름, 입력한 검색어, 접속 시간, 데이터 전송량, 접속 성공 여부 등을 수집하는 경우, 그러한 유동 IP주소는 개인정보에 해당한다. 즉, CP가 "공중에 접근 가능하도록 한 웹사이트에 어떤 사람이 접근할 때 기록되는 유동 IP주소는 그가 인터넷 서비스 제공자가 보유하고 있는 추가적 정보를 이용하여 개인을 식별할 법적 수단을 가지고 있다면" 그와의 관계에서 개인정보에 해당한다고 본 것이다.

즉, 개인정보보호지침 고려이유 26의 "통제자(controller)나 제3자에 의하여 그 사람을 식별하기 위하여 합리적으로 사용될 수 있는 모든 수단(all the means likely reasonably to be used)을 고려"한다는 규정은, 어떤 정보를 '개인정보'로 취급하기 위해서는 "정보주체의 식별을 가능하게 하는 모든 정보가 한 사람의 손 안에 있을 것을 요구하지 않는다"는 뜻으로 해석되어야 하지만, 유동 IP와 ISP가 보유하고 있는 추가적 정보와 결합 가능한지 여부를 검토하기 위하여서는 '합리적으로 사용될 수 있는 모든 수단' 여부 또한 검토할 것을 요구한다고 한다. 그런데 결합을 위하여 법에 의하여 금지된 수단이나 "시간, 비용 및 노동력이라는 점에서 과도한 노력"이 요구된다면, 식별의 위험이 근소하기 때문에(insignificant) 식별가능성을 부정하여야 한다는

[94] CJEU Case C-582/14 Patrik Breyer v. Deutschland

것이다[95].

그런데 비록 법률에 의하여 ISP가 유동 IP주소와 결합하여 개인을 식별할 수 있는 추가 정보를 제3자에게 유출하는 것이 금지되어 있다고 할지라도, 사이버 공격이 발생한 경우, CP가 "관련 당국을 접촉하여 ISP로부터 그러한 정보를 획득하기 위하여 필요한 절차를 밟아서 형사절차를 시작할 수 있다면" 합법적 결합 가능성을 인정할 수 있다고 한다[96].

요컨대, CP가 적법한 수단 또는 과도하지 않은 노력으로 개인을 식별하기 위하여 필요한 추가정보를 입수할 가능성이 있다면 유동 IP주소는 개인정보가 될 수 있다는 것이다. 이 판결은 일응 개인정보의 통제자(처리자)인 CP의 입장에서, 합리적으로(적법하게 또는 과도한 노력 없이) 입수 가능한 추가 정보의 유무를 기준으로 개인정보성을 판단하고 있는바, 우리나라의 견해들 중 상대설과 상통하는 것으로 보인다. 그러나 CP가 사용할 수 있는 '합리적 수단'의 범위를 발생 여부가 불투명한 예외적인 경우에 사용 가능한 수단까지 확장시키고 있으므로 결과적으로는 개인정보의 범위를 매우 넓게 보는 것으로 평가할 수 있을 것이다.

다. 일반 개인정보보호규칙

유럽연합 집행위원회는 각국의 개인정보보호법을 통일하기 위하여 2012. 1. 25. 일반 개인정보보호규칙안을 발표하였고, 장기간에 걸친 논의 끝에 2016. 4. 27. 유럽 개인정보보호규칙이 제정되었다[97]. 이 규칙은 2018. 5. 25.부터 개인정보보호지침을

[95] CJEU Case C-582/14 Patrik Breyer v. Deutschland, 42~46

[96] CJEU Case C-582/14 Patrik Breyer v. Deutschland, 47

[97] 일반 개인정보보호 규칙의 제정 과정에 관하여는 채성희, "목적외 이용과 프로파일링 관련 규제에 관한 비교법적 검토 – EU 개인정보보호지침, 규칙안, 정보통신

대체하고 유럽연합 전 국가에 직접적인 효력을 가지는 단일 규범으로서 시행될 것이다(일반 개인정보보호규칙 제94조 제1항, 제99조 제2항).

이 규칙 제4조 제1항은 개인정보의 개념에 관하여 아래와 같이 정의하고 있다:

'개인정보'란 식별된 또는 식별 가능한 자연인('정보주체')에 관한 모든 정보를 의미한다. 식별 가능한 개인이란 특히 이름, 식별 번호, 위치 정보, 온라인 식별자(online identifier) 또는 그 사람의 육체적, 생리학적, 유전적, 정신적, 경제적, 문화적 또는 사회적 동일성에 특유한 하나 또는 그 이상의 요소들을 언급함으로써 직접적으로 또는 간접적으로 식별될 수 있는 사람이다.

지침의 고려이유 26에 해당하는 내용은 규칙 고려이유 26인데, 여기서는 지침의 고려이유 26과 마찬가지로 식별가능성 여부를 판단하기 위하여서는 통제자 및 제3자가 합리적으로 사용할 수 있는 모든 수단을 고려하여야 한다는 원칙을 확인하고 있다. 다만, 규칙안에서는 '합리적'인지 여부를 판단하기 위한 기준으로, "식별을 위하여 필요한 비용과 시간과 같은 모든 객관적 요소들을 검토하여야 하며, 처리 시점에 사용 가능한 기술과 기술적 발전도 고려하여야 한다"고 구체적 기준을 제시하고 있다.

규칙안은 익명화에 대하여도 지침과 마찬가지로, 식별된 또는 식별 가능한 개인과 관계가 없는 정보나 정보주체가 식별 가능하지 않도록 익명화된 정보에 관하여는 규칙이 적용되지 않는다고 명시함으로써 익명 정보(anonymous information)는 개인정보가 아님을 밝히고 있다(고려이유 26).

망법 및 개인정보보호법을 중심으로", LAW & TECHNOLOGY 제12권 제1호, 2016, 43~44면을 참고하라.

IP주소를 비롯한 정보들에 관하여는 규칙 또한 명확한 태도를 취하고 있지 않은 것으로 보인다. 그러나 규칙 제4조 (a)에서 개인정보를 정의하며 “식별 가능한 개인이란 특히 ... 온라인 식별자 ...를 언급함으로써 직접적으로 또는 간접적으로 식별될 수 있는 사람이다”라고 함으로써 ‘온라인 식별자’를 직접 언급하고 있고, 고려이유 30 또한 “IP주소, 쿠키 ID, RFID 태그 같은 온라인 식별자는 고유 식별자(unique identifier)와 다른 정보와 결합함으로써 개인의 프로파일을 형성하고 개인을 식별하는 데 사용될 수 있는 흔적을 남길 수 있다”고 함으로써, 온라인 식별자가 개인의 식별에 사용될 수 있는 가능성을 언급하고 있다. 더욱이 가명화된 정보(pseudonymized data)에 대하여 “추가적인 정보를 사용함으로써 자연인에게 귀속될 수 있는 정보”라고 정의하고, 개인정보에 해당한다고 명시한 점(고려이유 26)에 비추어 보면, 키 코드화된 정보나 유동 IP 주소, 기타 그 자체로는 개인의 신원을 알 수 없는 온라인 식별자들에 대하여 비록 통제자(처리자) 자신이 이를 가지고 개인을 식별할 수 없더라도 개인정보성을 인정하게 될 가능성은 상당히 높아 보인다.

라. 소결론

유럽연합 개인정보보호지침 하에서, ‘식별’ 개념은 개인을 다른 사람으로부터 구별할 수 있고, 그를 범주화하여 그에게 영향을 미치는 어떤 결정을 할 수 있는 상태를 의미한다. ‘식별가능성’을 누구를 기준으로 판단할 것인지에 관하여 WP29는 정보처리자 뿐 아니라 제3자의 관점까지 고려한다는 입장이었으나, CJEU는 정보처리자를 기준으로 판단한다는 것을 확인하였다. 식별을 위하여 사용될 수 있는 수단에 관해서도, 불법적인 수단까지 고려 요소로 삼았던 WP29와는 달리 CJEU는 원칙적으로 적법한 수단만을 고려하는 것으로 판시하였다. 단, 그러한 적법 수단의 범위에 관하여, CP가 사이버 공격 등이 발생하였을 때 수사기관에

의뢰함으로써 IP주소로부터 개인을 확인할 수 있는 경우까지 고려함으로써 적법 수단의 범위를 매우 넓게 파악하고 있다.

한편 정보 통제자에게 개인정보이지만, 제공받는 자는 그 정보로부터 개인을 식별할 수 없는 정보에 관하여, WP29는 키 코드화된 정보의 제공이라는 맥락에서, 그러한 정보도 완전 총계화가 되지 않은 한에서는 개인정보이며, 그 제공도 개인정보의 제공에 해당한다는 입장이다.

3. 독일

가. 개인정보보호법의 개요

1970년 헤센(Hessen) 洲가 세계 최초의 개인정보보호법을 제정한 이래 각 주(Bundesland)에서 개인정보보호법을 제정하여 현재까지 총 16개의 주법이 존재한다. 연방 차원에서는 1977년 1월 27일 연방 개인정보보호법(Bundesdatenschutzgesetz, 이하 'BDSG')이 제정되었다. BDSG는 독일의 연방 공공단체(öffentliche Stellen)와 민간부문의 정보보호에 관한 기본법이고[98], 각 주의 개인정보보호법은 원칙적으로 각 주의 공공단체에 적용된다. 그 밖에도 개별 분야별로 정보보호에 관한 특별규정이 존재하는데, 대표적인 것으로 텔레커뮤니케이션 망과 방송망을 통한 신호의 전송에 관하여 규정하는 텔레커뮤니케이션법(Telekommunikationsgesetz, 'TKG')과, 방송법의 적용대상을 제외한 모든 전자적 정보통신서비스에 적용되는 텔레미디어법(Telemediengesetz, 이하 'TMG')이 있다. 본고에서는 민간부문을 규율하는 BDSG와, 우리나라의 정보통신망법상 개인정보보호규정에 상응하는 TMG상 개인정보보호규정이 주된 검토대상이 될 것이나, TMG에서의

[98] BDSG 제2조 제4항, 제1조 제2항

개인정보 개념은 BDSG의 그것과 동일하므로, 결국 BDSG의 개인정보개념에 관한 해석론이 중심이 될 것이다.

독일에서 개인정보 개념과 관련하여 가장 활발하게 논의가 이루어지는 부분은 바로 식별가능성(Bestimmbarkeit)의 개념으로, 구체적으로는 IP 주소의 개인정보성 여부라는 문제로 드러나고 있다. 이하에서는 이러한 견해 대립에 관하여 살펴보되, 그 전에 독일 개인정보보호법의 헌법적 기초를 형성하였고, 식별가능성 개념의 해석과 관련하여서도 자주 원용되고 있으며, 우리나라 개인정보 자기결정권 개념 정립에까지 지대한 영향을 미친[99] 정보자기결정권 개념에 관하여 간단히 살펴보기로 한다.

나. 정보자기결정권

BDSG에 명시되어 있지는 않으나, 독일에서 개인정보보호의 헌법적 근거가 정보자기결정권(Recht auf informationelle Selbstbestimmung)이라는 점에 대해서는 광범위한 합의가 존재하는 것으로 보인다[100]. 정보자기결정권이라는 개념은 연방헌법재판소가 1983. 12. 15. 선고한 이른바 인구조사판결(Volkszählungsurteil)[101] 에서 최초로 사용되었고, 이후 다수의 판례들을 통하여 발전되었다. 개인정보 개념에 관한 논의에서 정보자기결정권의 개념이 적지 않게 원용되므로, 이하에서 그 의미에 관하여 간략히 살펴 보기로 한다.

---

[99] 권영준(주50), 92면

[100] Simitis, in Simitis[Hrsg.], *Bundesdatenschutzgesetz*, Nomos(2011), §1 Rn.25(p.191).

[101] BVerfGE 65,1

(1) 정보자기결정권의 개념

정보자기결정권의 핵심 내용은 개인정보에 관한 자기결정권(Selbstbestimmungsrecht über personenbezogene Information)이고, 이는 자기의 개인정보의 누설(Preisgabe)과 사용에 관하여 스스로 결정할 권리라고 정의할 수 있다[102]. 여기에는 누가, 무엇을, 언제, 그리고 어떤 기회에 그에 대하여 알고 있는지를 알 권리와 그의 개인정보에 대한 무제한적 수집, 저장, 사용, 전달 및 공개로부터 보호받을 권리가 포함된다[103]. 여기서의 개인정보 개념은 BDSG의 그것과 동일하다[104].

(2) 정보자기결정권의 법적 근거 및 성질

독일 연방헌법재판소는 정보자기결정권을 독일 기본법 제1조 제1항과 결합한 제2조 제1항에서 기인한, 일반적 인격권(allgemeine Persönlichkeitsrecht)으로부터 도출하였다[105]. 학설에 따라서는 정보자기결정권이 단순한 일반적 인격권이 아니라 독립한 헌법상의 권리인 '정보보호에 대한 기본권'이라고 보는 설도 있으나, 기본적으로 현대 사회에서 정보통신 기술의 발달로 인하여 강력해진 개인정보 처리자 앞에서 개인을 특별히 보호할

---

[102] BVerfGE 65,1 (LS Nr.1), (43); Hoeren/Sieber/Holznagel, Multimedia-Recht, C.H.Beck, 2015, Rn. 22; Maunz/Dürig, Grundgesetz-Kommentar, C.H.Beck, 2015, Rn. 174

[103] Maunz/Dürig(주102), Rn. 176; Hoeren/Sieber/Holznagel(주102), Rn.23

[104] Maunz/Dürig(주102), Rn. 174; 정태호(주7), 203면

[105] BVerfGE 65,1 (43). 우리나라와 달리 독일 기본법에는 사생활의 비밀과 자유에 관한 독립한 기본권이 존재하지 않는다. 이와 같이 개별 조항에서 명시되지 않았지만 인간의 존엄과 인격의 자유발현을 위하여 보호되어야 하는 기본권을 독일에서는 일반적 인격권으로 관념한다. 그 헌법적 근거는 독일 기본법 제1조 제1항의 인간의 존엄과 연결된 제2조 제1항의 인격의 자유발현권이라고 이해된다. 정태호(주7), 205면

필요가 대두되자, 이에 부응하여 일반적 인격권의 한 측면을 강조하는 것일 뿐이라고 이해하는 것이 보다 일반적인 듯하다[106]. 즉, 개인정보의 수집, 처리, 결합에 의한 프로파일 형성, 전달 및 공개 등이 용이해진 상황에서 개인을 더욱 보호한다는 것이다[107].

그런데, 연방헌법재판소가 정보자기결정권에 관하여 개인의 인격권적 측면 뿐 아니라 자유민주적 기본질서의 유지를 위한 필수 요소라는 측면도 강조하고 있다는 점에 유의할 필요가 있다. 즉, 개인의 작위나 부작위에 대한 결정 및 그에 따른 행위의 자유를 의미하는 개인의 자기결정(Selbstbestimmung)은 "시민의 행위능력(Handlungsfähigkeit) 과 참여능력(Mitwirkungsfähigkeit)에 기반한 자유 민주적 공동체(freiheitlichen demokratischen Gemeinwesens)의 기본적인 기능 조건" [108]인데, 자기에 대하여 누가 무엇을 언제 어떤 기회에 알고 있는지를 알 수 없다면 개인은 그러한 자기결정의 자유를 침해당할 것이고, 특히 자기의 집회 참여나 시민운동와 같은 행동에 관한 정보가 국가에 의하여 기록되고 있을지도 모른다고 의심하면 집회의 자유와 결사의 자유와 같은 기본권(기본법 제8조 및 제9조)을 포기할 우려가 있다. 이로써 개인적인 발전 기회 뿐 아니라 자유민주적 공동체의 기능이라는 공익(Gemeinwohl)이 침해된다는 것이다 [109] . 이처럼 정보자기결정권은 비록 일반적 인격권의 한 형태이기는 하지만, 사상의 자유, 집회의 자유, 결사의 자유, 통신비밀, 주거의 불가침과

---

[106] Maunz/Dürig(주102), Rn. 172~173; Gola/Schomerus, *Bundesdatenschutzgesetz*, C.H.Beck, 2015, §1 Rn.12; Hoeren/Sieber/Holznagel(주102), Rn.22; 정태호(주7), 214면

[107] BVerfGE 65,1 (42)

[108] BVerfGE 65,1 (43)

[109] BVerfGE 65,1 (42, 43)

같은 기본권의 보호와도 관련이 있으며, 주관적 공권으로서의 성격 뿐 아니라 객관적 가치질서의 구성요소라는 성격도 모두 가지고 있다[110].

(3) 정보자기결정권의 범위

자동화된 정보처리의 맥락에서, 정보자기결정권에 의하여 보호되는 개인정보의 종류에 관하여는 내용적인 제한이 없다[111]. 인구조사 판결 이전의 연방헌법재판소는 정보의 보호와 관련하여 개인의 사적인 또는 내밀한 영역(der Bereich der Privat- oder gar Intimsphäre)과 주제적 관련(thematischer Bezug)이 있는 경우에 한하여 기본권의 침해를 인정하고 있었으나(이른바 마이크로센서스 판결[112]), 인구조사 판결은 이러한 태도에서 탈피한 것이다[113].

즉, 동 판결의 유명한 판시와 같이, 침해 여부를 판단함에 있어 "정보의 종류에만 초점을 맞출 수 없다. 결정적인 것은 그것의 유용성(Nutzbarkeit)과 사용가능성(Verwendungsmöglichkeit)이다. 이것은 한편으로는 수집이 봉사하는 목적과, 다른 한편으로는 정보기술에 고유한 처리가능성(Verarbeitungsmöglichkeiten)과 연결가능성(Verknüpfungsmöglichkeiten)에 달려 있다. 이로써 그 자체로 보면 사소한 정보가 새로운 중요성을 얻을 수 있다. 그러한 한에서, 자동화된 정보처리의 조건 하에서 '사소한(belanglos)

---

[110] Simitis in Simmitis[Hrsg.](주100), Rn. 35, 38

[111] Maunz/Dürig(주102), Rn.172; Simitis in Simmitis[Hrsg.](주100), §1 Rn.35(p.194)

[112] BVerfGE 27,1

[113] 물론 뒤에서 살펴보는 바와 같이, 문제가 되는 정보가 개인의 내밀한 사적 영역에 관한 것이라면 침해 여부 판단에 있어 보다 엄격한 기준을 적용할 수 있을 것이다.

정보란 더 이상 존재할 수 없다" [114] 그리하여 직접성(Unmittelbarkeit)과 최종성(Finalität)을 특징으로 하는 고전적인 침해 판단 기준을 넘어, 모든 종류의 개인정보에 관한, 모든 형태의 수집, 저장, 사용, 전달 등이 정보자기결정권의 침해행위가 될 수 있다[115].

(4)정보자기결정권 제한의 정당화요건

정보자기결정권도 규범의 명확성(die Normenklarheit) 원칙과 비례원칙(der Grundsatz der Verhältnismäßigkeit)에 부합하는 합헌적 법률로써 제한할 수 있다. 그리고 입법자는 "인격권의 침해의 위험에 대하여 반작용할 수 있는 조직적이고 절차법적인 예방조치(organisatorische und verfahrensrechtliche Vorkehrungen)를 취하여야 한다" [116]. 이는 자동화된 정보처리의 사용이라는, 기술적으로 진보된 정보처리 과정의 위험에 대응하기 위한 관점에서 요구되는 사항이다[117].

먼저 비례원칙에 따라, 제한 입법에 대하여 요구되는 수준은 비교적 높다고 한다[118]. 정보자기결정권의 제한을 정당화하는 목적은 보다 우월한 공익(überwiegenden Allgemeininteresse)에 관한 것이어야 하고(목적의 정당성) [119], 이러한 목적은 명확성 원칙에 따라 명확히 확정되어야 한다. 정보는 이와 같이 확정된 목적을 위하여서만 사용되어야 하며, 목적으로부터 이탈(Zweckfremdung)되는 결과가 발생하지 않도록, 전달의

---

[114] BVerfGE, 65,1 (44, 45)

[115] Maunz/Dürig(주102), Rn. 176

[116] BVerfGE 65,1 (LS. Nr.2)

[117] BVerfGE 65,1 (44); Maunz/Dürig(주102), Rn. 182

[118] Maunz/Dürig(주102), Rn. 181, 182

[119] BVerfGE 65,1 (LS. Nr.2)

금지(Weitergaveverbote)와 이용의 금지(Verwertungsverbote), 설명의무(Aufklärungspflichten), 정보제공의무(Auskunftspflichten), 삭제의무(Löschungspflichten)와 같은 보호조치가 필요하다[120]. 한편 그 제한은 필요최소한이어야 하므로 공적인 이익의 보호를 위하여 불가결한 이상으로 제한되어서는 아니된다(수단의 적합성 및 침해의 최소성). 국가기관이 이용하고자 하는 정보가 개인의 사적 영역에 관한 사항을 더 많이 담고 있을수록, 정보의 사용이 집중적일수록 더 엄격한 요건이 적용되어야 한다(법익의 균형성)[121].

(5) 개인정보와 익명화된 정보에 관하여 적용되는 제한의 정당화요건

연방헌법재판소에 따르면, 취급되는 정보가 개인정보인지 익명화된 형태의 것인지에 따라 명확성 원칙과 비례원칙에 따라 요구되는 정당화 요건의 정도가 다르다. 개인정보의 수집 및 사용의 경우, 이러한 원칙은 엄격하게 적용된다. 그러나 익명화된 통계를 작성하기 위한 목적으로 정보를 수집하는 경우, 사전에 용처를 특정하기 어렵다는 통계의 특성상, 좁고 구체적인 목적 구속(Zweckbindung)은 요구되지 아니한다[122]. 그러나 그런 만큼 통계 정보의 생산을 위한 개별 정보의 수집과 처리에 관해서는, 개인이 단순한 정보의 대상이 되지 않도록 보장함으로써 개인의 인격권을 보호할 수 있는 명확히 정의된 정보처리의 조건이 필요하다.

그러한 조건으로, 입법자는, 인구조사를 통하여 통계정보를 만들기 위하여 개인에게 설문을 하고 그에 대한 응답의무를 부과함에 있어,

---

[120] BVerfGE 65,1 (45)

[121] Maunz/Dürig(주102), Rn. 181

[122] BVerfGE 65,1 (47)

먼저 이것이 개인에 대하여 사회적 낙인효과를 가져올 수 있는지, 수집의 목적이 익명화된 조사를 통하여 달성할 수 있는지를 심사하여야 한다. 또한, 수집된 정보가 통계화되기 전 즉 정보의 수집 및 저장 단계에서도 그러한 수집 및 처리의 수행 및 조직을 위한 특별한 사전조치가 필요하다. 예컨대 식별표지로서 요구되고 재식별화를 쉽게 가능하게 되는 정보에 대한 삭제규정, 외부에 대한 실효성 있는 봉쇄(Abschottung) 규칙 즉 가능한 빨리 익명화를 하고, 익명화되기 전의 개인정보에 대해 비밀유지의무를 부과하며 재식별화를 방지하는 사전조치에 대한 규정이 필요하다. 이러한 사전조치가 갖추어 있어야만 비로소 시민에 대하여 자신의 정보를 제공할 의무를 부과할 수 있고, 익명화된 정보를 다른 국가기관과 공유할 수 있는 것이다. 역으로 그러한 정보에 아직 개인관련성(Personenbezug)이 있는 한, 사전에 특정된 것과 다른 목적, 예컨대 집행 목적으로 다른 관청에 전달하는 것은 허용되지 않는다[123].

(6) 민간 부문에의 적용

민간 주체가 개인의 정보를 수집하는 것은 1차적으로는 국가에 의한 기본권 침해의 문제가 아니라 그 민간 주체의 기본권과 개인의 정보자기결정권 사이의 충돌 문제이다. 당연하게도, 정보를 수집하는 민간 주체는 영업의 자유 등 기본권의 주체이지 기본권의 수범자가 아니다. 이 경우에는 정보자기결정권은 오로지 민사상 불법행위 규정, 방해배제청구 규정 등을 통하여 간접적으로만 발현될 수 있다(이른바 기본권의 간접효). 물론 국가는 기본권에 대한 보호의무가 있으므로, 필요한 경우 정보자기결정권을 보호하기 위한 입법을 하여야 한다[124].

---

[123] BVerfGE 65,1 (48~50)

[124] Maunz/Dürig(주102), Rn. 189 f.

(7) 소결

이상에서 살펴본 바와 같이 정보자기결정권은, 정보화사회에서는 내밀한 사적 영역에 국한되지 않는 정보라 할지라도 보호할 필요가 있으며, 국가가 개인의 정보를 수집하고 처리하는 것은 비례원칙을 준수하는 명확한 법률에 의해서만 할 수 있고, 이러한 법률은 조직적이고 절차법적인 예방조치 또한 규정하여야 한다는 점을 명확히 하기 위한 개념이다. 독일 개인정보보호법은 여기에 입각해서 국가의 기본권 보호의무를 다하기 위하여 제정되어 국가 및 민간 영역에 적용되는 규범이다.

다. 개인정보의 개념 요소들

독일 연방 개인정보보호법(BDSG) 제3조 제1항은 개인정보를 다음과 같이 정의하고 있다:

개인정보(Personenbezogene Daten)는 식별된(bestimmt) 또는 식별 가능한(bestimmbar) 자연인(정보주체:Betroffener)의 인적 또는 물적 관계(persönliche oder sachliche Verhältnisse)에 관한 개별 정보(Einzelgaben)이다.

이러한 정의에 따르면, ㈀ '개별 정보' 로서 ㈁식별된 또는 식별 가능한 자연인에 관한 것이고, ㈂ 그의 인적 또는 물적 관계에 관한 것으로 (4) 생존하는 자연인에 관한 것이라는 요건이 충족되어야 개인정보 해당성이 인정될 수 있다.

(1) 개별 정보

개별 정보란, 3인 이상을 모집단으로 하여 통계적으로 처리된 집합적 정보(aggregierte Daten)와 대척적인 개념이다. 그러나 통계적인 값이라 할지라도, 모집단의 구성원이 가지고 있는 값이 서로 유사하거나, 기타 그 값이 개별 구성원에게 귀속될 수 있는

맥락이 존재한다면 개인정보에 해당할 여지가 있다고 한다[125].

(2) 식별 및 식별가능한 자연인에 관한 정보

다음으로, '식별된 또는 식별 가능한 자연인에 관한' 정보라는 부분이다. 이 중 '자연인'이란 오로지 살아 있는 사람만을 의미하며, 망자에 관한 정보는 오로지 그것이 생존하는 개인에 관한 정보로 볼 수 있는 경우에 한하여 개인정보성을 인정할 수 있다[126]. '식별' 개념과 '식별 가능성' 개념에 관하여는 학설 및 판례가 대립하고 있으므로 다음 항목에서 좀더 자세히 검토해 보기로 한다.

(3) 인적 또는 물적 관계에 관한 정보

인적 관계란 이름, 주소, 가족관계, 생년월일, 건강상태 등 정보주체 자신의 동일성 내지 특성에 관한 정보이며, 물적 관계란 정보주체의 부동산 소유, 제3자와의 계약적 관계, 통화 내용, 위치 등 정보주체와 관련 있는 사태에 관한 정보를 말한다고 설명된다[127].

그러나 이러한 구별은 법적으로 의미가 없다. '인적 또는 물적 관계'라는 문언은, 한 개인에 관한 서술이라면 그 성격이 어떠한 것인지 즉 지극히 내밀한 사적 영역에 관한 것인지 또는 그의 공적인 활동에 관한 것인지, 비밀로 유지되고 있는 것인지 아니면 일반적으로 접근 가능한 것인지, 사실에 관한 것인지 아니면 제3자의 가치판단에 관한 것인지를 불문함을 밝히는 의미일 뿐이라 해석된다(실제로 어느 정보가 여기에 포함되는지를 따지는 것은 불가능하기도 하다)[128]. 요컨대 '인적 또는 물적 관계에 관한 개별

[125] Dammann, in Simitis[Hrsg.](주100), §3 Rn.14

[126] Gola/Schomerus(주106), §3 Rn.12

[127] Gola/Schomerus(주106), §3 Rn.6~7

[128] Dammann, in Simitis[Hrsg.](주100), §3 Rn.7~12(pp.303~305); Roßnagel, 전게서, 4.1. Rn. 18

정보’ 란 우리 개인정보보호법의 ‘개인에 관한 정보’에 상응하는 개념이라 생각된다.

라. 독일 개인정보보호법상 식별가능성 개념을 둘러싼 견해의 대립

(1) 식별 개념

식별(Bestimmtheit)의 개념은 ‘개인의 동일성이 확인된 상태’ 또는 다른 사람과 개인이 구별된 상태라 정의되기도 하고[129], ‘정보가 어떤 사람에게만 관련되어 있고 다른 사람에게는 관련되어 있지 않은 것’이라고 정의되기도 한다[130]. 일반적으로 개인의 성명 등이 확인되면 해당 개인은 식별되었다고 볼 수 있을 것이나, 처리자가 정보를 취급하는 정보주체의 집단의 규모가 커서 동명이인이 다수 존재하는 경우라면 성명의 존재만으로 식별되었다고 하기는 어려울 것이고, 여기에 주소, 신체적 특징 등 다른 추가적 정보가 필요할 것이다[131].

이와 같이 식별의 개념이 필요한 것은, 앞서 살펴본 바와 같이 개인정보보호의 헌법적 근거가 정보에 대한 자기결정권인 이상, 문제의 정보가 누구에 관한 것인지 전혀 알 수 없는 이상 그러한 정보는 임의로 처리되더라도 정보자기결정권을 침해할 위험이 없을 것이기 때문이라고 설명된다[132].

(2) 식별가능성

식별가능성(Bestimmbarkeit, Identifizierbarkeit)이란 개인이

---

[129] Wolff/Brink, *Datenschutzrecht*, C.H.Beck(2013), §3 Rn.17~18

[130] Dammann, in Simitis[Hrsg.](주100), §3 Rn.22

[131] Dammann, in Simitis[Hrsg.](주100), §3 Rn.22

[132] Dammann, in Simitis[Hrsg.](주100), §3 Rn.20

식별될 수 있는 가능성을 말한다[133]. 성명, 사회보장번호(Sozialversicherungsnummer) 등과 같이 정보주체와 특별한 관련성이 있는 표지(Kennzeichen)가 존재하는 경우 직접적인(direkt) 식별가능성이 있는 것으로 보고, 이들 이외의 다른 방법으로 식별 가능한 경우에는 간접적으로(indirekt) 식별가능하다고 정의하기도 하나, 전자의 경우는 이미 식별된 것으로 보기도 한다[134]. 후자의 경우와 관련하여, 식별가능성을 부여하는 정보의 종류에 대하여는 제한이 없다. 어떤 정보이든 간에 개인의 재인식을 가능하게 한다면 이에 해당할 것이다[135].

이러한 식별가능성은 '합리적 식별가능성'을 말한다. 이 점에 관하여는 뒤에서 자세히 살펴보다시피 거의 대립이 존재하지 아니하나, 그 의미에 관하여는 학설과 판례가 첨예한 대립을 보이고 있다.

이와 같이 식별 가능성에 관하여 다툼이 있는 큰 이유는, 독일의 개인정보보호법이 성립한 이후 정보처리 실제가 크게 바뀌었기 때문이라고 한다 즉, 입법 당시에는 개인에 대한 정보와는 상관없는 학술적 통계적 처리와 개인에 대한 취급과 관련되어 있는

---

[133] 식별된 상태와 식별가능한 상태의 법적 취급에 관하여 서로 차이가 있다는 견해와 그렇지 아니하다는 견해가 대립하나, 본고에서 다루고자 하는 쟁점과는 무관하므로 따로 언급하지 아니한다.

[134] Roßnagel[Hrsg.], *Handbuch Datenschutzrecht,* C.H.Beck(2003), p.492; BGH: Speicherung von IP-Adressen durch die Bundesrepublik, ZD(2015), 80~81; Gola/Schomerus(주106), §3 Rn.10; Krüger/Maucher, "Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit grossen Auswirkungen auf die Praxis", MMR(2011), 434; Bergt, "Die Bestimmtbarkeit als Grundproblem des Datenschutzrechts-Überblick über den Theorienstreit und Lösungsvorschlag", ZD(2015), 366

[135] Wolff/Brink(주129), §3 Rn.19

행정, 상업 영역이 명확하게 구별되어 있었기 때문에 식별 가능성을 판단하기가 상대적으로 용이하였으나, 정보처리기술의 발달로 그러한 구별이 뚜렷하지 않게 된 것이다. 예컨대 전통적 식별자인 이름과 주소 외에도 IP주소, 쿠키를 사용한 가명과 단말 아이디 등이 식별의 목적으로 다양하게 사용되고 있는바, 이들을 어떻게 취급할 것인지라는 문제가 새롭게 대두된 것이다[136].

한편, 식별가능성에 관한 이러한 견해 대립에도 불구하고, 만일 정보처리자가 추후 개인을 식별할 목적으로 그 자체로는 개인식별이 불가능한 정보를 보유하고 있는 것이 증명된다면, 그러한 정보는 개인정보라고 보아야 한다는 데 상당 부분 견해가 일치하고 있는 것으로 보인다[137].

(가) 식별가능성의 판단 기준 1: 객관적 식별가능성과 상대적 식별가능성

식별가능성이 특히 문제되는 지점은, 정보처리자[138]가 보유하고 있는 어떤 정보(A)만으로는 개인을 직접 식별할 수 없으나, 제3자가 보유하고 있는 다른 추가적 정보(Zusatzwissen) B와 결합할 경우 개인의 식별이 가능해질 수 있는 경우이다. 이 때, 식별가능성 판단에 있어 이러한 추가적 정보의 존재를 어느 정도 고려할 것인가? 예컨대, 당해 정보처리자가 추가적 정보 B를 보유하고 있는 경우에 한하여 A의 개인정보성을 인정할 것인가?

---

[136] Dammann, in Simitis[Hrsg.](주100), §3 Rn.21

[137] Dammann, in Simitis[Hrsg.](주100), §3 Rn.25; Bergt, BGH: Speicherung von IP-Adressen durch die Bundesrepublik Beschluss vom 28.10.2014, ZD 2015, Rn.84

[138] 독일법상 이에 해당하는 법적 용어는 '책임 있는 자' (verantwortliche Stelle, BDSG §3(7))이고, 식별가능성에 관한 학설대립의 맥락에서는 (정보를) 저장하는 주체(speichernde Stelle)라는 용어가 빈번하게 사용되나, 본고에서는 편의상 '정보처리자' 라는 용어를 사용하기로 한다.

아니면 정보처리자에게는 그것이 가능하지 않더라도 다른 제3자가 추가적 정보를 보유하고 있어 그가 정보 A를 입수하는 경우 정보 B를 결합하여 개인식별을 할 수 있기만 하다면 개인정보성을 인정할 것인가? 앞서 살펴본 개인정보 개념에 대한 정의규정은 이 문제에 대하여 어떠한 논리필연적 답을 내포하고 있지 않으므로, 학설과 판례가 첨예하게 대립하고 있다.

전자의 입장을 따를 경우 특정 정보의 개인정보 해당 여부는 정보처리자가 누구인지에 크게 좌우되지 않으므로 이를 객관설(objektive Theorie, objektiver Ansatz) 또는 절대적 식별가능성설(absolute Bestimmbarkeit)이라 하고, 후자의 입장을 따를 경우 어떤 정보처리자에게 개인정보인 것이 다른 정보처리자에게는 개인정보가 아닐 수도 있으므로 이를 상대설(relative Theorie, relativer Ansatz) 또는 상대적 식별가능성설(relative Bestimmbarkeit)이라고 한다. 독일에서 두 설의 대립은 주로 유동 IP주소의 개인정보성이라는 이슈를 둘러싸고 두드러지고 있으며, 이러한 논의는 현재까지 활발하게 진행되고 있다.

즉 ISP의 경우, 자신과 계약을 체결한 개인에 대하여 IP주소를 할당하고, 어떤 개인에게 어떤 주소를 할당하였는지에 대한 기록을 보유하고 있으므로 IP주소를 가지고 개인을 식별할 수 있다. 따라서 ISP에 대하여 유동 IP주소가 개인정보에 해당한다는 점에 관하여는 거의 이론이 없어 보이며, 이 점은 독일 연방헌법재판소 및 연방최고재판소에서도 여러 차례 확인된 바 있다[139]. 그러나 ISP 아닌 CP는 위와 같은 할당 관련 기록을 가지고 있지 아니한바,

[139] BVerG, U.v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08[=MMR 2010, 356], BGH, U.v. 12. 5. 2010 – I ZR 121/08[=MMR 2010, 565]; BGH, U.v. 13.1.2011–III ZR 146/10[=MMR 2011, 341]; Breyer, Personenbezug von IP–Adressen Internetnutzung und Datenschutz, ZD(2014), 400

이러한 경우 CP에 대한 IP주소의 취급이 문제되는 것이다.

(나) 관련 문제: 익명화 개념의 판단기준과 위법한 수단을 이용한 재식별가능성의 고려 여부

이와 별개로, 독일에서의 개인정보 개념 관련 논의에서 특징적인 사항으로, 익명화 개념에 대한 견해 대립이 개인식별성 개념과 별도의 차원에서 일부 존재하고 있다는 점을 언급하여 둔다. 즉, BDSG 제3조 제6항에 따르면, "익명화(Anonymisieren)란, 인적·물적 관계에 대한 개별 진술을 더 이상 식별할 수 없는 또는 단지 시간, 경비 및 노동력에 있어 불균형적인 과다한 비용의 소모를 통하여서만 식별하는 또는 식별할 수 있는 자연인에게 귀속될 수 있는 방법으로 개인정보를 변경하는 것"을 의미한다. 그러나 BDSG에는 이러한 익명화가 개인정보성을 배제한다는 명문의 규정은 존재하지 아니하며, 익명화 자체가 일부 맥락에서 법적 의무로 규정되어 있을 뿐이다. 그렇기 때문에 위 제3조 제6항에 규정된 바와 같은 익명화가 개인정보성을 배제하는지 여부에 관하여, 객관설 내부에서 견해 대립이 있다.

즉, 개인정보성을 배제하기 위하여 제3조 제6항의 익명화 즉 과다한 비용 소모가 있어야만 재식별이 가능한 상태면 충분한 것인지 아니면 비용의 다과와 상관 없이 절대적으로 재식별이 불가능하여야 하는지가 다투어지고 있는 것이다.

또한, 식별가능성을 판단함에 있어, 어떤 정보가 그 자체만으로는 개인식별이 불가능하고 식별을 위하여 추가정보의 입수가 필요한 경우, 처리자 또는 제3자가 위법한 수단으로 이를 입수할 수 있다는 가능성이 식별가능성 판단에 고려되어야 할 것인가라는 쟁점도 존재한다. 즉, 추가 정보의 입수 수단으로서 적법한 수단만 고려하여야 할지, 위법한 수단도 고려하여야 할지의 문제이다. 객관설을 취하는 입장들은 대개 위법한 수단도 고려하여야 한다는

입장인 것으로 보이나, 상대설을 취하는 입장 중에서는 대립이 있는 것으로 파악된다.

이하에서는 이러한 쟁점들을 염두에 두고, 관련한 학설과 판례, 규제기관의 입장을 검토해 보겠다.

(다) 학설

(1) 객관설

가) 객관설 개요

이 학설은 주로 규제기관 종사자들에게서 많이 발견된다[140]. 객관설의 가장 대표적인 논거는 바로 유럽연합 개인정보보호지침 고려이유 26이다. 즉, 여기에 따르면, 식별가능성은 "통제자나 제3자에 의하여 그 사람을 식별하기 위하여 합리적으로 사용될 수 있는 모든 수단"을 고려하여야 하므로, 특정 통제자와 같이 제한된 자의 시점에서 식별가능성을 판단하여서는 안되고, 제3자의 관점도 두루 검토하여야 하는바, 그러할 경우 어떤 정보의 식별가능성은 그것을 처리하는 사람마다 달라지는 것이 아니고, 언제나 일정하게 평가되어야 한다는 것이다[141].

---

[140] 객관설을 주장하는 논자 중 Weichert는 2015년까지 슐레스비히-홀스타인 주의 정보보호 담당관이었고, Schaar는 함부르크의 정보보호 담당관이었다. Brink는 2016. 10. 현재 라인란트 팔츠 주의 정보보호담당관청에서 근무하고 있다.

[141] Pahlen-Brandt, Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um "Personenbezogene Daten", DuD(2008), vol.1, s.34 ff.; Schild, Beck'scher Online-Kommentar Datenschutzrecht, Wolff/Brink 14. Edition(2015), §3, Rn.19~21; Schaar, Datenschutz im Internet-Die Grundlagen, Verlag C.H.Beck, 2002; Forgó, Krügel, "Der Personenbezug von Geodaten - Cui bono, wenn alles bestimmbar ist?", MMR(2010), 17; Breyer, Personenbezug von IP-Adressen Internetnutzung und Datenschutz, ZD(2014), 400; Karg, "IP-Adressen sind personenbezogene Verkehrsdaten",

객관설은 또한, 상대설과 같이 개별적·구체적 사정을 고려하여 개인정보를 처리하는 자가 누구인지에 따라 개인정보 개념이 달라진다면, 동일한 정보에 대하여도 누가 처리를 하느냐에 따라(처리자의 재정적·기술적 능력에 따라) 개인정보 해당 여부가 달라지고[142], 심지어 동일한 처리자가 처리를 한다고 하더라도 그가 정보를 저장만 하고 있는지 전송을 하고 있는지에 따라 개인정보 여부가 달라질 수도 있기 때문에[143] 법적 안정성을 저해하는 결과가 발생한다고 본다.

정보주체의 보호 또한 객관설이 주장하는 중요한 근거이다. 구체적으로, (i) 개별 상황에 관하여 가장 잘 아는 것이 개인정보처리자 자신이고 규제기관도 이를 정확히 알기 어려우므로 개인정보 여부를 판단함에 있어 개별 상황을 일일이 고려하여야 한다면, 결국 개인정보 여부를 개인정보처리자가 자의적으로 결정함으로써 정보주체의 개인정보자기결정권을 침해하게 되며, 더욱이 정보자기결정권 침해는 정보주체가 알 수 없는 사이에 발생하는데, 식별가능성을 상대적으로 평가하게 되면, 침해의 결과가 발생하였다 하더라도 정보주체가 그 결과를 어떤 침해행위와 관련짓기가 어려우므로 정보주체의 보호가 소홀해지기 쉽다는 견해[144], (ii) BDSG의 목적은 오로지 개인정보의 보호인데, 상대설은 정보의 경제적 이용가능성까지 고려하므로 BDSG의 취지에 맞지 않는다는 견해[145], (iii) 인구조사판결에서 설시된 바와

MMR-Aktuell, 2011, 315811

[142] Schild(주141); Forgó, Krügel(주141); Breyer(주141), Karg(주141).

[143] Breyer(주141), 404

[144] Pahlen-Brandt(주141), s.37

[145] Brink, in Brink/Eckhardt, Wann ist ein Datum ein personenbezogenes Datum?, ZD(2015), 1

같이 정보자기결정권은 개별 사실관계에서의 구체적 침해로부터 개인을 보호하는 것을 넘어 식별에 따르는 두려움으로 인하여 인격의 자유로운 발현이 제약되는 것을 막기 위한 권리이고, 이러한 효과는 특정한 개별 정보처리보다는 제3자 및 공공 일반으로부터 오는 것이므로, 개인정보 개념을 획정할 때에도 제3자의 관점까지 광범위하게 고려하여야 하며, 상대설을 취할 경우 정보자기결정권의 의미를 개별 구체적인 침해에 관한 것으로 축소하는 것이 되므로 인구조사판결의 취지에 맞지 않는다는 견해[146] 등이 있다.

그 밖에, 정보를 처리하는 주체가 누구인지, 그가 어떤 의도를 가지고 있는지, 실제로 식별 가능한지와 무관하게 구체적 사안에서의 객관적 귀속가능성을 중심으로 개인관련성을 결정하여야 하는데, 제3자가 귀속을 위한 추가지식을 가지고 있고 이것이 처리자에게 알려질 가능성을 배제할 수 없다면 개인관련성을 인정하여야 함을 전제로, 현대에는 인터넷에 의하여 정보의 공간적 제한이 더 이상 존재하지 않으므로, 처리자가 접근 가능한 누군가가 귀속가능성을 가지고 있다면 개인정보성을 인정하여야 한다고 보는 견해가 있다. 얼핏 상대설의 입장 같지만 결론에 있어서는 절대설과 상통한다. 이 견해에 따르면, 개인관련성은, 오늘날 아직 익명으로 간주되는 정보가 미래의 평가 능력이 발전함에 따라 식별 가능하게 될 수 있다는 점에서만 상대적일 수 있다는 것이다[147].

한편, 유럽연합 지침 고려이유 26, 법적 안정성 등을 이유로 기본적으로 객관설적 접근을 지지하는 견해 중에서는, 정보처리가

---

[146] Brink, in Brink/Eckhardt(주145); Breyer(주141)

[147] Weichert, Geodaten-datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, DuD(2009), 347; Weichert, Der Personenbezug von Geodaten, DuD(2007), 113

“폐쇄된 네트워크”, 즉 기술적 및 계약적 보호조치에 따라 보안이 잘 이루어져서 외부의 제3자가 접근 불가능한 네트워크에서 일어나는 경우에는 상대설에 입각하여야 한다고 보는 견해도 존재한다[148]. 이 설은 스스로 절충설이라고 보나, 기본적인 전제가 객관설에 입각하여 있기 때문에 본고에서는 객관설로 분류하였다.

나) 위법수단의 고려

그 자체로는 개인을 식별할 수 없으나 다른 추가적 정보와 결합할 경우 개인을 식별할 수 있는 정보의 식별가능성과 관련하여, 그 결합되는 추가적 정보가 합법적인 수단으로 입수할 수 있는 것이어야 하는지, 위법한 수단으로만 입수할 수 있는 것도 고려할 수 있는지의 문제이다. 필자가 검토한 범위 내에서는, 객관설 문헌 중 이 문제에 관하여 언급한 것은 전부 위법한 수단으로 입수할 수 있는 정보도 고려하여야 한다고 본다[149].

그 근거로는, i) 유럽 개인정보보호지침, BDSG 제3조 제1호, 제3조 제6호 어떤 것도 적법한 수단만을 고려하여야 한다고 명시하고 있지 않다는 점, 구체적으로는 제3조 제6호가 익명화 여부를 판단함에 있어 시간, 경비, 노동력 등의 비용 요소만을 고려하였을 뿐 합법성 여부는 고려하고 있지 않다는 점[150]과 ii) 적법한 수단만 고려할 경우, 예컨대 IP주소를 수집하는 웹사이트 운영자의 경우

---

148 Forgó/Krügel(주141)

149 Weichert(주147, 2007), 115; Schaar(주141), Rn. 158~160; Breyer(주141); Pahlen-Brandt(주141)의 경우 이 문제에 관하여 명시적으로 언급하고 있지 않으나 뒤에서 다시 언급하듯이 결합 자체가 물리적으로 거의 불가능한 경우가 아닌 한 식별가능성을 인정하는 입장인 점에 비추어 볼 때 당연히 위법수단 고려설을 전제하고 있다고 이해된다.

150 Breyer(주141), 405

자신이 인터넷 접속 서비스 제공자로부터 IP주소를 이용한 식별에 필요한 정보를 제공받을 합법적 방법이 없다는 이유로 IP주소를 제한 없이 사용하거나 제3자에게 제공할 수 있게 되나, 다른 제3자가 이를 가지고 개인을 식별할 가능성을 배제할 수 없다는 점[151], iii) 이와 같은 맥락에서, 만일 합법수단만 고려하게 된다면, 가명화된 정보가 사용되고 제공되는지 여부와 그 방법에 관하여 정보주체가 통제할 수 없어지므로 정보주체의 개인정보자기결정권이 침해될 우려가 있다는 점[152] 등이 꼽히고 있다.

다) 절대적 익명화설과 상대적 익명화설

절대적 익명화설을 가장 뚜렷하게 지지하는 논자는 팔렌-브란트이다. 이 학설에 따르면, BDSG상 식별가능성을 부정할 수 있는 익명화란, 정보처리자의 관점에서 정보의 가치에 비하여 과도한 비용과 노력이 들어간다는 의미의 사실적 익명화가 아니라, 현존하는 기술수단을 사용할 때 재식별이 거의 불가능한 수준의 익명화 즉 절대적 익명화를 의미한다고 한다. 유럽연합 개인정보보지침이 '익명화' 개념을 정의하고 있지 않고, 고려이유 26이 익명화에 관하여 '정보주체를 더 이상 식별 가능하지 않은 것'이라고 규정하고 있을 뿐 정보처리자가 재식별을 위하여 투입하여야 하는 노력을 고려하라고 규정하고 있지 않은 점을 그 근거로 하고 있다[153].

---

[151] Scharr(주141), Rn. 174

[152] Breyer(주141), 405

[153] Pahlen-Brandt(주141), s.38. 물론 앞서 객관설의 근거로 인용하였던 근거들 또한 절대적 익명화설을 뒷받침하는 논거로 사용하고 있다. 여기서는 '절대적 익명화설'에만 특유하게 적용되는 논거만을 언급하였다.

샤(Schaar) 또한 절대적 익명화설을 취하고 있는 것으로 보인다. 즉, 완전한 익명 정보(vollständig anonyme Daten)과 사실적 익명성(faktische Anonymität)을 구별하여 양자를 다르게 취급한다. 즉, 모든 상정 가능한 경우 하에서 제3자가 정보를 개인에게 귀속시키는 것이 불가능한 경우가 되어야 개인관련성이 탈각된다는 것이다. 인터넷 환경 하에서는 이러한 완전한 익명화를 하는 것이 매우 어려우나 모든 식별정보(Bestimmungsdaten, 예컨대 식별자(Kennungen)과 IP주소 같은 것을 의미한다)와 추가 정보를 사용하여 재식별화를 가능하게 하는 정보가 로그 기록으로부터 삭제된 경우에는 익명화가 가능하다고 한다[154].

반면 상대적 익명화설을 취하는 견해들도 있다. BDSG 제3항 제6호에 규정된 바와같이, 재식별에 소요되는 지출이 재식별로 인하여 얻을 수 있는 결과에 대하여 비례적인지 여부를 평가함으로써 익명화 여부를 판단하고, 이것이 BDSG의 적용 여부를 판단하는 기준이 된다는 것이다. 단, 이 때 그러한 판단은 정보처리자 외에 제3자를 기준으로서도 하여야 할 것이다[155].

(2) 상대설

가) 상대설의 기본 입장

상대설이란, 정보의 개인식별가능성 여부를 판단하기 위하여 정보를 저장하고 있는 자 또는 처리하고 있는 자의 관점에서만 판단하는

---

[154] Schaar(주141), Rn. 158~160

[155] Weichert(주147, 2009), 347; Weichert(주147, 2007), 113; Forgó/Krügel(주141), 18~19; Specht/Müller-Riemenschneider, Dynamische IP-Adressen: PErsonbezogene Daten für den Webseitenbetreiber? Aktueller Stand der Diskussion um den Personenbezug, ZD(2014), 71

견해이다. 독일의 학설 중에서는 상대설이 다수설이다[156]. 상대설 중에서는 위법한 수단을 이용하여 식별에 필요한 추가 정보를 수집할 수 있는 경우를 식별가능성 판단에 고려하여야 한다는 설과 고려하여서는 안된다는 설이 있는데, 전자가 다수설인 것으로 보인다.

상대설을 가장 체계적으로 서술하고 있는 논자는 마이어디어크스(Meyerdierks)이므로, 이하에서는 마이어디어크스의 논문[157]을 중심으로 하되, 다른 논자들의 주장을 보완해 가며 상대설의 근거 및 내용을 살펴 보겠다.

첫째, 앞서 살펴본 바와 같은 BDSG 제3조 제6호의 익명화 규정이다. 위 조항이 익명화 개념과 관련하여 '인적 또는 물적 관계에 대한 개별진술을 더 이상 또는 단지 시간, 경비 및 노동력에 있어 과다한 비용의 지출을 통하여서만 특정한 또는 특정 가능한 자연인에게 귀속될 수 있는 방법으로 개인정보를 변경하는 것' 이라 정의하고 있다는 점은 앞서 살펴보았다. 이들 견해는 이 조항의 익명화가 개인정보성을 배척하는 것이라고 본다. 그러므로 식별이 절대적으로 불가능한 경우는 물론 시간, 경비 및 노동력에 있어 과다한 비용의 지출이 필요한 경우에도 익명화가 인정되며, 따라서 식별을 위하여 시간, 경비 및 노동력에 있어 과다한 비용의 지출이 필요한 정보라면 이는 개인정보가 아니라는 입장이다. 과다함 여부가 바로 유럽연합 개인정보보호지침 고려이유 26이 말하는 '합리성' 판단과 일치한다. 이러한 과다함 여부 또는 합리성 유무는 당연히 개별 사안별로 판단하여야 하는데, 그렇다면 정보처리자와 상관 없는 제3자의 관점은 고려할 여지가 없다고

---

[156] Hoeren/Sieber/Holznagel, Multimedia-Recht, C.H.Beck, 2015 Rn. 103

[157] Meyerdirks, "Sind IP-Adressen personenbezogene Daten?", MMR, 2009, 8

한다[158].

이러한 '과다한 비용의 지출' 여부는, 결국 비용과 정보가치의 형량에 의하여 판단된다고 한다. 정보를 가지고 개인을 식별함으로써 얻을 수 있는 이익과 식별에 소요되는 비용 사이의 비례관계, 즉 정보가치에 비하여 개인식별에 드는 비용이 과다한지 여부를 심사한다는 것이다[159]. 이 중 비용과 관련하여서는 식별을 위하여 사용될 수 있는 모든 시간, 금전, 노하우, 노동력 등을 고려하여야 하는데, 동기의 측면, 즉 식별에 관한 이해관계(Interesse), 그리고 저장기간이 얼마나 장기인지(Dauer der Aufbewahrungsfrist)도 고려하여야 한다고 한다(저장기간이 길수록 식별가능성이 높아진다)[160]. 이와 같은 기준을 취할 때, 정보를 처리하는 자가 암호화된 정보의 재식별을 위한 키를 가지고 있더라도, 제3자가 그러한 키를 보유하고 있지 않다면 그러한 정보는 제3자와의 관계에서 개인정보가 아닐 수 있다고 보게 된다[161].

둘째, BDSG 제30조 제1항은 "개인정보가 이를 익명화된

---

[158] Meyerdirks(주157), 10; 同旨, Dammann, in Simitis[Hrsg.], §3 Rn. 310; Gola/Schomerus(주106), §3 Rn. 44a; 한편 상대설은 개인정보보호지침 고려이유 26이 제3자의 식별가능성에 대해서도 명시하고 있는 것과 일견 모순되는데, 이 점에 관하여 골라는 위 고려이유가 '제3자'의 식별가능성을 언급하고 있으나, 개인정보를 처리하는 자와 제3자가 보유하는 정보가 서로 결합될 가능성이 있는 경우에 한하여 제3자의 식별가능성을 고려한다는 취지로 해석한다.

[159] Gola/Schomerus(주106), §3 Rn. 44; Tinnefeld, in Roßnagel[Hrsg.](주134), 4.1. Rn.24

[160] Lundevall-Unger/Tranvik, "Was sind personenbezogene Daten? Die Kontroverse um IP-Adressen", ZD-Aktuell 2012, 03004

[161] Tinnefeld, in Roßnagel[Hrsg.](주134), 4.1. Rn.24

형식으로(in anonymisierter Form) 전송하기 위하여 업무적합하게 수집되고 저장되었다면, 인적 또는 물적 관계에 대한 개별 진술이 그와 함께 식별된 또는 식별 가능한 자연인에게 귀속될 수 있는 표식들은 분리되어 저장되어야 한다. 이러한 표식들은 저장목적의 실행을 위하여 또는 학문적 목적을 위하여 요구되는 범위에서만 개별진술과 결합될 수 있다(zusammenführen)." 고 규정하고 있다. 마이어디어크스와 담만에 따르면, 이러한 조항은 정보를 전송하는 자가 자신은 개인식별이 가능하지만 전송받는 자에게는 식별이 불가능한 형태를 예정하고 있으므로, BDSG상 상대설을 인정하는 근거가 될 수 있다고 한다[162].

셋째, 마이어디어크스에 따르면, 만일 어디인가에 개인을 식별할 수 있게 하는 추가정보가 있다는 이유만으로 모든 정보가 개인정보가 된다면, 어떤 정보를 처리하는 주체는 자신이 모르는 사이에 그 정보에 관하여 개인정보보호법의 적용을 받게 되고, 더 나아가 만일 추가정보를 가지고 있는 제3자가 당해 정보를 보유하고 있으면 개인정보보호법의 적용을 받게 되고, 그 자가 그 정보를 자신도 모르는 사이에 삭제해 버리면 개인정보보호법의 적용을 받지 않는다는 이상한 결과가 발생하게 된다. 결국 개인정보보호법의 적용 범위를 모호하게 함으로써 법적 안정성을 저해하는 결과를 낳을 수 있다.[163]

넷째, 객관설을 지지하는 논자의 주된 근거는 상대설을 주장할 경우 정보주체 보호에 흠이 생긴다는 것이지만, 그런 사태는 발생하지 않는다는 것이다. 만일 처리자가 제3자로부터 추가정보를 임의로 입수하여 개인을 식별할 수 있게 되면 이는 "개인정보는

---

[162] Meyerdirks(주157), 10; Dammann, in Simitis[Hrsg.](주100), §3 Rn. 310

[163] Meyerdirks(주157), 10

관련당사자로부터 수집되어야 한다"는 BDSG 제4조 제2항에 반하는 결과가 되며, 제3자가 처리자로부터 정보를 수집하는 경우에도 마찬가지다. 또한 처리자가 제3자에게 자기가 보유하고 있는 정보를 전송하게 된다면 이것은 개인정보의 제공에 해당하므로 법이 규정하는 적법요건이 요구된다[164]. 기타 민법상 부작위의무 등에 의한 제재가 가능하기도 하다[165].

한편 이와 관련하여, 처리자가 제3자에게 그 자체로는 개인 식별이 불가능한 개인에 관련된 어떤 정보를 전송할 때, 그러한 행위가 개인정보의 전송인지 여부는 제3자가 보유하고 있거나 입수할 수 있는 추가적 정보가 어떤 것인가에 따라 달라질 것이므로, 정보를 전송하는 자에게 당해 전송행위가 BDSG 제28조 및 제29조의 요건을 충족하고 있는지 여부를 결정할 의무가 있다고 보는 견해가 있다[166]. 즉, 이러한 정보 전송의 경우 사후적으로 개인식별이 가능하다는 점이 밝혀지면 정보를 전송하는 자가 BDSG 위반의 책임을 진다는 것이다. 그렇다면, 위 '의무'라는 것은 충분한 주의를 기울이면 면할 수 있는 주관적 주의의무인가 아니면 재식별의 결과에 대하여 주관적 귀책사유 유무와 관계 없이 부과되는 결과책임인가? 만일 주관적 주의의무라면 그 내용은 무엇이 되어야 하는가?

골라/쇼메루스의 경우 이 부분에 대한 태도가 분명치 아니하나, 담만은 이 경우 정보 전송자가 지는 책임은 일종의 결과책임이라고 보는 듯하다. 즉, 정보를 전송하는 자 입장에서는 그 전송행위가 개인정보의 전송인지 여부를 확실히 알 수 없다. 그럼에도 불구하고

---

[164] 同旨, Gola/Schomerus(주106), §3 Rn. 44a; Dammann, in Simitis[Hrsg.](주100), §3 Rn. 31

[165] Meyerdirks(주157), 11~12

[166] Gola/Schomerus(주106), §3 Rn. 44a

정보를 전송하였으나 재식별의 위험이 실현된다면, BDSG상 전송에 필요한 요건을 갖추지 못하였다면 이는 개인정보의 위법한 전송이 된다. 그러나 이 부분에 관하여 법은 "허용된 위험을 알지 못"하고, 따라서 정보를 전송하는 시점에서 합리적인 수단으로는 식별이 불가능해 보인다는 사정이 있다고 하여 전송자가 법위반의 책임을 면할 수 없으며, 더욱이 전송 당시 전송으로 인하여 발생하는 재식별 위험을 주의 깊게 심사하였더라도 재식별 가능성을 알지 못하였을 것이라는 점이 인정되더라도 그러하다는 것이다(물론 이 경우 형사법적 의미에서의 고의는 없어질 것이라고 한다). 그러므로 사실상 정보를 전송하는 사람은, 그 정보가 개인정보인 것처럼 취급하지 않을 수 없다고 본다[167].

다섯째, 체계적 해석에 따르더라도, BDSG의 여러 규정들은 처리자가 정보주체의 신원을 알고 있음을 전제로 짜여져 있으므로 상대설이 타당하다고 한다[168]. 예컨대 정보주체의 열람권 같은 경우 처리자가 정보주체를 모르면 이를 이행할 수 없다. 또한, 개인정보 자기결정권에 기하여 인터넷 접속 시점이 지나면 IP주소를 저장하지 말라는 민법상 청구가 있다고 가정할 경우, 상대설에 따를 경우 어차피 개인정보가 아니기 때문에 원고의 청구를 받아들일 수 없을 것이지만, 객관설에 따라 유동 IP 주소가 개인정보라고 보더라도 피고가 부작위 청구의 대상이 되는 행위를 특정할 수 없기 때문에 어차피 원고의 청구는 수용될 수 없다고 한다. 즉, 당해 행위를 특정하기 위하여서는 당해 원고가 언제 인터넷 접속을 하였다는 점을 특정 가능하여야 하는데 그러기 위하여서는 ISP에게 관련 정보를 요구하여야 하고, ISP는 형법 등에 의하여 그러한 정보를 제3자에게 제공하는 것이 금지되어 있으므로 결국은

---

[167] Dammann, in Simitis[Hrsg](주100), §3 Rn. 38

[168] Meyerdirks(주157), 12~13

부작위의 대상이 되는 행위를 특정하는 것이 법률적 불능 상태에 있게 된다는 것이다.

이러한 상대설의 입장에서는, 객관설을 위할 경우 오로지 절대적 익명화가 있어야만 개인정보성을 탈각할 수 있는데, 이러한 절대적 익명화는 현실적으로 불가능하므로 절대적 익명화를 전제하는 것은 현실적이지 않다[169]. 이로 인하여 모든 정보가 개인정보에 해당하는 결과가 되는바, 이는 개인식별 가능한 정보에 한하여 개인정보로 보는 정보자기결정권의 취지에도 맞지 않는다고 본다. 이와 같이 보지 않으려면, 제3자의 정보를 제한적인 범위에서만 고려하여야 하는데, 객관설은 그 기준을 어떻게 세워야 할지에 대하여 아무런 답을 주지 않는다. 그러므로 오히려 상대설보다 객관설이 법적 안정성을 저해한다. 상대설의 경우 적어도 처리자 스스로는 식별가능성 여부를 평가할 수 있기 때문이다[170]. 객관설의 입장을 따르는 것이 정보주체의 보호에 오히려 불리하다는 견해도 있다. 즉, 절대적 익명화를 요구할 경우, 어떠한 조치를 하더라도 개인정보성을 탈각하기 어려우므로, 암호화와 가명화 같은 조치의 유인이 없어지고, 따라서 결과적으로 개인정보 보호에 소홀해지게 된다는 것이다[171].

나) 합리성 유무의 판단에 위법한 수단의 사용 가능성도 고려할 것인가

대부분의 상대설적 견해들은, 위법한 수단을 사용하여 정보를

---

[169] Härting, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2005

[170] Eckhardt, in Brink/Eckhardt(주145), 2

[171] Kirchberg-Lennartz/ Weber, "Ist die IP-Adresse ein personenbezogenes Datum?", DuD 7/2010 p.480

식별하는 것은 합리적이지 않고, 일반적으로 정보 식별을 위하여 과다한 비용을 발생시킬 것이므로, 그러한 수단의 사용은 식별가능성의 평가에는 고려되어서는 안된다는 입장이다 [172] . 여기에 따르면, 객관설은 개인의 보호를 명목으로 위법한 수단까지 고려하여야 한다고 주장하나, 어떤 수단을 이용한 식별이 위법하다면, 그것으로 이미 충분한 법률적 보호가 주어진 것이고[173], 어차피 객관설 주장과 같이 개인정보보호법을 적용하더라도 법에 위반하는 행위를 막을 수는 없기 때문에 의미가 없다고 한다[174].

반면 일률적으로 위법한 수단의 사용 가능성을 배제할 것은 아니고, 원칙적으로는 위법한 수단은 합리적이지 않은 수단으로서 식별가능성 판단에서 배제되어야 하나, 그러한 수단의 사용을 막는 규범이 현실적으로 관철 가능한지 여부를 고려하여야 한다고 보는 견해도 있다. 여기에 따르면, 개인의 식별을 금지하는 법률 규정은 물론 계약 조항의 존재도 '합리성'의 존재를 배제하는 근거가 될 수 있으나, 예컨대 문제의 계약이 일방이 소급적으로 취소 가능한 것이라거나, 실질적으로 금지된 정보의 거래가 활발하게 이루어지는 암시장이 존재하는 등의 사유가 있다면, 그러한 경우에는 개인정보성 판단에 있어 위법한 수단을 사용하여 개인을 식별할 수 있는 가능성을 고려하지 않을 수 없다는 것이다[175].

---

[172] Meyerdirks(주157), 12; Krüger/Maucher, 전게 논문, 438; Eckhardt in Brink/Eckhardt, 전게 논문, 2; Kirchberg-Lennartz/ Weber, 전게 논문, 480; Lundevall-Unger/Tranvik, 03004

[173] Krüger/Maucher(주134), 438

[174] Eckhardt, in Brink/Eckhardt(주145), 2

[175] Dammann, in Simitis[Hrsg.](주100), §3 Rn. 26~31

(라) 판례

(1) 객관설을 지지하는 판결들

대표적인 것이 베를린 중부 시법원(Amtsgericht Berlin-Mitte)의 2007년 3월 27일자 판결[176]이다. 이것이 앞서 살펴본 CJEU의 *Patrik Breyer v. Bundesrepublik Deutschland(Case C-582/14)* 판결의 발단이 된 사건이다.

즉, 원고 파트릭 브라이어(Patrik Breyer)는 일반적으로 접근 가능한 사이트인 독일 법무부 홈페이지의 사용자였다. 피고 독일은 위 홈페이지에 방문하는 이용자에 관한 정보를 프로토콜 데이터에 저장하고 있었는데, 저장되는 정보는 요청된 정보의 이름(사이트), 이용자가 입력한 검색어, 요청일시, 전송된 정보량, 요청이 성공적이었는지에 대한 보고, 접근하는 호스트 시스템의 IP주소였다. 독일 TMG 제15조는 서비스 제공자는 사용자의 개인정보는 오로지 텔레미디어 서비스의 사용 및 요금 정산을 위하여 필요한 한에서만 수집하고 사용할 수 있다고 규정하고 있었는데, 위 정보들은 개인정보에 해당하므로, 피고 독일이 위 정보들을 사이트의 개별 접속이 종료한 후에도(접속 종료 후 14일간) 저장하고 있는 것이 위 조항에 위반된다는 것이 원고의 주장 요지였다(원고는 이를 근거로 개인정보를 저장하지 말라는 부작위를 구하였다).

법원은 웹사이트 운영자는 유동 IP가 있으면 제3자의 도움을 받아 어렵지 않게 개인을 식별할 수 있으며, 만일 이를 개인정보로 보지 않으면 웹사이트 운영자가 이를 임의로 ISP에게 제공하여 식별 가능한 상태로 만들 수 있기 때문에 개인정보로 보아야 한다고 하였다[177]. 이 판결은 항소되었고, 이 쟁점은 뒤에서 살펴보는

[176] AG Berlin-Mitte, 27.03.2007 - 5 C 314/06

[177] time.lex CVBA, Study of case law on the circumstances in which IP

베를린 지방법원(Landgericht Berlin)의 2013. 3. 1.자 판결에서 판단되었다.

비스바덴 주 행정법원(Verwaltungsgericht Wiesbaden)도 2009. 2. 27.자 판결에서 유럽사법재판소의 Promusicae/Telefonica(Case C-275/06)의 법무담당관 의견서와 WP29의 2005. 1. 18.자 의견서(WP104) 및 2008. 5. 14.자 의견서(WP 150)를 원용하며 유사한 결론을 도출하였다[178].

2) 상대설을 지지하는 판결들

뮌헨 시법원((Amtsgericht München)은 2008.9.30.자 판결[179]에서, 원고가 웹사이트 운영자인 피고에 대하여 개별 인터넷 접속 종료 후에는 원고의 IP주소를 저장하지 않도록 부작위 청구를 한 사안에서, 정보를 저장하는 주체(datenspeichernde Stelle)가 개별 정보 뒤에 있는 개인을, 그가 통상 처분 가능한 지식과 수단을 사용하여, 과도한 노력(unverhältnismässigne Aufwand)을 들이지 않고 식별할 수 있을 때 식별가능성이 있다고 전제한 뒤, 피고는 오로지 ISP의 도움을 받아서만 사용자를 알아낼 수 있는데 ISP는 법적인 근거 없이는 피고에게 사용자 식별에 필요한 정보를 주어서는 아니되고, 이에 반하여 ISP가 불법적으로 정보를 넘김으로써 식별이 가능해지는 것은 식별가능성 개념에서 배제되어야 한다는 입장을 취하였다. 그러한 불법적 취급은 정상적인 것이 아니며 상당한 노력을 발생시키는 방법으로 보아야 하기 때문이다.

베를린 지방법원(Landesgericht Berlin)의 2013. 1. 31.자

---

addresses are considered personal data D3. Final Report(2011), p.124

[178] time.lex CVBA(주177), pp.142~142, Krüger/Maucher(주134), 433

[179] AG München, BeckRS2008, 23037

판결[180]은 앞서 살펴본 베를린 중부 시법원 판결에 대한 항소심으로, 상대설의 입장에서 이 이슈에 관하여 한층 더 상세하게 논하고 있다.

법원은, 이른바 객관설에 따를 경우 식별가능성 판단에 있어 거의 세계 전체에 존재하는 지식(gesamte Weltwissen)을 고려하여야 하므로, 보호대상이 되는 정보의 경계가 비실제적으로 확장된다고 절대설을 비판한다. 구체적으로, 객관설은 개인관련성이 있을 가능성이 이론적으로라도 인정되면 식별성을 인정하나, 순수하게 이론적인 식별가능성이 있다고 하여 정보자기결정권의 보호를 부여한다는 것은 설득력이 없고, 개인의 보호가치 있는 이익과도 무관할 뿐 아니라, 이론적으로만 식별 가능한 것은 사실상 식별가능하지 않다고 보아야 한다는 것이다. 또한 객관설은 큰 노력 없이(ohne grosse Aufwand) 정보의 결합이 가능하면 개인관련성을 인정하나, 이러한 경우 노력은 오로지 기술적인 관점에서만 본 노력이기 때문에, 결합과 관련하여 존재하는 법률적 장애물을 간과하는 결과를 낳는다고 한다.

법원은 객관설에 대한 이러한 비판에 기초하여 상대설을 명시적으로 지지한다. 즉 구체적 처리주체에게 개인의 식별이 기술적으로는 물론 법률적으로도 가능하여야 하고, 식별을 위하여 정보처리자에 대하여 정보의 사용과 과도하지 않은 노력이 요구되지 않아야만 식별가능성을 인정할 수 있다는 것이다. 즉 식별의 실제적 가능성(praktisch bestimmbar) 또는 문제의 정보와 추가적 지식 간의 실제적 결합가능성 또는 쉽고 직접적인 결합가능성(eine leichete und direkte Möglichkeit, die Daten zu verknüpfen)을 판단 기준으로 삼아야 한다는 입장을 취하였다.

이러한 가능성을 판단하기 위하여서는 개별사안에서 정보보호가

[180] LG Berlin, ZD(2013), 618

필요한지, 필요하다면 그 범위는 어떠해야 할지에 관한 형량이 필요한데, 형량에 있어 고려할 사항으로 법원이 제시한 내용은 다음과 같다:

i) 처리자가 추가적 정보에 도달하기 전에 어떠한 장애물이 존재하는가ii) 남용 시나리오가 문제되는가, 문제된다면 어떤 것인가 iii) 원고의 보호가, 원고가 요구하는 포괄적인 정보보호 없이도 충분한가
iv) 인터넷에서의 범죄행위에 대한 형사소추에 대한 사회적 요구가 인터넷에서의 익명성에 대한 요구라는 관점에서의 원고의 보호와의 관계에서 어떻게 평가되어야 하는가
v) 사실상 관련 없는 인터넷 서비스 계약자(Anschlussinhaber)가 지명될(ermittelt wird) 위험이 얼마나 큰가

이를 적용하여, 법원은 유동 IP주소에 관하여 다음과 같이 판시하였다:

i) 유동 IP주소가 서버 접근시점 없이 단독으로 저장되는 경우에는 이것과 정보주체 사이의 관련을 찾아내는 것이 기술적으로 불가능하므로 그러한 유동 IP주소는 개인정보가 아니다.

ii) 유동 IP주소가 서버 접근시점과 함께 저장되는 경우라 하더라도 이용자가 웹사이트의 입력 양식 등에 실명이나 이메일 주소 등을 제출하는 등 웹사이트 운영자에게 이용자 식별이 기술적 및 법률적으로 가능한 경우에 한하여 유동 IP주소는 개인정보가 될 수 있다.

iii) 수사 또는 형사절차 또는 저작권법 제101조에 따른 정보의 제공 절차 [181] 에서, 이러한 절차가 아니었더라면 개인정보가

[181] 우리 저작권법 제129조의 2에 해당함

아니었을 정보에 관하여 개인관련성이 생성되는 것으로 인하여 그 정보가 그 자체로서 이미 개인정보라고 보아야 한다는 결론을 내릴 수 없다. 즉, ISP가 보유하고 있는 IP주소로부터 개인을 식별하기 위하여 필요한 정보는 위와 같은 경우가 아니면 제3자에게 제공될 수 없으므로, 위와 같은 절차를 통하여 웹사이트 운영자가 보유하고 있는 유동 IP주소를 ISP가 보유하고 있는 정보와 결합하여 개인을 식별할 수 있게 되더라도, 이를 이유로 웹사이트 운영자가 보유하고 있는 유동 IP가 개인정보라고 단정할 수 없다는 것이다. 이러한 경우는 앞서 언급한 바와 같이 결합의 법률적 가능성이 차단된 것으로 보아야 한다고 한다. CJEU가 이러한 논리를 배척하였다는 점은, 앞서 Breyer 판결을 검토하며 살펴본 바와 같다.

iv) 앞의 ii)에서 본 바와 같이 유동 IP주소를 개인정보를 만들 수 있는 추가적 정보와 관련하여, 처리자가 그러한 정보와 IP주소를 분리하여 수집, 저장 및 처리한다고 해서 유동 IP가 개인정보에 해당하지 않게 되는 것은 아니다. 피고는 이러한 경우 개인정보가 아니라는 취지의 항변을 하였으나, 법원은 정보처리자의 서로 다른 부문에서 처리되더라도 두 종류의 정보는 모두 처리자의 처분 권한 안에 있으며, 처리자가 두 종류의 정보를 매칭할 것을 의욕하는지 여부는 고려대상이 아니라고 하며 이를 기각하였다.

원피고 모두 이 판결에 대하여 상고하였다. 이에 따라 독일 연방대법원(Bundesgerichtshof, BGH)는 2014. 10. 28. 유럽사법재판소에 대하여, "유럽연합 개인정보보호지침 제2조 a항이, 서비스 제공자(Dienstanbieter)가 그의 인터넷 사이트에의 접근과 관련하여 저장하는 IP주소가, 제3자(여기서는 ISP: Zugangsanbieter)가 정보주체를 식별하는 데 필요한 추가적 정보를 가지고 있는 경우, 서비스 제공자에 대하여 개인정보가 되는가"라는 문제에 관한 선결적 판결(preliminary ruling)을

구하였다[182]. 여기서 BGH 자신은 객관설과 상대설 중 어느 설을 명시적으로 지지하였다고 보기 어렵지만, "불법적인 행위는-무엇보다도 국가 기관(staatliche Stelle)들에 있어서는-정보 조달의 수단으로 보아서는 아니된다"고 판시한 점에 주목할 만하다. 이를 근거로 BGH가 상대설적 입장을 취한 것으로 보는 견해도 있으나[183], 판결의 다른 부분에서 상대설을 지지하는 언급을 명시적으로 하지 않은 것으로 보아, BGH가 명시적으로 상대설을 취하였다기보다 특히 법을 준수할 책임이 있는 국가기관의 경우 개인 식별에 있어 불법적 수단을 사용하는 것이 합리적이지 않다는 점을 강조한 데 그친다고 볼 수도 있을 듯하다.

기타 밤베르크 시법원, 프랑켄탈 주법원, 부퍼탈 주법원, 뒤셀도르프 행정법원, 뮌헨 고등법원, 함부르크 고등법원 등이 상대설적 견해를 채택하였다[184].

(마) 정보보호 감독기관들의 입장

독일의 정보보호 감독기관들은 반복하여 유동 IP가 개인정보에 해당한다는 입장을 밝힘으로써 객관설을 확고히 지지하고 있는 것으로 보인다.

예컨대 독일 연방 정보보호 및 정보자유담당관(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) [185] 은 2007년 및 2008년

[182] BGH, ZD 2015, 80 이하

[183] Bergt(주134), 367

[184] Bergt(주134), 364

[185] BfDI는 BDSG 재22조에 의하여 설치된 연방 기내무성 산하 기관이다. 연방의 공공부문에서 BDSG 및 정보보호 관련 다른 규정의 준수 여부를 통제하고(BDSG 제24조), 관련된 권고 및 협의를 수행한다(BDSG 제26조). 통신 및 우

활동보고서에서 고정 IP주소와 유동 IP주소를 구분하지 않고 모두 개인정보에 해당한다고 밝힌 바 있다[186].

연방 및 주의 개인정보보호 담당관 회의(die Konferenz der Datenschutzbeauftragten des Bundes und der Länder)[187]의 전문위원회인 '미디어 작업 그룹(Arbeitskreis Medien)'은 IP주소의 개인정보 해당성과 관련하여 명시적으로 이러한 입장을 취한 바 있다[188].

뒤셀도르프 그룹(Düsseldorfer Kreis)[189]도, 2009.11.26. IP주소가 CP에게도 개인정보임을 전제로 IP주소를 사용한 이용행태 분석은 정보주체의 동의 하에서만 허용될 수 있다고 결의하였다[190].

이들이 객관설을 지지하는 근거는 바로 개인정보의 실효적

편 영역 등에서는 민간 기업에 대해서도 관할을 가진다. http://www.bfdi.bund.de/DE/BfDI/Artikel_BFDI/AufgabenBFDI.html

[186] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, *22. Tätigkeitsbericht zum Datenschutz 2007 – 2008*, p.96 (2016. 10. 9. 확인) <http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/22TB_07_08.html?nn=5217212>

[187] 독일 연방 및 주의 개인정보보호 담당관들이 모여 개인정보 관련 이슈에 관하여 입장을 표명하는 협의체이다.

[188] Arbeitskreis Medien, *Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten*, 3.1. (2016. 10. 9. 확인) <https://www.datenschutz.hessen.de/_old_content/tb31/k25p03.htm>

[189] 뒤셀도르프 그룹은 위에 언급된 연방 및 주의 개인정보보호 담당관 회의의 전문위원회 중 하나이다. 여기서 독일의 개인정보보호 담당관들이 민간 영역의 개인정보 이슈에 대한 결의를 수시로 발행한다.

[190] Der Düsseldorfer Kreis, B*eschuluss des Düsseldorfer Kreises vom 27 Nov. 2009: Datenschutzkonforme Ausgestaltung von Analyseverfaren zur Reichweitenmessung bei Internet-Angeboten*, p.2

보호이다. 즉, 현대사회에서는 정보의 유통이 활발한데, 예컨대 IP주소와 같이 ISP가 보유하고 있는 자료에 기하여 식별이 가능한 정보가 ISP가 아닌 처리자에 대하여 개인정보가 아니라고 한다면, 그 처리자가 이를 임의로 ISP를 포함한 제3자에게 양도할 수 있게 되는바, 그 정보를 입수한 제3자가 자신이 보유하고 있는 정보를 사용하여 개인을 식별할 위험이 상존하게 되므로 개인의 기본권 보호에 공백이 생길 수 있다는 것이다[191].

마. 소결론

이상에서 살펴본 바와 같이 독일에서는 객관설과 상대설의 대립이 첨예하게 드러나고 있으며, 그 과정에서 각 설을 지지하거나 비판하는 논거가 풍부하게 제시되고 있다. 비록 유럽사법재판소의 판결에 의하여 이러한 논의들이 상당 부분 정리될 것으로 보이지만, 그럼에도 불구하고 독일의 논의는 아직 개인정보 개념에 관한 통일된 해석이 없는 우리나라의 논의에서 유용한 참고자료가 될 수 있을 것으로 보인다.

한편, 앞서 유럽연합의 경우에서 검토한, 키 코드화된 정보를 제공하는 행위가 개인정보의 제공에 해당하는지라는 논의와 같은 맥락에서, 개인정보처리자가 자신은 다른 추가적 정보와 결합하여 개인을 식별할 수 있으나, 정보 자체로는 개인을 식별할 수 없는 어떤 정보를 제3자에게 제공하는 경우의 취급에 관한 논의가 독일에도 존재한다. 여기에 대하여 많은 논의를 발견하지는 못하였지만, 정보를 전송하는 자가 이후 식별이 발생하였을 때 책임을 진다는 취지의 서술이 중요한 주석서들에서 발견되고 있다.

[191] Arbeitskreis Medien(주188), 3.1.; AG Berlin-Mitte v. 27.3.2007

4. 영국

가. 개인정보보호법의 규정

영국은 개인정보보호에 관한 일반법으로 개인정보보호법(Data Protection Act 1998, 이하 'DPA')을 두고 있다. 동법 제1조 (1)은 개인정보(personal data) 개념에 관하여 다음과 같이 정의하고 있다.

"개인정보"란 (a) 그 정보로부터 또는 (b) 그 정보(those information)와, 정보 통제자(data controller)가 점유하고 있거나 그의 점유에 들어올 가능성이 있는(likely to come into) 다른 정보(other information)로부터 식별될 수 있는 생존하는 개인에 관한 정보를 의미하고, 그 개인에 관한 의견의 표현과 정보통제자나 제3자가 그 개인에 관하여 가지고 있는 의도의 표시를 포함한다.

DPA상의 개인정보 개념 또한 WP29와 마찬가지로 1) 정보, 2) 관련성, 3) 개인의 식별 또는 식별가능성, 4) 생존하는 개인이라는 개념 요소를 포함하고 있다. 그러나 식별가능성에 관하여 앞서 살펴본 지침이나 독일법 규정과는 달리, '다른 정보' 즉 '추가지식(Zusatzwissen)'에 해당하는 것은 '정보 통제자 자신'이 점유하고 있거나 그의 점유에 들어올 가능성이 있는 것이어야 한다고 명시적으로 규정하고 있다. 이하에서 영국에서 관련성 요건 및 개인의 식별 또는 식별가능성 요건이 해석되는 방식에 관하여 간단히 살펴보도록 한다.

나. 관련성 요건의 해석

영국에서는 관련성 요건에 관하여 법원 및 규제기관에서 장기에 걸친 논의가 있었고, 그것이 앞서 살펴본 WP 29가 2007년 발표한

관련성 개념[192]과 유럽 사법재판소의 YS 판결의 논의에도 상당한 영향을 미쳤으므로 간단히 살펴 보기로 한다.

(1) *Durant* 판결

영국에서 관련성 개념에 관한 논의를 촉발시킨 것은 2003년의 이른바 *Durant* 판결[193]이다. 듀란트(Durant)라는 개인이 영국 재정청(Financial Services Authority, 'FSA')에 바클레이(Barclay) 은행에 대한 민원을 제기한 적이 있는데, 이후 FSA에 대하여 DPA 제7조의 정보주체의 개인정보 접근권에 기하여 해당 민원과 관련된 문서의 제출을 요구하였다. FSA는 관련 문서를 듀란트에게 제공하면서 그 내용을 일부 삭제(redact)하였는데, 그 이유는 해당 부분이 듀란트에 관한 정보를 포함하고 있지 않거나, 제3자의 성명 등 개인정보를 포함하고 있다는 것이었다. 듀란트는 삭제된 부분에 대하여도 열람청구를 하였으나 FSA가 이것을 거절하여 그 거절의 당부가 문제된 사안이다. 문제의 자료가 듀란트의 개인정보인지와 관련하여, 그 자료가 듀란트에 '관련한' 것인지 여부가 쟁점이 되었다.

사건을 심리한 잉글랜드 및 웨일스 항소법원 민사부(England and Wales Court of Appeal Civil Division)의 올드 판사(Lord Justice Auld)는 관련성을 부인하면서, DPA 제7조의 정보주체의 접근권은 개인이 그가 언급된 모든 정보에 접근할 수 있도록 하는 것은 아니며 정보주체가 통제자가 그의 개인정보를 적법하게 처리하고 있는지를 확인하여 필요한 경우 법적 절차를 밟을 수 있도록 하기 위한 것이라고 전제한 후, 정보가 개인의 프라이버시에 영향을 미칠 수 있어야 관련성을 인정할 수 있다고 판시하였다. 위 법원은 이를 판단하기 위한 구체적 기준으로 첫째, 문제의 정보가 관련 개인과

---

[192] WP 29(주73)

[193] Michael John Durant v. Financial Service Authority [2003] EWCA Civ 1946

중요한 의미에서 전기적 관련이 있어야 하고(biographical in significant sense), 둘째 문제의 개인이 정보의 초점에 있어야 한다(the information should the putative data subject as its focus)는 두 가지 요건을 제시하였다[194]. 이는 관련성 요건을 매우 제한적으로 해석한 판시이다[195].

(2) Durant 판결 이후 규제기관의 대응

위 판결의 입장은 이후 많은 논란을 불러일으켰다. 위 판결 논리에 대응하기 위하여, WP 29는 2007년 6월에 위에서 언급한 개인정보의 개념에 관한 의견(WP 136)을 발표하여 내용-목적-결과라는 세 가지 기준을 제시함으로써 광의의 관련성 개념을 주장하였다[196].

영국 DPA상 규제기관인 ICO(Information Commissioner's Office) 또한 2007년에 '무엇이 개인정보인지 결정하기(Determining what is personal data)'라는 제목의 가이드라인을 발간하였고, 관련성 요건에 관하여 정보가 명백히 그 개인에 관한(obviously about the individual) 것인지, 정보가

---

[194] Michael John Durant v. Financial Service Authority [2003] EWCA Civ 1946, para. 27~28

[195] 한편, 국내 문헌 중에는 *Durant* 판결에 관하여, 이 판결은 개인정보의 요건으로서 '관련성'을 요구한 것이며, 이 때의 관련성 개념은 WP 29가 제시한 바와 같이 내용, 목적, 결과의 관련성을 의미하며, 이로부터 우리나라법 해석에 관해서는 "직접적으로 당해 개인과 관련한 정보만을 그 특정 개인의 개인정보라고 보아야 한다"고 한다고 논평한 것들이 있다. 윤주희 등(주30), 141~142면; 박유영(주30), 55면. 그러나, '관련성'이 개인정보개념의 요소라는 점은 이 판결이 아니라 이미 DPA에 의하여 명확히 요구된 것이며, 이 판결이 관련성 개념을 해석한 방식은 WP 29의 그것과 상당히 다르다는 점에서 이러한 해석은 정확하지 않은 것이라 생각된다.

[196] Peter Carey, Data Protection, 4th Edition(Kindle Version), Oxford University Press, 2015, p.23

개인에게 연결되었는지(linked to), 정보가 그 개인에 관한 결정에 정보를 제공하거나 여기에 영향을 미치기(inform or influencing decisions) 위한 것인지, 전기적 중요성(biographical significance)이 있는 것인지, 개인이 정보의 초점(focus or concentrate)에 있는지, 정보가 개인에게 잠재적/현실적으로 영향을 미치는지(impact) 등을 제시하였다[197]. 이들은 누적적인 요건이 아닌바[198], 앞서 살펴본 Durant 판결의 내용과 달리 관련성에 관하여 WP 29의 내용-목적-결과 기준을 포함한 넓은 개념을 취하고 있으며[199], Durant 판결 내용과 대조적으로 개인의 프라이버시와 직접 관련이 없는 사안에까지 개인정보 범위를 확대하는 것으로 이해될 여지가 있다[200].

(3) 이후의 판결들

이후 잉글랜드 및 웨일스 고등법원(행정법원)은 2013년 *Kelway* 사건[201]에서, *Durant* 판결이 관련성 요건을 평가하는 유일한 기준이 될 수 없음을 명시적으로 판결하였다. 위 판결은, *Durant* 판결은 사안 자체가 WP 29 및 ICO가 제시한 관련성 판단 기준 중 결과 요소와 관련이 없는 것이었기 때문에, 애초에 개인정보 개념에 관한

---

[197] Information Commissioner's Office, Determining what is personal data, version 1.1(2012)

[198] 예컨대 어떤 정보의 초점이 문제의 개인에게 있지 않더라도, 그 정보가 개인에게 영향을 미칠 수 있다면 그 정보의 개인관련성은 인정된다. ICO(주197), p.17, p.21

[199] Damien Welfare, "Clarifying the scope of personal data", Privacy & Data Protection, 2012, 12(7), pp.7~8

[200] Renzo Marchini, "The UK Guidance on 'Persona Data': How it relates to *Durant*", Data Protection Law & Policy, November 2007

[201] Dr Peter Stuart Kelway v. The Upper Tribunal (Administrative Appeals Chamber), Northumbria Police Defendants and The Information Commissioner, [2013] EWHC 2575 (Admin)

결정적인 가이드로서 의도된 것이 아니라고 선을 긋고, 관련성 요건을 판단하기 위하여 먼저 *Durant*이 제시한 기준의 만족 여부를 심사한 후 이것이 만족되지 않을 경우 WP 29가 제시한 기준과 위 ICO 기준을 결합한 기준을 적용하여야 한다고 보았다[202].

그 후 *Durant* 판결을 선고한 동일한 법원인 잉글랜드 및 웨일스 항소법원도 2014년의 *Edem* 사건[203]에서 *Durant* 판결의 적용 영역을 제한하기에 이르렀다. 이 사안에서는, 원고인 에뎀이 FSA에 대하여 정보자유법(Freedom of Information Act, FOIA) 제40조에 기하여 그가 FSA에 제기한 이전 민원의 취급에 관한 자료 일체의 제공을 요청하였으나, FSA가, 요청 대상인 정보 중 제3자의 개인정보가 포함되어 있을 경우에는 공개의무를 면제할 수 있다는 FOIA 제40조 제2항에 기하여, 문제의 자료 중 민원을 담당한 직원 3명의 성명의 제공을 거부한 행위가 정당한지가 문제되었다. 구체적인 쟁점은 해당 직원의 성명이 해당 직원들에 '관련한' 것으로 개인정보에 해당할 것인지 여부, 즉 개인의 이름(그 개인이 FSA에 근무한 시점 및 당시의 직급이라는 정보와 결합하여 식별가능성이 인정되는)을 기록한 정보가 자동적으로 개인정보인지, 아니면 *Durant* 판결이 설시한 전기적 관련성과 초점이라는 두 가지 요건이 추가적으로 만족되어야 비로소 개인정보라고 할 수 있는지 여부였다.

법원은 ICO의 기준을 적용하는 한편 앞서 언급한 유럽사법재판소의 *Lindqvist* 판결을 언급하며 전자의 태도를 취하면서 *Durant* 기준의 적용을 거부하였다. 법원에 따르면, 동 법원이 *Durant* 판결에서

---

[202] Dr Peter Stuart Kelway v. The Upper Tribunal (Administrative Appeals Chamber), Northumbria Police Defendants and The Information Commissioner, [2013] EWHC 2575 (Admin), para. 57~59

[203] Efifiom Edem v. Information Commissioner and Financial Services Authority [2014] EWCA Civ 92

전기적 중요성과 초점이라는 두 가지 요건을 제시한 것은, *Durant* 사건에서는, 한 개인의 이름으로 검색하였을 경우 발견되는 모든 결과를 개인정보로 봄으로써 DPA상 정보주체의 접근권을 제3자와의 분쟁에 필요한 정보공개의 수단으로 악용하려는 원고의 시도를 저지한다는 의도가 있었기 때문이었다. 성명이 개인정보에 해당하는지 여부는 이러한 맥락과 무관하며, 따라서 *Durant* 기준을 적용할 필요 없이 바로 개인 식별이 가능한 한 개인정보에 해당한다고 보아야 한다는 것이다[204]. 요컨대 정보는 그 내용이 명백하게 개인에 관한 것이거나(obviously about), 그가 다루어지는 방법을 결정하거나 그에 영향을 미칠 목적으로 처리되므로 개인에게 분명히 연결된(clearly linked to) 것이라면 개인정보이고, *Durant* 판결의 기준은 위 두 경우가 아닌 경우에만 고려될 수 있다는 ICO 입장과 같은 취지로 이해된다[205].

(4) 소결

영국에서는 한때 관련성 요건을 *Durant* 판결과 같이 전기적 중요성 및 초점이라는 두 가지 요건이 충족되어야 인정하는 것으로 해석되었고, 이는 WP 29나 ICO의 그것과 대립되는 것으로 이해되었으나, 최근 *Kelway*나 *Edem*과 같은 일련의 판결들을 통하여 두 입장의 화해가 이루어져 *Durant* 요건은 제한된 상황에서만 적용되는 것으로 일단 정리되었다고 볼 수 있다. 그러나 최근 유럽사법재판소의 YS 판결이 *Durant* 판결과 유사한 사안에서 개인정보 개념은 정보주체의 정보 접근권 행사를 의미 있게 하는 한에서만 제한적으로 인정하여야 한다고 전제하며 개인에 관한 법률의견에 대한 정보주체의 접근권을 거부하였는바, *Durant* 판결의 취지는 이런 한에서 아직 유효하다고 할 것이며, 향후 이러한

---

[204] Efifiom Edem v. Information Commissioner and Financial Services Authority [2014] EWCA Civ 92, para. 17~21

[205] Peter Carey(주196), p.24

입장이 WP 29나 ICO의 기존 입장과 어떻게 조화될 수 있을지에 대하여 주시할 필요가 있을 것이다.

다. 식별 또는 식별가능성 요건의 해석

식별 개념에 관하여, ICO는 개인이 구분되어 다른 사람들과 다르게 취급될 수 있다면 그는 식별 가능한 것이라는 입장이다[206]. 한편 식별이란 어떤 개인의 동일성이 확인 가능한 상태를 말하고, 식별된 사람이란 물질적인 세계에서(in the physical world) 누구인지 알려져 있는 자를 말한다고 설명되기도 한다[207]. 즉, 그룹 내의 다른 사람들과 구분 가능할 뿐 아니라 현실 세계의 개인에 대하여도 관련지울 수 있는 상태를 식별의 지표로 보고 있는 것으로 생각된다.

다음으로 식별가능성 개념에 관하여 본다. DPA 제1조 (1)의 규정상 식별가능성은 정보 통제자의 점유에 있는 또는 점유에 들어올 수 있는 정보를 기준으로 판별한다. 그러므로 한 조직이 보유하고 있는 정보는, 현재는 그 정보로부터 생존하는 개인이 식별될 수 없는 경우라도, 관련된 추가 정보가 그 조직에 의하여 획득되고 그러한 획득이 가능한 경우('likely')라면 개인정보가 될 수 있다. 단, 여기서의 식별가능성은 합리적인 수준의 것(reasonable likelihood)이어야 한다[208].

그러나 개인이 식별되었거나 식별가능하다고 하여서 반드시 그 개인을 직접 알 수 있거나 그 개인에 직접 접촉 가능하다는 것을

---

[206] Peter Carey(주196), p.21

[207] Rosemary Jay and Angus Hamilton, Data Protection – Law and Practice, Second Edition, Sweet & Maxwell, 2003, p.80

[208] Information Commissioner's Office, Anonymisation: managing data protection risk code of practice, 2012, p.12

의미하지는 않는 것으로 이해된다. 앞서 언급한 *Edem* 사건에서, 원고 에뎀의 'FSA의 직원의 성명을 알게 되더라도 FSA가 더 이상 존재하지 않고 직원들도 더 이상 그곳에 근무하지 않으므로 이들을 찾아낼 수 없는 이상 식별이 불가능하다' 는 취지의 주장에 대하여, 잉글랜드 및 웨일스 항소법원은 "성명과 그것이 사용된 맥락이 조합에 의하여 한 개인이 식별될 수 있다면 그들에게 접촉하는 것이 어려울 수 있다는 점은 아무런 의미가 없다. 개인정보는 '식별 가능한' 살아 있는 개인에 관한 것이다. 이것은 그 사람이 사실상 접촉되거나 추적될 수 있다는 것과는 다른 개념이다" 라고 판시하였다[209].

한편, DPA 제1조는 '정보 통제자' 만을 기준으로 식별가능성을 판단하고 있는바, 이는 앞서 살펴본 일본의 태도와 유사하나, 정보 통제자 및 제3자 모두를 기준으로 식별가능성을 판별하는 유럽연합 개인정보보호지침의 문언과 입장을 달리하는 것으로 보인다[210]. 여기에 대하여, "비록 이들 문언은 통제자에 의한 식별을 요구하는 것으로 일반적으로 받아들여지고 있지만, 통제자 아닌 다른 누군가가 그렇게 할 수 있다면, 반드시 통제자가 자신이 처리하는 정보의 정보주체를 식별할 수 있어야 하는 것은 아니라 할 수 있다" [211] 고 개인정보보호지침과 가깝게 이해하는 해석 또한 존재한다.

어쨌든, 이와 같이 영국법이 '통제자를 기준' 으로 식별가능성을 평가하는 점에 관하여, 영국에서는 다음 두 가지 쟁점이 존재하고 있는 것으로 보인다.

---

[209] Efifiom Edem v. Information Commissioner and Financial Services Authority [2014] EWCA Civ 92, para.14

[210] Elliot, Mackey, O' Hara and Tudor, "The Anonymisation Decision-Making Framework", UKAN Publications, 2014, pp.10~11

[211] Peter Carey(주196), p.22

첫째, 정보 통제자가 식별가능성 판단의 기준이라면, 정보 통제자에게 식별가능성이 있는 정보는 언제나 제3자에 대해서도 식별가능성이 있다고 할 수 있는가.

둘째, 정보 통제자에게 식별가능성이 없는 정보는 언제나 식별가능성이 없다고 할 수 있는가.

이하에서는 식별가능성에 관한 위 두 가지 쟁점에 관하여 차례로 살펴 보겠다.

(1) 첫 번째 쟁점: 정보 통제자에게 식별가능성이 있는 정보는 제3자에 대해서도 식별가능성이 있다고 보아야 하는가?

이 쟁점은, 예컨대 정보 통제자가 보유하고 있는 개인정보에 대하여, 식별가능성을 없애는 조치를 취한 후 제3자에게 전달하는 사안에서 문제가 된다. 즉 정보 통제자가 보유하고 있는 정보 원본을 이용함으로써 식별가능성을 없앤 정보로부터 개인을 식별하는 것이 가능하다면, DPA상 식별가능성은 정보 통제자를 기준으로 하므로, 그 정보를 전달받은 자가 개인을 식별할 수 있는지 여부를 떠나 그러한 전달행위는 언제나 개인정보의 전달이 될 것이다. 식별가능성의 판단 기준을 정보통제자의 인식으로 제한함으로써 일견 식별가능성의 인정 범위가 좁아질 것처럼 보이지만, 오히려 제3자의 입장까지 폭넓게 고려하는 지침의 문언에 비하여 개인정보의 범위를 넓혀 버리는 해석이 가능한 것이다[212]. 정보의 키 코드화, 암호화 관련하여서도 동일한 문제가 제기될 수 있을

[212] 흥미롭게도 우리나라에서는 위 영국법 조항을 우리법상 개인정보 개념을 좁게 보면서위와 같은 제3자 제공의 경우 개인정보의 제3자 제공이 성립하여서는 안 된다는 근거로 원용하는 견해들이 다수 발견되고 있다. 대표적으로 이인호(주 43), 62면, 78면 참고. 그러나 정작 영국에서는 이와 반대로, 위 조항이 동일한 제3자 제공 행위에 관하여 개인정보보호법의 적용을 긍정하는 근거로 원용되고 있는 것이다.

것이다[213].

(가) ICO의 입장

일부 위와 같은 강경 노선을 따르는 견해도 없지는 아니하나, ICO는 이러한 해석을 배제하는 입장을 취하여 왔다. 즉 2012년 가이드라인에 따르면, 키 코드화된 정보의 경우, 정보의 수신자가 그 정보로부터 개인을 식별할 수 없도록 하기 위한 충분한 기술적 장치가 되어 있다면, 그 정보는 개인정보라고 볼 수 없다[214]. 익명화에 관한 2012년 가이드라인에서도, "한 조직이 개인정보를 익명화된 형태로 변환하여 그것을 공개하면, 이는 개인정보의 공개에 해당하지 않을 것이다. 이는 정보를 공개하는 그 조직이 재식별이 가능하게 하는 다른 정보를 아직 보유하고 있는 경우라 하더라도 마찬가지다"라고 명시함으로써 이러한 입장을 재차 확인하였다[215].

(나) *CSA* 판결

영국의 판례 중 이와 관련한 대표적인 판결로 귀족원(House of Lords)의 이른바 *CSA* 판결(2008)[216]과 잉글랜드 및 웨일스 고등법원의 *Department of Health* 판결(2011)[217]이 있다. 또한, 비록 상급 재판소(Upper Tribunal)의 판례이기는 하지만 비슷한

---

[213] Kuan Hon, 'Personal data' in the UK, Anonymization and Encryption (2016. 10. 9.확인), <http://www.cloudlegal.ccls.qmul.ac.uk/Research/49700.html>

[214] ICO(주197), p.28

[215] ICO(주208), p.13

[216] Common Service Agency v. Scottish Information Commissioner, [2008] UKHL 47

[217] The Queen on the Application of Department of Health v. Information Commissioner, [2011] EWHC 1430(Admin)

시기에 선고된 *APPGER* 판결(2011)[218] 또한 참고할 만하다고 생각되어 소개하기로 한다. 이들 판례들은 결론적으로는 ICO와 유사한 입장이나 그에 이르는 논리에 있어서는 미묘한 차이가 있다.

먼저 *CSA* 판결에서는 스코틀랜드의 국회의원이 스코틀랜드의 Common Service Agency('CSA')[219] 에 대하여, 스코틀랜드 정보자유법(Freedeom of Information (Scotland) Act 2002, 'FOISA 2002' [220]) 제38조에 기하여 특정 지역에서의 연도별 아동 백혈병 발병 건수에 관한 통계 자료의 열람을 청구하였으나 해당 자료가 관련 아동들에 대한 식별가능성이 있다는 이유로 이를 거절당한 사안이다. 여기서는 해당 정보가 이른바 바나디제이션(barnardisation)이라는 방법으로 처리되어 개인 식별 가능성이 저감되었되었다고 가정할 경우, 그 정보가 DPA 제1조 (1)의 개인정보에 해당하는지, 따라서 CSA가 FOISA 제38조 제2항에 기하여 그러한 정보를 청구인에게 제공해서는 안되는지 여부가 다투어졌다.

다수의견에 따르면[221], 더 이상 개인을 식별화할 수 없을 정도로

---

[218] All Party Parliamentary Group on Extraordinary Rendition v. The Information Commissioner & The Ministry of Defence, [2011] UKUT 153 (AAC)

[219] 스코틀랜드 건강보험을 운영하는 기구로 보인다. https://en.wikipedia.org/wiki/NHS_National_Services_Scotland 참고(2016. 10. 9. 확인).

[220] FOISA는 앞의 *Edem* 판결에서 적용된 FOIA와 거의 동일한 법이다. 여기서 개인정보에 해당함을 이유로 정보공개청구를 거부할 수 있는 근거가 되는 FOISA 38조 제2항은 FOIA 제40조 제2항과 동일하다. Common Service Agency v. Scottish Information Commissioner, [2008] UKHL 47 para.2

[221] 5명의 귀족원 판사가 본 판결의 작성에 참여하였으나, 실제로 그 중 4명이 결론에 이르는 논리를 달리하고 있었고, 호프 경(Lord Hope of Craighead)의 의견만 호프만 경(Lord Hoffmann)의 완전한 지지를 받고 있었기에 다수의견이

익명화한 정보는 개인정보로 취급하지 않는다는 유럽 개인정보보호지침 전문의 고려이유 26의 해석기준이 영국법에도 적용되어야 한다. 그러므로 익명화된 정보는 개인정보가 아니라고 본다. 그런데 DPA 제1조 (1) (b)의 "그 정보(those information)와, 정보 통제자가 점유하고 있거나 그의 점유에 들어올 가능성이 있는 다른 정보(other information)"라는 문언상, '그 정보(those information)'와 '다른 정보(other information)'는 모두 개인의 식별에 기여하는 바가 있어야 한다. 즉 '그 정보'가 그 자체만으로 개인 식별이 불가능할 뿐 아니라 '다른 정보'의 도움을 받아서도 개인식별이 될 수 없는 형태로 되어 있다면, 식별은 오로지 '다른 정보'에 의하여서만 가능할 뿐 '그 정보'에 의하여 가능해지는 것이 아니므로, '그 정보'는 식별가능성이 없어 개인정보가 아니라고 보아야 한다. 그러므로 CSA가 바나디제이션의 방법으로 가공한 아동 백혈병 발병에 대한 통계 수치('그 정보')는, 만일 그것이 충분히 익명화된 것이라고 한다면, 비록 CSA가 위 통계 정보를 도출해 낸 원 정보('다른 정보')를 보유하고 있다고 할지라도, 개인정보라고 볼 수 없고, 따라서 공개할 수 있다고 한다[222].

요컨대, 통계 정보는, 그것이 개인정보보호지침 고려이유 26이 규정한 바와 같이 충분히 익명화되어 있다면, 정보 통제자가 그 정보를 도출해 낸 근거가 된, 개인 식별이 가능한 '다른 정보'를 보유하고 있더라도 개인정보가 아니라는 것이다. 여기에 대하여 리치몬드의 헤일 남작(Baroness Hale of Richmond)의 보충의견은, 다수의견과는 달리, CSA는 문제의 통계 정보 외에도 개인 식별이 가능한 원 정보를 보유하고 있으므로, 통계 정보는 CSA와의

되었다.

[222] Common Service Agency v. Scottish Information Commissioner, [2008] UKHL 47, para. 24~27

관계에서는 개인정보라고 보아야 할 것이나, 그 정보의 수신인은 그로부터 개인을 식별할 수 없으므로, 그 정보의 공개라는 맥락에 있어서는 식별가능성이 없다고 설시하였다[223].

(다) Department of Health 판결

이 사건에서는 익명화된 후기 임신중절건 관련 연도별 통계를 FOIA에 기하여 공개할 수 있는지 여부가 문제되었다. 담당 판사인 크랜스턴 판사(Justice Cranston)는 *CSA* 판결의 다수의견에 입각하여 논리를 전개하였다[224]. 즉 DPA 제1조 (1)의 '그 정보'와 '다른 정보'와 결합하여 식별을 가능케 하는 경우 '그 정보'가 식별에 기여하는 바가 있어야 개인정보로서의 성격을 인정할 수 있다는 법리를 확인한 후[225], 비록 정보 통제자인 CSA가 "공개청구된 정보와 관련 있는 아동들의 신원에 관한 정보를 보유하고 있었지만, 그 정보가 충분히 익명화된 것이라면, 공개되었을 때 개인정보라고 볼 수 없다"는 점을 인정하였다는 데 *CSA* 판결의 다수의견의 의의가 있다고 설시하였다[226]. 즉 그와 같은 정보를 공개한 후에 공중이 그 정보로부터 생존하는 개인을 식별해낼 수 있는지 여부가 문제이지 정보 통제자가 식별할 수 있는지가 문제는 아니며, 만일 후자와 같이 본다면 현실과 유리된 결과가 도출될 것이라고 하였다[227].

(라) APPGER 판결

원고 APPGER(All Party Parliamentary Group on Extraordinary

---

[223] 위 판결, para. 92

[224] The Queen on the Application of Department of Health v. Information Commissioner, [2011] EWHC 1430(Admin), para.45

[225] 위 판결, para. 46~47

[226] 위 판결, para. 51

[227] 위 판결, para. 52~54

Rendition)가 영국 국방부(Ministry of Defence)에 대하여 FOIA에 근거하여, 이라크와 아프가니스탄에 억류된 영국 군인에 관한 통계 자료의 공개를 요청하였다가 해당 군인들에 관한 개인정보가 포함되어 있음을 이유로 거절한 사건이다.

상급 재판소 단계에서는 두 가지 부류의 정보가 개인정보인지 여부가 문제되었는데, 하나는 각각의 군인에 대한 구금 일자, 이송 일자 및 장소에 관한 정보로, 군인들의 성명 등을 알 수 없도록 익명화된 정보이고, 다른 하나는 특정한 또는 특정 종류의 구금시설로 이송된 군인의 수에 대한 통계적 정보였다.

전자의 정보에 관하여 상급 재판소는, '해당 정보를 공공 영역으로 공개하는 것이 개인식별을 가능하게 할지'가 쟁점이라고 하면서, 증거를 검토한 결과 식별 가능성이 없다고 함으로써 개인정보 해당성을 부정하였다[228]. 후자의 정보에 관하여는, 피고 영국 국방부가 '국방부 자신이 편집되지 않은 정보를 이용하여 개인식별이 가능하므로 DPA 제1조 (1)의 (b)에 의하여 개인정보에 해당한다'[229]는 취지로 주장하였으나 상급재판소는 *CSA* 판결을 원용하며 이를 기각하였다. 구체적으로, 상급재판소는 정보 통제자가 개인식별이 가능하다고 하여 식별성을 제거한 정보를 모든 경우 개인정보로 취급하는 것은 불합리하다고 보았는데, 그 근거로 *CSA* 판결에서 보충 의견을 제시한 헤일 남작의 견해를 따랐다[230]. 즉 "정보 통제자가

228 All Party Parliamentary Group on Extraordinary Rendition v. The Information Commissioner & The Ministry of Defence, [2011] UKUT 153 (AAC), para. 109

229 위 판결, para. 124

230 본 판결 판시에 따르면, Department of Health 사건에서 다수의견은 두 명의 판사가 동조한 것이기 때문에 일반적인 다수의견으로서의 효력이 없어 상급재판소는 여기에 기속되지 않는다고 한다. 위 판결, para. 125.

익명화(anonymisation)를 하고, 편집되지 않은 정보나 개인을 재식별화할 키를 보유하고 있거나 편집되지 않은 정보를 가지고 있다면" 익명화한 해당 정보는 개인정보로 보아야 하나[231], 정보가 완전히 익명화되었다고 한다면 "공개하는 순간 그 정보는 개인정보로서의 성질을 상실"한다고 보았다[232].

(마) 소결론

ICO 및 영국 법원은 DPA 제1조 (1)의 해석에 관하여 공통적으로, 식별성을 제거한 정보를 제3자에게 공개하는 맥락에서, 오로지 정보 통제자가 원 정보를 보유하고 있다는 사실만으로 그 정보를 개인정보로 취급하여서는 안된다는 점을 분명히 하였다. 특히 익명화된 통계 정보의 경우, 이를 통제자가 보유하는 경우에도 개인정보로 취급할 것인지에 대해서는 통일된 입장이 존재한다고 보기 어려우나, 최소한 이 정보로부터 개인을 식별할 능력이 없는 제3자에게 공개될 경우라면 그러한 공개는 개인정보의 공개로 볼 수 없다는 데에 의견이 일치하는 것으로 보인다.

(2) 두 번째 쟁점: 정보 통제자 내지 정보를 제공받은 자에게 식별가능성이 없는 정보라면, 그 정보로 개인을 식별할 수 있는 제3자의 존재에도 불구하고 식별가능성이 없다고 보아야 하는가?

이 문제는, 앞서 살펴본 DPA 제1조 (1) (b)는 정보 통제자를 중심으로 식별가능성을 판단하므로, 정보 통제자 아닌 제3자의 관점은 고려되어서는 아니되는가라는 문제와 맞닿아 있다. 예컨대 명백히 개인과의 관련성은 존재하나 정보 통제자 자신이 식별할 수 없는 정보는 개인정보라고 할 것인가? 정보 통제자가 그러한 정보를 제3자에게 공개할 경우, 그러한 공개행위는 개인정보의

231 위 판결, para. 127

232 위 판결, para. 128

공개행위라고 보아야 하는가?

ICO는 앞서 언급한 2012년의 '무엇이 개인정보인지 결정하기' 가이드 부록 D(Appendix D)에서, 그 정보를 가지고 직접 개인을 식별할 수는 없으나 그 정보를 수신하는 사람이 개인을 식별할 합리적인 가능성이 있다면 개인정보에 해당한다는 입장을 천명하였다. 즉, DPA 규정상으로는 식별가능성 유무의 판단이 '통제자' 만을 기준으로 하는 것으로 보이지만, 유럽 개인정보보호지침 규정을 참조하였을 때, 개인 식별을 가능케 할 수 있는 정보를 공개하는 경우에는 개인정보 해당성을 긍정하여야 한다는 것이다[233]. 이와 관련하여 ICO가 든 사례는 누군가 FOIA에 기하여 한 기관에 대하여, 그 기관에 근무하는 스태프의 주소를 공개할 것을 청구하였는데, 그 사람이 그 주소로부터 스태프를 식별할 수 없더라도 누군가가 그 주소로부터 스태프를 식별할 수 있는 합리적 가능성이 있다면 개인정보성을 인정하여야 한다는 것이었다. 일응 객관설적 관점을 취하고 있는 것으로 해석할 여지도 없지 않으나, '주소' 라는 정보가 개인식별과 밀접한 관련이 있는 점, 공개된 주소가 다시 다른 제3자에게 전달될 가능성이 현실적으로 존재하는 점 등을 감안하면 반드시 그렇게 볼 수는 없다고 생각된다. 뒤에서 언급하다시피, ICO가 유동 IP주소에 관하여 개인정보성을 인정하는 듯한 태도를 취하는 점을 감안하면 더욱 그러하다 할 것이다.

(3) 키 코드화된 정보와 IP주소의 취급

(가) 키 코드화된 정보의 경우

앞서 살펴본 *CSA* 판결과 *Department of Health* 판결의 결론에 따르면, 일견 DPA 제1조 (1)의 규정에도 불구하고 정보 통제자의

[233] ICO(주197), p. 29

관점만 가지고 식별가능성 유무를 판단하여서는 아니되며, 정보 통제자에게 식별 가능한 정보라 하더라도 제3자가 식별할 수 없다면 그 제3자에 대한 공개라는 맥락에서는 개인정보가 아니라는 일반적 결론이 도출되는 것처럼 보인다.

그러나 과연 익명화된 통계정보가 아닌 키 코드화된 정보나 암호화된 정보에 대하여도 판결의 결론이 타당하게 적용될 수 있을지는 의문이 없지 않다. 전술한 바와 같이, 최상급심인 귀족원의 판결인 *CSA* 판결이 채택한 주된 논리는, "'그 정보'가 그 자체로 개인식별을 가능케 하지 못하더라도 '다른 정보'와 결합하여 식별가능성을 인정받으려면 '다른 정보'와 결합하였을 때 식별에 기여하여야 하는데 익명화된 문제된 통계정보는 그러한 가치를 가지지 못하였으므로 개인정보로 볼 수 없다"는 것이었다. 이는 익명화된 정보라면 그 성질상 정보 통제자에 대해서도 개인정보로 볼 수 없다는 취지로 해석될 수 있는 대목이다. 앞서 살펴본 바와 같이 헤일 남작이 '익명화된 통계정보라 할지라도 정보 통제자에 대해서는 개인정보로 취급되어야 한다'는 점에서 다수 의견과 구분되는 보충의견을 제시하였다는 점을 감안하면 더욱 그러하다.

그런데 익명화된 통계정보와는 달리, 키 코드화된 정보('그 정보')는 환자를 식별할 수 있게 하는 키 정보('다른 정보')와 결합될 경우, 키 정보에 더하여 그 환자에 관한 구체적인 사실을 추가적으로 제공한다는 점에서, 환자의 식별에 기여한다고 볼 수 있을 것이며, 암호화된 정보의 경우에도 이 점은 마찬가지라 할 수 있을 것이다. 그렇다면 이들에 대해서는 CSA 판결이 익명화된 통계정보의 개인정보성을 부정하는 데 사용한 위 논리가 적용되지 않는 것은 아닐까? 그렇다면 이들 정보의 공개는 어떻게 취급할 것인가? *CSA* 판결은 이 점에 관하여 명확한 답을 주고 있지 않다.

따라서, 적어도 판례상으로는, 키 코드화된 정보나 암호화된 정보를

제3자에게 전달한 경우, 그러한 맥락에서 해당 정보가 개인정보라고 볼 수 있는지, 그러한 전달행위에 관하여 개인정보보호법을 적용할 수 있을지의 문제가 완전히 명쾌하게 정리되었다고 보기는 어려울 것 같다. 단, *Department of Health* 판결에서는 제3자에게 통계정보를 공개하는 것과 관련하여, '공중이 그 정보를 가지고 개인을 식별할 수 있는지가 문제'라는 취지로 판시하였는바, 여기에 따르면 위와 같은 정보를 제3자에게 제공하는 경우 개인정보성을 부정한다는 논리적 귀결이 가능할 수도 있다고 생각된다. 물론 규제기관인 ICO가 명시적으로 이와 같은 결론을 지지하고 있다는 점은 앞서 살펴본 바와 같다.

(나) IP주소의 취급

1) ICO의 견해

IP주소와 관련하여, ICO는 고정 IP의 경우에는 개인정보에는 해당하고, 유동 IP의 경우는 인터넷 접속 서비스 아닌 다른 제3자에 대하여는, 그 제3자가 유동 IP와 함께 다른 식별자 등을 함께 수집하는 경우가 아니라면 DPA의 적용을 긍정하기 쉽지 않으나, 현실적으로 유동 IP와 고정 IP를 구별하기가 쉽지는 않을 것이라는 견해를 피력한 바 있다[234].

2) *BT* 판결

2011년 4월에 선고된 잉글랜드 및 웨일스 고등법원의 *BT* 판결[235]에서, 저작권자가 특정 일시에 파일 공유 행위가 일어난 유동 IP 주소를 ISP에 제공하고 그 일시에 당해 유동 IP 주소로

[234] Information Commissioner's Office, Data Protection Good Practice Note, Collecting personal information using websites, 20 June 2007. p.3

[235] British Telecommunications Plc & Anor, R v The Secretary of State for Business, Innovation and Skills [2011] EWHC 1021(Admin) (20 April 2011)

접속한 자를 특정할 것을 요구하는 경우, 저작권자가 온라인상에서 저작권 침해 파일을 공유한 행위자들을 식별할 수 있다고 볼 수 있는지가 심리되었다.

법원은 먼저 앞서 살펴본 WP 29의 의견 즉 유동 IP주소의 경우 ISP에 대해서는 개인정보이고, ISP 아닌 통제자가 처리하는 경우라도 컴퓨터의 사용자를 식별할 목적으로 처리되는 상황이라면 개인정보에 해당한다는 의견을 논의의 전제로 삼았다[236]. 여기에 대하여 '저작권자들이 IP주소로써 식별할 수 있는 것은 ISP와 인터넷 서비스 사용 계약을 맺은 계약자(subscriber)이지 행위자(infringer)이므로 식별가능성이 없다'는 취지의 주장이 있었지만, "유동 IP주소를 통하여 식별될 수 있는 계약자는, 비록 침해자가 아니어서 침해에 대하여 법적인 책임이 없더라도, 넓은 의미에서 그 침해를 조장한 자로서 불가피하게 그 정보(유동 IP 주소를 포함한 저작권 침해의 상세 사항)에 연결되어 있기 때문에 그 정보는 그럼에도 불구하고 식별된 또는 식별 가능한 개인에 관련" [237] 되어 있으므로 "저작권자에 의하여 처리되는 관련 정보들이 개인정보"[238]라고 판시하였다.

3) *Golden Eye* 판결[239]

이 판결에서도 저작권자가 인터넷 접속 서비스 제공자에 대하여 유동 IP를 이용하여 불법으로 파일을 공유한 고객의 성명 및 주소를 제공하여 달라고 요청한 것과 관련하여, 유동 IP 주소가 침해자를 식별할 수 있는 가능성이 문제되었다. 이 사안에서는 유동

---

[236] 위 판결, para. 153~154

[237] 위 판결, para. 156

[238] 위 판결, para. 157

[239] Golden Eye(International) Ltd & Anor v Telefonica UK Ltd [2012] EWHC 723 (Ch) (26 March 2012)

IP주소가 개인을 잘못 식별하는 여러 가지의 시나리오가 식별가능성을 부정하는 근거로 제시되었으나[240], 법원은 그럼에도 불구하고 문제의 일시에 관련 유동 IP 주소를 통하여 저작권 침해가 발생한 점, 인터넷 접속 서비스가 식별해낸 사람의 다수(전부는 아니지만) 실제로 불법적 파일 공유행위를 한 점 등을 들어 식별가능성을 긍정하였다[241].

라. 소결론

이상에서 살펴본 바와 같이, 영국의 경우 개인관련성에 관한 논의가 상당히 깊이있게 전개되어 왔으며, WP29의 태도와는 달리, 정보 통제자를 기준으로 식별가능성 유무를 판단한다는 기준이 확고하게 정립되어 있다.

그러나 통제자에게 개인정보인 정보를 개인을 식별할 수 없도록 가공하여 제3자에게 전달하는 경우, 이것이 개인정보의 제공에 해당하는지의 문제에 대하여는 논란이 있다. 실제 결론에 있어서는, 판결과 ICO의 논리에서 약간의 차이가 감지되기는 하나, 정보 수령자가 개인을 식별할 수 없다는 점이 충분히 확실하기만 하면 제3자 제공에 해당하지 않는 것으로 취급하는 경향이 있다.

---

[240] 즉, 인터넷 접속 서비스 제공자라고 할지라도 유동 IP를 사용하여 계약자를 식별하는 과정에서 일정 비율의 오류를 범할 수 있다는 점, 반드시 계약자와 침해자가 일치하지는 않는데 예컨대 가정용 컴퓨터를 계약자 아닌 다른 구성원이나 방문자가 사용할 수 있다거나, IP주소가 라우터에 배당된 것인 경우 동일 라우터를 사용하는 다른 컴퓨터를 사용하는 자가 있는 경우, 라우터의 접속이 안전하지 아니하여(insecure) 가족 구성원 아닌 다른 사람이 그 라우터로 무단 접속하는 경우, 문제의 라우터나 컴퓨터가 트로이 바이러스 등에 감염되어 가족 구성원 외의 누군가가 인터넷 접속을 위하여 문제의 컴퓨터를 사용하는 경우, 인터넷 카페나 도서관, 컴퓨터 등의 와이파이 스팟이 사용된 경우 등을 그 예로 들었다. 위 판결 para. 103

[241] 위 판결, para. 105

5. 일본

가. 개요

일본의 개인정보보호법은 크게 2003년에 제정된 ‘개인정보의 보호에 관한 법률(個人情報野保護に関する法律)’, ‘행정기관이 보유하는 개인정보의 보호에 관한 법률(行政機関の保有する個人情報に関する法律, 이하 ‘행정기관 개인정보보호법’)’, ‘독립행정기관이 보유하는 개인정보에 관한 법률(独立行政機関の保有する個人情報に関する法律, 이하 ’독립행정기관 개인정보보호법’)’의 세 법률에 의하여 규정되고 있다. 이 중 개인정보의 보호에 관한 법률은 개인정보보호에 관하여 공공부문 및 민간부문 모두에 적용되는 일반 원칙을 제시하는 한편 민간 부문에 대한 규율을 담고 있고, 나머지 두 개의 법률은 개인정보보호법에 규정된 일반 원칙에 따라 공공 부문을 규율한다. 구체적으로, 개인정보의 보호에 관한 법률 중 제1장 내지 제3장에 해당하는 부분 즉 개인정보보호의 기본이념, 국가 및 지방공공단체의 책무와 시책, 기본방침의 제정 등에 관한 부분은 민간 및 공공 부문 모두에 적용되는 기본법이고, 제4장 이하는 민간 부문에만 적용된다[242]. 본고의 목적에 따라, 본고에서는 일반법이자 민간영역에 관한 법률인 개인정보의 보호에 관한 법률을 중심으로 검토하기로 한다.

개인정보의 보호에 관한 법률은 2003년 제정된 이후 수 차례의 사소한 개정을 거쳤으나, 정보통신기술의 발달에 대응하여 소비자 프라이버시권 보호를 강화하는 한편 개인정보의 활용성을 높인다는 목표 하에 2015년에 대폭 개정되었다. 구체적으로, 1) 개정 당시에 예상치 못하였던 새로운 정보통신기술이 발전함에 따라 고도화된

[242] 宇賀克也, 個人情報保護法の逐條解說, 第2版, 有斐閣, 2008, 21면; 日巴置美·板倉陽一郎, 平成27年改正個人情報保護法のしくみ `商事法務 `2015 , 150면

정보처리의 양상(예컨대 빅데이터)에 대응하고, 2) 종래에는 각 사업자의 업무분야를 소관하는 주무대신이 개인정보보호 관련 권고, 명령 등을 담당함으로써 규제의 중첩 및 혼란이 발생하였는바, 개인정보보호 관련 감독 업무를 개인정보보호위원회로 일원화함으로써 그러한 문제를 해결하고, 3) 기업활동의 글로벌화로 인하여 발생한 국경을 넘는 정보처리 문제에 대응하고자 함이 개정법의 문제의식이었다[243].

이 중 첫 번째 문제의식과 관련하여 보면, 정보통신기술의 발달에 따라 개인정보 개념의 해석에서 발생하는 어려움들을 해소하고자 기존의 개인정보개념에 추가하여 '개인식별부호'와 '익명가공정보'라는 개념이 개정법에 새로 도입되었는바, 이는 다른 입법례들에서 해석에 의존하던 개인정보 개념 획정 문제를 입법론적으로 해결하고자 하였다는 점에서 주목할 만한 시도라고 생각된다. 이하에서는 개정전 개인정보의 보호에 관한 법률(이하 '구법')상 확립되어 온 개인정보 개념에 관한 해석을 기본으로 하되, 2015년 개정된 개인정보의 보호에 관한 법률(이하 '개정법')에서 새로 도입된 '개인식별부호', '익명가공정보' 개념에 대하여 살펴보고자 한다.

나. 개인정보의 개념

구법 제2조 제1항은 개인정보를 "생존하는 개인에 관한 정보로서, 당해 정보에 포함되어 있는 성명, 생년월일 기타의 기술 등에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 照合하는 것이 가능하여, 그에 의하여 특정의 개인을 식별할 수

243 高度情報通信ネットワーク社会推進戦略本部 ` パーソナルデータの利活用に関する制度改正大綱(2015), 10~16면; 瓜生和久 編, 平成27年改正個人情報保護法, 商事法務, 2015, 3면; 한은영, "일본 개인정보보호법 개정의 배경 및 개정안의 주요 내용", 정보통신방송정책 제26권 13호(2014), 19~22면

있게 되는 것을 포함한다)을 말한다.”고 정의하고 있다.

이에 대하여 개정법 제2조 제1항은, 개인정보란 ①“생존하는 개인에 관한 정보”로서, 개인식별부호를 제외하고 “당해 정보에 포함된 성명, 생년월일 기타의 기술 등...에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 照合하는 것이 가능하여, 그에 의하여 특정의 개인을 식별할 수 있게 되는 것을 포함한다)”(제1호)과 ②“개인식별부호가 포함되어 있는 것”(제2호)이라고 한다.

이처럼 개정법 제2조 제1항은, 구법상 개인정보 개념을 제1호에서 그대로 계승하는 한편, 제2호에서 생존하는 개인에 관한 정보로서 ‘개인식별부호’가 포함된 정보를 여기에 추가하고 있다. 이와 같은 변경은 개인정보의 개념 자체를 변경하는 것이라기보다는, 정보통신기술의 발달에 따라 다양해진 정보들 중에 무엇이 개인정보인지 보다 쉽게 판단하게 하기 위하여 개인정보 개념을 명확화하는 것이라고 이해된다[244].

---

[244] 그러므로 구법과 개정법상 개인정보개념에 대한 해석은 동일하다. 개정법은 다만 구법상의 개인정보 개념을 변경한 것이 아니라 명확화한 것일 뿐이라고 한다. 衆議院 內閣委員會 第4号 平成 27年 5月 8日 회의록 중 山口 국무대신 발언 참고. “お尋ねの保護対象の件でありますが `これは `保護対象を明確化するというふうな観点から `現行法において保護対象に含まれると考えられるもの `具体的には `身体の一部の特徴をデータ化したもの等につきましては政令で定めるというふうなことにするものでありまして `個人情報の定義を拡大 `拡充するものではないというふうなことであります. また `個人情報の定義の要件となっております特定の個人を識別することができるもの `これにつきましても `今回の改正において従来の解釈を変更するものではなくて `社会通念上 `一般人の判断力や理解力をもって `情報の分析等によって生存する具体的な人物と情報との間に同一性を認めるに至ることができるものというこれまでの解釈と同様であります”(2016.4. 9. 확인)
<http://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000218920150508004.htm#p_honbun>; 同旨, 瓜生和久(주243), 10면, 12~13면;

즉 개정법에서도 개인정보 개념 자체는 유럽연합 지침과 마찬가지로 i) 정보 ii) 개인관련성, iii) 식별 또는 식별가능성, iv) 생존하는 개인에 관한 정보라는 네 가지 요건으로 이루어져 있다. 다만 이 중 비교적 판단이 쉬운 i) 및 iv) 요건을 충족하고, '개인식별부호'를 포함하는 정보에 대해서는 판단이 까다로운 ii) 및 iii) 요건의 만족 여부를 따로 심사하지 않고 바로 개인정보성을 인정하는 구조를 취하고 있다고 할 수 있다.

이러한 사정을 배경으로, 일본에서의 개인관련성 및 식별가능성 개념에 대하여 검토해 보도록 한다.

(1) 개인관련성

개인관련성이란 "개인의 속성·행동, 개인에 대한 평가, 개인이 창작한 표현 등, 당해 개인과 관계하는 모든 정보"를 지칭하기 위한 개념으로, 공지의 것인지 여부를 묻지 않는다[245]. 사실 뿐 아니라 타인의 평가 및 판단에 관한 사항도 광범위하게 포함한다[246]. 요컨대, 개인의 속성에 관한 모든 정보로 넓게 이해되는 것으로 보인다[247]. 영국의 경우와 같이 개인관련성 개념을 특별히 제한하는 논의는 보이지 아니한다.

日巴置美·板倉陽一郎(주242), 33면, 42면

[245] 宇賀克也(주242), 34면; 菅原貴与志, 詳解 個人情報保護法 企業法務, 第5版, 民事法研究會, 2014, 25면

[246] 內閣官房 個人情報保護擔當室, 個人情報の保護に関する法律案 逐條解說(2003), 6면

[247] 鈴木正朝·高木浩光·山本一郎, ニッポンの個人情報 「個人を特定する情報が個人情報である」と信じている方へ `翔泳社, 2015, 21면

(2) 식별가능성

(가) 식별 개념에 관하여

1) 구법상의 논의

개인정보보호법이 '식별' 또는 '식별가능성' 개념을 둔 취지는, 개인의 권리이익 보호라는 법의 목적과 관련하여, 권리나 이익의 침해 우려를 판단하기 위한 기준이라고 일반적으로 이해되고 있다[248].

'식별'의 구체적 정의를 상론하는 문헌은 많지 아니하나, "사회통념상, 일반인의 판단력과 이해력을 가지고, 정보의 분석에 의하여 생존하는 구체적인 인물과 정보와의 동일성을 인식할 수 있는 것"이라는 정의가 통용되고 있는 것으로 보이며, 이러한 식별 개념 자체는 구법에서나 개정법에서나 동일하다고 한다[249]. 그러나 구법에 기한 실무에서는 이를 "어디의 누구인가를 알 수 있는 상태"로 해석하여, 통상 성명, 주소, 생년월일, 성별 등을 알 수 있는 정도까지 이르러야 식별을 인정하였다고 한다[250].

따라서 운전면허번호, 여권번호와 같은 정보에 대해서도 그 자체로 개인식별을 가능케 하는 정보인지에 관하여 다툼이 있었을 뿐 아니라[251], 더 나아가 현실적인 인간의 시점에서는 개인을 특정할 수 없으나 정보통신기술을 활용하여 개인을 구별해 내고 그 개인에

---

[248] 內閣官房 個人情報保護擔當室(주246), 7면; 日巴置美·板倉陽一郎(주242), 30면; 森亮二, "パーソナルデータの匿名化をめぐる議論(技術検討ワーキンググループ報告書)", ジュリスト `2014年 3月(No.1464), 有斐閣,28~29면

[249] 衆議院 內閣委員會(주244), 平井 의원의 질문에 대한 山口 국무대신 발언. 日巴置美·板倉陽一郎(주242), 31면도 위 발언을 그대로 인용하고 있다.

[250] 森亮二, "実務解説 平成27年改正個人情報保護法 第2回 個人情報の定義", NBL No.1061(2015.11.1.), 商事法務 `42면

[251] 森亮二(주250), 42면

접촉하거나 도달하는 데 쓰일 수 있는 류의 정보들에 대해서는 식별이 지속적으로 부정되어 왔다. 예컨대 일본 경제산업성의 “개인정보의 보호에 관한 법률에 관한 경제산업문야를 대상으로 하는 가이드라인”(2014)은 법인 등의 단체정보, 통계정보와 함께 “기호와 숫자 등의 문자열만으로 특정개인의 정보인지 아닌지를 구별을 할 수 없는 메일 주소 등의 정보”는 개인정보에 해당하지 않는다고 명시하고 있으며[252], 총무성의 “이용자시점에 입각한 ICT 서비스에 관련한 제문제에 관한 연구회”도 쿠키 기술을 사용하여 생성된 식별정보, 휴대전화 사업자가 계약자에게 할당하는 계약자 고유ID(휴대전화 단말 정보와 웹서핑을 하는 브라우저 정보를 포함한다) 등에 대하여 개인식별성을 명시적으로 부정한 바 있다(물론 이러한 정보들도 다른 정보와 용이하게 조합되어 개인을 식별할 수 있는 경우에는 개인정보에 해당할 수 있다)[253].

2) 개정법상의 식별 개념

개정법상의 개인식별부호 개념은 이러한 배경 아래에서, 구법과 동일한 식별 개념을 유지하는 한편 식별되었다고 볼 수 있는 구체적 사례를 명확히 하고자 한 것으로, 중요한 의미를 갖는다. 개정법 제2조 제2항의 개인식별부호란 첫째, 특정 개인의 신체적 특징을 전자적 처리를 위하여 변환한 문자, 번호, 기호 기타 부호로 당해 개인 식별이 가능한 것(제1호) 또는 둘째, 개인에게 제공된 상품·서비스와 관련하여 할당되거나 개인에게 발행된 카드 등에 기재·기록된 문자·번호·기호 기타의 부호로서, 사람마다 다르게 할당·기재·기록됨으로써 특정 개인 식별이 가능한 것(제2호)으로서, 政令으로 정하는 것이다. 일응 제1호의

[252] 経済産業省, 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン, 2014

[253] 利用者視点を踏まえたICTサービスに係る諸問題に関する研究会 第２次提言, 2010

개인식별부호에는 지문인식 정보, 유전자 정보, 얼굴사진 등이, 제2호의 개인식별부호에는 여권번호, 운전면허번호, 신용카드 번호 등이 해당될 것이나, 최종적인 범위는 정령에 따라 결정될 것이다. 이와 같이 개인식별부호를 법률에 의하여 정하지 않고 정령으로 정하는 이유는, 개인정보 처리와 관련된 정보통신기술의 변화 및 국제적 규범 지형 변화에 유연하게 대응하기 위한 것이라고 한다[254].

2016년 9월 현재 개인식별부호의 내용을 정하는 政令은 존재하지 않으나, 개정법의 입법 과정에서 정부가 개인식별부호 해당 여부를 판단하는 기준을 제시한 바 있다. 개인식별부호란 그 자체로 개인식별이 가능한 것으로 인정되는 부호이므로, 무엇이 여기에 해당하는지를 판별하는 기준이 곧 '식별' 개념의 기준이라고도 할 수 있을 것인바, 식별 개념을 고찰함에 있어 이러한 기준의 검토는 필수적이라 생각된다. 2015. 5. 8. 개정법안에 대한 衆議院 내각위원회의 제2차 대정부질문에서 야마구치(山口) 국무대신은 시오가와(塩川) 의원의 질문에 대하여 일의성(개인과 부호가 1대 1의 관계로 대응되는 것), 불변성(부호의 변경이 빈번하게 일어나지 않는 것), 본인도달성(부호에 기초해서 직접 개인에게 접근하는 것이 가능할 것)이라는 기준을 제시하였다[255].

이러한 기준에 따라 구체적으로 어떤 정보에 '식별성'이 인정되는지에 관하여, 정부측 참고인인 무카이(向井) 변호사는, "단지 기기에 부여된 휴대전화 통신단말 ID는 개인식별부호에 해당하지 않고" (...) 운전면허증 번호, 여권번호, 기초연금번호는 개인식별부호이며, 휴대전화번호, 신용카드 번호, 메일 주소 또는 서비스 제공을 위한 회원 ID는 "여러 가지 계약 형태와 운용 실태가 있기 때문에 현시점에서는 일률적으로 개인식별부호에

254 日巴置美·板倉陽一郎(주242), 34면

255 衆議院 內閣委員會(주244), 塩川 의원의 질문에 대한 山口 국무대신 발언

해당한다고 말하기 어렵다”는 입장을 표명하였다[256].

3) 소결

이상에서 살펴본 바와 같이, 개정법의 제정 과정에서 ‘일의성’, ‘불변성’, ‘본인도달성’이 식별의 개념 요소로 제시되고, 여기에 따라 종래 논란의 대상이 되었던 운전면허증 번호, 여권번호 등의 식별성 유무가 상당 부분 정리되는 등 식별 개념이 보다 분명해진 것으로 보인다. 이로써 구법상 묵시적으로 통용되던 ‘어디의 누구인지 알 수 있는 정보’라는 막연한 기준이 지양되었고, ‘어디의 누구인지 알 수 없는 정보’라도 일정한 성질을 가지면 개인정보에 해당함이 명백하여졌다고 볼 수 있다[257].

그러나 위와 같은 기준에 따르더라도 일의적인 식별성 판단이 가능하다고 단정할 수는 없을 것이며, 결국 개별 기준에 대한 해석이 필요할 것이다. 특히 단말 ID가 개인식별부호에 해당하지 않는다는 입장에 대하여는, 예컨대 휴대전화의 경우 단말과 개인의 관계가 긴밀하여 단말의 ID와 개인이 일의성, 불변성, 본인도달성이라는 세 가지 요건을 모두 충족할 수 있으며, 기계 ID라고 하여 식별성을 인정하지 않는다면 예컨대 기계를 초소화하여 인체에 이식할 경우라 할지라도 식별성을 인정하지 않아야 하는 것 아닌가라는 비판적 견해가 존재한다[258]. 일본 정부

---

[256] 衆議院 内閣委員會(주244), 塩川 의원의 질문에 대한 向井 참고인 발언

[257] 森亮二(주250), 42면. 그런 한에서 구법에서 개인정보에 해당하지 않았던 정보가 신법에서 개인정보에 해당할 수도 있게 된다는 언급으로, 宇賀克也, “個人情報・匿名加工情報・個人情報取扱事業者”, ジュリスト `2016年 2月(No.1489), 有斐閣, 37면

[258] 宇賀克也 外 5, 座談會 “個人情報保護法・マイナンバー法改正の意義と課題”, ジュリスト `2016年 2月(No.1489), 有斐閣, 17면, 長田三紀, 森亮二 발언 참고. 同旨, 小向太郎, “ライフログの利活用と法律問題", ジュリスト `2014年 3月(No.1464), 有斐閣, 55면; 日巴置美·板倉陽一郎(주242), 34면

또한 이 점을 의식하여 구체적인 판단은 기술 진보, 변화하는 사회 실태, 외국에서의 동향을 충분히 고려하고 전문가의 의견을 반영하여 이루어질 것이라고 유보한 바 있다[259].

(나) 용이조합성 개념에 관한 일반적 해석

일본에서도 "다른 정보와 용이하게 照合하는 것이 가능하여, 그에 의하여 특정의 개인을 식별할 수 있게 되는 것"이라는 제2조 제1항 제1호 단서의 해석, 보다 구체적으로 '용이하게 照合[260]하는 것이 가능(이른바 용이조합성)'한지 여부를 어떻게 판단할 것인가의 문제가 매우 중요하다. 이는 유럽 개인정보보호지침의, 어떤 추가적 정보가 '합리적으로 사용될 수 있는' 수단인가를 판단하는 문제와 체계상 상통하는 것으로 보인다.

용이조합성의 판단 기준에 대하여, 개인정보취급사업자 [261] 를 중심으로, 그가 통상적·일반적으로 수행하는 업무의 내용 및 방식에 비추어 용이하게 결합할 수 있는지를 검토함으로써 상대적·개별적으로 판단한다는 원칙이 확립되어 있으며, 이 부분에 관해서는 異論이 없다.

이 원칙의 구체적 적용에 관하여는, "보유하고 있는 각 정보에 악세스할 수 있는 자의 존부, 사내 규정의 정비 등의 조직적인 체제, 정보 시스템의 악세스 제어 등의 기술적인 체제, 취급하는

---

[259] 衆議院 內閣委員會(주244), 塩川 의원의 질문에 대한 山口 국무대신 발언

[260] 여기서 '照合'이란 '서로 대조해 봄으로써 확인하는 것'을 의미한다 dictionary.goo.jp). 비록 우리말에서 흔히 쓰이는 '組合'과는 다른 한자를 사용하고 있지만, 일본에서도 두 단어를 혼용하여 사용하는 사례가 있는 것으로 보아 이 단어에 특별한 의미가 있는 것 같지는 않다. 宇賀克也(주242), 34면 참고.

[261] '개인정보처리자'에 상응하는 일본법상의 개념이다. 개정법 제2조 제5항.

개인정보의 내용과 이활용의 방법” 등이 고려 요소가 된다[262]. 그 결과 “다른 사업자에게 통상의 업무로는 행하고 있지 않은 특별한 조회를 하거나, 당해 타 사업자에 있어, 상당한 조사를 해서야 비로소 회답이 가능한 경우”는 물론 심지어 내부 조직 간에서도 “시스템의 차이 때문에 기술적으로 조합이 곤란한 경우, 조합을 위하여 특별한 소프트웨어를 구입하여서 인스톨하는 필요가 있는 경우”[263], “사내 규정 등에 의하여 용이하게 악세스할 수 없도록 되어 있는 경우”[264]에도 용이조합성이 부인된다는 것이 일본 경제산업성[265] 및 학계의 지배적인 견해이다[266].

(다) 개인정보의 제3자 제공에 있어서 용이조합성의 판단 기준

그런데, 개인정보취급사업자에게 개인정보이면 이를 익명화·가명화하여 제3자에게 제공하는 행위도 개인정보 제공에 해당하는가라는 문제에 대해서는 비교적 뚜렷한 견해 대립이 있는 것으로 보인다. 먼저 부정설은 정보를 제공받는 상대방에게 식별가능성이 없으면 개인정보의 제공이 아니라고 보나[267], 동조하는 견해는 많지 않다고 한다[268]. 긍정설은, 개인정보취급사업자를 기준으로 개인정보성을 판단하는 기준을 일관되게 적용함으로써 일단 정보를 제공하는 개인정보취급사업자에게 개인정보라면 그 정보의 제공은

---

[262] 瓜生和久(주243), 13면; 日巴置美·板倉陽一郎(주242), 43~46면. 同旨, 宇賀克也(주242), 35면

[263] 宇賀克也(주242), 29면; 同旨, 内閣官房 個人情報保護擔當室(주246), 7면

[264] 瓜生和久(주243), 13면

[265] 同旨, 経済産業省, 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」に関するQ&A, 2014, Q&A.14

[266] 이 부분에 대해서는 비판적인 견해가 없지 아니하다. 대표적인 것으로, 森亮二(주248), 25면 이하를 참고

[267] 岡村久道, 個人情報保護法, 新訂版, 有斐閣, 2009, 34면

[268] 森亮二(주248), 26면

개인정보의 제공에 해당하는 것으로 보아야 한다는 견해이다. 이는 일본 정부의 입장이기도 하다는데, 그 논거는 다음과 같다[269].

첫째, 제3자 제공에 관하여 정보주체의 동의 등을 받을 개인정보보호법상 의무는 개인정보취급사업자에게 부과된 의무이므로, 개인정보취급사업자의 행위시에 그 행위가 여기에 해당하는지가 분명해야 하는데, 정보를 수령한 제3자가 제공받은 정보를 이용하여 식별을 할 것인지, 할 수 있는지 여부는 제공 후의 사정이므로 이를 제공행위의 성립 요건으로 제공행위시에 고려하는 것은 옳지 않고, 둘째, 제3자의 사정을 제공행위의 요건으로 고려한다면, 사업자 입장에서는 그 제3자가 제공된 정보를 이용하여 식별을 할 의도가 있는지, 식별을 할 능력이 있는지 등을 살펴야 할 것인데, 현실적으로 정보를 제공하는 사업자는 그러한 의도와 능력에 관하여 정확히 알기 어려우므로, 결국 제3자 제공의 성립 여부는 구체적인 상황에 따라 사업자에게 그 의도와 능력을 파악할 주의의무가 있는지, 주의의무가 있다면 그 정도는 어떠한지의 판단 문제로 귀결된다. 이러한 접근은 정보주체에게 손해가 발생하였을 때 사후적으로 민사상 불법행위에 기한 책임 유무를 판단하는 데 적합한 것으로, 행정적 규제로서의 개인정보보호법 즉 개인의 권리이익침해와 관련이 있는 특정의 행위유형에 대한 사전적·일률적 규범으로서의 개인정보보호법의 적용 기준으로서는 부적합하다. 셋째, 부정설에 따를 경우 정보를 제공받는 제3자를 기준으로 어떤 정보가 개인정보취급사업자에게 개인정보인지 여부를 결정하게 되는바, 이는 사업자를 기준으로 조합용이성을 판단하는 확고한 원칙과 모순된다. 넷째, 개정법은 익명가공정보 개념을 도입하고, 익명가공정보의 재식별화 금지의무, 금지의무의

[269] 이하 긍정설의 논거는 鈴木正朝, “個人情報保護法のグローバル化への対応”, ジュリスト `2016年 2月(No.1489), 有斐閣, 62~64면의 논지를 정리한 것이다. 일본 정부가 긍정설을 지지하고 있다는 입장도 위 논문에서 인용한 것이나, 이를 지지하는 일차 문헌은 발견하지 못하였다.

위반시 부과되는 제재, 개인정보보호위원회의 조사 권한 등을 규정하고 있으므로, 긍정설을 따를 경우 발생할 수 있는 정보 활용 저하 등의 문제는 이러한 규정을 통하여 해결될 수 있다.

다. 익명가공정보

일본의 개정 개인정보보호법은 제2조 제9항에서 '익명가공정보'라는 개념을 도입하고 있다. 여기에 따르면 '익명가공정보'란 "개인정보를 특정의 개인을 식별하는 것이 가능하지 않도록 가공하고, 또 당해 개인정보를 복원하는 것이 불가능하도록 한 것"이다.

여기서 '특정의 개인을 식별하는 것이 가능하지 않다'는 것은 개인식별이 절대적으로 불가능한 상태를 의미하지는 않는다고 이해된다. 통상인의 능력으로 특정의 개인을 식별할 수 없고, 원래의 개인정보로 복원 불가능한 정도면 족하다고 한다[270]. 구체적으로, 식별자의 삭제, 상세 항목의 치환, 교환 방법, 노이즈 추가 등의 방법 등을 생각해 볼 수 있다[271]. 여기에서 알 수 있듯이, 통계 정보와 같은 것은 익명가공정보라기보다는 애초에 개인정보가 아니어서 개인정보보호법의 적용을 받지 않는 것으로 이해된다[272].

이러한 익명가공정보는 정보의 제3자 제공(제23조 제1항) 및 목적외 이용(제16조)에 있어 정보주체의 동의를 요하지 않는다. 따라서 위 나.(다)항에서 언급한, 개인정보 제3자 제공시 발생하는 문제를 해결할 수 있게 되는 셈이다. 그러나 이러한 제3자 제공과 목적외 이용이 제한 없이 허용되는 것은 아니고, 재식별 방지 및

[270] 瓜生和久(주243), 41면

[271] 瓜生和久(주243), 42면

[272] 瓜生和久(주243), 40면

정보주체의 통제권 보호를 위한 일정한 제한이 필요하다. 즉, ① 개인정보보호위원회 규칙이 정하는 기준에 따라 적정한 가공을 하는 것, ② 익명가공정보를 작성한 때에는 개인정보보호위원회 규칙이 정하는 기준에 따라, 삭제한 정보와 가공의 방법에 관한 정보의 누설을 방지하기 위하여 안전관리조치를 강구하는 것, ③ 작성한 익명가공정보에 포함되는 정보의 항목을 공표하는 것, ④ 작성의 기초가 된 개인정보의 본인을 식별하기 위한 행위를 하지 않을 것 등이 요구된다(개인정보보호법 제36조 제1항 내지 제5항).

라. 소결

이상에서 살펴본 바와 같이, 일본도 처리자를 기준으로 개인정보 여부를 판단한다.

처리자는 식별 가능하나 제공받는 자는 식별 불가능한 제3자 제공의 경우 개인정보의 제공에 관한 규정의 적용을 인정하는 원칙을 가지고 있다. 다만, 이 경우 발생할 수 있는 불합리를 익명가공정보라는 개념으로 해결하고자 한다는 점이 일본법의 두드러진 특징이다. 동일한 처리자의 서로 다른 구성부분이 개인정보와 개인을 알아볼 수 없는 정보를 보유하고 있는 경우 '용이조합성'을 부정하고 있다는 특징도 주목할 만한 부분이다.

이러한 관점에서 보면 키 코드화된 정보의 경우, 그것이 익명가공정보에 해당한다면 자유로운 제공이 가능할 것이다. 유동 IP주소에 관하여는, 처리자를 기준으로 판단한다는 입장이 확고하므로, 식별에 필요한 추가적 정보를 보유하고 있지 않은 CP에 대해서라면 개인정보성이 부정될 가능성이 커 보인다.

6. 소결론

이상에서 개인정보 개념, 그리고 그 자체로 식별이 어려운 정보를 제3자에게 제공하였을 경우의 처리에 관한 외국의 해석례들을 검토해 보았다.

먼저 식별가능성의 판단 기준에 관하여, 유럽연합과 독일의 경우 정보를 처리하는 자 외에 다른 제3자의 관점 및 불법한 수단의 사용가능성까지 광범위하게 고려한다는 입장이었으나, Breyer 판결(CJEU Case C-582/14 Patrik Breyer v. Deutschland)로 인하여 정보를 처리하는 자를 기준으로 하며, 적법한 수단만을 고려한다는 쪽으로 정리될 것으로 보인다. 영국, 일본도 마찬가지로 정보를 처리하는 자 기준으로 식별가능성을 평가하고 있다. 한편, 일본의 경우 그 자체로 개인식별이 어려운 정보와 그 정보와 결합하여 개인식별을 가능하게 하는 추가정보가 한 개인정보처리자 내부에 있더라도 각각의 정보에 대한 취급부문이 다르면 그 자체로 개인식별이 어려운 정보를 개인정보로 취급하지 않는다는 견해가 우세한 특징이 있다.

그 자체로 개인식별이 어려우나 개인정보처리자에게는 개인정보에 해당하는 정보의 제공행위를 어떻게 취급할지의 문제에 관해서는, 국가마다 태도가 일치하지 않고 있다. 영국의 경우 이를 개인정보의 제공으로 보지 않는 것이 일반적인 경향으로 보인다. 일본의 경우 개정 개인정보보호법이 '익명가공정보'라는 개념을 도입함으로써, '익명가공정보'의 요건을 충족하고 그에 수반하는 의무들을 준수하면 그러한 정보의 제3자 제공이 폭넓게 허용될 수 있다는 특징이 있다. 이로써 결과적으로는 영국과 유사하게 그러한 제3자 제공의 가능성이 열리게 된 것이다. 반면 유럽연합, 독일, 일본의 경우 그러한 정보의 제공이라도 개인정보의 제공으로 취급하는 입장으로 생각된다.

그러나 그것이 유럽연합이나 독일에서도 우리나라와 같이 정보주체의 동의나 법령상 근거가 없이는 그러한 정보를 제공할 수 없다는 것(개인정보보호법 제17조 제1항 참고)을 의미하지는 않는다. 그러한 제공을 개인정보의 제공으로 관념할 것인지의 문제와, 개인정보에 관한 구체적인 행위규범이 그러한 제공을 어느 수준까지 허용하고 있는지는 다른 문제이기 때문이다. 독일법에 관하여는 어느 정도 추가적인 연구가 필요하나, 적어도 유럽연합 개인정보보호지침 하에서는. 뒤에서 언급하다시피, 정보주체에 대한 적절한 보호조치가 갖추어져 있다면 그러한 제공이 허용될 가능성이 존재한다.

IV. 우리 개인정보보호법상 개인정보 개념에 관한 검토

1. 서론 – 개인정보 자기결정권의 인정 의의

이상에서의 검토 결과를 바탕으로, 이하에서는 우리 개인정보보호법과 정보통신망법상 개인정보 개념을 어떻게 해석하여야 할지에 관하여 검토해 보겠다. 우선, 그 논의의 전제로서 개인정보 자기결정권 개념에 관하여 간단히 살펴보기로 한다.

개인정보 자기결정권이란, 헌법재판소 2005. 5. 26.자 99헌마513, 2004헌마190(병합) 결정 등에 따르면 “자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리”를 말한다. 정보화기술의 발달로 개인에 관한 정보가 무제한으로 집적 및 유통될 수 있게 됨으로써 개인의 결정의 자유가 침해당하며 자유민주체제의 근간이 총제적으로 훼손될 가능성을 예방하기 위하여, 헌법 제10조, 헌법 제17조, 자유민주질서, 국민주권의 원리 등에 기하여 인정되는 권리라는 점은 앞서 살펴본 바와 같다. 우리 헌법재판소에 따르면 이 권리는 헌법 제37조 제2항에 따라, 비례원칙과 명확성의 원칙 등 기본권 제한의 일반 원칙에 따라 제한 가능하고, 다른 기본권과의 충돌이 발생하는 경우에도, 기본권 충돌의 일반 법리의 적용을 받는다. 상충하는 법익들의 보호와 제한 사이의 비례성 심사가 필요한 것이다.

즉, 개인정보 자기결정권은 어떤 경우에도 우선적으로 관철시켜야만 하는 절대적인 권리가 아니다. 다른 기본권과 마찬가지로 정당한 목적에 의하여 비례원칙에 따라 제한될 수 있다. 언론·출판의 자유,

직업의 자유 등 다른 기본권과의 충돌이 발생하는 경우에도 이 권리가 다른 기본권보다 우선하는 것이 아니라 비례원칙에 따라 상충하는 다른 권리와 조화롭게 공존하는 방향을 모색하여야 한다.

이 점은 개인정보 자기결정권이 유래한 독일에서도 마찬가지이다. 독일 연방헌법재판소가 인정한 '정보자기결정권'은 우리의 '개인정보 자기결정권' 개념과 비교하였을 때 그 개념 및 제한 원리에 있어 매우 유사한 것을 발견할 수 있었다[273]. 특히 독일 연방헌법재판소는 정보자기결정권 침해에 있어 "개인정보의 종류, 수집 목적, 정보를 처리하는 기술에 고유한 처리가능성과 연결가능성(Verarbeitungsmoeglichkeiten und Verknuepfungsmoeglichkeiten) 등 구체적 사정을 고려함으로써 개인정보를 수집하는 행위가 정보자기결정권의 침해에 해당하는지 여부를 판단하여야 한다"고 명시하였다[274]. 즉, 개인정보 자기결정권의 보호는 다른 충돌하는 기본권의 보호 또한 염두에 두면서, 구체적인 상황을 최대한 고려하여 유연하게 접근해야 하는 것이다.

---

[273] 다만 '자기 정보를 통제할 수 없는 개인은 사회생활상의 각종 결정에 있어 위축될 수 밖에 없고, 특히 국가와의 관계에서는 집회 및 결사의 자유와 같은 정치적 표현과 관련된 자유가 제약당할 수 밖에 없다'는 점을 정보자기결정권의 존재이유로 명시함으로써 정보자기결정권의 규범적 가치를 우리나라 헌법재판소에 비하여 보다 구체적으로 설명하고 있다는 차이를 찾을 수 있다. 즉, 우리나라 헌법재판소의 논리에 따르면 '정보화기술의 발달로 개인에 관한 정보가 무제한적으로 집적 및 유통'되는 것과 "개인의 결정의 자유 침해", 더 나아가 '자유민주체제의 근간의 훼손'이 서로 어떠한 관련성이 있는지가 다소 불투명한데 독일 연방헌법재판소는 이 점을 보다 구체적으로 설명하여 주고 있는 것이다. 개인정보의 보호, 익명으로 행동할 권리가 시민적 자유의 중요한 부분이라는 인식은 우리나라의 개인정보자기결정권 개념의 해석에 있어서도 매우 중요한 시사점이라 생각된다.

[274] BVerGE 65, 1(45)

2. 관련성 개념에 관하여

우리나라에서는 관련성 요건은 별로 논의되고 있지 않지만, 유럽에서는 여기에 관한 논의가 비교적 활발하다. WP29와 같이 내용, 결과, 목적에 있어서의 개인관련성만 있으면 관련성을 인정하는 견해도 있으나[275], 유럽사법재판소는 YS 사건 판결[276]에서 특정인의 개인정보에 근거하여 도출된 문서라고 하여 바로 개인에 관한 정보인 것은 아니고, 개인이 타인이 보유하고 있는 그러한 정보에 대하여 접근권(access right)을 행사함으로써 그 정보가 정확하고 적법한지 여부를 점검하도록 하는 것이 타당한 경우에 한하여 개인에 대한 관련성을 인정할 수 있다고 판시함으로써 개인관련성을 제한적으로 해석하였다. 향후 우리나라의 논의에서도 참고 가치가 있는 부분이라 생각된다.

3. 식별 가능한 개인에 관한 정보 v. 개인을 식별할 수 있는 정보

먼저, 개인정보 개념에 관하여, 우리 법은 공통적으로 “개인을 알아볼 수 있는 정보”라는 문언을 사용하고 있다(개인정보보호법 제2조 제1호, 정보통신망법 제2조 제1항 제6호). 일본 또한 “특정의 개인을 식별할 수 있는 것”(신법 제2조 제1항)으로 규정하고 있다.

한편 유럽연합은 “식별된 또는 식별 가능한 자연인에 관한 정보”(개인정보보호지침 제2조 (a)), 독일은 “식별된 또는 식별 가능한 자연인의 인적 물적 관계에 관한 개별 정보”(BDSG 제3조

---

[275] WP29(주73), pp.10~12

[276] CJEU Joined Cases C-141/12 and C-372/12 YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S(2014)

제1항), 영국은 "식별될 수 있는 생존하는 개인에 관한 정보"(DPA 제1조 (1))라고 각 규정함으로써 "식별된 또는 식별 가능한 개인에 관한 정보"라는 규정형식을 취하고 있다.

이와 같이 우리나라와 유럽 개인정보보호법의 개인정보 개념은 문언상 차이를 보이고 있다. 과연 '개인을 식별할 수 있는 정보'와 '식별된 또는 식별 가능한 개인에 관한 정보'는 의미론적으로 다르게 취급되어야 하는 것인가? 즉, '개인을 식별할 수 있는 정보'란, 그 문언만 놓고 보면 '식별에 사용될 수 있는 정보'를 의미하는 것처럼 보인다. 이로부터 즉각적으로 연상되는 개념은 바로 '식별자(identifier)'이다. 반면 '식별된 또는 식별 가능한 개인에 관한 정보'는 식별에 사용될 수 있는 정보 뿐 아니라, 개인이 식별되었거나 식별 가능함을 전제로 그 개인에 관한 일체의 속성(attribute)까지 포함하는 것처럼 보인다. 이렇게 보면, 두 개념 사이에는 의미론적인 차이가 있는 것이다.

그러나 이러한 외관상 차이에도 불구하고, 다음의 두 가지 이유에서 두 개념은 사실상 동일한 것으로 취급되어야 한다는 것이 필자의 견해이다.

첫째, 식별자만이 '개인을 식별할 수 있는 정보' 즉 개인 식별에 사용될 수 있는 정보인 것은 아니며, 어떤 정보이든지 개인 식별에 사용될 수 있다. 흔히 식별자에는 직접적 식별자(direct identifier)와 준식별자(quasi-identifier) 또는 간접적 식별자(indirect identifier)가 있다고 한다. 먼저, 직접적 식별자는 "정보 내의 모든 사람들에게 구조적으로 고유한(unique) 속성(attribute) 또는 속성의 조합"을 말한다[277]. 주민등록번호, 지문, 홍채 스캔 결과, 전화번호, 신용카드 번호, 유동 IP 주소 같은

[277] Elliot et al.(주210), p.81

것이 여기에 해당한다[278]. 간접적 식별자란 특정 정보집합물 내에서 또는 전체 인구집단 내에서 몇몇 개인에게 고유할 수 있는 속성이다. 성별, 연령 같은 것이 통상 여기에 해당한다고 한다[279]. 그러나 이와 같이 '식별자'로 취급되는 정보 이외의 다른 모든 정보도 정보가 처리되는 맥락에 따라서는 '개인을 식별할 수 있는 정보'가 될 수 있다. 예컨대 甲이 보유하고 있는 A라는 사람에 관한 정보가 그 사람에 대한 성명, 전화번호, 연령, 2016년 3월의 소득, 그 기간 동안의 대출금액, 보유 차량의 브랜드라고 하자. 그리고 乙이라는 사람은 동일한 사람에 대하여, 2015년 3월의 소득, 그 기간 동안의 대출 금액, 신용카드 사용액을 알고 있다고 가정하자. 乙은 자신의 보유 정보를 甲이 보유하고 있는 정보와 결합하는 방식으로 이용함으로써 A라는 사람의 성명, 연령 및 보유 차종까지 알게 되었다. 그런데 乙이 보유한 바와 같은 정보 즉 일반적으로는 한 개인의 2015년 3월의 소득이나 대출 금액 같은 정보는 '개인을 식별할 수 있는 정보'가 아니라고 여겨질 것이다. 그러나 乙은 그러한 정보를 개인을 식별하는 데 적어도 간접적으로라도 사용하였다(즉, 이 정보는 이른바 '기본 변수key variable'로 사용되었다고 할 수 있다). 그러므로 구체적인 맥락에서 반드시 식별자만이 '개인을 식별할 수 있는 정보'가 되는 것은 아니다. 모든 정보가 이와 같은 논리로 '개인을 식별할 수 있는 정보'가 될 수 있다. 독일 연방헌법재판소가 "사소한 정보란 더 이상 존재할 수 없다"[280]고 한 것도 이런 취지에서 이해할 수 있을 것이다.

---

[278] Elliot et al.(주210), p17

[279] Elliot et al.(주210), p.81

[280] BVerfGE, 65,1 (44, 45)

둘째, 개인정보 자기결정권을 보호하는 취지상, ‘개인을 식별할 수 있는 정보’와 ‘식별 가능한 개인에 관한 정보’를 분리하여서는 아니되며, 실제 우리 실무도 그와 같이 취급하고 있지 않다. 위 사례에서, 乙은 정보 결합을 통하여 A라는 사람의 ‘보유 차종’이라는, A에 관한 새로운 정보를 알게 되었다. 이 정보는 개인을 식별하는 데 사용되지 않았다. 그렇다면 이 정보는 위 사례에서 ‘개인을 식별할 수 있는 정보’가 아니라 ‘식별된 개인에 관한 정보’일 뿐이므로 개인정보가 아니라고 할 것인가? 그렇지 않다. ‘보유 차종’ 자체는 개인정보가 아니고, 위 정보 상황(data situation)에서 개인식별에 사용되지 않을지 몰라도, 이미 다른 정보에 의하여 식별된 또는 식별 가능한 개인과 연결지워지는 순간 개인에 관한 새로운 사실을 알게 한다. 앞서 살펴본 바와 같이, 개인에 관한 원치 않는 정보의 수집 및 처리로부터 개인을 보호함으로써 개인의 결정의 자유를 보장한다는 개인정보자기결정권의 취지가 바로 이 지점을 겨냥하는 것이다. 그러므로 이러한 정보는 개인정보로 취급하여야 하고, 그러한 정보를 새로 취득하는 행위는 개인정보의 수집에 해당할 것이다[281]. 실제로 우리 실무도 이러한 정보의 수집을 개인정보의 수집에 해당한다고 보는 것이 일반적이다.

그러므로, 우리나라 및 일본의 ‘개인을 식별할 수 있는 정보’와 유럽의 ‘식별된 또는 식별 가능한 개인에 관한 정보’는 동일한 개념이라고 생각되고, 앞으로 이러한 전제를 기초로 논의를 진행하기로 한다.

---

[281] 同旨, Elliot et al.(주210), p.21 “속성의 부여(attribution)만으로도 비밀성(confidentiality)을 깰 수 있다. ICO는 신뢰할 만한 속성 부여는 DPA 해석에 있어 재식별로 취급한다.”

4. 식별 개념의 해석

가. 문제의 소재

식별 개념이 기본적으로 '한 그룹의 사람 중 한 사람을 다른 사람과 구분 내지 구별하는 것'을 개념요소로 한다는 점에서는 외국에서든 우리나라에서든 이론이 없어 보인다[282].

그러나 영국에서는 ICO가 '개인이 구분되어 다른 사람들과 다르게 취급될 수 있는 것'을 식별로 본다고 함으로써[283] '다른 사람들과 다르게 취급될 수 있는 가능성'이라는 요소를 추가하고 있으며, 우리나라의 일부 견해는 여기에 더하여, '개인식별정보(PII)와의 결합'이라는 요소를 요구하면서 쿠키나 단말 ID의 존재만으로는 식별을 인정할 수 없다고 함으로써[284], 거의 개인의 신원까지 특정되어야만 '식별'을 인정하고 있다(일본의 종래 통설이라는 '어디의 누구인지 알 수 있을 정도'라는 개념[285]도 이와 유사한 태도인 것으로 이해된다). 요컨대 식별의 개념에 관하여 '구분'설, '구분+다르게 취급될 수 있는 가능성'설, '구분+신원확인'설이 있다고 간단히 정리할 수 있을 것이다. 과연 이와 같은 세 가지 견해 중 어떤 것이 타당한가?

나. '식별'에 관한 각 학설의 검토

---

[282] 행정안전부(주32), 8면; 이창범(주25), 18면; 경정익(주39), 94면; WP29(주73), p.12; Peter Carey(주196) , p.21 등

[283] Peter Carey(주196), p.21

[284] 박상철(주40), p,120. 이 견해가 '식별'의 개념을 정의하면서 '개인식별정보'라는 개념을 사용함으로써 동어반복을 범하고 있다는 점에 관하여는 앞서 설명한 바 있다.

[285] 森亮二(주250), 42면

이 문제를 구체적으로 살펴보기 위하여, 예컨대 어떠한 직접적 식별자나 정확한 간접적 식별자도 포함하지 않고 오로지 속성만으로 구성된 정보집합물로서, 개인은 오로지 1부터 100까지의 일련번호로만 표시되는 아래와 같은 표를 가정해 보자. 다음 각각의 경우, 개인은 식별되었다고 볼 수 있는가[286]?

일련번호	연령	병명	입원기간	투약한 약물	부작용	…
1	40대	간암	1년	A	없음	…
2	50대	위염	없음	B	있음	…
3	30대	폐렴	3주	C	없음	…
…						
100	60대	공황장애, 심장병	없음	D	없음	…

i) 일련번호 '100'을 실제 개인 누군가의 신원과 연결시킬 만한 어떠한 고리도 존재하지 않는 상황. 그러나 이 표에서 환자 100은 환자 1, 그리고 나머지 다른 환자들로부터 구분 내지 구별 가능하다.

ii) 환자 100이 실제로 강남구에 거주하는 60세 여성 '최순심'이라는 추가 정보가 있는 경우

iii) 위의 ii)와 같은 추가 정보는 없지만, 위 데이터가 甲이 자신이

[286] 여기서는 '식별가능성'이 아니라 '식별'의 개념을 논하는 것이므로, 이 정보가 추가적으로 다른 사람에게 전달되어 다른 정보와 결합하는 등의 경우에 관하여는 생각하지 않기로 한다

개발한 태블릿 PC용 건강관리 앱을 통하여 수집한 정보로서, 태블릿의 기기 ID, 유동 IP 등과 같은 추가 정보와 함께 앱을 통한 서비스 제공(예컨대 각각의 상황에 맞는 건강 조언을 전달하는 서비스)에 사용된 경우

우선 ii)의 경우 위의 세 가지 설 어느 것에 의하더라도 개인이 식별되었다는 점에 대해서는 이론이 없을 것이다.

i) 의 경우는, 우선 위 정보의 존재가 현실의 개인에 대하여 미칠 수 있는 영향이 거의 미미할 것이다. 즉, "간암에 걸려 1년간 입원하며 A라는 약물 치료를 받았으나 부작용은 발견되지 아니한 40대의 사람' 이라는 정보가 특정한 개인에게 무슨 영향을 미칠 수 있을지 생각해 내는 것은 거의 불가능해 보인다. 그렇다면, 개인정보자기결정권의 취지에 비추어 볼 때, 이러한 정보의 사용을 법적으로 규율할 이유가 있을까? 이러한 상태를 '식별'로 봄으로써 위 정보를 개인정보로 처리하는 것은 바람직하지 않아 보인다. "개인정보라는 관점에서는, 비밀로 되어야 할 것(confidential matter)은 그 정보가 특정 개인에 관련되어 있다는 점이다. 정보주체로서, 나는 (보통) 어떤 정보 사용자가 나의 속성을 가진 한 사람이 있다는 것을 안다고 해서 별로 신경쓰지 않는 것이다." [287] 개념적으로 보더라도 이와 같이 어떤 속성의 집합이 한 정보집합물에서 단 하나만 존재하는 경우, 이를 '유일하다(unique)' 고 일컫는다. 속성들의 유일한 결합이 유일할 경우 해당 개인이 식별될 가능성이 비교적 높아지는 것은 사실이다. 그러나 unique하다는 것은 그 자체로 식별을 의미하지 않으며, 식별과는 구별되어야 하는 완전히 다른 개념이라는 것이 일반적인 이해이다[288].

---

[287] Elliot et al.(주210), p.9

[288] Elliot et al.(주210), p.30; Ann Cavoukian and Khaled El Emam.

그러면 iii)의 경우는 어떠한가? 개인의 신원이 알려진 상태 또는 "어디의 누구인가를 알 수 있는 상태" 는 분명히 아니다. 우리나라의 일부 견해가 주장하는 바와 같이 'PII' 와 결합한 것도 아니다. 그러나 위와 같은 정보를 보유함으로써 앱 개발자는 앱을 통하여 특정 개인에게 정보를 보내거나 자기 나름의 로직을 통하여 그 개인에 대한 모종의 정보를 생성할 수 있을 것이다. 그렇다면 이 경우 환자 100에 관한 정보는 단순히 위 표 안에서 구분되는 것을 넘어, 현실의 개인으로서의 환자 100과 연결되어 그에게 일정한 영향을 미치는 데 사용될 수 있게 되었다. 그렇다면 환자 100으로서는 그러한 영향에 관하여 알고 개인정보 열람, 정정, 삭제에 관한 권리를 행사하는 등으로 이를 통제할 필요가 있을 것이다[289]. 더욱이, 이와 같이 어떤 개인을 구별하여 그에게 도달할 수 있는 상태가 있음에도 불구하고, 개인의 신원을 알 수 있는 상태에 도달하지 못하였다는 이유로 식별성을 부정한다면, 대부분의 정보처리가 기계에 의하여 이루어지므로 보통 사람들이 식별되었다고 직관적으로 생각하는 상태 즉 신원을 알 수 있는 상태에 이르지 아니하여도 정보주체에 대하여 충분한 영향을 미칠

De-identification Protocols: Essential for Protection Privacy, Information and Privacy Commissioner of Ontario, 2014, pp. 8~9

[289] 이 사례에서 앱 개발자가 태블릿 ID 번호를 암호화하거나 매번 변하는 다른 임시 ID를 사용한다고 가정하더라도, 환자 100의 위 표에 기재된 정보가 동일한 이상, 앱 개발자 입장에서는 이 표의 정보를 마치 식별자처럼 사용하여 환자 100을 다른 사용자와 구별함으로써 앱을 통하여 환자 100에게 도달할 수 있을 것이다. 그렇다면, 이미 환자 100과 위 정보 사이에 어느 정도 지속적인 관련성이 존재하므로, 식별이 있다고 보아야 할 것이며, 이러한 맥락이 있다면 반드시 태블릿 ID 등의 표지가 항구적이어야만 식별이 존재한다고 볼 수 있는 것은 아니다. 그러나 일반적으로는, 개인에 관한 다른 신원정보 없이 기계에 관련한 표지 내지 부호만이 존재하는 상황에서는, 일본 국무부의 설명과 같이, 일의성, 불변성, 본인도달성이라는 요소가 갖추어져야 개인에 대한 식별 상태를 인정할 수 있을 것이다. 衆議院 內閣委員會(주244), 塩川 의원의 질문에 대한 山口 국무대신 발언(본 논문 III.4.나. 항목 참고)

수 있다는 현대 정보화 사회의 상황에서, 개인정보 자기결정권의 보호에 소홀해지는 결과가 되는 것이 아닌가 한다. 유럽사법재판소가 *Lindqvist* 판결에서 개인은 이름 아닌 다른 수단으로도 식별 가능하다고 본 것도 이런 맥락에서 이해될 수 있지 않을까[290].

그러므로, 필자의 견해로는, 앞서 살펴본 ICO의 견해와 같이, '식별'이란 '개인이 그룹 내의 다른 개인으로부터 구분'될 뿐 아니라 구분된 정보와 개인 사이에 연결 관계가 있음으로써 그로 인하여 '다른 사람들과 다르게 취급'될 수 있는 상태를 말하는 것으로 정의되어야 하며, 반드시 '개인의 신원을 알 수 있을 것'까지 요구할 필요는 없다. 즉, "'식별되었다'는 것이 반드시 '이름을 알게 되었다(named)'는 것을 의미하지는 않고 어떤 정보와 알려진 개인 사이의 '신뢰할 만한 연결고리'를 성립하는 것만으로 충분할 수 있다"[291 292]. WP29 또한, '구별'이라는 명시적 정의에도 불구하고 실제로는 같은 태도를 취하고 있는 것으로 생각된다. 예컨대, 컴퓨터 파일링 시스템에서 개인들을 그 성명이 아니라 고유한 ID를 사용하여 구별하는 경우, 또는 개인이 사용하는 특정 단말의 ID만을 보유하고 있는 경우, 관련 개인의 성명이나 주소에 관한 정보가 없어도 그를 다른 사람과 구분/구별할 수 있고, 그를 범주화하여 그에게 영향을 미치는 어떤 결정을 할 수 있다면 개인의 식별을 인정해야 한다는 것이다[293294].

---

[290] CJEU Case C-101/01 Lindqvist (2003)

[291] Elliot et al.(주210), p.21

[292] 우리나라의 이른바 IMEI 판결도, 결과적으로는 이러한 입장을 취한 것인바, 전체적으로는 정당하다고 본다는 점에 대하여는 앞서 언급하였다.

[293] WP 29(주73), pp.13~14, p.20

[294] 물론 이러한 '연결고리의 존재'가 반드시 현실적으로 문제의 개인이 현실적으로 추적 가능하거나 접촉 가능하다는 것을 의미하는 것으로 해석되어서는 안될 것

다. 정보주체와의 지속적 연결

이 경우 '다르게 취급' 될 수 있는 상태 또는 '신뢰할 만한 연결고리' 의 존재를 인정하기 위하여서는, 문제의 정보가 어떤 개인과 단지 짧은 시간 동안 일시적으로 연결되는 것에 그치지 않고 상당 기간 동안 지속적으로 연결 가능하여야 할 것인바, 일본 정부가 개인식별부호 해당 여부를 판단함에 있어 '본인도달성' 과 함께 '불변성' 을 요구한 것도 이러한 맥락에서 이해할 수 있을 것이다[295]. 먼저 이름, 주소, 여권번호 등으로 개인의 신원이 알려진 경우에는 이러한 요건을 쉽게 인정할 수 있을 것이다. 그러나 기기 정보나 IP주소 같은 것은 사안에 따라 식별 여부를 달리 판단할 필요가 있다.

예컨대 온라인상에서 신용카드 명의를 도용하여 재산적 이익을 취하는 범죄자가 카드 회사에 IP주소, 단말의 MAC 주소, UUID 등의 기기 정보를 남겼다면, 이는 대개 일회적으로 사용되는 것이거나 잘못된 정보일 가능성이 높으므로, 본인도달성 및 불변성의 결여로 식별을 인정할 수 없는 경우가 많을 것이다. 마찬가지로 PC방에 설치된 PC의 IP주소에 대하여도 식별자로서의 성격을 인정하기는 어려울 것이다. 우리나라 검찰이 "만약에 도심에서 하나의 기지국 내에 수십명에서 수백 명의 스마트폰 사용자들이 있고 그들이 동시에 또는 시간차를 두고 스마트폰으로 인터넷에 접속하였다가 종료하는 것을 반복하며, 이동통신사가 트래픽의 분산을 위하여 여러 AP를 설치한 경우라면 순간적으로 '동일한 IP주소' 에 '다수 이용자' 가 접속한 상태가 될

이다. 영국의 Edem 판결(주 203) 참고. 예컨대 신원이 알려져 있다면, 주소나 전화번호 같은 연락처에 관한 정보가 없더라도 당연히 식별의 존재를 인정해야 할 것이다.

[295] 衆議院 內閣委員會(주244), 塩川 의원의 질문에 대한 山口 국무대신 발언

것이라는 점을 고려하여 기지국의 공인 IP주소만으로 이용자를 특정할 수는 없다고 판단"[296]한 것도 이와 같은 맥락으로 이해될 수 있을 것으로 보인다.

참고로 미국의 경우에도, 2012년 소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)을 바탕으로 2015년 법안화된 소비자 프라이버시 권리장전 법안(Consumer Privacy Bill of Rights Act)의 경우 제4조 (a)에서 "개인정보"의 개념을 정의하며, "특정한 개인 또는 한 개인에 의하여 연결되어 있거나 일상적으로 사용되는 기기에 연결"되는 경우를 포함시키고 있는바, 필자의 견해와 유사한 입장으로 생각되며, 특히 기기와의 연결 가능성과 관련하여 "일상적으로 사용되는 기기"라는 점을 강조한 것으로 보아, '불변성' 요건에 대한 고려를 포함하고 있는 것으로 보인다.

5. 식별가능성의 해석 – '쉽게 결합하여'의 의미

가. '쉽게 결합하여'의 의미

앞서 살펴본 여러 견해들에 의하더라도, 독일의 일부 견해를 제외하면, '쉽게 결합'의 의미가 '합리적 수단을 사용한 결합'이라는 점, '합리적'이라는 의미가 '시간, 비용, 노력의 과도한 지출 없이' 라는 의미라는 점에 대해서는 거의 이견이 없어 보인다.

다만, i) 그러한 합리적 결합 가능성의 판단 기준을 누구로 할 것인가(객관설과 상대설), ii) 불법적인 수단을 써서 결합할 수 있는 경우도 '쉽게 결합'에 해당한다고 볼 것인가(불법수단 고려설과

[296] 구태언, "개인정보 정의조항, 동의제도 및 형사처벌의 합리화에 관한 연구", 고려대학교 정보보호대학원 석사학위논문, 2013, pp.80~81

불고려설), iii) 동일한 처리자 내부의 다른 개인들이 각각 단독으로는 개인식별이 불가능하나 서로 결합하면 개인식별이 가능한 정보를 보유하고 있는 경우 '쉽게 결합' 할 수 있다고 볼 수 있는가(동일 처리자 내 결합용이성 부정 여부)가 문제이다. 이하에서 각각의 쟁점에 관하여 하나씩 살펴 보도록 한다.

나. 합리적 결합가능성의 판단기준 – 객관설 v. 상대설

(1) 문제의 소재

개인정보 개념의 요건 중 '쉽게 결합' 가능 여부의 판단에 있어 객관설은 처리자가 식별에 필요한 추가 정보를 쉽게 입수하고 결합할 수 있는지와 상관 없이, 불특정 다수의 제3자 입장까지 두루 고려한다는 견해이며, 상대설은 처리자가 식별에 필요한 추가 정보를 쉽게 입수하고 결합할 수 있는지에 따라 판단한다는 견해이다. 그러므로 어떤 정보의 개인정보 여부는, 전자의 견해에 따를 때에는 처리자가 누구인지와 상관 없이 대체로 일정하나, 후자의 견해에 따르면 처리자가 누구인지에 따라 상대적으로 결정될 수 있게 된다.

그런데 우리나라에서는 상대설도 개인정보처리자 기준설[297]/처리자 및 (제공 등의 경우) 제3자 고려설[298], 제반사정 고려설(절충설)[299] 등으로 다시 나누어지고 있는 것으로 파악된다. 이 중 절충설은 개별 경우의 제반 사정을 종합하여 개인정보성을 판단한다는 것이므로 개인정보 개념에 대한 일률적인 기준을 제공하여 주지

[297] 이인호(주43)

[298] 행정자치부 외, "개인정보 비식별 조치 가이드라인 – 비식별 조치 기준 및 지원·관리체계 안내– ", 2016

[299] 장주봉(주42), "개인정보의 의미와 규제범위" , 개인정보보호의 법과 정책, 박영사, 2014

못하는바, 개인정보 개념의 해석에 관한 통일적인 기준을 수립하고자 하는 본고의 취지와는 맞지 않다고 생각되므로, 이 부분의 검토에서는 제외한다.

처리자[300] 및 제3자 고려설은 비식별조치 가이드라인이 취하는 견해로, "개인을 식별할 수 있다는 것은 해당 정보를 '처리하는 자' 및 '제공 등에 따라 향후 처리가 예정된 자'의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다"는 것을 의미한다"고 보는 입장이다[301]. 이 입장은, 그 문언 ("처리하는 자 **및** 제공 등에 따라 향후 처리가 예정된 자")으로부터 '처리하는 자' **및** '제공받는 자' 모두가 개인을 식별할 수 있어야 개인정보성을 인정한다는 것으로 해석된다. 그리고 여기서 처리자 외의 제3자는 '제공에 따라 향후 처리가 예정된 자'가 아니라 '제공 **등**에 따라 향후 처리가 예정된 자'이므로, 정보를 유출시키는 자 또는 유출시키는 자로부터 정보를 전달받는 자까지 검토 대상에 포함하여야 하는 것으로 해석될 여지가 있어 보인다. 그러나 이와 같이 해석할 경우, 정보처리자 입장에서는 정보처리행위를 할 때 유출시키는 자와 유출시키는 자로부터 정보를 받는 자가 누구인지를 사전에 특정할 수 없다는 점에서, 사실상 정보처리자 이외의 모든 제3자에 관계된 상황을 고려하여야 하는 것과 같은 결과가 되는바, 이는 사실상 객관설과 동일한 결론이므로 굳이 '정보처리자'를 위주로 개인정보성 여부를 판단한다고 주장하는 의미가 없어지게 된다.

---

[300] 여기서 법령상 용어인 '개인정보처리자'라는 용어를 사용하는 것이 보다 정확해 보일 수 있으나, 아직 처리 대상인 정보가 개인정보 여부가 확실치 않은 상황에서 이를 판단하기 위한 기준을 논하는 단계이므로, '개인정보처리자'로 지칭하는 것은 적절치 않다고 생각된다. 따라서, 본고에서는 '정보처리자' 내지 '처리자'라는 용어를 사용하기로 한다.

[301] 행정자치부 외, "개인정보 비식별 조치 가이드라인 – 비식별 조치 기준 및 지원·관리체계 안내– ", 2016, p.55

그러므로 이러한 해석은 처리자 및 제3자 기준설의 기본 취지와 양립하기 어려운 것으로 생각된다. 그러므로 이하에서는 처리자 및 제3자 기준설은 처리자와, 처리자의 제공행위로 제공받는 자만을 기준으로 하고, 유출의 상대방은 고려하지 않는 것으로 보고 논의를 진행한다. 또한, 이 점을 반영하여 이 설을 '처리자 및 제공받는 자 기준설'로 지칭하기로 한다.

(2) 학설 대립의 실익

먼저, 이러한 학설 대립의 실익에 관하여 살펴본다. 어떤 정보가 한 처리자의 수중에 있는 경우, 그러한 정보는 식별 가능성과 관련하여, i) 누구나 개인을 식별할 수 있는 정보이거나, ii) 누구도 그 정보를 이용하여 개인식별을 할 수 없는 정보, iii) 그 자체로는 개인식별이 불가능한 정보로서 처리자 자신은 다른 정보와 결합하여 개인을 식별 할 수 있으나 처리자 이외의 다른 사람은 그러한 결합을 할 수 없으므로 개인을 식별할 수 없는 정보, iv) 그 자체로는 개인식별이 불가능한 정보로서 처리자 자신은 그 정보를 이용하여 개인을 식별할 수 없으나 다른 제3자는 그 정보와 다른 정보를 결합하여 개인을 식별할 수 있는 정보로 구분할 수 있을 것이다. 이 중 첫번째 경우는 언제나 개인정보이고, 두번째 경우는 어떠한 경우에도 개인정보가 아니라는 점이 분명하므로, 세번째 경우와 네번째 경우를 중심으로 살펴보면 될 것이다.

(가) 처리자는 개인식별이 불가능하나 특정 제3자는 식별가능한 정보(사안유형 1)

우선, 처리자는 그 정보를 이용하여(처리자가 합리적으로 입수 및 결합 가능한 다른 정보와 결합하는 경우를 포함) 개인을 식별할 수 없으나, 제3자는 그 정보와 결합하는 추가정보를 가지고 있는 등으로 그러한 식별이 가능한 경우에 관하여 본다. 이 경우 해당 정보에 대한 처리행위에 개인정보보호법이 적용되는지 여부를 살펴

보면 다음 표와 같다.

	객관설	처리자기준설	처리자+제공받는자 기준설
수집 관련 규정	O	X	X
보유시 준수해야 할 규정들	O	X	X
정보주체의 권리	O	X	X
제공 관련 규정	O	X	X
유출 관련 규정	O	X	X

① 객관설을 적용하면, 그러한 정보는 어떠한 경우에나 개인정보이므로, 개인정보보호법의 전 규정이 적용될 것이다. 그러나 정보주체가 합리적 수단으로 개인을 식별할 수 없는 정보에 대하여, 정보주체의 식별을 전제로 하는 개인정보보호법상 규정들을 적용할 수 없다는 문제가 있다. 예컨대, 이러한 정보에 관하여 열람·정정·삭제청구권을 비롯한 정보주체의 권리를 행사하게끔 하는 것이 가능할까? 정보처리자가 사후적으로 정보를 제공하거나 목적외 이용을 하고자 하는 경우, 정보주체로부터 그에 대한 동의를 받을 수 있는가? 유출 사고가 발생하였을 때, 정보주체에게 법이 정한 고지를 행하는 것이 가능한가? 모두 불가능하다고 보아야 할 것이고, 이로부터 우리 개인정보보호법 및 정보통신망법은 적어도 객관설을 전제하는 것은 아니라는 해석이 가능하다[302].

[302] Meyerdirks(주157), Rn.12~13

② 처리자 기준설의 경우, 처리자 입장에서 식별가능성이 없어 개인정보가 아니라면 모든 경우에 개인정보가 아닐 것이다. 심지어 해당 정보를 제3자에게 제공할 때, 그 제3자가 그 정보를 이용하여 개인을 식별할 수 있다고 하더라도 그러한 제공이 제3자 제공에 해당하지 않을 것이며, 그 제3자만이 개인정보의 동의 없는 '수집'에 관하여 책임을 질 뿐이다. 또한, 그러한 정보에 대하여는 기술적 관리적 보호조치 의무나 유출시 신고의무 등이 인정되지 아니할 것이다. 이와 관련하여 정보주체의 보호가 불충분하다는 문제제기가 있을 수 있다 생각되나, 어쨌든 객관설의 단점, 즉 우리 개인정보보호법 체계와의 부정합성이라는 문제는 발생하지 않는다.

③ 처리자 및 제공받는 자 기준설은, 처리자 및 제공받는 자 모두에게 식별가능성이 있어야만 개인정보라고 보므로, 이 사안에서는 처리자 기준설과 같은 결론이 도출될 것이다. 그러므로 처리자 기준설과 동일한 장점과 단점을 가진다

(나) 처리자는 개인식별이 가능하나 특정의 제3자는 개인식별이 불가능한 정보(사안유형 2)

반대로 처리자는 어떤 정보로부터 개인을 식별 가능하나 이것이 제3자에게 제공되는 경우 그 제3자는 개인 식별이 불가능한 경우도 있을 수 있다.

예컨대 처리자가 이미 보유하고 있는 정보집합물(dataset)에서 식별자를 제거한 새로운 정보집합물을 만들고, 후자의 정보집합물만을 제3자에게 제공하였는데, 그 제3자로서는 새로운 정보집합물로부터 개인을 식별할 수 없는 경우이다. 이 경우 처리자 입장에서는 자신이 보유하고 있는 정보집합물 원본과 새로운 정보집합물을 대조함으로써 새로운 정보집합물에서 개인을 식별해낼 수 있지만, 제3자로서는 그렇지 아니하다. 이러한 경우

처리자의 각 행위를 어떻게 평가할 것인지 검토해 보자.

	객관설	처리자기준설	처리자+제공받는 자 기준설
수집 관련 규정	O	O	O
보유시 준수해야 할 규정들	O	O	O
정보주체의 권리	O	O	O
제공 관련 규정	O	O	X
유출 관련 규정	O	O	O

① 객관설을 취할 경우 이러한 정보의 모든 처리행위와 관련하여 개인정보보호법이 그대로 적용될 것이다.

② 처리자 기준설에 따를 때에도 객관설과 마찬가지의 결론이 도출된다. 이 경우 처리자 기준설을 논리적으로 엄격히 적용하면, 상대방 입장에서는 전혀 식별 불가능한 정보를 제공하더라도 개인정보의 제공에 해당하게 된다.

③ 처리자 및 제공받는 자 기준설에 따를 경우, 그 결과는 기본적으로 처리자 기준설과 동일하다. 그러나 이러한 정보의 제공과 관련하여서는 다른 결론이 도출될 수 있다. 즉, '처리자 **및** 제공받는 자'의 입장을 고려하여야 하므로, 이러한 경우 처리자에게는 식별가능성이 있더라도 제공받는 자에게 합리적 식별가능성이 없다면 그러한 제공은 개인정보의 제공에 해당하지 않을 것이다. 앞서 살펴본 바와 같이 우리나라의 학설들 중 일부는 이와 동일한 결론을 도출하기 위하여 영국법 조항을 원용하며

'처리자 기준설'을 취하고 있지만, 이는 해당 조항의 취지에 대한 오해라 생각되고, 논리적으로 그다지 엄밀한 주장은 아니라 생각된다.

(다) 검토

1) 객관설에 대한 검토

① (가)에서 살펴보았다시피, 우리나라 개인정보보호법령의 많은 규정들은 개인정보 처리자가 개인을 식별할 수 있다는 점을 전제로 하고 있기 때문에, 객관설을 채택하기는 어렵다고 생각된다.

문언적으로 보더라도, 앞서 살펴본 바와 같이 독일에서 객관설을 지지하는 주된 근거가 바로 유럽연합 개인정보보호지침의 고려이유 26이 '제3자'의 관점을 고려한다는 점을 명시하고 있었기 때문인데, 우리나라 개인정보보호법 및 정보통신망법에는 그러한 명시적 규정이 없다. 굳이 객관설을 주장할 특별한 법률 문언상의 근거도 없는 것이다.

② 오히려 객관설을 취할 경우 이 세상에 존재하는 거의 모든 정보가 개인정보가 된다는 이상한 결과로 이어질 수 있다.

그것이 아니라면, 개인정보와 그렇지 않은 정보를 구분하여야 할 것인데, 앞서 살펴본 팔렌-브란트의 주장 즉 정보 자체가 식별을 가능케 하는 타 정보와 결합하는 것이 기술적·물리적으로 불가능한 정도에 이르러야 식별가능성을 부정할 수 있다는 주장을 제외하면[303], 객관설은 그러한 기준을 전혀 제시하지 못하고 있다. 또한, 정보를 처리하는 자로서는 누가 이 정보를 이용하여 어떤 방법으로 개인을 식별할 수 있을지 전혀 알 수가 없다. 결국

[303] 주 149 참고.

개인정보보호법 적용 여부에 관하여 법적 안정성이 심각하게 저해되는 결과가 될 것이다. 이론적으로는 식별에 필요한 추가정보를 가지고 있는 제3자가 당해 정보를 보유하고 있으면 개인정보보호법의 적용을 받게 되고, 그 자가 그 정보를 자신도 모르는 사이에 삭제해 버리면 개인정보보호법의 적용을 받지 않게 된다는 이상한 결과까지 발생할 수 있다[304]. 정보처리자로서는 이러한 결과를 피하기 위하여 자신이 보유하고 있는 거의 모든 정보에 대하여 개인정보보호법이나 정보통신망법 등이 적용되는 것으로 취급하지 않을 수 없을 것이다. 결국 처리자 입장에서는 모든 정보가 개인정보인 것과 다름 없는 결과가 된다.

이와 같은 결과가 가져올 수 있는 현실적인 불합리에 대해서는 말할 필요도 없을 것이다. 더욱이, 앞서 살펴본 바와 같이 개인정보 자기결정권도 헌법상 여느 기본권과 마찬가지로 대립하는 다양한 법익들과의 형량을 거쳐 그 보호범위가 결정되어야 하는바, 모든 정보처리에 우리 개인정보보호법처럼 경직된 법률을 일률적으로 적용함으로써 정보처리자의 직업의 자유 등을 침해하는 것은 헌법상 개인정보 자기결정권의 법리에도 맞지 않는 결과라 생각된다.

③ 한편 객관설을 주장하는 논자들은 상대설이 법적 안정성을 저해한다고 비판하나, 오히려 객관설을 취하는 경우 법적 안정성이 저해될 우려가 있다는 점은 앞서 본 바와 같다. 정보를 처리하는 자 자신이야말로 스스로 보유하고 있는 정보의 상황, 현재 또는 장래의 정보 취득 계획을 잘 알고, 그에 기하여 식별가능성 및 쉽게 결합 가능한지 여부를 판단할 수 있는 지위에 있기 때문에, 정보처리자의 상황에 따라 개인정보 여부를 판단하도록 하는 것이 법적 안정성이라는 관점에서 보다 바람직할 것이다. 물론 객관설을

[304] Meyerdirks(주157), Rn. 10

극단적으로 적용하여 모든 정보를 개인적으로 취급할 경우 법적 안정성이 가장 확실히 보장되겠지만, 이는 법적 안정성만을 위하여 정보처리자의 직업의 자유 기타 헌법상 기본권을 지나치게 희생하는 결과로 바람직하지도 않고 현실적이지도 못하다고 본다.

④ 객관설이 상대설을 비판하는 또다른 중요한 논거는 상대설을 취할 경우 정보주체의 권리 보호에 소홀해질 수 있다는 점이다. 이와 관련하여, 우리나라의 한 견해는 개인정보처리자가 보유하고 있는 개인정보를 불법으로 제3자에게 제공하고, 그 제3자가 제공받은 정보 중 개인식별이 가능한 부분만을 삭제한 후 스팸메일 발송 등의 방식으로 임의로 사용할 경우, 상대설에 따르면 제3자가 자신의 정보는 개인정보가 아니라고 주장할 수 있게 되는데, 수사기관 입장에서는 그러한 주장을 반박할 증거를 발견하기가 현실적으로 어려우므로, 결국 정보주체의 권리 보호가 어려워진다고 주장하고 있다[305]. 그러나 이 견해는 타당하지 않다.

첫째, 위 사안에서는 이미 개인정보의 제3자 제공, 목적외 이용, 정보통신망법 50조 위반이라는 법위반이 발생하였기 때문에 객관설에 의하든 상대설에 의하든 충분히 제재를 가할 수 있다.

둘째, 위 견해는 식별 개념을 좁게 보는 전제에 입각하여 있다. 즉 위 견해를 주장한 논문의 다른 곳에서는 '성명, 주민등록번호, 영상이 고유식별자이기는 하지만 그 정보만으로는 실제적으로 개인식별이 되지 않는다' 는 취지의 기재가 발견되는바[306], 이는 식별 개념을 매우 좁게 본 해석으로, 식별 개념을 이와 같이 보지 않고 필자가 보는 바와 같이 넓게 본다면 이 문제도 해결될 수 있을 것으로 본다. 즉, 이 사안에서 제3자는 이메일 주소 등을

[305] 주민철, 전게논문, pp.28~32

[306] 주민철, 전게논문, pp.22~23

이용하여 정보주체에게 현실적으로 접근을 하였고, 더욱이 이메일 주소는 약간의 노력만 기울인다면 개인을 현실적으로 식별하는 데 필요한 추가 정보를 입수하기도 쉬운 성질의 정보이므로 개인정보로 보는 것이 가능할 것이다. 더욱이 이러한 사안에서는, 정보를 제공한 자와의 관계에서 그러한 정보주체에 관한 추가적인 사실을 알게 될 수도 있다. 예컨대, A라는 카드회사로부터 받은 이메일 주소 목록이라면, 단순한 이메일 주소 뿐 아니라, 자료 내에 있는 정보주체가 A사의 카드를 보유한 사람이라는 사실까지 추가적으로 알 수 있는 것이다.

셋째, 이와 같이 불법적인 정보 교환이 이루어진 상황이라면 정보를 제공받은 자로서는 정보를 제공한 자나 다른 불법적인 루트를 통하여 식별에 필요한 추가 정보를 입수할 가능성이 충분히 있는 경우가 많을 것이므로, 정보 입수 상황을 충분히 고려하지 않고 쉽게 개인정보 해당성을 부정하여서는 안된다.

이상에서 살펴본 바와 같이, 상대설을 취할 경우 정보주체의 권리보호가 소홀해질 수 있다는 주장은, 필자가 보기에는 지나치게 관념적인 면이 있다. 실제로 객관설과 상대설 중 처리자 기준설을 비교해 보아도, 현실적인 차이가 있는 것은 앞서 언급한 (가)의 경우 즉 사안유형 1의 경우와, (나)의 경우 즉 사안유형 2의 경우 중 제3자에게 정보를 제공하는 경우 뿐이다.

그런데 사안유형 1의 경우, 객관설을 적용하여 개인정보성을 긍정하더라도 어차피 정보처리자는 정보주체를 식별할 수 없으므로 수집동의, 제3자 제공 동의, 유출 통지, 정보주체의 열람권 보장에 관한 규정을 현실적으로 적용 내지 집행할 수가 없다. 물론 (가)의 경우라 할지라도 문제의 정보가 처리자에게 개인정보에 해당하는 것으로 본다면 그에 대하여 기술적 관리적 보호조치를 취하게 함으로써 정보주체의 보호에 보다 긍정적인 역할을 할 수 있다는 점은 인정하지 않을 수 없다. 그러나 상대설을 취하더라도 이러한

사안에서 제공이나 유출에 의한 식별이 일어날 경우, 그로 인하여 식별을 한 자에게 개인정보 수집에 관한 책임이 발생할 것이라는 점에서, 규제의 사각지대가 발생한다고는 보기 어려울 것이다(이 점에 관해서는 뒤에서 상론한다). 이를 감안해 본다면 이러한 객관설의 긍정적인 면들이 지금까지 살펴본, 객관설을 취하였을 때의 다른 많은 단점들까지 상쇄할 수 있는 것인지는 의문이다.

⑤ 객관설을 주장하는 일부 견해는, 상대설에 따를 경우 개인정보 해당 여부에 대한 판단을 정보처리자에게 맡기는 것이 부당하다고 한다[307]. 그러나 불확정개념을 포함한 모든 규제에서, 자신의 행동이 해당 불확정개념에 포섭되는지 판단할 일차적인 책임은 그 수범자에게 있다. 규제기관 및 사법기관은 수범자가 그 판단을 제대로 하였는지 당시의 객관적 상황을 바탕으로 사후적으로 판단할 권한을 가진다. 그러므로 위와 같은 주장은 규제의 일반론에 비추어 볼 때 타당성이 없다고 생각된다(물론, 법률이나 규제기관의 가이드라인으로써 수범자가 그러한 판단을 제대로 할 수 있도록 하기 위하여 준수하여야 할 사항을 규정해 둔다면 더욱 좋을 것이다)

2) 상대설의 검토

① 상대설은 앞서 살펴본 객관설의 약점을 상당 부분 극복하고 있는 것으로 보인다. 특히, 정보주체에 대한 통지 및 정보주체의 동의를 요건으로 하는 우리 개인정보보호법 및 정보통신망법의 제반 조항들은 상대설을 전제로 한 것으로 보이므로, 관련 법령의 체계적 해석상 상대설이 타당하다고 생각한다. 관련 법률의 문언상으로도, 우리 개인정보보호법제에는 '제3자'가 사용 가능한 수단까지 두루 고려한다는 표현이 없기 때문에 상대설을

[307] Pahlen-Brand(주141)

취하더라도 해석상 크게 문제될 부분이 없다.

더욱이, 객관설을 주장하는 독일의 일부 견해는, "사소한 정보란 더 이상 존재할 수 없다"[308]라는 독일 연방헌법재판소의 인구조사 판결의 판시를 근거로 모든 정보가 개인정보가 되어야 한다고 주장하기도 하나[309], 같은 판결이 정보의 유용성(Nutzbarkeit)과 사용가능성(Verwendungsmöglichkeit), 정보기술에 고유한 처리가능성(Verarbeitungsmöglichkeiten)과 연결가능성(Verknüpfungsmöglichkeiten) 등의 요소를 두루 고려하고 있는 것[310]을 고려하면, 위 판시가 반드시 모든 정보를 개인정보로 취급하여야 한다는 취지라 볼 것은 아니라 생각된다.

② 한편 상대설은 객관설과 비교할 경우, 사안유형 1과 관련하여 정보주체의 보호가 취약한 것이 아닌가라는 의문이 제기될 수 있다. 즉, 정보처리자로서는 자신에게는 개인정보가 아닌 정보에 대하여서는 그 정보가 제3자의 수중에서는 개인정보가 될 가능성이 있더라도, 개인정보보호법령을 준수할 의무가 없다. 그러므로 그 정보가 적어도 정보처리자의 수중에 있는 동안에는, 처리자로서는 이러한 정보에 관하여 안전성 확보조치 또는 기술적·관리적 보호조치를 취할 개인정보보호법령상 의무가 없고, 더욱이 이러한 정보의 제3자에 대한 제공 또한 정보주체의 동의 기타 법령상 근거 없이 자유롭게 할 수 있다. 이로 인하여 상대설에 따르면 정보의 유출·제공 및 유출·제공 후 식별이 용이하여짐으로써 정보주체의 보호에 흠결이 생긴다는 비판이 제기될 수 있을 것이다[311].

---

[308] BVerfGE, 65,1 (44, 45)

[309] Pahlen-Brandt(주141), s.39

[310] BVerfGE, 65,1 (44, 45)

[311] 장주봉(주49), 2012, 27면.

그러나 이러한 경우 반드시 정보주체의 보호에 흠결이 발생하는 것은 아니다. 첫째, 어떤 정보가 정보처리자에게 개인정보가 아니라는 것은 정보처리자가 공개된 정보원으로부터 식별에 필요한 추가 정보를 입수할 수 없는 것을 포함, 합리적으로 가능한 여러 수단을 동원하더라도 추가 정보 입수 및 그러한 정보와의 결합을 할 수 없다는 것을 말한다. 그렇다면 그러한 정보가 해커 등의 타겟이 될 가능성은 그렇지 않은 정보에 비하면 높지 않다고 생각되며, 대개의 경우 유출되었을 경우 정보주체에 미치는 영향 또한 비교적 크지 않을 것으로 생각된다. 둘째, 그러한 정보를 제공받거나 유출 등의 방법으로 입수하여 개인을 식별한 자에 대해서는 개인정보보호법령상 불법한 수집 및 이용에 관한 책임이 성립할 수 있을 것이다. 셋째, 그러한 정보의 처리자에 대해서는, 개인정보보호법령상 규제가 직접 적용되지 않더라도 구체적인 상황에 따라 해당 정보의 유출 및 제공, 그리고 그로 인한 재식별에 과실이 있었다면 이를 이유로 한 불법행위 책임 또는 동의 없는 개인정보수집 및 이용(문제의 정보를 제공받아 식별에 사용한 제3자의 책임)에 대한 고의·과실에 의한 공범 또는 공동불법행위자로서의 책임이 성립할 수 있다.

③ 이상을 종합하여 보면, 객관설보다 상대설이 우리 법의 해석론으로 보다 타당해 보인다.

3) 처리자 기준설의 타당성

상대설을 취한다고 할 때, 처리자 기준설과 처리자 및 제공받는 자 기준설 중 무엇이 더 타당한가? 두 설은 사안유형 2와 관련하여, 개인정보의 제3자 제공을 인정할 것인지 여부와 관련하여 차이가 있다. 두 설은 각각 장단점이 있으나, 개인정보보호법을 엄격히 해석한다면, 다음의 이유로 처리자 기준설이 타당하다고 생각한다.

① 우선, 처리자 및 제공받는 자 기준설에 따르면, 개인정보라는

행위객체에 대한 '개념'을 정의함에 있어 '제3자 제공'이라는 특수한 행위의 맥락만을 특별히 고려하게 되는바, 이는 어떤 객체의 개념이 그 객체를 대상으로 하는 행위가 어떤 것이냐에 따라 달리 정의되는 것으로서, 올바른 개념정의라고 보기 어렵다.

② 더욱이 처리자 및 제공받는 자 기준설을 취하더라도 실제로는 큰 실익이 없다. 왜냐하면 자신에게는 개인정보인 어떤 정보를 제3자에게 제공하는 자 입장에서는, 자신이 제공하려는 정보가 그 제3자에게 개인정보인지 여부를 확실히 알 수 있는 방법이 사실상 없기 때문이다. 이를 알기 위해서는 그 제3자가 현재 보유하고 있는 정보, 향후 보유할 수 있는 정보, 제3자가 식별을 위하여 투입할 수 있는 노력, 식별된 후의 정보가 제3자에 대하여 가질 수 있는 가치 등 제3자의 식별 의도, 식별 능력 등에 대한 정확한 정보가 있어야 하는데, 통상의 거래에서 이를 정확하게 파악하기란 불가능하다. 제공자가 여기에 대한 정보를 가지고 있더라도, 제3자가 제공자에게 제공한 정보가 부정확하거나 제3자가 그러한 사항에 관하여 제공자를 기망하는 경우라면 개인정보제공자가 최선의 주의를 기울였더라도 결과적으로 해당 정보의 제공 행위는 개인정보의 제공에 해당하게 될 것이다. 그러므로 자신에게 개인정보인 어떤 정보를 제공하고자 하는 자는, 그 정보가 제공받는 상대방에 대하여도 개인정보라고 가정하고 행동하는 것이 합리적일 것이다[312].

물론, 처리자 및 제공받는 자 기준설을 취할 경우, 처리자(제공하는 자)가 위에 열거된 상황을 충분히 고려함으로써 자신이 제공하는 정보가 제공받는 자에 대하여 개인정보가 아니라는 점에 대하여 상당한 주의를 기울였음에도 제공되는 정보가 제공받는 자의 입장에서도 개인정보라는 점을 알지 못하였다고 한다면, 제공자는

[312] Dammann, in Simitis[Hrsg](주100), §3 Rn. 38

개인정보의 제공행위에 관하여 고의 및 과실이 없으므로 주관적 구성요건을 요건으로 하는 책임을 면한다는 논리가 가능해진다.

그런데 이는 개인정보 여부의 문제를 과실판단의 문제로 치환하여 버리는 결과가 된다. '특정 법익의 침해에 대한 사전적·일률적 규제로서의 행정법규인 개인정보보호법의 적용 여부를 행위자의 주관적 귀책사유 즉 고의·과실 유무에 조건지우는 것은 바람직하지 않다' 는 일본 정부의 지적이나[313], 이러한 상황에서 '허용된 위험' 을 이유로 한 면책을 인정하여서는 아니된다고 보는 독일의 학설도 같은 맥락에서 제기된 것이 아닌가 한다.

③ 한편 처리자 기준설을 취하여, 제공받는 자가 개인을 식별할 수 없는 정보를 제공하는 행위가 언제나 개인정보 제3자 제공에 해당한다고 엄격하게 본다면, 개인정보 자기결정권의 실질적 보호 및 다른 법익과의 균형이라는 관점과 맞지 않는 면이 있는 것은 사실이다.

즉, 개인정보 자기결정권이란 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리"이므로 정보 제공에 관한 통제권은 개인정보 자기결정권의 중요한 구성요소이다. 실제로 개인정보가 누구에게 있는지를 아는 것은 정보주체가 개인정보에 대한 자신의 권리를 행사함에 있어 매우 중요하다. 그러나 (나)의 경우와 같이, 정보를 제공받는 자가 개인을 식별할 수 없는 경우라면 제공행위로 인하여 정보주체에 대한 위험 수준이 더 높아진다고 볼 수 없을 것이다. 이러한 경우까지 개인정보 제3자 제공으로 규율함으로써 통제할 필요가 있는가? 과연 이러한 통제가

[313] 同旨, 鈴木正朝(주269), 62~64면

침해 가능한 법익과 정보의 활용을 통한 경제적 가치 또는 공익적 가치의 실현이라는 대립하는 법익의 균형이라는 관점에서 바람직한 것인가? 그렇게 볼 수는 없을 것이다.

그러나 우리 개인정보보호법상 이러한 경우 정보의 활용을 통한 가치 실현이라는 법익 달성을 도모하고자 하는 조항이 존재하지 않는 것은 아니다. 제18조 제2항 제4호가 그것이다. 여기에 따르면, "통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공"하는 것은 "정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는" 가능하다. 이러한 조항만으로는 예외의 인정 범위가 너무 좁다는 문제의식에 대하여는 '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우'를 적절히 넓게 해석하는 방법을 고려해 볼 수 있을 것이다. 그리고 여기서 '특정 개인을 알아볼 수 없는 형태'의 의미는 행정규범의 해석의 문제이므로, 그 해석에 관하여 정부가 가이드라인을 제정함으로써 그 내용을 구체화하더라도 이상할 것이 없다[314].

더욱이 처리자 및 제공받는 자 기준설을 채택하게 되면 제18조 제2항 제4호의 존재의미를 설명하기 어렵게 된다. 왜냐하면 이 설에 따를 경우 상대방이 "개인을 알아볼 수 없는 형태"의 정보는 이미 그 상대방에게 개인정보가 아니므로 제공에 아무런 제약을 받지 않는다. 그렇다면 굳이 제18조 제2항 제4호와 같은 규정을 둘 이유도, 제공의 정당화 사유를 "통계작성 및 학술연구 등"으로 한정할 이유도 없지 않을까. 그렇다면, 제18조 제2항 제4호의 존재를 감안한 우리 개인정보보호법의 체계적 해석상으로도 처리자 기준설이 타당하다고 할 수 있다.

---

[314] 비식별조치 가이드라인에 기재된 바와 같은 내용들이 그 기준으로 사용될 수 있을 것이다.

④ 앞서 살펴본 바와 같이 우리 정부는 비식별조치 가이드라인을 통하여 처리자 및 제공받는 자 기준설을 천명하고 있는바, 여기에는 몇 가지 난점이 있다.

비식별조치 가이드라인이 취하고 있는 처리자 및 제공받는 자 기준설의 핵심은 개인정보처리자가 자신이 보유하는 개인정보에 대하여 비식별조치를 거치면 그 정보는 더 이상 개인정보가 아니게 되므로, 해당 정보를 제3자에게 제공하더라도 개인정보의 제공이 아니게 된다는 것이다.

첫째, 비식별조치 가이드라인에 따르더라도, 개인정보처리자가 비식별조치를 거친다고 하여 그것만으로 그 정보가 완전히 개인정보가 아니게 되는 것은 아니다. 처리자 및 제공받는 자 기준설을 일관되게 적용하면, 비식별조치를 한 개인정보는 처리자에게는 여전히 개인정보이다. 처리자로서는 비식별조치가 되기 전의 원 데이터를 가지고 있기 때문에 이것과의 대조를 통하여 비식별화된 정보로부터 개인을 식별하는 것이 가능할 수 있기 때문이다[315]. 비식별조치의 완성은 개인정보의 제공이라는 맥락에서도 비식별화된 정보가 더 이상 개인정보가 아니도록 하지 못한다. 그러므로 이 경우 제공되는 정보는 개인정보가 아닌 것으로 단지 '추정' 될 뿐이며, 이후 식별될 경우 개인정보로 본다고 한다[316].

---

[315] 그러므로 이러한 정보에 대하여 제3자 제공 뿐 아니라 목적외 이용의 예외를 이용한다는 비식별조치 가이드라인의 태도에 대해서는 동조할 수 없다. 정보처리자 입장에서는 그 정보는 여전히 개인정보이기 때문이다. 또한 뒤에서 언급하다시피 한 처리자 내부의 다른 부문에서 비식별화되기 전의 정보와 비식별화된 후의 정보가 각각 처리된다고 할지라도, 두 부문 사이에 완전한 분리가 존재하며, 이것이 회사 운영 구조상 확실히 보장되는 경우가 아니라면 그러한 분리처리만을 이유로 비식별화된 정보의 개인정보성을 부정하여서는 안된다.

[316] 행정자치부 등(각주37), 3면, 16면("비식별 정보가 재식별된 경우에는 … 해당 개인정보가 유출되지 않도록 필요한 조치를 하여야 함"이라고 기재하고 있는바, 비

앞서 언급하였다시피 정보를 제공하는 자가 아무리 비식별조치 등 조치를 취하더라도, 실제로 정보를 제공받는 자 입장에서 식별이 가능하다면, 그러한 정보의 제공은 개인정보의 제공에 다름 아니며, 논리적으로 보았을 때 이는 처리자 기준설을 취하든 처리자 및 제공받는 자 기준설을 취하든 마찬가지이다. 그러므로 '추정' 과 같은 애매한 서술은 처리자 및 제공받는 자 기준설에 기하여 비식별조치를 정의할 경우 피할 수 없는 귀결이다. 이것은 문제의 정보가 개인정보가 아닌 것은 아니지만 관련자에게 책임은 묻지 않겠다는 뜻으로, 정보를 제공할 경우 제공자의 과실이 없는 것으로 보아 준다는 의미에 다름 아니다. 결국, 앞서 언급한 바와 같이 '개인정보' 라는 개념의 해석 문제를 과실판단의 문제로 치환하게 되는 것이다.

두번째, 비식별조치 자체의 법률적 근거를 찾기가 어렵다. 정보를 제공하는 자가 비식별조치를 한 후 이를 제3자에게 제공할 경우, 이러한 비식별조치 및 제공에 관하여 정보주체의 동의 기타 제15조 제1항 각호 및 제17조 제1항 각호가 정하는 법률적 근거가 없다고 한다면, 개인정보처리자는 무슨 법적 근거로 개인정보를 제3자에게 제공하기 위하여 비식별조치를 할 수 있는가?

개인정보보호법 제15조에 따르면 개인정보처리자는 제1항 각호에 속하는 사유가 있는 경우에 한하여 개인정보를 '수집' 할 수 있고 그 '수집 목적의 범위에서' '이용' [317] 할 수 있다. 개인정보의

식별조치를 취한 정보라도 이것이 재식별되면 개인정보로 본다는 취지이다)

[317] 물론 이 경우 개인정보보호법 제2조 제2호가 "처리" 란 개인정보의 수집, 생성, (…) 가공, (…) 이용, 그 밖에 이와 유사한 행위를 말하는 것으로 규정하고 있는 것으로부터, 비식별조치에 해당하는 '가공' 과 '이용' 은 전혀 별개의 행위이므로 '이용' 만을 대상으로 하는 제15조는 적용되지 않는다고 주장할 수 있을지도 모른다. 그러나 위 조항에 열거된 각 행위 태양이 반드시 상호 배타적인 것은 아니며, 무엇보다도 이 같은 논리에 따르면 개인정보의 동의 없는 생성이나 임의적 가공까지 정당화할 수 있다는 결과가 되므로 현행법의 해석으로는 바람직하지 않다고 생

비식별화처리는 일종의 개인정보 이용행위이다. 그렇다면, 개인정보처리자가 정보주체로부터 정보를 수집할 때 개인정보 비식별화에 관한 동의를 받지 않았다면, 그러한 비식별화 처리는 '수집 목적'에 포함되지 않으므로 개인정보처리자는 비식별화 처리라는 형태로 개인정보를 이용하여서는 안된다(개인정보보호법 제3조 제2항 참고). 제15조 제1항 제1호의 동의 뿐 아니라 나머지 제2호 내지 제6호에 기하여 개인정보를 수집한 경우에도 마찬가지이다. 애초에 정보를 수집한 목적에 '비식별화 조치'가 포함되어 있지 않은 한 그러한 목적을 벗어나 비식별화 조치를 하여서는 안된다는 것이 원칙적인 해석이다.

더욱이 현행법 체계상 개인정보의 목적외 이용이 허용되는 것은 제18조 제2항 각호에 기재된 사유가 존재하는 경우뿐이고, 비식별화처리 즉 개인을 알아볼 수 없도록 하는 처리행위 또한 이러한 한에서만 가능하다. 즉, 개인정보보호법 제18조 제2항 각호의 다른 사유, 즉 동의, 법률 규정 등의 근거가 없는 한, 비식별조치를 정당화할 수 있는 조항은 단 하나, 위 조항 제4호의, "통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우"인 것이다. (즉 이 규정은 비식별조치된 정보의 제공 근거일 뿐 아니라 비식별조치라는 개인정보의 처리 내지 이용행위에 대한 법적 근거이기도 하다)

그렇다면 우리 정부의 비식별조치 가이드라인은 개인정보보호법 제18조 제2항 제4호에 근거하고 있는 것인가? 그렇지 않다. 비식별조치 가이드라인은 비식별조치라는 개인정보의 처리(이용) 행위의 법적 근거에 대하여 설명을 하고 있지 않다. 오히려 이 가이드라인은, 개인정보보호법 제18조 제2항 제4호의 '특정

각한다.

개인을 알아볼 수 없는 형태로' 개인정보를 가공하는 행위를 '비식별조치'와 별도의 것으로 관념하고 있다. 즉, 가이드라인상의 비식별조치란 1단계부터 4단계의 절차를 모두 밟는 것임을 전제로, 제18조 제2항 제4호와 같이 개인정보를 '특정 개인을 알아볼 수 없는 형태'로 변경하는 것은 비식별조치 중 제3단계에 해당하는 '적정성 평가'를 생략하는 것을 말한다고 서술하고 있는 것이다[318] [319]. 그러므로 비식별조치 가이드라인상 비식별조치의 근거가 개인정보보호법 제18조 제2항 제4호가 아닌 것은 분명하다.

즉, 비식별조치 가이드라인상 '비식별조치'라는 처리 내지 이용행위에 대한 현행법상 근거를 찾기가 어려워 보인다.

④ 위와 같은 점은 유럽법과의 비교에서도 드러난다.

유럽 개인정보보호지침상 개인정보의 처리 일반(수집, 이용, 제공을 모두 포함하는 개념[320]이다)는, 유럽 개인정보보호지침 제6조 제1항 (b)와 같이 수집시 특정된 목적과 양립불가능(incompatible)하지 않아야 하고, 동시에 제7조에 의한 적법 근거가 있다는 전제하에 가능하다[321].

우선 제6조에 관하여 보면, 목적외 이용을 전부 불허하는 구조가

---

[318] 행정자치부 등(주37), 6면

[319] 비식별조치 가이드라인에 따르면, 개인정보보호법 제18조 제2항 제4호의 체계상 지위에 관한 문제 또한 발생한다. 가이드라인에 따르면 비식별조치 가이드라인에 따르면 위 조항에 따라 개인정보를 "특정 개인을 알아볼 수 없는 형태"로 변경하는 것은 총 4단계의 비식별조치 중 제3단계 '적정성 평가'만을 생략하는 것을 의미하며, 제4단계 조치는 여전히 요구된다고 한다(6면).

[320] 유럽 개인정보보호지침 제2조 (b)

[321] 이 두 조항은 누적적인 것이다. 채성희(주97),47면

아니라, 수집 당시 목적과의 '양립가능성'을 심사함으로써, 반드시 수집된 목적 자체가 아닌 다른 목적으로라도 개인정보의 처리가 허용될 가능성을 열어 두고 있음을 알 수 있다. 이러한 양립불가능 여부는 사안별로, i) 정보가 수집된 목적과 추가적 처리(제공)의 목적, ii) 수집시 정보주체가 정보처리에 대하여 가지는 합리적 기대, iii) 정보주체의 성질과 추가 처리(제공)이 정보주체에 미치는 영향, iv) 통제자가 공정한 처리(fair processing)를 보장하고 정보주체에 대한 부당한 영향을 예방하기 위하여 취하는 보호조치 등을 종합하여 판단한다[322]. 여기에 따르면, 연구 등의 목적으로 정보주체를 충분히 식별할 수 없도록 처리하는 행위는, 물론 다른 보호조치들의 존재를 요구할 수도 있으나, 애초 수집 목적과 양립불가능하지 않다고 인정될 여지가 있는 것이다.

다음으로 유럽 개인정보보호지침 제7조의 개인정보 처리의 적법 근거 요건에 관하여 살펴본다. 먼저 이 조항은 동의 뿐 아니라 개인정보 처리 일반에 대하여 적용되는 규정이다. 이 조항에는 우리 개인정보보호법 제15조 제1항, 제17조 제1항과 마찬가지로 동의, 법령상 근거도 있지만, 또다른 적법 근거인 (f)항이 있다. 즉, 개인정보 처리는 "통제자 또는 정보가 공개되는 제3자에 의하여 추구되는 합법적인 이익(legitimate interest)을 달성하기 위하여 필요한 경우, 제1조 제1항에 기한 보호를 필요로 하는 정보주체의 기본권과 자유를 위한 이익이 그러한 이익이 우선하는 경우를 제외하고" 정당화될 수 있다[323]. 즉, 동의가 없더라도 (f)항과 같은 '합법적인 이익' 달성을 근거로 개인정보의 처리가 가능한 구조이며, 앞서 언급한 대로 여기서의 '처리'는 '동의' 뿐 아니라 '제공'까지 포함하므로, '합법적인 이익'을 근거로

[322] WP 29, Opinion 03/2013 on purpose limitation(WP203), 2013, p.3

[323] 일반 개인정보보호 규칙 제6조 제1항 (f)도 유사한 규정을 두고 있다.

제3자 제공까지 정당화될 수 있게 되는 것이다. 더욱이 (f)항은 개인정보처리자의 이익만을 고려 요소로 삼는 우리 개인정보보호법 제15조 제1항 제6호와는 달리 '통제자' 즉 개인정보처리자 뿐 아니라 '정보가 공개되는 제3자'의 관점도 고려하고 있다. 여기서 이 조항의 적용 여부는 통제자 등의 합법적 이익 유무, 정보주체에 대한 영향 평가, 두 법익간 비교, 추가적 보호조치의 유무 등을 고려하여 판단하는데[324], 개인정보에 대한 익명화 기술을 적용하였는지 여부가 이러한 비교를 수행함에 있어 중요한 역할을 하게 된다[325]. 그렇다면, 비록 이 의견서에 이에 상응하는 구체적인 언급은 존재하지 아니하지만, 개인정보를 가공하여 개인을 식별할 수 없도록 하는 행위와 이를 제3자에게 제공하는 행위에 대하여 '합법적인 이익'을 인정할 수 있는 소지도 없지 않은 것이다. 실제로 영국 ICO는 '개인을 알아볼 수 없도록 처리하는 것 즉 익명화(anonymisation) 처리의 법적 근거에 관하여, 익명화를 포함한 개인정보 처리의 적법 근거는 여러 가지가 있고, 동의는 그 중 하나일 뿐'이라는 취지로 명시하고 있는바, 이는 비식별화 처리에도 법적 근거가 필요하며, 유럽연합 법제에서는 이것이 위 '합법적인 이익'을 포함, 제7조 각호에 규정된 사유들(영국 Data Protection Act 1998 Schedule 2)일 수 있다는 점을 밝힌 것으로 해석된다[326]. GDPR의 규정 내용들도 대동소이하다[327].

이상을 종합하면, 유럽연합에서는 개별 사실관계에 따라 정보주체의

---

[324] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014, pp. 33~43

[325] WP 29(주320), p.56

[326] ICO(주208), p.28; 同旨, Eliott et al.(주210), p.13.

[327] GDPR의 관련 규정에 대한 자세한 설명은, 채성희(주97)를 참고하라.

동의 없이도 당초 수집 목적을 벗어나는 비식별화조치를 취할 수 있으며, 나아가 비식별화된 정보를 제3자에게 제공할 수 있는 여지까지 존재한다고 볼 수 있다.

반면 우리나라의 경우 "개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다"는 개인정보보호법 제15조 제1항 및 "개인정보처리자는 개인정보를 제15조 제1항에 따른 범위를 초과하여 이용하…여서는 아니된다"는 개인정보보호법 제18조 제1항의 문언, 그리고 제18조 제1항의 예외 사유를 제한적으로 열거하고 있는 제18조 제2항의 규정체계상, 정보주체의 동의 기타 제18조 제2항 각호에 규정된 사유 없이는 수집 목적에 포함되지 않은 비식별화 조치를 하는 것을 정당화하기는 어려워 보인다(제17조 및 제18조의 내용을 종합하여 볼 때 그러한 정보의 제공 또한 극히 제한적으로만 허용된다).

⑤ 물론, 실무적 관점에서는 오히려 유럽연합의 위와 같은 법을 근거로, 우리도 통계적, 학술적 목적 이외의 개인정보 제공 및 목적외 이용을 허용할 여지를 두어야 하므로 개인정보보호법 조항들을 완화하여 해석할 수 있다는 견해도 성립할 수 있을 것이다. 구체적으로, 개인정보보호법 제15조 제1항을 완화하여 해석하는 방안이 있다. 즉, 어차피 개인정보보호법 제15조 제1항 제6호와 같은 사유가 있다면 비식별조치를 할 목적으로 동의 없이 개인정보를 수집하고 이용하는 것이 가능하므로, 애초에 비식별조치를 염두에 두고 정보를 수집하지 않았더라도 제15조 제1항 제6호에 따라 개인정보를 이용하는 것도 당연히 허용되어야 한다는 해석이 그것이다. 정보의 비식별조치는 '이용'이라기보다는 '가공'에 가까운 행위이므로 목적외 이용에 관한 규정을 엄격히 적용할 필요가 없다는 논리도 성립할 수 있다고 본다. 더욱이 대법원도 2006. 8. 17. 선고 2014다235080 판결을 통하여

개인정보보호법의 문언에 얽매이지 않는 해석을 통하여 공개된 개인정보의 활용 가능성을 명문의 규정에 비하여 넓게 인정한 바 있으므로, 이로써 개인정보보호법의 유연한 해석을 뒷받침하는 것도 가능할 것이다. 이러한 점들을 종합하면, 실무적으로는 비식별조치 가이드라인과 같은 실용적 해석이 성립할 가능성도 충분히 존재한다. 구체적 사안에서의 개별적 타당성이라는 관점에서 본다면 이러한 해석이 보다 옳을 수 있겠지만, 이론적으로는 앞의 해석이 좀더 정합적이고 간명해 보인다.

4) 소결론

이상에서 살펴본 바와 같이 우리 법의 해석상으로는 개인정보 개념에 관한 상대적 접근이 타당하다. 처리자 기준설과 처리자 및 제공받는 자 기준설 중에서는 처리자 기준설이 법 문언의 해석에 충실하다. 처리자 기준설을 취하더라도 개인정보보호법 제18조 제2항 제4호의 사유가 존재하는 경우 개인을 알아볼 수 없도록 개인정보를 가공한 후 이를 제3자에게 제공할 수 있으므로, 개인정보의 이용을 통한 편익 증진이라는 가치를 전혀 달성할 수 없는 것은 아니다.

그러나 그렇다고 하더라도 현대 정보화사회 속에서, 개인정보를 개인을 알아볼 수 없도록 가공한 후 제3자에게 제공하는 것과 같은 활동을 보다 폭넓게 허용할 필요가 있다는 점에서 처리자 및 제공받는 자 기준설의 입장과 이것과 연관된 비식별조치 가이드라인의 내용을 이해하지 못할 바는 아니다. 특히 정보통신망법이 적용되는 경우 개인정보보호법 제18조 제2항 제4호가 적용될 수 없다고 해석될 수도 있는 점을 감안하면 더욱 그러할 것이며, 이는 개인정보자기결정권과 다른 법익의 조화를 감안할 때 바람직한 결과도 아니다. 근본적인 입법적 개선이 필요한 부분이라 생각된다.

다. 합법적 수단 v. 불법적 수단

우리나라에서 '쉽게 결합하여'가 '합리적으로 활용할 가능성이 있는 수단을 사용하여'와 일반적으로 같은 의미로 받아들여지고 있다는 점은 앞서 살펴본 바와 같다. 구체적으로, 정부에 따르면, '쉽게 결합'이란 추가적 정보의 입수가능성 및 추가적 정보와 보유 정보의 결합 가능성을 의미하는데, '입수가능성'은 합법적인 방법의 정보 입수만을 의미하고, '결합가능성'은 현재의 기술 수준에 비추어 결합이 가능한 경우와 결합하는 데 비합리적인 수준의 비용이나 노력이 수반되지 않는 경우를 말한다는 취지로 해석하고 있다[328]. '결합가능성'의 의미에 대하여는 별 이견이 없는 것으로 보이나, 앞서 살펴본 바와 같이 '입수가능성'과 관련하여 합법적인 방법의 정보 입수만을 의미한다고 보아야 할지에 관하여는 (특히 독일에서) 상당한 견해 대립이 존재한다.

필자의 견해로는, '쉽게 결합하여'가 '합리적인 수단'을 의미하는 한, 원칙적으로 합법적인 수단만 고려하는 것이 옳다고 본다[329]. 정상적인 상황에서라면 사회의 구성원들이 합법적으로 행위하리라고 기대하는 것이 합리적이기 때문이다.

그러나 해당 정보를 둘러싼 정보처리의 관행, 업계의 사업 관행, 정보의 가치 등을 고려해 볼 때, 불법적인 수단의 사용이 별 문제제기 없이 이루어지고 있다거나, 문제되는 정보의 가치가 높은 반면 불법적인 수단을 사용하였을 경우의 위험은 그다지 높지 않다는 등의 예외적인 사정이 있다면 이를 감안할 수 있다고 생각한다[330]. 뒤에서 보다 자세히 설명하겠지만, 합리적인 범위를

---

[328] 행정자치부 등(주37), p.55

[329] CJEU C-582/14 Patrik Breyer v. Deutschland, 46

[330] 同旨 WP29(주73), pp. 15~16;, Dammann, in Simitis[Hrsg.](주100), § 3 Rn.

넘어선 '과다한 비용의 지출' 여부는 지출되는 비용 자체 뿐 아니라, 그 비용을 지출함으로써 얻어지는 정보의 가치까지 고려하여 형량을 함으로써 판단될 수 있는 것이기 때문이다[331].

또한 우리 개인정보보호법은 '쉽게 결합'이라고 하였지 '적법하게 결합'과 같이 수단의 적법성 유무를 식별가능성의 요건으로 규정하고 있지 않은바, 어떠한 결합이 쉬운지 여부는 그 결합을 둘러싼 제반 상황으로부터 가치중립적이고 객관적으로 결정하여야지, 그 결합이 적법한지 불법한지를 가지고 판단할 문제는 아니기 때문이다[332]. 유럽연합의 경우 원칙적으로 적법한 수단만 고려하는 입장인 것으로 보이기는 하나[333], 사회 전반적으로 개인정보 보호의 중요성에 대한 인식이 다소 미흡한 우리나라의 현실상 불법한 수단에 의한 추가정보 입수 가능성을 쉽게 배제해서는 안된다고 생각된다[334].

26~31

[331] Gola/Shomerus(주106), §3 Rn.44; Tinnefeld, in Roßnagel[Hrsg.](주134), 4.1. Rn. 24

[332] 同旨, Breyer(주141)

[333] CJEU Case C-582/14 Patrik Breyer v. Deutschland

[334] BGH는 Breyer 사건에서 유동 IP주소의 개인정보성에 관하여 유럽사법재판소에 선결적 판단을 구하면서, "불법적인 행위는-무엇보다도 국가 기관(staatliche Stelle)들에 있어서는-정보 조달의 수단으로 보아서는 아니된다" 고 판시한 바 있다(BGH, ZD 2015, 80 이하). 그러나 우리나라에서는 아직 이러한 전제는 성립하기 어렵다고 본다.

라. 통상적인 업무 과정상 입수 가능한 정보만 고려할 것인지 여부 – 사내 정보활용의 경우를 중심으로

(1) 서론

우리나라의 일부 학설 중에서는, 일본 개인정보보호법상의 '용이조합성' 개념에 관한통설적 해석을 근거로, 우리나라에서도 "정보처리자가 통상적인 업무과정에서 쉽게 입수할 수 있는 다른 정보"만이 '쉽게 결합'될 수 있는 정보라고 보아야 한다는 견해가 있다[335]. 여기에 따르면, 식별에 필요한 추가 정보의 입수를 위하여 "다른 사업자에게 조회해야 하는 경우 또는 당해 사업자 내부에서도 취급 부문이 다른 경우" 및 "내부조직 사이에서도 시스템의 차이 때문에 기술적으로 조합이 곤란한 경우, 조합을 위하여 특별한 소프트웨어를 구입하여 인스톨할 필요가 있는 경우" 입수 및 결합의 용이성이 부정된다.

그러나 필자는, 동일 회사의 다른 부서 또는 사업부문에 식별에 필요한 추가 정보가 존재하는 경우에는 특별한 사정이 없는 한 '쉽게 결합'할 수 있는 가능성을 인정하는 것이 옳다고 보며, 결합이 용이한지 즉 '시스템의 차이 때문에 기술적으로 조합이 곤란하거나 조합을 위하여 특별한 소프트웨어를 구입하여 설치할 필요가 있는 경우' 결합이 용이하다고 볼 수 있을 것인지는 이와 같이 일률적으로 판단해서는 안되며, 개별 사안에 따라 정보의 결합으로 얻을 수 있는 편익과 결합에 소요되는 비용을 종합적으로 검토함으로써 판단해야 한다고 본다.

(2) 일본 개인정보보호법의 특수성

필자가 이와 같이 보는 이유는, 첫째, 일본 개인정보보호법은 일견

[335] 구태언(주52), 88~ 92면; 이인호(주43), 81면.

우리 개인정보보호법과 유사해 보이지만, 실은 기본적인 원리와 체계가 다르기 때문이다. 일본 개인정보보호법은 제정 당시부터 **민간의 자율성을 존중**하여 필요최소한도의 규율만 정한다는 입장에서 출발한 법률로, 공공영역은 물론 민간에 대하여도 광범위한 규제를 시행하고자 하는 우리 개인정보보호법과는 그 출발점을 달리한다.

2003년 개인정보보호법안을 제안하였던 일본 정부의 내각관방 개인정보보호담당실은 '개인정보의 보호에 관한 법률안 축조해설'에서 개인정보보호법은 개인의 권익침해를 방지하기 위한 '필요최소한도의 규율'임을 명시한 바 있다[336]. 이는 일본 개인정보보호법의 체계적 해석에 의해서도 뒷받침된다. 즉 행정기관 개인정보보호법과 독립행정기관 개인정보보호법은 제2조 제2항에서 '개인정보'에 대한 정의규정을 별도로 두고 있으나, 여기에는 '용이성'이라는 개념요소가 포함되어 있지 않다. 그 취지는, 공공기관에 대하여는 개인정보의 범위를 넓게 인정하여 개인정보보호의무를 폭넓게 부과하고, 민간 부문에 대해서는 이를 좁게 인정함으로써 관련 의무를 경감하여 영업의 자유를 존중함에 있다고 한다[337]. 실제로 민간분야의 실질적 규제는, 주무부처의 가이드라인과 자율규제에 의하여 이루어지고 있으며[338], '정치적 상황에 따라 반년 만에 급하게 만들었으므로, 개별 사업자에 대해서는 최대한 무리가 가지 않게 만든 법'이라는 평가마저 받고

---

336 内閣官房 個人情報保護擔當室(주246), 7면

337 宇賀克也(주242), 34면, 菅原貴与志(주245), 25면. 同旨: 鈴木正朝·高木浩光·山本一郎(주247), 47면.

338 김상미, "일본의 개인정보보호 법제", KISO저널 제7호, 2012(2016. 4. 8. 확인) <http://journal.kiso.or.kr/?p=608>; 고려대학교 산학협력단(총괄책임자 박노형), "EU 및 일본의 개인정보보호법제 및 감독체계 개편내용 분석", 방송통신위원회 방통융합정책연구, 2014, 52면

있는 실정이다[339]. 일본 개인정보보호법의 규율 내용 자체도 정보 수집시 동의를 취득할 의무를 규정하고 있지 않고, 옵트아웃 방식을 전제로 한 제공도 허용하고 있는 등(제23조 제2항) 우리의 그것에 비하여 상당히 느슨한 수준이다.

요컨대, 일본 개인정보보호법은 제정 당시부터 '사업자에 대한 최소한의 부담' 이라는 요소가 중요하게 작용하였던 것으로 보이고, 실제 체계 및 규율 또한 그러한 방식으로 이루어진 측면이 있어 보인다. 반면 우리나라 개인정보보호법은 민간과 공공을 아우르는 강력한 보호규범으로 제정된 것이므로, 일본법의 해석을 우리나라법에 무비판적으로 그대로 도입하는 것은, 모든 외국법리의 도입이 그렇지만 이 경우에는 특히, 경계할 필요가 있다.

(3) '쉽게 결합' 의 판단기준 – 우리나라 및 다른 나라의 경우

우리 정부의 비식별조치 가이드라인에 따르면 '결합 가능성' 은 "현재의 기술 수준에 비추어 결합이 가능한 경우와 결합하는 데 비합리적인 수준의 비용이나 노력이 수반되지 않는 경우"에 한하여 인정되며, "일반적으로 사업자가 구매하기 어려울 정도로 고가의 컴퓨터가 필요한 경우라면 '쉽게 결합' 하기 어렵다"고 한다[340].

유럽연합 WP29의 경우 '결합 가능성' 의 '합리성' 여부를 판단하며, 단순히 사업자에게 소요되는 비용 뿐 아니라, "식별에 드는 비용, 정보처리 목적, 정보처리가 짜여진 구조, 통제자가 예상하는 이점, 그 개인들과 관련하여 문제되는 이익들, 조직의 기능 장애(organzational dysfunction, 예컨대 정보유출과 같은

[339] 鈴木正朝·高木浩光·山本一郎(주247), 41면

[340] 행정자치부 등(주37), p.55

사태) 가능성, 정보처리에서 통제자가 추구하는 목적, (개인 식별이라는 목적이 없는 경우) 식별을 방지하기 위하여 취해진 기술적 보호조치의 유무" 등[341] 그 비용을 지출함으로써 얻을 수 있는 개인정보처리자의 편익, 정보주체에 대한 예상 리스크까지 두루 고려한다. 즉, 비용과 편익(위험)의 비례성이라는 관점에서 '합리성'을 파악하고 있는 것이다. 유럽사법재판소 또한 앞서 살펴본 Breyer 판결에서, "정보주체의 식별이 법에 의하여 금지되어 있거나, 시간, 비용, 인력이라는 의미에서 과도한(disproportionate) 노력을 요구함으로써 재식별의 위험이 현실적으로 사소한(insignificant) 것이라면" 합리성을 부정한 바 있다[342].

우리나라에서도, 개인정보자기결정권과 다른 법익이 충돌하는 경우 비례성 원칙에 입각한 이익형량이 이루어져야 한다는 점에 비추어 볼 때, '비합리적인 수준의 비용이나 노력' 유무에 관하여 정보의 가치와 법익 침해의 위험을 함께 고려하는 것이 타당한 접근이라 생각된다. 반면 일본과 같은 접근을 지지하는 견해들은 '정보처리자의 통상적인 업무 과정에서 정보를 쉽게 입수 및 결합할 수 있는가'만을 기준으로 하고 있기 때문에, 비록 식별을 위한 정보의 입수 및 결합이 통상적인 업무 과정에서는 이루어지지 않더라도 정보처리자의 필요가 발생할 경우 예외적인 업무 과정을 통하여 이루어질 수 있는 가능성을 무시하고 있다. 현실에서 어떤 정보가 개인 식별을 위하여 사용될 수 있는 경우의 수가 다양한 점 등을 고려하면, 이와 같은 단순한 접근은 정보주체의 보호라는 관점에서 바람직하지 않다고 생각된다.

---

[341] WP 29(주73), pp.15~16

[342] CJEU Case C-582/14 Patrik Breyer v. Deutschland

(4) 같은 회사 내에서 정보의 결합을 금지하는 정책 등이 있는 경우의 취급

한편 위와 같이 일본의 학설을 차용하자는 견해가 "당해 사업자 내부에서도 취급 부문이 다른 경우" 및 "내부조직 사이에서도 시스템의 차이 때문에 기술적으로 조합이 곤란한 경우" 합리적 결합가능성을 부정하자고 주장한다는 점은 앞서 언급한 바 있다. 그러나 독일과, 심지어 유럽연합 내부에서 개인정보보호에 관하여 상당히 완화된 태도를 취하고 있는 것으로 이해되는 영국의 경우에도 위와 같은 입장에 동조하는 견해는 찾아 보기 어렵다.

오히려 앞서 살펴본 바와 같이, 영국에서는 "한 조직의 한 부서로부터 암호화된 데이터베이스를 동일한 조직의 다른 부서로 전송함으로써 익명화를 시도하는 것은, 암호화 프로세스의 '키'를 전송하는 부서가 보유하고 있는 경우 항상 성공적일 수는 없다"[343]는 견해가 있다. 독일에서는 유동 IP주소의 개인정보성을 다투는 과정에서 베를린 지방법원(Landesgericht Berlin)은 2013. 1. 31.자 판결[344]에서 유동 IP주소로 개인정보를 만들 수 있는 추가적 정보와 관련하여, 그 자체로 개인을 식별할 수 없는 정보와 이 정보와 결합함으로써 식별을 가능케 하는 정보가 정보처리자의 서로 다른 부문에서 처리되는 경우라 하더라도 두 종류의 정보는 모두 처리자의 처분 권한 안에 있다고 보아야 하며, 처리자가 두 종류의 정보를 서로 결합할 의도를 가지고 있는지는 고려할 필요가 없다고 판시한 바 있다.

필자의 견해로는, 같은 회사 내부에서 사업 부문이 다르다거나, 내부조직 사이의 시스템 차이로 인한 결합의 어려움이 있다고 하여 일률적으로 결합에 비합리적인 노력이 필요하다고 인정하여서는

[343] Peter Carey(주196) , p.22

[344] LG Berlin, ZD(2013), 618

안된다. 전자의 경우 서로 다른 사업 부문을 총괄하는 의사결정권자가 결합에 대한 결정을 할 가능성은 늘 열려 있다고 보아야 할 것이고, 후자의 경우, 회사의 필요가 발생한다면 시스템의 차이는 얼마든지 극복할 수 있는 것이기 때문에 그러하다.

회사가 식별에 필요한 추가 정보에 관하여 접근 권한을 통제하는 정책을 쓰는 경우라면 어떠한가? 단순히 그러한 정책이 있는 것만으로는 불충분하고, 회사의 구성원들이 그 정책을 충분히 인지하고 실행에 옮길 수 있을 만큼 정책 내용이 구체적이고, 정책이 실질적으로 집행될 수 있는 통제체제가 존재하며, 이를 위반할 경우 적발 및 처벌할 수 있는 강력한 컴플라이언스 프로세스가 존재하는 상황이라면 결합에 비합리적인 노력이 필요하다고 볼 여지도 있다고 생각한다. 그렇지 않고 형식적인 정책의 존재만으로 충분하다고 본다면, 직원들의 개인정보에 대한 인식 부족, 통제 프로세스의 부재로 의도적이든 아니든 간에 재식별이 일어날 가능성을 배제할 수 없을 것이고, 특히 회사 전체적인 컴플라이언스 문화가 충분히 확립되어 있지 않다면 고위 임원들의 지시에 의하여 기존 프로세스의 집행이 회피되는 경우도 발생할 수 있을 것이기 때문이다.

그런 의미에서, 개인정보에 대하여 비식별조치를 취한 후 "원본정보 관리부서와 비식별정보 관리부서간 비식별조치 관련 정보공유를 금지" 및 "비식별 정보파일에 대한 접근권한 관리 및 접근통제"를 지키기만 하면 원본정보가 사내에 있더라도 비식별화된 정보를 개인정보로 보지 아니한다는 행정자치부 등의 비식별조치 가이드라인의 입장[345]은, 그러한 금지 및 관리·통제가 실질적으로 매우 철저히 이루어지고 있는 한에서 타당할 수 있다고 생각된다.

[345] 행정자치부 등(주37), 14면

6. 소결론

이상에서 살펴본 바와 같이, 우리나라법의 해석상 '개인을 알아볼 수 있는 정보'는 유럽연합 개인정보보호지침의 '식별할 수 있는 개인에 관한 정보'와 같은 의미로 읽어야 한다. '식별'이란 개인을 다른 개인으로부터 구별하여 다르게 취급할 수 있는 가능성을 의미한다.

식별가능성에 관한 객관설과 상대설 중 상대설이 우리나라 법체계상 적합한 해석이다. 그리고 상대설 중에서는 처리자 기준설이 타당하다. 여기에 따르면, 개인을 알아볼 수 없도록 하는 비식별조치 및 비식별조치를 취한 정보의 제3자 제공은, (제15조 제1항 및 제17조 제1항이 정하는 동의 등의 법적 근거가 없는 경우에는) 오로지 제18조 제2항 제4호의 요건이 갖추어지는 한에서만 가능하다. 그 이상으로 개인정보 제공을 활성화하기 위해서는 원칙적으로 입법적 개선이 필요하다.

식별을 위한 수단이 합리적인지 여부의 판단과 관련하여 원칙적으로는 적법한 수단만을 고려하되, 예외적으로 위법 수단도 고려할 수 있어야 한다.

일반적으로 식별에 필요한 다른 정보가 한 회사 내에 존재하는 경우라면, 식별가능성을 인정하여야 한다. 그러나 회사 내부에 식별에 필요한 추가 정보와 대상 정보가 서로 결합되지 않도록 충분히 통제할 수 있는 장치가 마련되어 있다면, 대상 정보의 식별가능성-개인정보성을 부정할 여지도 있을 것이다.

V. 결론

이상에서 현행 헌법 및 개인정보보호법령의 문언적·체계적 해석이라는 관점에서, 외국의 사례를 참고하여, 개인정보 개념을 검토해 보았다.

개인정보 개념을 논의함에 있어 핵심적인 주제는 첫째, 식별가능성 개념을 이를 처리하는 주체에 따라 상대적으로 판단할 것인지 여부와, 둘째, 개인정보처리자가 자신에게는 개인정보인 어떤 정보를, 정보 자체로 개인식별이 어려운 형태로 가공하여 제공하는 경우 그러한 정보가 개인정보의 제공에 해당하는지 여부이다. 그 밖에, 식별가능성 판단에 있어 식별에 사용될 수 있는 수단으로서 합법적인 수단만 고려할 것인지 아니면 불법적인 수단도 고려할 것인지라는 문제와, 동일한 개인정보 처리자 내의 서로 다른 두 부문이 같은 정보를 취급하고 있을 때 그 중 한 부문에 대하여 식별가능성이 없음을 이유로 그 부문에 대하여 개인정보성을 부정할 수 있을지에 관한 쟁점도 있다.

첫번째 쟁점에 관하여 우리나라의 경우, 비록 판례는 다르게 해석될 여지가 있지만, 전자의 쟁점에 대해서는 대체로 상대설이 우선하는 것으로 보인다. 그리고 이는 유럽연합, 독일, 영국, 일본의 공통된 태도이기도 하다. 필자도 상대설에 찬동한다.

두번째 쟁점에 관하여 유럽연합과 일본은 그러한 정보의 제공도 개인정보의 제공이라고 보는 듯하나, 영국의 경우는 반대의 태도를 취하고 있다. 우리나라의 학설 및 정부의 태도에서는 영국의 경우와 유사하게 해석하려는 경향이 감지된다. 이러한 주장들은 주로 i) 식별가능성 개념은 '개인정보처리자'를 기준으로 판단되어야 하므로

식별가능성 판단시에 제3자의 입장도 고려되어야 한다거나[346], ii) 개인정보처리자 및 이로부터 정보를 제공받을 자 모두의 입장을 기준으로 개인정보 여부를 판단하여야 한다는 식의[347], 개인정보 개념 자체에 대한 해석론을 근거로 한다. 위 학설들은 비록 표현 방식은 다르지만 정보를 제공하는 정보처리자 입장에서는 개인정보이나 제공받는 자 입장에서 개인을 식별할 수 없는 정보의 제공은 개인정보의 제공이 아니라고 보는 점에서 일치한다.

그러나 현행법을 엄격하게 해석할 경우, 이와 같은 해석이 어려울 수 있다는 것이 필자의 견해이다. 식별가능성 개념은 정보를 처리하는 자를 기준으로 판단하여야 하고, 제공받을 자의 사정까지 감안하여 판단할 것이 아니다. 제공하는 자는 개인식별이 가능하나, 제공받는 자 입장에서 개인식별이 불가능한 정보의 제공은, 정보주체의 동의 등 제17조 제1항 각호가 규정하는 법률적 근거가 없는 상황이라면 개인정보보호법 제18조 제2항 각호, 특히 제4호의 요건을 갖추어 하여야 한다는 것이 현행법의 기본 체계이다. 요컨대 '개인을 알아볼 수 없도록' 하는 처리 즉 비식별처리를 하고 통계 목적 또는 학술적 목적이 있는 경우에 한하여 제18조 제2항 제4호에 의하여 제공을 정당화할 수 있다는 것이다.

이러한 필자의 견해에 따를 때, '비식별화 조치를 취하면 통계적 또는 학술적 목적이라는 제공 목적에 구애받지 않고, 개인정보의 제3자 제공을 자유롭게 할 수 있다'는 비식별조치 가이드라인 식의 해석에 비하여 개인정보의 유통 및 활용이 원활치 않아지는 것은 사실이다. 비식별조치 가이드라인의 해석도 정부의 유권해석이니만큼 존중할 필요가 있고, 더욱이 관점에 따라서는

[346] 대표적으로, 김진환(주3), 전응준(주50) 등

[347] 행정자치부 등(주37)

법리적으로 정당화할 여지도 충분히 있다고 본다. 이러한 가이드라인을 이용하여 우리 개인정보보호법의 한계를 극복할 현실적 요청 또한 존재한다.

이와 관련하여, 본고를 통하여 필자가 시도한 것은, 우리 개인정보보호법을 문언적·체계적 해석원리에 따라 엄격히 해석할 경우 나타나는 있는 그대로의 모습을 밝히는 것임을 밝히고자 한다. 즉, 현실적인 문제의 해결을 위한 유연한 해석이라는 관점은 반영하지 않은 것이다. 그러므로 본고의 작업은 실무적 활용을 염두에 둔 고찰이라기보다는, 개인정보보호법의 입법적 개선을 위한 전제작업의 성격이 강하다고 생각된다. 현행 개인정보보호법이 지나치게 경직적이어서 개정할 필요가 있다는 점에 대해서는 이론의 여지가 없는바, 현행법을 엄격히 해석함으로써 그 개선점을 정확히 짚어내는 것은 법 개정을 위하여 반드시 필요한 작업이기 때문이다.

개인정보보호법 개정의 방향에 관하여, 개인정보 개념 자체는 명확하게 정하여 두되(상대설, 처리자 기준설), 구체적 개인정보 처리행위들(수집, 이용 뿐 아니라 제공 및 목적외 이용을 포함)의 허용 여부 판단에 제반 상황을 고려한 이익형량이 반영될 수 있도록 행위 규범에 유연성을 부여하는 것이 바람직하다고 생각한다. 그리고 그것이 앞서 살펴본 유럽연합, 영국, 일본의 접근 방향과도 일치한다. 이와 같이 할 경우, 개인정보 여부에 대한 판단 및 행위의 허용 여부에 관한 1차적인 형량은 어떤 정보에 대하여 특정 처리행위를 하려는 정보처리자에 의하여 수행될 것인바, 정보처리자가 그러한 이익형량을 적정하게 수행할 수 있도록 담보하는 여러 가지 장치들(예컨대 Privacy by Design, Privacy Impact Assessment)을 충분히 규정하는 접근이 개인정보의 보호와 활용의 조화 및 이론적 정합성을 통한 예측가능성의

확보라는 관점에서나 바람직하다고 생각된다[348].

[348] 이러한 문제의식에 관해서는, 채성희(주97)을 참고.

<참고문헌>

단행본

국내 문헌

경정익, 스마트시대 개인정보보호 이해와 해설, 부연사, 2015
곽윤직 편, 민법주해 XVIII, 박영사, 2005
권건보, 개인정보보호와 자기정보통제권, 서울대 법학연구총서 3, 경인문화사, 2006
김동희, 행정법 I(제13판), 박영사, 2010
김주영・손형섭, 개인정보 보호법의 이해-이론・판례와 해설, 법문사, 2012
김철수, 헌법학신론(제21전정신판), 박영사, 2013
백윤철 등, 인터넷과 개인정보보호법, 한국학술정보(주), 2012
성낙인, 헌법학(제15판), 법문사, 2015
윤주희 등, 개인정보의 범위에 관한 연구, 개인정보보호위원회 연구결과보고서, 2014
이창범, 개인정보보호법, 법문사, 2012
정종섭, 헌법과 기본권, 박영사, 2010
허영, 한국헌법론(전정10판), 박영사, 2014
홍정선, 기본행정법(제3판), 박영사, 2015

외국 문헌

Carey, Peter, *Data Protection*, 4th Edition(Kindle Version), Oxford University
Elliot, et al., *The Anonymisation Decision-Making Framework*, UKAN Publications, 2014
European Union Agency of Fundamental Rights and Council of Europe,

Handbook on European Data Protection Law, Publications Office of the EU, 2014

Gola/Schomerus, *Bundesdatenschutzgesetz*, C.H.Beck, 2015

Hoeren/Sieber/Holznagel, *Multimedia-Recht*, C.H.Beck, 2015

Jay, Rosemary and Angus Hamilton, D*ata Protection – Law and Practice*, Second Edition, Sweet & Maxwell, 2003

Maunz/Dürig, *Grundgesetz-Kommentar*, C.H.Beck, 2015

Plath, *Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG*, Verlag Dr.Otto Schimidt, 2013

Robinson et al, *Review of the European Data Protection Directive*, RAND Corporation Technical Report Series, Rand Corporation, 2009

Roßnagel[Hrsg.], *Handbuch Datenschutzrecht,* C.H.Beck, 2003

Schaar, *Datenschutz im Internet-Die Grundlagen*, Verlag C.H.Beck, 2002

Simitis[Hrsg.], *Bundesdatenschutzgesetz*, Nomos(2011)

time.lex CVBA, *Study of case law on the circumstances in which IP addresses are considered personal data D3. Final Report,* 2011

Wolff/Brink, *Beck'scher Online-Kommentar Datenschutzrecht*, 14. Edition, C.H.Beck, 2015

宇賀克也, 個人情報保護法の逐條解說, 第2版, 有斐閣置, 2008

日置巴美, 板倉陽一郎, 平成27年改正個人情報保護法のしくみ、商事法務、2015

瓜生和久 編, 平成27年改正個人情報保護法, 商事法務, 2015

鈴木正朝, 高木浩光, 山本一郎, ニッポンの個人情報-「個人を特定する情報が個人情報である」と信じている方へ、翔泳社, 2015

菅原貴与志, 詳解 個人情報保護法 企業法務, 第5版, 民事法研究會, 2014

鈴木正朝, 高木浩光, 山本一郎, ニッポンの個人情報 「個人を特定する情報が個人情報である」と信じている方へ、翔泳社, 2015

內閣官房 個人情報保護擔當室, 個人情報の保護に関する法律案 逐條解說, 2003

岡村久道, 個人情報保護法, 新訂版, 有斐閣, 2009

논문

국내 논문

강석철, “독일의 개인정보 보호에 관한 법률 및 제도 연구”, 국외훈련검사 연구논문집II 제28집, 2013, 법무연수원

고려대학교 산학협력단(총괄책임자 박노형), “EU 및 일본의 개인정보보호법제 및 감독체계 개편내용 분석”, 방송통신위원회 방통융합정책연구, 2014

고학수, 최경진, “개인정보의 비식별화 처리가 개인정보 보호에 미치는 영향에 관한 연구”, 개인정보보호위원회 연구과제 최종보고서, 2015

구태언, “현행 개인정보 법제상 ‘개인정보’ 정의의 문제점”, 개인정보보호법제 개선을 위한 정책연구보고서, 프라이버시 정책연구포럼, 2013

———, “개인정보 보호법의 제문제”, 법학평론 제3권, 2012

——— , 개인정보 정의조항, 동의제도 및 형사처벌의 합리화에 관한 연구, 고려대학교 정보보호대학원 석사학위논문, 2013

권건보, “개인정보보호의 헌법적 기초와 과제”, 저스티스 통권 제144호

권영준, “개인정보 자기결정권과 동의제도에 관한 고찰”, 2015 Naver Privacy White Paper, 2015

권영준・이동진, “개인정보 유출에 대한 과실 및 손해 판단기준”, 개인정보 보호의 법과 정책, 박영사, 2014

김상미, “일본의 개인정보보호 법제”, KISO저널 제7호, 2012(http://journal.kiso.or.kr/?p=608)

김진환, “개인정보 보호법의 해석 원칙을 위한 제언(提言)과 시론(試論): 개인정보에 대한 정의 규정의 해석을 중심으로”, 법학평론 제3권, 2012

———, “개인정보보호의 규범적 의의와 한계-사법 영역에서의 두 가지 주요 쟁점을 중심으로”, 저스티스 통권 제144호(2014.10), 한국법학원

문재완, “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 한국공법학회, 2014
박경신, “사생활의 비밀의 절차적 보호규범으로서의 개인정보보호법리”, 공법연구 제40집 제1호, 한국공법학회, 2011
———, “개인정보의 정의와 위치정보보호법의 개선 방안 - 익명위치정보, 허가제 및 즉시동의요건을 중심으로”, 법학연구제37집, 전북대학교 법학연구소, 2012
박상철, “행태기반서비스(위치기반서비스 포함) 관련 법령 정비 방안”, 개인정보보호법제 개선을 위한 정책연구보고서, 프라이버시 정책 연구포럼, 2013
박유영, 개인정보 보호범위에 관한 헌법적 연구-민간부문에서의 개인정보 보호범위를 중심으로, 서울대학교 법학석사학위논문, 2015
박준석, “저작재산권법에서 바라본 개인정보 보호”, 개인정보보호의 법과 정책, 박영사, 2014
박혁수, 빅데이터 시대에 개인정보 개념의 재검토, Law & Technology 제10권 제1호(2014)
윤주희 등, 개인정보보호위원회, 개인정보의 범위에 관한 연구, 2014
이대희, “개인정보 개념의 해석 및 범위에 관한 연구”, 고려법학 제79호, 2015
이인호, “「개인정보 보호법」상의 ‘개인정보’ 개념에 대한 해석론”, 정보법학 제19권 제1호, 2015
이창민, 개인정보자기결정권 연구-개인정보처리의 자유와의 충돌 해결을 중심으로-, 서울대학교 법학석사논문, 2009
임규철, “개인정보의 보호범위”, 한독법학 제17호, 2012
장주봉, “개인정보의 의미와 보호범위”, 법학평론 제3권, 2012
———, “개인정보의 의미와 규제범위”, 개인정보보호의 법과 정책, 박영사, 2014
전응준, “위치정보법의 규제 및 개선방안에 관한 연구”, 정보법학 제18권 제1호, 2014
정상조 外, 비식별개인정보의 보호 및 활용에 관한 연구, 방송통신위원회

연구결과 보고서, 2010
정상조, “위치기반서비스 규제에 관한 연구”, 2015 Naver Privacy White Paper, 2015
정신교, “형법상 허용된 위험의 체계적 지위”, 법학연구 제28집, 한국법학회, 2007
정태호, “현행 인구주택총조사의 위헌성-독일의 인구조사판결(BVerGE65, 1)의 법리분석과 우리의 관련법제에 대한 반성-”, 법률행정논총 제12집, 2000
주민철, 개인정보보호조치 위반의 형사적 책임, 서울대학교 석사학위논문, 2015
채성희, “검색엔진에 대한 자기정보삭제권 행사의 범위와 한계-유럽사법재판소의 이른바 ‘잊혀질 권리’ 판결을 중심으로”, LAW & TECHNOLOGY 제10권 제4호, 2014
———, “목적외 이용과 프로파일링 관련 규제에 관한 비교법적 검토 - EU 개인정보보호지침, 규칙안, 정보통신망법 및 개인정보보호법을 중심으로”, LAW & TECHNOLOGY 제12권 제1호, 2016
한은영, “일본 개인정보보호법 개정의 배경 및 개정안의 주요 내용”, 정보통신방송정책 제26권 13호(2014)
함인선, “개인정보 처리와 관련한 법적 문제-우리나라 「개인정보 보호법」과 EU의 ‘2012년 규칙안’을 중심으로 하여-”, 경제규제와 법 제6권 제1호, 2013

외국 논문

Breyer, Personenbezug von IP-Adressen Internetnutzung und Datenschutz, ZD(2014)
Bergt, Die Bestimmtbarkeit als Grundproblem des Datenschutzrechts-Überblick über den Theorienstreit und Lösungsvorschlag”, ZD(2015)
——, BGH: Speicherung von IP-Adressen durch die Bundesrepublik

Beschluss vom 28.10.2014, ZD(2015)

Brink/Eckhardt, *Wann ist ein Datum ein personenbezogenes Datum?,* ZD(2015)

Cavoukian, Ann and Khaled El Emam. De-identification Protocols: Essential for Protection Privacy, Information and Privacy Commissioner of Ontario, 2014

Church, Peter. "EU-What is personal data? Just the facts..." , Linklaters Technology Media And Telecommunication Newsletter, December 2014, from http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-8-December-2014/Pages/EU-What-is-personal-data.aspx

Cumbley, Richard and Peter Church, "EU-What is personal data?" , Linklaters Technology Media And Telecommunication Newsletter, October 2008, from http://www.linklaters.com/Insights/Publication1403Newsletter/PublicationIssue20081001/Pages/PublicationIssueItem3513.aspx

Damien Welfare, "Clarifying the scope of personal data" , Privacy & Data Protection, 2012, 12(7)

Eneken Tikk, "IP addressed subject to personal data regulation" , International CyberSecurity Legal and Policy Proceedings, Eneken Tikk and Anna-Maria Talihärm, NATO Cooperative Cyber Defence Centre of Excellence, 2010

Forgó & Krügel, *Der Personenbezug von Geodaten - Cui bono, wenn alles bestimmbar ist?*, MMR(2010)

Garfinkel, "De-identification of Personally Identifiable Information" , National Institute of Standards and Technology, 2015

Härting, *Anonymität und Pseudonymität im Datenschutzrecht*, NJW(2013)

Karg, *IP-Adressen sind personenbezogene Verkehrsdatedn*, MMR-Aktuell(2011)

Kirchberg-Lennartz/Jürgen Weber, "Ist die IP-Adresse ein

personenbezogenes Datum?", DuD 7/2010

Kristof van Quathem, "Controlling Personal Data-The Case of Clinical Trials", Covington & Burling, 2009, from https://www.cov.com/~/media/files/corporate/publications/2005/10/oid64167.ashx

Krüger/Maucher, "Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit grossen Auswirkungen auf die Praxis", MMR(2011)

Kuan Hon, 'Personal Data' in the UK, Anonymization and Encryption, from http://www.cloudlegal.ccls.qmul.ac.uk/Research/49700.html

Patrik Lundevall-Unger/Tommy Tranvik, "Was sind personenbezogene Daten? Die Kontroverse um IP-Adressen", ZD-Aktuell 2012, 03004

Meglena Kuneva, Keynote Speech in Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 2009

Meyerdirks, "Sind IP-Adressen personenbezogene Daten?", MMR, 2009, 8

Pahlen-Brandt, *Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um "Personenbezogene Daten"*, DuD(2008), vol.1

Renzo Marchini, "The UK Guidance on 'Persona Data': How it relates to *Durant*", Data Protection Law & Policy, November 2007

Specht/Müller-Riemenschneider, *Dynamische IP-Adressen: PErsonbezogene Daten für den Webseitenbetreiber? Aktueller Stand der Diskussion um den Personenbezug*, ZD(2014), 71

Schwarz, Paul and Daniel Solove, THE PII PROBLEM: PRIVACY AND A NEW CONCEPT OF PERSONALLY IDENTIFIABLE INFORMATION, 86 N.Y.U.L. Rev. 1814 2011

Weichert, Der Personenbezug von Geodaten, DuD(2007)

————, *Geodaten-datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen*, DuD(2009)

森亮二, "パーソナルデータの匿名化をめぐる議論（技術検討ワーキンググ

ループ報告書）"，ジュリスト 、2014年 3月(No.1464), 有斐閣
———，“実務解説　平成27年改正個人情報保護法　第2回　個人情報の定義"，NBL No.1061(2015.11.1.), 商事法務
宇賀克也，　“個人情報・匿名加工情報・個人情報取扱事業者”，　ジュリスト 、2016年 2月(No.1489), 有斐閣
宇賀克也 外 5, 座談會，“個人情報保護法・マイナンバー法改正の意義と課題”，ジュリスト 、2016年 2月(No.1489), 有斐閣
小向太郎，　“ライフログの利活用と法律問題"，ジュリスト 、2014年　3月(No.1464), 有斐閣
鈴木正朝，“個人情報保護法のグローバル化への対応”，ジュリスト 、2016年 2月(No.1489), 有斐閣

정부, 규제기관 보고서, 가이드라인 등

방송통신위원회・한국인터넷진흥원, 위치정보의 보호 및 이용 등에 관한 법률 해설서, 2010
———————————————，정보통신서비스 제공자를 위한 개인정보보호 가이드, 2012
행정안전부, 개인정보 보호법령 및 지침・고시 해설, 2011
행정자치부 외, “개인정보 비식별 조치 가이드라인 - 비식별 조치 기준 및 지원•관리체계 안내-“, 2016
Article 29 Data Protection Working Party, Working Document Privacy on the Internet - An integrated EU approach to On-line Data Protection-(WP37), 2000
———————————————, Opinion 4/2007 on the concept of personal data(WP136), 2007
———————————————, Opinion 1/2008 on Data Protection Issues related to Search Engines(WP 148), 2008
———————————————, Opinion 03/2013 on purpose limitation(WP203), 2013

———————————————, Opinion 05/2014 on Anonymisation Techniques, 2014

———————————————, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014

Arbeitskreis Medien, *Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten*

Der Düsseldorfer Kreis, B*eschuluss des Düsseldorfer Kreises vom 27 Nov. 2009: Datenschutzkonforme Ausgestaltung von Analyseverfaren zur Reichweitenmessung bei Internet-Angeboten*

Information Commissioner's Office, Determining what is personal data, version 1.1(2012)

———————————————, Data Protection Good Practice Note, Collecting personal information using websites, 20 June 2007

———————————————, Anonymisation: managing data protection risk code of practice, 2012

高度情報通信ネットワーク社会推進戦略本部、パーソナルデータの利活用に関する制度改正大綱, 2015

経済産業省, 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン, 2014

経済産業省, 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」に関するQ&A, 2014

利用者視点を踏まえたICTサービスに係る諸問題に関する研究会、第２次提言, 2010

衆議院 内閣委員會 第4号 平成 27年 5月 8日 会議録

Abstract

On the concept of personal information: comparative study of European, Japanese and Korean law

The key concept of data protection law is personal information. In Korea, personal information is defined as “any information relating to a living natural person (such as individual customers of a company) from which the individual can be identified through one’s name, resident registration number, visual image and so on (including any information which, if combined with other information, can make a specific individual identifiable)”.

In Korean, there is no consensus upon the interpretation of the concept of personal information. Particularly, there has been a continuing controversy surrounding i) the meaning of “identifiability” and ii) the treatment of the transfer of key-coded or pseudonymised data.

In this thesis, the laws, legal precedents, the statements of the regulators and the academic discussions regarding these issues in European Union, Germany, United Kingdom, Japan and Korea were comprehensively reviewed and based on the result thereof, a systematic interpretation of Korean data protection laws was conducted. These are the conclusions of this thesis:

1) Under Korean law, the identifiability of certain information should be determined from the perspective of those who process the information.

2) The transfer of key-coded data of which the key a data controller (the transferring party) retains should be considered as the transfer of personal information even in case the receiving party is not able to identify a personal from the transferred data. However, such transfer could be legitimised if the requirements provided in the subparagraphs of Article 18-② of the Personal Information Protection Act are met. In this regard, the requirement of Article 18-②-4 will be especially relevant, which sets forth that a transfer of personal information can be legitimized without any additional legal basis(e.g. consent of data subjects) provided that the personal information to be transferred is de-identified and that the purpose of such transfer is statistical, academical or the like.

Keywords: The concept of personal information, personal data, identifiability, de-identification, anonymisation, pseudonymisation, data protection, Korea

Student Number: 2013-23342