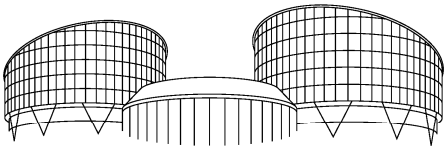

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

유럽인권협약재판소

유럽인권협약
주제별 해설서

데이터 보호

2025 년 8 월 31 일 개정

헌법재판소
Constitutional Court of Korea

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

이 문서의 전부 또는 일부를 인쇄물 또는 전자 출판물의 형태로 번역 또는 복제하고자 하는 출판사나 단체는 *번역본 복제 또는 재출판 요청* 문의 양식을 작성하여 승인 절차에 관한 정보를 문의하시기 바랍니다.

현재 판례 해설서가 어느 언어로 번역되고 있는지 살펴보고자 하는 경우 홈페이지에서 '*진행 중인 번역(pending translations)*'을 확인하시기 바랍니다.

이 해설서는 원래 프랑스어로 작성되었습니다. 이 해설서는 정기적으로 개정되며 가장 최근에는 2025 년 8 월 31 일에 개정되었습니다. 이 해설서는 편집을 위해 수정될 수 있습니다.

판례 해설서는 *https://ks.echr.coe.int* 에서 다운로드할 수 있습니다. 해설서 개정 관련 정보는 유럽인권재판소의 X 계정 *https://twitter.com/ECHR_CEDH*에서 확인할 수 있습니다.

목차

일러두기

이 해설서는 유럽인권재판소(이하 “재판소”, “유럽재판소” 또는 “스트라스부르 재판소”)가 선고한 주요 판결과 결정에 관한 정보를 법실무에 종사하는 사람들에게 제공하기 위해 재판소가 발간하고 있는 유럽인권협약해설서 시리즈 중 하나입니다. 그 시리즈 중 이 해설서는 유럽인권협약(이하 “협약” 또는 “유럽협약”)의 여러 조항에 따라 데이터 보호와 관련된 판례를 분석하고 요약한 것입니다. 조문별 판례 해설서와 유기적으로 연결되어 있으므로 함께 참고해야 합니다.

인용된 판례는 리딩케이스이거나 중요한 의미가 있는 것, 그리고 최근의 판결과 결정 중에서 선별한 것입니다.*

재판소는 판결과 결정을 통해 제소된 개별사건 판단할 뿐만 아니라, 보다 일반적으로 협약상의 원칙을 명확히 밝히고 보장하며 발전시킴으로써, 각국이 협약당사국으로서의 이행사항을 준수하도록 합니다(*Ireland v. the United Kingdom*, 1978 년 1 월 18 일, § 154, Series A no. 25, 및 더 최근의 사건으로는, *Jeronovičs v. Latvia* [GC], no. 44898/10, § 109, 2016 년 7 월 5 일).

유럽인권협약 체제를 설립한 목적은 이처럼 일반의 이익에 관련된 공공정책의 여러 문제를 판단함으로써, 협약당사국들 전체의 인권보호 수준을 높이고 인권법제를 확충하는 것입니다(*Konstantin Markin v. Russia* [GC], 30078/06, § 89, ECHR 2012). 실제로, 재판소는 유럽인권협약이 인권 분야에서 “유럽의 공공질서에 대한 헌법적 문서”의 역할을 하고 있음을 강조해 왔습니다(*Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, § 156, ECHR 2005-VI, 더 최근 사건인 *N.D. and N.T. v. Spain* [GC], nos. 8675/15 및 8697/15, § 110, 2020 년 2 월 13 일).

최근 유럽인권협약 제 15 의정서는 협약 전문에 보충성의 원칙을 추가하였습니다. 이 원칙은 인권보호와 관련하여 “당사국과 재판소 간에 공동의 책임을 부과”하며, 국가 당국과 법원은 유럽인권협약과 그 의정서에 정의된 권리와 자유에 완전한 효력을 부여하는 방식으로 국내법을 해석하고 적용해야 합니다(*Grzęda v. Poland* [GC], § 324).

---

* 인용된 판례는 재판소와 유럽인권위원회(European Commission of Human Rights)의 공식 언어(영어 및 프랑스어) 중 하나 또는 두 언어 모두로 작성되었을 수 있습니다. 특별한 표시가 없는 한, 모든 인용문은 소재판부(Chamber)가 선고한 본안판결(judgment on the merits)에 대한 것입니다. 약칭 “(dec.)”은 재판소의 결정에서 인용하는 것을 의미하고, “[GC]”는 해당 사건이 대재판부(Grand Chamber)에서 심리된 것임을 나타냅니다. 소재판부의 판결은 있지만 이 개정판 발간 당시 최종적인 것이 아닌 때에는 별표(*)로 표시되어 있습니다.

서문

1. 기술 진보로 감시, 감청, 데이터 보유 능력이 비약적으로 발전하게 되자 개인데이터 보호 영역은 거대한 난관에 부딪히게 되었다. 공공기관이 한 사람의 개인데이터를 저장·보관하는 문제는 1987 년 *Leander v. Sweden* 사건 판결에서 "구(舊)" 재판소가 최초로 분석한 이래, 여러 협약 기구에서 다양한 판례를 내놓으며 상당한 발전이 있었다.

2. 재판소는 이 문제와 관련된 쟁점을 제기하는 다양한 사안을 수년간 심리하였다. 이제는 개인데이터를 수집, 저장, 이용, 유포하는 등의 광범위한 운용 행위 관한 다양한 판례를 여러 협약기구에서 찾아볼 수 있다. 이 해설서는 이러한 판례를 소개한다. 정보통신기술이 급격히 발전하자 판례도 그에 맞게 발전하였다.

I. 데이터 보호의 기본 개념과 원칙

3. 개인데이터 보호권은 협약에 규정된 여러 권리와 자유처럼 독자적인 권리는 아니다. 그러나 재판소는 협약 제 8 조가 보장하는 사생활과 가족생활, 주거 및 통신을 존중받을 권리를 향유하려면 개인데이터 보호가 본질적으로 중요하다는 점을 인정하였다(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 137; *Z v. Finland*, 1997, § 95; *L.B. v. Hungary* [GC], 2023, § 103). 협약 체계에서 개인데이터는 주로 제 8 조가 보호하지만, 보호와 관련되어 고려할 사항은 협약 및 협약 의정서의 다른 여러 조항에서도 고려해야 한다.

A. 데이터 보호 용어

4. 기술 발전으로 개인데이터 관련 운용 과정에서 "자동처리"될 수 있는 유형이 늘어나게 되었다. 재판소는 "사생활(private life)" 개념을 폭넓게 정의하는 방식으로 사회 발전에 맞게 판례를 발전시켰지만, 어떤 특정한 데이터처리 운용 행위가 무조건 제 8 조의 적용 범위에 속한다거나 제 8 조가 보호하는 이익을 침해한다고 볼 수는 없다.

1. 개인데이터의 개념과 범위

5. 재판소가 판결에서 "개인데이터(personal data)" 개념을 설명하기 위해 참조하는 유럽평의회 개인데이터 자동처리에 따른 개인의 보호를 위한 협약 제 108 호("*협약 108*")는 1981 년 1 월 28 일 채택되어 1985 년 발효 후 2018 년에 개정되었고, 그 목적은 "각 당사국

영역 내 모든 개인을 대상으로 ... 개인별로 관련된 개인데이터 자동처리에 따른 권리, 기본적인 자유 및 특히 사생활의 비밀권이 존중되도록 보장하는 것"(제 1 조)이다(*Amann v. Switzerland* [GC], 2000, § 65; *Haralambie v. Romania*, 2009, § 77). 재판소는 *협약 108* 제 2 조에 따라, 개인데이터 개념은 "신원이 확인되었거나 확인할 수 있는 개인에 관한 모든 정보"로 정의된다는 점을 분명히 밝혔다(*Amann v. Switzerland* [GC], 2000, § 65; *Haralambie v. Romania,* 2009, § 77).

6. 이러한 데이터에는 개인("데이터 주체")을 곧바로 알아볼 수 있는 정보인 성과 이름뿐만 아니라(*Guillot v. France*, 1996, §§ 21–22; *Mentzen v. Latvia* (dec.), 2004; *Güzel Erdagöz v. Turkey*, 2008, § 43; *Garnaga v. Ukraine*, 2013, § 36; *Henry Kismoun v. France,* 2013, § 25; *Hájovský v. Slovakia*, 2021, §§ 11–12 및 41), 동적 IP(인터넷 프로토콜) 주소처럼 개인을 간접적으로 알아볼 수 있는 요소도 모두 포함된다(*Benedik v. Slovenia*, 2018, §§ 107–108; 또한, VPN 으로 가린 IP 주소와 관련하여, *Le Marrec v. France* (dec.), 2024, §§ 51 및 54 참조).

7. 개인데이터 보호 문제는 주로 개인의 제 8 조상 사생활 존중권과 관련된 것으로 보이지만, 법인체라면 "통신"이나 "주거" 존중권을 침해하는 조치로 인한 영향을 직접 받는 경우 재판소에서 이 권리에 의거할 수 있다. 예컨대 한 회사가 다른 여러 회사와 공유하는 서버에 있는 모든 데이터 사본을 제출하라는 명령을 받은 사건(*Bernh Larsen Holding AS and Others v. Norway*, 2013, § 106) 및 국방부가 영장을 근거로 시민의 자유 관련 비정부기구의 통신을 감청한 사건(*Liberty and Others v. the United Kingdom*, 2008, §§ 56–57)이 이에 해당한다. 다만, 종교 단체 구성원의 개인데이터 보호와 "사생활" 존중 관련 조치에 관한 사건에서는, 해당 단체가 직접적인 영향을 받지 않았으므로 협약 제 34 조가 의미하는 "피해자"가 아니었다(*Avilkina and Others v. Russia*, 2013, § 59).

8. 개인데이터의 형태는 매우 다양할 수 있다. 그 예는 다음과 같다.

- 특정 시점에 부여된 구체적인 동적 IP 주소에 연계된 인터넷 가입자 정보(*Benedik v. Slovenia*, 2018, §§ 108–109)로, 청구인의 신원 확인과 위치 파악이 가능한 경우, VPN 으로 가린 IP 주소 역시 포함(*Le Marrec v. France* (dec.), 2024, § 54)
- 음성 표본으로 사용하기 위해 녹음된 자료로서, 영구적 성격을 지니며 다른 개인데이터 맥락에서 개인 신원 확인과 직접적으로 관련된 분석 과정의 대상이 되는 경우(*P.G. and J.H. v. the United Kingdom*, 2001, § 59)
- 세포 검체와 DNA 프로필(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 70–77) 또는 지문(*ibid.*, § 84)으로, 객관적이고 반박할 수 없는 성격인 데다,

당해 개인의 고유 정보가 담겨 있어 광범위한 상황에서 적확하게 신원을 파악할 수 있게 하는 경우(*ibid.*, § 85)

- 특정 개인에 관하여 은행 문서에서 얻은 정보(민감한 세부 사항 또는 직업 활동 관련 사항 포함)(*M.N. and Others v. San Marino*, 2015, §§ 51 이하) 또는 납세자 정보 서비스 데이터베이스에서 얻은 정보로 특히 소득과 순자산 내역, 세무 당국에 계류 중인 사건 관련 내역 등을 포함(*Casarini v. Italy* (dec.), 2024, §§ 56-57).
- 경찰이 수집·보관한, 신원이 확인되었거나 확인할 수 있는 개인의 직업에 관한 데이터(*Khelili v. Switzerland*, 2011, § 56)
- 직장에서 직원의 인터넷 및 메신저(야후) 사용과 관련하여 감시를 통해 얻은 데이터(*Bărbulescu v. Romania* [GC], 2017, § 18, §§ 74-81)
- 법률 사무소에서 압수된 전자 데이터 사본으로서, 해독·전사되거나 소유자에게 공식적으로 귀속되지 않았더라도 해당하는 경우(*Kırdök and Others v. Turkey*, 2019, § 36)
- 대학교에서 감추지 않고 실시한 비디오 감시 맥락에서 수집된 데이터(*Antovic and Mirkovic v. Montenegro*, 2017, §§ 44-45)
- 다수 개인의 과세소득 및 자산에 관한 정보로서, 일정 조건을 갖추면 대중이 접근할 수 있었던 데이터도 해당(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 138)
- 개인의 출생과 유기(遺棄)에 관한 데이터로, 개인의 신원에서 중요한 부분에 관한 진실을 알려면 필요한 정보 포함(*Gaskin v. the United Kingdom*, 1989, § 39; *Mikulić v. Croatia*, 2002, §§ 54-64; *Odièvre v. France* [GC], 2003, §§ 28-29; *Gauvin-Fournis and Silliau v. France*, 2023, §§ 106 및 112; *Cherrier v. France*, 2024, § 50)
- 이혼 합의서에 포함된 데이터로서, 부부 재산 분할, 미성년 자녀의 양육권과 거주지, 위자료 합의, 청구인의 자산/소득 현황에 관한 세목을 포함하는 경우(*Liebscher v. Austria*, 2021, §§ 31 및 68)
- 업무상으로 개인이 비밀 카메라를 사용해 대화를 촬영한 영상으로서, 이후 형사절차에서 청구인에게 불리한 증거로 사용된 경우(*Sârbu v. Romania*, 2023, §§ 39-41)

9. *협약 108* 제 2 조에 따라, "데이터처리(data processing)"에는 "개인데이터를 대상으로 한 모든 운용 또는 운용의 집합으로서, 개인데이터의 수집, 저장, 보존, 변경, 검색, 공개,

제공, 삭제, 파기 또는 논리적 및/또는 산술적 연산 운용"이 포함된다. 기술 발전으로 처리에 해당할 수 있는 개인데이터 관련 운용 유형이 늘어났고, 재판소에서 확인한 전형적인 사례는 다음과 같다.

- 경찰이 인터넷 제공업체로부터 개인의 구체적인 동적 IP 주소에 연계된 가입자 정보를 수집한 경우(*Benedik v. Slovenia*, 2018, §§ 108–109)
- 개인의 정치 활동 등에 관한 공적 정보를 수집·보관한 사실(*Rotaru v. Romania* [GC], 2000, §§ 43–44; *Association "21 December 1989" and Others v. Romania*, 2011, §§ 167–168; *Amann v. Switzerland* [GC], 2000, §§ 65–67; *Catt v. the United Kingdom*, 2019, § 93).
- 개인을 유관 부처 내부 사법 데이터베이스에 올린 경우(*L.F. v. France* (dec.), 2024, § 30), 성범죄자 국가 사법 데이터베이스에 올린 경우(*Gardel v. France*, 2009, § 58) 또는 개인을 대상으로 제기된 모든 형사절차를 기록한 국가 데이터베이스에 올린 경우(*N.F. and Others v. Russia*, 2023, §§ 34 및 49) 및 피의자 지문을 수집·저장한 경우(*M.K. v. France*, 2013, § 29)
- 경찰서에서 개인의 음성 표본을 은밀히 녹음하여 영구 저장한 후 다른 개인데이터와 연계된 분석 과정에서 당해 개인의 신원 확인에 사용한 경우(*P.G. and J.H. v. the United Kingdom*, 2001, §§ 59–60)
- 보안 목적으로 설치한 노출된 카메라로 경찰 조사실에서 개인을 촬영하고, 그 영상을 영구 녹화 후 추후 사용할 편집물에 포함시킨 경우(*Perry v. the United Kingdom*, 2003, § 41)
- 대상자의 소재와 공개된 행방을 나타내는 GPS 점검·확인 데이터를 체계적으로 수집·보유한 경우(*Uzun v. Germany*, 2010, §§ 49–53)
- 당사자 동의 없이 촬영된 유명인의 사진을 첨부한 기사를 잡지에 게재한 경우(*Von Hannover v. Germany (no. 2)* [GC], 2012, §§ 95–99)
- 공공장소에서 자살을 시도하는 개인을 촬영한 CCTV 영상을 녹화한 뒤 언론에 공개한 경우(*Peck v. the United Kingdom*, 2003, §§ 59–63)
- 경찰이 개인의 직업을 추정하여 데이터를 기록·보관한 경우(*Khelili v. Switzerland*, 2011, § 56)
- 정신병원이 환자의 사생활 관련 고도로 민감한 비밀 정보를 언론에 공개한 경우(*Mockutė v. Lithuania*, 2018, § 99)

- 국가가 스포츠 도핑방지 조치의 일환으로, 주말 포함 엘리트 운동선수들의 소재와 일상 생활에 관한 정보를 수집한 경우(*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, 2018, §§ 155-159)
- 수용자(收容者)의 사적 서신(수발신 모두)을 체계적으로 스캔하여 국가 사법망 서버에 올린 경우(*Nuh Uzun and Others v. Turkey*, 2022, §§ 80-82)
- 텔레그램 채널에 게시된 사진·영상을 바탕으로, 사전 신고 없이 1 인 시위를 한 청구인을 안면인식기술로 신원 확인한 뒤, 지하철 이동 도중 위치를 추적하여 체포한 경우(*Glukhin v. Russia*, 2023, § 73)

10. 재판소는 이러한 여러 조치를 거의 대부분 데이터 주체의 사생활, 주거 또는 통신 존중권에 대한 제한으로 간주하며, 그 심각성의 정도는 사안에 따라 달리 평가한다.

11. 다만, 개인데이터 운용이라고 해서 모두 제 8 조의 적용 범위에 속하거나 해당 권리를 자동으로 제한하는 것은 아니다. 예컨대 *Mehmedovic v. Switzerland* (dec.), 2018 사건 § 18 에서 재판소는, 청구인에 관한 몇 안 되는 정보가 우연히 수집되었고 문제 된 수사와 무관하여 어떠한 방식으로도 체계적이거나 지속적인 데이터 수집을 구성하지 않았으므로 청구인의 사생활 존중권을 제한하지 않았다고 보았다. 또한 *Cakicisoy and Others v. Cyprus* (dec.), 2014 사건 §§ 50-52 에서 당국이 유해가 청구인들의 사망한 친족인지 확인하는 발굴 프로그램에서 DNA 프로필을 추출할 목적으로 혈액 검체를 채취하였고 동의서 기한이 만료되자 검체를 폐기한 사실은 청구인들의 사생활 존중권에 대한 제한이 아니라고 보았다.

12. 재판소의 판례에 따르면, 개인을 특정하여 정보를 수집한 경우(*Amann v. Switzerland* [GC], 2000, §§ 66-67; *Rotaru v. Romania* [GC], 2000, §§ 43-44), 문제 된 데이터가 체계적이거나 지속적으로 기록된 경우(*Uzun v. Germany*, 2010, § 51), 그 데이터를 다른 개인데이터와 연계하여 개인의 신원 파악을 직접적으로 의도한 분석 과정에 활용한 경우(*P.G. and J.H. v. the United Kingdom*, 2001, § 57) 또는 그 데이터가 데이터 주체의 합리적인 예상 범위를 넘어 공개된 경우(*Peck v. the United Kingdom*, 2003, §§ 58-59; *Perry v. the United Kingdom*, 2003, § 38) 이러한 개인데이터 운용 행위는 제 8 조의 적용 범위에 속한다. 그 외에도 개인에 관한 정보가 기록·보관된 구체적인 맥락, 기록의 성격, 기록물이 사용·처리되는 방식, 도출될 수 있는 결과물 등을 고려해야 한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 67).

13. 개인이 사생활 보호를 합리적으로 기대할 수 있는지는 결정적인 정도까지는 아니더라도 그만큼 중요하게 고려해야 할 사항이다(*Perry v. the United Kingdom*, 2003, § 37; *Bărbulescu v. Romania* [GC], 2017, § 80; *Glukhin v. Russia*, 2023, § 66). 온라인

활동에서는, 평가 시 핵심 요소는 개인정보의 익명성으로, 인터넷 서비스 제공업체에 가입한 자가 동적 IP 주소를 숨기지 않았다는 사실은 사생활의 비밀성 관련 기대가 객관적으로 보아 합리적이었는지 평가할 때 결정적인 요소가 아니었다(*Benedik v. Slovenia*, 2018, § 116). 직장 내에서는, 고용주가 지시한다고 해서 직장 내 사적인 사회적 교류를 완전히 없앨 수는 없다. 사생활과 통신의 비밀은 제한이 필요한 범위 내에서는 제약될 수 있다고 하더라도 존중되어야 한다(*Bărbulescu v. Romania* [GC], 2017, §§ 80–81; 또한, 업무 맥락인 경우, *Sârbu v. Romania*, 2023, §§ 37–38 참조; 또한, 정당이 당원의 전자통신을 점검·확인한 맥락인 경우, *Tena Arregui v. Spain*, 2024, § 38 참조). 공공장소에서 감시 수단으로 개인의 행위나 이동을 점검·확인하는 경우, 그러한 개인데이터를 체계적·지속적으로 기록하기 시작하는 순간 제 8 조의 적용 범위에 속할 수 있고(*Glukhin v. Russia*, 2023, § 66), 공개하는 방식이나 범위가 개인이 합리적으로 예상할 수 있는 범위를 벗어나는 경우에도 제 8 조의 적용 대상이 된다(*Peck v. the United Kingdom*, 2003, § 62; *Perry v. the United Kingdom*, 2003, §§ 41–43). 한편, 드라마 배우가 체포된 사진을 첨부한 언론 기사와 관련하여 재판소는 배우가 여러 차례 인터뷰로 사생활의 세부 사항을 스스로 공개하는 방식으로 " 적극적으로 주목을 받으려고"한 사실 때문에 사생활이 실효적으로 보호될 것이라는 "정당한 기대"는 약화되었다고 판단하였다(*Axel Springer AG v. Germany* [GC], 2012, § 101).

14. 수집된 데이터의 성격과 관련하여, 어떤 유형의 개인데이터와 특정한 처리 방식은 개인의 행위·의견·감정에 관한 좀 더 민감한 정보를 공개하기 때문에 다른 것보다 더 문제가 될 수 있다(재판소가 GPS 로 수집된 데이터를 영상·음성 감시장치로 수집된 데이터와 비교한 *Uzun v. Germany*, 2010, § 52). 개인의 건강 등에 관한 대단히 내밀하거나 민감한 데이터를 데이터 주체의 동의 없이 저장·공개하는 경우는 당연히 제 8 조의 적용 범위에 속한다(*Z v. Finland*, 1997, § 71; *Radu v. Republic of Moldova*, 2014, § 27; *Mockutė v. Lithuania*, 2018, §§ 93–95). 세포 표본에 포함된 개인정보의 성격과 양을 고려할 때, 비록 그 정보의 일부만 당국이 실제로 추출·사용하거나 즉각적인 불이익이 발생하지 않더라도, 보유 그 자체가 당해 개인의 사생활 존중권 제한으로 간주되어야 한다(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 70–77).

15. 이미 공적 영역에 있거나 대중이 접근할 수 있는 개인데이터라도 반드시 제 8 조의 보호 범위에서 제외되는 것은 아니다(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 134; *L.B. v. Hungary* [GC], 2023, § 104). 공적 성격의 데이터라 하더라도 체계적으로 수집·보관된 데이터는 개인의 "사생활"에 속할 수 있고(*P.G. and J.H. v. the United Kingdom*, 2001, § 57; *Peck v. the United Kingdom*, 2003, §§ 58–59; *Perry v. the United Kingdom*, 2003, § 38), 이때 비밀 감시 수단이 사용되지 않았더라도

마찬가지이다(*Rotaru v. Romania* [GC], 2000, §§ 43-44; *Antovic and Mirkovic v. Montenegro*, 2017, §§ 44-45). 협약 제 8 조는 일종의 정보 자기결정권을 보장하여, 설령 중립적인 데이터일지라도 집합적으로 수집·처리·유포되고 그 형식이나 방식 때문에 제 8 조상 권리가 문제가 될 수 있는 경우라면, 개인은 사생활 존중권에 의거할 수 있다(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 137; *L.B. v. Hungary* [GC], 2023, § 103).

16. 당국의 데이터 주체 수사 또는 국내 법원 사법절차에서 증거 수집이 개인데이터 처리의 목적인 대부분의 경우, 재판소는 데이터처리가 제 8 조의 적용 범위에 속하고 해당 개인의 사생활 존중권을 제한하는 결과를 초래했다고 판단하였다(*Perry v. the United Kingdom*, 2003, §§ 39-43; *Uzun v. Germany*, 2010, §§ 51-52; *Vukota-Bojić v. Switzerland*, 2016, §§ 57-59; *López Ribalda and Others v. Spain* [GC], 2019, § 94; *Sârbu v. Romania*, 2023, §§ 38 및 41; 이와 대조하여, 당국에 자발적으로 제출되었거나 과거 체포와 관련하여 경찰이 촬영한 사진을 청구인의 신원을 파악할 목적으로 경찰이 이용한 *Lupker and Others v. the Netherlands*, 1992; 집회 도중 당국이 청구인들의 교통 법규 위반 수사를 개시할 목적으로 촬영한 사진에 관한 *Friedl v. Austria*, 1994, §§ 50-51).

17. 마지막으로, 제 8 조가 적용되려면 개인데이터처리 결과가 일정한 수준의 심각성에 도달하고, 사생활 존중권 향유에 불이익을 야기하는 방식이어야 한다(*M.L. and W.W. v. Germany*, 2018, § 88). *Vučina v. Croatia* (dec.) 2019 사건 § 50 에서, 재판소는 여성 잡지에 청구인의 사진을 다른 사람으로 잘못 지칭한 제목을 달아 게재한 사안에 관한 청구를 물적 관할권에 부합하지 않는다는 이유로 각하하였다. 재판소의 견해에 따르면, 오류의 심각성 정도가 낮고 야기된 불편도 매우 제한적이라서 제 8 조를 적용할 만하지 않았다.

2. 데이터의 구체적인 범주

18. 재판소의 견해에 따르면, 정보가 대단히 내밀하거나 민감하다면 보호를 강화하는 것은 의심의 여지 없이 정당하다. 그 외 다른 범주에 속하는 데이터라도 기술 발전으로 접근 가능성이 확대되고 상호운용성이 커지고 있으므로 주의 깊게 다루어야 한다.

a. 이른바 "민감한" 범주

19. *협약 108* 제 6 조에 따르면, 인종 출신, 정치적 견해, 종교적·기타 신념을 드러내는 개인데이터와 개인의 건강이나 성생활 또는 범죄 유죄 판결에 관한 정보는 국내법이 적절한 보호조치를 규정하지 않는 한 자동으로 처리될 수 없다. 재판소가 "민감"하다고 묘사하는 이 범주의 정보는 보호 수준을 강화해야 한다.

i. 인종 또는 민족 출신을 드러내는 데이터

20. 개인의 민족적 정체성은 사생활의 중요한 요소로 간주되어야 한다(*S. and Marper v. the United Kingdom*, [GC], 2008, § 66; *Ciubotaru v. Moldova*, 2010, § 49). 특히 유전학과 정보기술 분야의 급속한 발전을 고려한다면, 데이터가 개인의 민족·기타 출신을 드러낼 수 있을 경우 특별히 우려하지 않을 수 없다(*S. and Marper v. the United Kingdom* [GC], 2008, § 71). 검체와 DNA 프로필에는 다량의 민감한 정보가 들어 있고, 당국은 이를 통해 개인 간 유전적 관계를 규명하고 민족 출신을 추정할 수 있다(*ibid.*, §§ 72–77; *Aycaguer v. France,* 2017, § 33). 개인의 민족 출신을 공식 등록부에 기록한 사건에서, 재판소는 그러한 데이터 기록이 고도로 민감하다는 점을 강조하면서, 데이터 주체가 객관적으로 검증 가능한 증거를 근거로 기록된 자신의 민족성을 변경하는 절차를 마련할 국가의 적극적 의무가 존재한다고 인정하였다(*Ciubotaru v. Moldova*, 2010, §§ 52–59).

ii. 정치적 견해 및 종교적·기타 신념(철학적 신념 포함)을 드러내는 데이터

21. 정치적 견해를 드러내는 데이터는 “민감한” 범주의 개인데이터로 간주되며, 재판소의 견해에 따르면, 국가 당국이 이러한 데이터처리에 있어서 보호를 강화할 필요성을 고려하지 않고 일반 국내 규정에 따라 처리하여 이 측면을 무시하는 것은 용납될 수 없다(*Catt v. the United Kingdom*, 2019, § 112). 평화적 시위자와 관련된 데이터를 경찰 데이터베이스에 보관한 *Catt v. the United Kingdom* 사건에서, 국내 법원은 해당 제한의 적법성을 심사하면서 일반적인 데이터 보호법만을 참조하였다. 재판소는 문제의 데이터에 담긴 민감성은, 재판소에서 그랬듯이, 국내 법원 심리에서도 핵심적인 요소가 되어야 했다고 지적하면서 제 8 조 위반이라고 판단하였다(*ibid.*, § 112). 재판소는 또한, 카탈루냐에서 직무를 수행하던 판사와 치안판사들이 이른바 “결정권”을 카탈루냐인들이 행사할 가능성을 지지하는 법적 견해를 밝히는 선언문에 서명한 것과 관련하여, 경찰이 작성한 보고서가 특히 청구인 일부의 정치적 견해를 드러낸 *M.D. and Others v. Spain*, 2022 사건 §§ 63–64 에서도 제 8 조 위반이라고 판단하였다. 재판소는 또한 정치적 견해를 드러내는 개인데이터는 보호 수준이 강화되어야 한다고 강조하였다(처리된 청구인의 개인데이터에 청구인이 평화적 시위에 가담한 사실이 포함된 *Glukhin v. Russia*, 2023, §§ 76 및 86; 수집된 개인 정보가 청구인의 정치적 견해 및 활동과 관련된 *Selishcheva and Others v. Russia*, 2025, § 33).

22. 개인의 종교적·기타 신념(철학적 신념 포함)을 드러내는 개인데이터 보호권은 *Sinan Işık v. Turkey*, 2010 사건 § 37 및 *Mockutė v. Lithuania*, 2018 사건 § 117 에서 재판소가 심리하였다. 청구인들의 신분증에 종교를 기재한 것과 관련하여, 재판소는 신앙인의 정체성과

인생관을 구성하는 가장 본질적인 요소 중 하나로서 협약 제 9 조의 보호 대상인 종교적 신념에 관한 데이터 보호권의 중요성을 강조하였다(*Sinan Işık v. Turkey*, 2010, § 37).

iii. 노동조합 가입 사실을 드러내는 데이터

23. 개인의 노동조합 가입 사실을 드러내는 개인데이터 역시 "민감한" 범주에 속하므로 보호를 강화해야 한다. *Catt v. the United Kingdom*, 2019 사건 § 112에서, 경찰은 청구인이 여러 노동조합이 조직한 시위에 참여한 사실에 관한 정보를 수집하면서 특히 이름, 참석 여부, 생년월일, 주소를 기록하였다. 청구인의 외모에 관한 묘사와 시위 도중 촬영된 사진이 포함되는 경우도 있었다(*ibid.*, § 10). 평화적 시위에 참여하는 행위는, 노동조합에 대한 특별 보호도 규정하고 있는 협약 제 11 조의 구체적인 보호 대상이다(*ibid.*, § 123). 재판소 견해에 따르면, 경찰이 청구인에 관한 개인데이터를 수집한 점은 정당화된다고 간주하더라도, 그러한 데이터를 보유하는 최장기간을 확정하는 규칙이 없는 상황에서 청구인의 개인데이터를 계속 보관해야 할 "강력한 필요"는 존재하지 않는다(*ibid.*, §§ 117–119).

iv. 유전 데이터 및 생체 데이터

24. 재판소는 다음과 같은 정보의 수집·보유에 관한 여러 사건을 다루었다.

- 세포 검체 *Van der Velden v. the Netherlands* (dec.), 2005; *Schmidt v. Germany* (dec.), 2006; *S. and Marper v. the United Kingdom* [GC], 2008; *Canonne v. France* (dec.), 2015; *Caruana v. Malta* (dec.), 2018; *Trajkovski and Chipovski v. North Macedonia*, 2020; *Boljević v. Serbia*, 2020)
- DNA 프로필(*Van der Velden v. the Netherlands* (dec.), 2005; *Schmidt v. Germany* (dec.), 2006; *S. and Marper v. the United Kingdom* [GC], 2008; *W. v. the Netherlands* (dec.), 2009; *Peruzzo and Martens v. Germany* (dec.), 2013; *Canonne v. France* (dec.), 2015; *Aycaguer v. France*, 2017; *Mifsud v. Malta*, 2019; *Gaughran v. the United Kingdom*, 2020; *Trajkovski and Chipovski v. North Macedonia*, 2020; *Dragan Petrović v. Serbia*, 2020)
- 지문(*McVeigh, O'Neill and Evans v. the United Kingdom*, 1981; *Kinnunen v. Finland*, 1993; *S. and Marper v. the United Kingdom* [GC], 2008; *Dimitrov-Kazakov v. Bulgaria*, 2011; *M.K. v. France*, 2013; *Suprunenko v. Russia* (dec), 2018; *Gaughran v. the United Kingdom*, 2020; *P.N. v. Germany*, 2020); *Willems v. the Netherlands* (dec.), 2021)
- 장문(掌紋)(*P.N. v. Germany*, 2020)

- 음성 표본(*P.G. and J.H. v. the United Kingdom*, 2001; *Allan v. the United Kingdom*, 2002; *Doerga v. the Netherlands*, 2004; *Vetter v. France*, 2005; *Wisse v. France*, 2005)

25. 재판소는 유전학과 정보기술 분야의 급속한 발전을 고려한다면, 향후 유전정보와 밀접하게 엮인 사생활적 이해관계가 새로운 방식이나 지금으로서는 정밀하게 예측할 수 없는 방식으로 부정적인 영향을 받을 가능성을 배제할 수 없다고 보았다(*S. and Marper v. the United Kingdom* [GC], 2008, § 71).

26. 세포 검체의 경우, 그 속에 담긴 개인정보의 성격과 양을 고려한다면, 보유하는 것 자체만으로도 당해 개인의 사생활 존중권을 제한하는 것으로 간주하여야 한다. 당국이 DNA 를 프로파일링하여 실제로는 이 정보의 일부만 추출하거나 이용하고, 특정 사건에서 즉각적인 불이익이 발생하지 않았다고 하더라도, 이러한 결론은 달라지지 않는다(*ibid.*, § 73; *Amann v. Switzerland* [GC], 2000, § 69).

27. DNA 프로필의 경우, 이를 통해 개인의 민족 출신을 추론할 수 있다는 점 때문에, 보유가 더 민감한 문제가 되어 사생활권에 영향을 미칠 수 있으므로 보호를 강화해야 한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 76). 프로필에 포함된 정보는 객관적이고 반박할 수 없는 것으로 볼 수도 있으나, 개인 간 유전적 관계를 규명할 수단이 된다는 사실만으로도, 주어진 사건에 보호조치가 존재하거나 불이익 발생 가능성이 어느 정도인지는 불문하고, 보유하는 것만으로도 당해 개인의 사생활 존중권을 제한한다고 결론 내릴 수 있다(*ibid.*, § 75; *Amann v. Switzerland* [GC], 2000, § 69). 정보가 암호화된 형태로 존재하여 컴퓨터 기술을 이용해야만 이해할 수 있고 소수의 사람만이 해독할 수 있다고 해도 결론에는 변함이 없다(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 74–75).

28. 지문의 경우, 지문에는 당해 개인의 고유한 정보가 객관적으로 포함되어 있어 다양한 상황에서 정확하게 신원을 확인할 수 있으므로, 당해 개인의 동의 없이 지문 정보를 보유하는 것을, 중립적이거나 사소하다고 간주할 수 없다(*ibid.*, § 84). 신원이 확인되었거나 확인할 수 있는 개인의 지문을 당국의 기록에 보유하는 것은 세포 검체 및 DNA 프로필 보유보다 사생활에 미치는 영향이 더 적을 수는 있으나(*ibid.*, § 69), 그러한 데이터가 객관적이고 반박할 수 없는 성격이라 하더라도, 사생활상의 중대한 우려가 없어지는 것은 아니다(*Kinnunen v. Finland*, 1996 사건에서 위원회가 내린 결정이 기초한 판례와 달리 본 *ibid.*, § 85). *Willems v. the Netherlands* (dec.), 2021 사건에서, 유럽연합 회원국이 발급하는 여권과 여행문서의 보안요소 및 생체인식 표준에 관한 유럽연합 규정이, 국가 당국에 아무런 재량이 남지 않은 상태에서, 국내법에 도입된 후, 여권법에 따라 여권 신청 시

지문 채취 의무와 채취한 지문을 전자칩에 저장하는 조치에 관한 청구는 유럽연합법상 "동등한 보호의 추정"에 의거하여 명백히 근거 없는 것으로 각하되었다(*ibid.*, §§ 26-36).

29. 세포 검체와 DNA 프로필은 그 속에 포함된 정보 때문에 지문 보유보다 사생활에 더 큰 영향을 미친다(*S. and Marper v. the United Kingdom* [GC], 2008, § 86). 다만, 정당성 여부를 판단하려면, 지문 채취·사용·저장인 경우와 세포 검체·DNA 프로필인 경우를 구분할 필요가 있기는 하지만 그와는 별개로 지문의 보유 자체가 사생활 존중권에 대한 제한이 된다.

30. 특히 친자 소송 같은 특정 상황이라면 당국은, 개인의 방어권이 보장되고 국내 법원이 당해 이해관계 사이에서 적절한 균형을 달성한다는 조건으로, 개인에게 DNA 검사를 강제할 수 있다(*Mifsud v. Malta*, 2019, §§ 77-78). 제 8 조는, 증거를 얻기 위하여 피의자나 증인의 의사에 반하여 의료 절차를 이용하는 것이 민사 영역 등에서 그 자체로 법의 지배나 자연적(절차적) 정의에 반하는 것은 아니기 때문에, 금지하지 않는다(*ibid.*, § 71). 한편, 잠재적 친부가 법원의 DNA 검사 명령에 따르도록 강제할 수단이 전혀 없는 제도라 하더라도, 독립 기관이 친자관계를 신속히 판단할 대체 수단을 제공한다면, 제 8 조에서 파생되는 의무에 원칙적으로 부합한다고 볼 수 있다(*Mikulić v. Croatia*, 2002, §§ 55, 64).

v. 건강, 성생활 또는 성적 지향에 관한 데이터

31. 개인의 건강에 관한 정보는 사생활의 핵심 요소가 된다(*Yvonne Chave née Jullien v. France,* 1991, § 75; *L.L. v. France*, 2006; *Radu v. Moldova*, 2014; *L.H. v. Latvia*, 2014, § 56; *Konovalova v. Russia*, 2014, §§ 27, 41; *Y.Y. v. Russia*, 2016, § 38; *Surikov v. Ukraine*, 2017; *Frâncu v. Romania*, 2020, § 52). 이러한 정보의 비밀성을 존중하여야만 환자는 프라이버시가 보장된다는 느낌을 받게 될 뿐만 아니라 의료 전문직과 보건 서비스 전반에 대한 환자의 신뢰를 유지할 수 있다. 특히 HIV 감염 사실에 관한 정보의 비밀성 보호 문제에서 고려해야 마땅한 사항이다(*Z v. Finland*, 1997, § 96; *Kiyutin v. Russia*, 2011, § 64; *Armonienė v. Lithuania*, 2008, § 40; *Biriuk v. Lithuania*, 2008, § 39; *I. v. Finland*, 2008, § 38; *C.C. v. Spain*, 2009, § 33; *Y. v. Turkey* (dec.), 2015, § 65; *P.T. v. Republic of Moldova*, 2020, §§ 5-6, 26; *Y.G. v. Russia*, 2022, § 45). 그러한 데이터를 공개하면 낙인과 배제의 위험에 노출시킴으로써 사회적·고용상의 지위뿐만 아니라 사생활과 가족생활에 극적인 영향을 미칠 수 있다(*Z v. Finland*, 1997, § 96; *C.C. v. Spain*, 2009, § 33; *P. and S. v. Poland*, 2012, § 128; *Avilkina and Others v. Russia,* 2013, § 45; *Y. v. Turkey* (dec.), 2015, § 65; *Y.G. v. Russia*, 2022, § 45).

32. 따라서 이러한 정보의 비밀성을 보호할 이익은, 추구되는 정당한 목적에 문제 된 제한이 비례하는지 판단할 때 중대한 비중을 차지한다. 그러한 제한은 공익상 압도적 필요 요건으로

정당화되지 않는 한 협약 제 8 조와 양립할 수 없다(*Z v. Finland*, 1997, § 96). 개인의 HIV 감염 여부는 대단히 내밀하고 민감한 성격의 정보이므로, 환자의 동의 없이 그러한 정보를 전달하거나 공개하도록 강제하는 국가의 조치라면 무엇이 되었든 재판소의 입장에서 가장 꼼꼼하게 심리해야 할 대상이다(*ibid.*, § 96).

33. 따라서 재판소는, 남편에 대한 형사절차 중 선고된 판결문에 아내의 신원과 HIV 감염 사실이 공개되고 언론에 보도된 *Z v. Finland*, 1997 사건 §§ 113–114, 이혼 판결문에 개인의 의료문서 발췌문이 그대로 전재된 *L.L. v. France*, 2006 사건 §§ 32–48, HIV 양성 간호사의 의료기록이 무단으로 접근할 수 없을 만큼 보호되지 않은 *I. v. Finland*, 2008 사건 §§ 35–49, 청구인의 HIV 감염 여부와 관련된 판결문에 신원이 공개된 *C.C. v. Spain*, 2009 사건 §§ 26–41, 강간 피해 후 임신한 여아가 낙태를 원했다는 정보를 공립 병원이 공개한 *P. and S. v. Poland*, 2012 사건 §§ 128–137, 동의 없이 의대생들 앞에서 출산해야 했던 청구인이 이의를 제기한 *Konovalova v. Russia*, 2014 사건 §§ 39–50, 다용도로 사용될 수 있는 증명서에 불필요하게 민감한 의료 데이터가 기재된 *P.T. v. Republic of Moldova*, 2020 사건 §§ 24–33, 한 시장의 부패 사건에서 건강 문제를 이유로 한 보석 신청의 비공개 심리를 허용하지 않은 *Frâncu v. Romania*, 2020 사건 § 52, 특히 청구인의 건강 데이터도 담긴 데이터베이스가 시장에서 판매 가능했던 점에 이의를 제기한 *Y.G. v. Russia*, 2022 사건 §§ 46–53 및 성적 학대에 대한 민사 손해배상 청구가 각하된 판결문 전문이, 청구인의 성명 및 주소와 함께, 특별히 비공개를 요청했음에도 공식 사법 온라인 데이터베이스에 공개된 *A.P. v. Armenia*, 2024 사건 §§ 150–159 등에서 제 8 조 위반이라고 판단하였다.

34. 개인의 정신건강에 관한 정보(정신병원이 환자의 정신 건강 데이터를 공개한 *Mockutė v. Lithuania*, 2018 사건 § 94, 청구인들의 강제입원 사실이 병원 기록에 기재된 *Malanicheva v. Russia* (dec.), 2016 사건 §§ 13, 15–18)는 개인의 성별 정체성 또는 성적 지향을 드러내는 데이터(*Dudgeon v. the United Kingdom*, 1981, § 41, *J.L. v. Italy*, 2021, § 136 및 *Drelon v. France*, 2022, § 79) 및 데이터 주체의 동의 없이 한 공공기관이 다른 공공기관으로 전달한 낙태 관련 데이터(*M.S. v. Sweden*, 1997, §§ 41–42) 같은 개인의 성생활에 관한 데이터와 마찬가지로 고도로 민감한 데이터가 된다. 국내 입법은 이러한 데이터가 협약 제 8 조상 보호조치에 부합하지 않는 방식으로 전달되거나 공개되는 것을 방지할 적절한 보장책을 마련해야 한다(*Z v. Finland*, 1997, § 95).

vi. 범죄 및 유죄 판결 데이터

35. 범죄, 형사절차, 유죄판결 또는 관련 예방조치에 관한 데이터는 *협약 108* 제 6 조에 따라 보호를 강화해야 하는 데이터 범주에 속한다(*M.M. v. the United Kingdom*, 2012,

§ 188; *Margari v. Greece*, 2023, § 59). 따라서 계속 중인 형사절차 또는 범죄 수사 맥락에서 민감한 데이터가 공개되는 경우, 해당 데이터는 그 무엇보다도 피고인에 대한 상황과 계속 중인 혐의를 정확히 반영해야 하며, 동시에 무죄추정 원칙이 준수되어야 한다(*ibid.*). 공소취소된 개인(*Brunet v. France,* 2014, §§ 38-40; *N.F. and Others v. Russia*, 2023, § 38), 주의조치를 받은 개인(*M.M. v. the United Kingdom*, 2012, §§ 188-190), 유죄판결을 받고 형이 선고된 개인(*Gardel v. France*, 2009, § 58; *Peruzzo and Martens v. Germany* (dec.), 2013, § 44; *Trajkovski and Chipovski v. North Macedonia*, 2020, § 46; *N.F. and Others v. Russia*, 2023, § 38) 또는 경찰서 유치 같은 관련 예방조치를 당한 개인(*Suprunenko v. Russia*, (dec.), 2018, § 61)에 관한 개인데이터처리 역시 해당 데이터 주체의 사생활 존중권을 제한하게 된다.

36. 재판소의 견해에 따르면, 범죄기록부에 포함된 데이터는 공적 정보라는 측면도 있기는 하지만, 중앙 기록부에 체계적으로 저장된다는 점 때문에 당사자를 제외하면 모두가 잊어버렸을 법한 시점마저 한참 지난 후에 공개될 수 있다. 따라서 유죄 판결이나 주의조치 자체가 점점 과거가 되어갈수록 존중받아야 할 개인 사생활의 일부가 되고(*M.M. v. the United Kingdom*, 2012, § 188), 그러한 데이터가 개인의 오랜 과거와 관련될 경우에는 더욱 그러하다(*B.B. v. France*, 2009, § 57; *Catt v. the United Kingdom*, 2019, § 93; *M.L. and W.W. v. Germany*, 2018, §§ 98-100).

37. 경찰 기록부에 개인의 신원데이터, 지문 및 신분증 사진을 보유하는 조치는 그 개인에게 심각한 결과를 초래하여 일상생활을 더 어렵게 할 수 있다(*Dimitrov-Kazakov v. Bulgaria*, 2011, §§ 8, 10, 13, 30). 강간 사건과 관련하여 조사를 받은 후 기소되지 않았지만 경찰 기록에 해당 개인을 "범죄자"로 기재하고 그대로 보유한 사건에서 재판소는 해당 데이터 주체가 바로 그 기재 때문에, 강간 고소 사건이나 여아 실종 사건과 관련하여 여러 차례 경찰 검문을 받게 되었음을 알게 되어 제 8 조 위반이라고 판단하였다(*ibid.*, §§ 8, 10, 13, 30).

38. 또한 청구인에게 선고된 대체적 행정벌(형사사건에서 무죄처분의 일종)에 관한 자료를 계속 보유하는 것은 협약 제 9 조에 따른 사생활 존중권의 제한에 해당한다(*Tonchev v. Bulgaria*, 2024, § 125). 재판소 판례에 따르면, 공공기관이 그러한 자료를 단순히 저장만 하여도 이후 사용 여부 및 사용 방법과 무관하게 제한에 해당한다. 재판소는 관련 불가리아 규정이 그 해석과 적용을 담당하는 국가 당국에 혼란을 초래할 정도로 모호하여 충분히 예측 가능하다고 할 수 없는 규정이었으므로 협약 제 8 조 위반이라고 판단하였다. 또한 이러한 불일치는 유럽연합 데이터 보호법의 적용에도 영향을 미쳤다(저장 기간 제한 원칙, *ibid*, § 137).

39. 또한, 공개적으로 접근 가능한 부패 공무원 등록부에 청구인을 식별하고 범죄 내용과 부과된 처벌에 대한 설명을 포함하는 정보를 공개하는 것은 제 8 조의 범위에 속한다(*Sytnyk v. Ukraine*, 2025, § 109). 이 사건에서 재판소는 먼저 혐의를 받고 있는 청구인의 부정행위가 공정한 사법 절차 내에서 입증되지 않았다고 판단했으며, 따라서 *Gillberg v. Sweden* [GC], 2012(§ 67) 배제 원칙의 적용과 관련된 정부의 주장을 기각했다. 재판소는 또한 "부패한"이라는 낙인이 찍힌 사실이 청구인의 평판에 심각한 영향을 미쳤을 것이며, 특히 그의 부패 방지 분야에서의 오랜 경력을 고려할 때 그의 전문적 업적에 대한 신뢰성을 훼손했을 것이라고 판단했다. 그러한 출판물의 낙인 찍힘, 문제의 등록부에 대한 영구적인 대중의 접근성, 그리고 그 등록부에 청구인의 이름이 포함되는 데 대한 시간적 제한의 부재는 청구인이 사생활 존중받을 권리를 향유하는 데 심각한 침해를 초래한다고 결론지었다(*Sytnyk v. Ukraine*, 2025, §§ 108–109).

b. 데이터의 기타 범주

40. “민감한” 것으로 분류된 데이터가 아니더라도, 감시 기법이 점점 정교해지고 정보통신기술로 데이터 주체의 일상생활이 더 어려워질 수 있게 되면서, 다른 범주의 개인데이터 역시 우려의 대상이 되었다.

i. 고용 데이터

41. 신원이 확인되었거나 확인할 수 있는 개인의 고용 관련 데이터를 기록하고 저장하는 것은 협약 제 8 조에 따른 데이터 주체의 사생활과 가족생활 존중권을 제한한다(*Khelili v. Switzerland*, 2011, § 56; *Sõro v. Estonia*, 2015, §§ 49 및 56; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, §§ 95–96). 오늘날 당국이 수집하여 기록에 보관하는 정보는 자동처리의 대상이 되어, 그러한 데이터에 대한 접근과 전송이 상당히 용이해지고 있기 때문에, 이러한 조치는 개인의 평판을 해치거나 일상생활을 어렵게 할 수 있는 심각한 결과를 초래할 수 있다. 재판소는 경찰이 청구인을 데이터베이스에 “성매매 종사자”로 기재하였다가 이후 “재봉사”로 정정·대체한 *Khelili v. Switzerland*, 2011 사건 § 64 및 청구인이 과거 국가보안기관 운전기사로 근무한 사실에 관한 데이터가 공개된 후 직장을 떠날 수밖에 없었던 *Sõro v. Estonia*, 2015 사건 § 63 에서 제 8 조 위반이라고 판단하였다. 청구인의 업무 수행 중 이동 거리(필요한 경우 사적 이동도 포함)를 점검·확인할 목적으로 고용주가 회사 차량에 GPS 시스템을 설치한 *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 사건 §§ 95–96 에서 재판소는 그렇게 수집된 정보는 개인데이터가 된다고 보았다. 나아가 재판소는, 직원은 시스템 비활성화 권한이 없어서 GPS

시스템이 주 7 일 하루 24 시간 내내 작동한 결과 상시적이고 체계적으로 감시하게 된 것은 명백히 청구인의 사생활을 제한하였다고 강조하였다[1].

ii. 재정 데이터

42. 개인의 은행 문서에서 얻은 정보는, 데이터 주체의 민감한 사적 정보이든 직업 활동에 관한 정보이든 상관없이, 개인데이터가 된다(*M.N. and Others v. San Marino,* 2015, § 51; *G.S.B. v. Switzerland*, 2015, § 51). 은행에서 얻은 데이터를 당국이 복사한 후 저장하는 행위는, "사생활"과 "통신"의 개념에 포함되며, 협약 제 8 조 목적상 제한에 해당한다(*M.N. and Others v. San Marino*, 2015, § 55).

43. 재판소는 형사 수사(*M.N. and Others v. San Marino*, 2015, §§ 7–9, §§ 53–55), 일반의 관심사에 관한 논의를 목적으로 언론이 금융데이터를 광범위하게 공개한 경우(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, §§ 172–173), 변호사가 자금세탁 등 의뢰인의 불법 행위에 대한 의심을 신고하는 과정에서 직업상 비밀 특권으로 보호되는 데이터를 공개해야 할 의무(*Michaud v. France,* 2012, §§ 91–92), 협약 당사국이 아닌 다른 국가 당국에 금융데이터가 전송된 경우(*G.S.B. v. Switzerland*, 2015, § 50), 청구인의 남편에 대한 형사사건을 다룬 텔레비전 보도에서, 청구인의 납세자 번호와 세금 신고 정보가 공개된 것과 관련된 청구가 기각된 경우(*Samoylova v. Russia*, 2021, §§ 83 및 90–93), 국세청 전산망에 저장된 데이터에 불법으로 접근하거나 이를 오·남용한 경우 (*Casarini v. Italy* (dec.), 2024, § 57)에 금융데이터의 수집, 처리 및 공개 문제를 심사하였다.

44. 대량의 세금 데이터를 열람·수집할 수 있게 하는 것이 공익에 부합한다고 해도, 그에 따라 반드시 또는 자동으로 그와 동일하게 아무런 분석도 가하지 않은 상태의 원자료를 원형 그대로 대량 유포하는 데에도 공익이 존재하는 것은 아니다(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, §§ 172–178, 198).

45. 조세 사안에서는, 데이터 주체의 신원과 밀접히 연관되지 않거나 개인데이터가 포함되지 않은 순순한 재정데이터의 보호 문제라면, 국가는 더 넓은 판단재량을 누리지만(*G.S.B. v. Switzerland*, 2015, § 93), 조세 데이터가 특정한 개인을 대상으로 수집·편집된 경우나, 데이터 주체가 합리적으로 예상할 수 있는 범위가 아닌 방식이나 정도로 공개된 경우에는 사생활 보장 문제가 발생한다(*M.N. and Others v. San Marino*, 2015,

[1] 또한, 아래 "GPS 위치 데이터" 참조.

§§ 52-53; *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 136).

iii. 트래픽 데이터

46. 트래픽 데이터에 포함되는 전화 사업자로부터 얻은 데이터로는 특정 통신의 발신자와 수신자, 날짜, 시각, 길이 등을 파악할 수 있지만 통신 내용 자체에 관한 것은 아니다(*Malone v. the United Kingdom*, 1984, §§ 83-84; *Copland v. the United Kingdom*, 2007, § 43). 형사 수사 맥락에서, 특정 전화기의 발신 번호, 통화 시각과 시간 등을 기록하는 장치(통화내역 기록기)를 이용하지만 통신 내용을 점검·확인하거나 가로채지 않는 절차인 "통화내역 기록(metering)"은 데이터 주체의 사생활을 제한하게 된다(*Malone v. the United Kingdom*, 1984, §§ 83-84). 이러한 데이터(특히 발신된 번호)는 "전화 통신을 구성하는 불가분의 요소"가 되기 때문에, 이용하게 되면 제 8 조에 따른 문제를 일으킬 수 있다(*Malone v. the United Kingdom*, 1984, § 84; *Copland v. the United Kingdom*, 2007, § 43). 재판소의 견해에 따르면, 가입자의 동의 없이 그러한 정보를 경찰에 제공하는 것 역시 협약 제 8 조가 보장하는 권리의 제한에 해당한다(*Malone v. the United Kingdom*, 1984, § 84).

47. "통화내역 기록" 관행은, 예컨대 전화 서비스 제공자가 가입자에게 정확한 요금을 부과하기 위한 목적이라면 제 8 조를 위반하지 않고, 그 성격상 통화 감청과는 구별된다(*Malone v. the United Kingdom*, 1984, §§ 83-84; *P.G. and J.H. v. the United Kingdom*, 2001, § 42). 한 개인이 여러 대의 휴대전화로 수·발신한 통화 데이터를 확보하고 이후 이동 경로를 추적할 수 있도록 전화회사가 기지국 데이터를 수집하라는 법원의 명령은, 법률이 허가하고 자의성을 방지하는 보호조치를 충분히 보장하는 한, 제 8 조와의 양립이 반드시 불가능한 것은 아니었다(*Ben Faiza v. France*, 2018, §§ 56, 59, 69). 재판소는 그러한 명령이 사전에 검사의 승인을 받아야 하고, 그렇지 않으면 무효가 되며, 법원에 의해 다툴 수 있고, 불법으로 얻은 데이터는 증거에서 제외될 수 있는 경우에는 제 8 조 위반이 아니라고 판단하였다(*ibid.*, §§ 79, 73).

48. 선불 심(SIM, 가입자 식별 모듈) 카드 사용자의 개인데이터(이동통신 가입자의 이름, 주소, 전화번호 등)를 서비스 제공자가 수집한 것은 "사소하다"고 볼 수 없다(*Breyer v. Germany*, 2020, §§ 92-95). 통신서비스 제공자가 그러한 가입자 데이터를 단순히 저장만 하여도 이후 사용 여부와 관계없이 데이터 주체의 사생활에 대한 제한이 된다(*ibid.*, § 92). 이러한 제한은 상대적으로 경미하고(*ibid.*, § 95), 유럽 차원의 합의가 없는 경우라면 국가 당국이 일정한 판단재량을 누리는 분야이다(*ibid.*, § 90). 한편, 자료 열람 절차에 대한 사전 통지가 없더라도, 독립 기관의 감독이 존재하여 해당 자료를 요청한 당국에 제공하는 것이 정당한지 심사할 권한이 있고, 자료 열람 절차나 데이터 요청 때문에 자신의 권리가

침해되었다고 생각한다면 항고할 가능성이 보장되는 한, 제 8 조와 양립 불가능하지 않다(*ibid.*, §§ 103-107).

49. 인터넷 접속 데이터의 경우, 사용자의 IP 주소와 이메일 주소, 통신 상대방, 사용된 통신 수단에 관한 정보, 추가로 요청되거나 사용된 서비스 및 그 제공자 등의 정보를 통해 사용자의 신원을 파악할 수 있다 *Benedik v. Slovenia*, 2018, § 96). 재판소의 견해에 따르면, 특정 시각에 부여된 동적 IP 주소와 연결된 가입자 정보는 개인데이터가 된다. 공개된 정보는 아니므로 전통적인 전화번호부나 차량 등록번호의 공적 데이터베이스에 수록된 정보와 비교할 수는 없다(*ibid.*, § 108).

50. 대규모 감시 맥락에서 통신데이터를 취득하는 것이 통신 내용 자체를 취득하는 것보다 침해성이 덜하다고 할 수는 없다(*Centrum för rättvisa v. Sweden* [GC], 2021, § 277 및 *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 363). 통신데이터의 감청, 보유 및 검색은 통신 내용에 적용되는 것과 동일한 보호조치를 기준으로 분석되어야 한다. 하지만, 통신데이터는 그 성격이 다르고 정보기관에서 사용하는 방식도 다르다는 점을 고려할 때, 앞서 언급한 보호조치가 존재하는 한, 그 처리에 관한 법 규정이 통신 내용 처리에 관한 규정과 모든 면에서 동일할 필요는 없다(*Centrum för rättvisa v. Sweden* [GC], 2021, § 278 및 *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 364).

51. 접속 데이터를 비밀로 해야 한다는 압도적 필요 요건도, 인터넷으로 범행한 가해자를 특정하고 소추하기 위한 실효적인 형사 수사를 방해하는 경우에는 협약 제 8 조에 부합하지 않을 수도 있다(*K.U. v. Finland,* 2008, § 49). 전기통신 및 인터넷 가입자의 사생활 존중권 보장보다 공공질서, 범죄 예방, 타인의 권리와 자유 보호 같은 여러 정당한 필요가 우선하는 경우도 있다(*ibid.*, § 49).

iv. 음성 표본

52. "도청(bugging)" 운용의 목표는 사유재산(*Vetter v. France*, 2005, §§ 10, 20) 또는 공공장소에 청취 장치를 설치하여 개인의 대화를 듣는 것이다(*P.G. and J.H. v. the United Kingdom*, 2001, §§ 38, 63; *Allan v. the United Kingdom*, 2002, § 35; *Doerga v. the Netherlands*, 2004, § 43; *Wisse v. France*, 2005, § 29).

53. 개인의 음성을 비밀리에 녹음하고 다른 개인데이터와 결합하여 해당 개인의 신원 파악에 직접적으로 관련된 분석 절차의 대상이 되는 영구 기록으로 보관하는 것은 개인데이터처리에 해당하고, 데이터 주체의 사생활 존중권을 제한한다(*P.G. and J.H. v. the United Kingdom*, 2001, §§ 59-60). 경찰이 자체 시설이나 사유 시설에 설치한 비밀 청취

장치의 사용을 규율하는 국내법이 존재하지 않았던 사건에서 재판소는 제 8 조 위반을 인정하였다(*ibid.*, §§ 38, 63).

54. 청취 장치를 이용한 대화 도청은 전화 감청과 마찬가지로, 데이터 주체의 사생활 존중권에 대한 중대한 제한에 해당한다(*Vetter v. France*, 2005, § 26). 따라서 이는 각별히 적확한 "법"에 기초하여야 하고, 무엇보다 유관 기술 과정이 계속해서 정교해지고 있기 때문에, 이 분야에서도 명확하고 상세한 규정의 존재는 불가결하다(*ibid.*, § 26). 재판소의 견해에 따르면, 그러한 "법"은 전화 감청의 경우에 우려되는 것과 동일한 유형의 남용으로부터 시민을 보호하는 적절한 보호조치를 포함해야 한다(*ibid.*, § 26). 따라서 특히, 그러한 조치의 대상이 될 수 있는 개인의 범주와 이를 정당화할 수 있는 범죄의 유형이 정의되어야 하고, 법원은 그러한 조치의 집행에 기한을 설정해야 하며, 감청된 대화의 보고서 작성 조건, 판사와 변호인이 검토하도록 녹음을 완전하고 온전한 상태로 전달하기 위한 주의사항, 특히 불기소 결정이나 무죄 판결 후 테이프를 삭제하거나 파기해야 하는 여러 사정을 규정하여야 한다(*Kruslin v. France*, 1990, § 35 에서 제시된 감청 증거 기준을 참고한 *ibid.*, § 26).

55. 민주사회에서 법의 지배에 따라 필요한 최소한의 보호조치 없이 개인의 음성이 녹음된 경우, 이는 제 8 조 위반이 된다(교도소 접견실에서 대화를 녹음하고 이를 이후 사용한 *Wisse v. France*, 2005, § 34; 교도소 독방에 청취 장치를 설치한 *Allan v. the United Kingdom*, 2002, § 36).

v. GPS 위치 데이터

56. GPS 장치로 수집한 데이터는 개인의 소재와 공개된 행방을 나타낼 수 있는 한 개인데이터가 된다(*Uzun v. Germany*, 2010, §§ 51-52; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, § 95). 이러한 데이터의 처리와 사용은 데이터 주체의 사생활 존중권에 대한 제한으로 간주될 수 있다(*Uzun v. Germany*, 2010, §§ 51-52; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, § 96). GPS 감시는 그 성격상, 보통 개인의 행위, 의견, 감정을 더 많이 드러내므로 사생활 존중권을 침해하기 더 쉬운 다른 시청각적 감시 방법과는 구별된다(*Uzun v. Germany*, 2010, § 52).

57. 이러한 유형의 조치는 전화 대화 감청보다 데이터 주체의 사생활을 덜 제한하는 것으로 보아야 하므로, 개인의 행방을 GPS 로 감시하는 경우에는 전화 감청의 구체적인 맥락에서 마련하고 적용하는 비교적 엄격한 기준을 그대로 적용하지 않는다(*ibid.*, § 66). 특정 사건에서 GPS 위치추적을 당한 개인이 제 8 조상 권리를 행사할 때 자의적 제한을 당하지 않도록 충분히 보호되었는지 판단할 때 법의 예측가능성을 살펴보는데, 이때 재판소는 전화

감청 사건에서 사용하는 특별히 엄격한 기준 대신 더 일반적인 원칙을 적용한다(*ibid.*, § 66 및 § 63 에 인용된 참조사항). 언제나 독립 기관이 영장을 발부해야 하는 것은 아니며, GPS 감시 이후 사후적 사법심사만으로도 자의성으로부터 보호할 수 있다(*ibid.*, § 72).

58. 재판소는 마약 밀매 형사 수사 과정에서 개인의 차량에 실시간 위치추적 장치를 설치한 조치는, 당시 국내법(성문법도 판례법도 아님)에서 당국이 이 영역에서 어느 정도, 어떤 방식으로 재량권을 행사할 수 있는지 명확하게 규정하지 않았기 때문에, 제 8 조를 위반한다고 판단하였다(*Ben Faiza v. France*, 2018, §§ 58-61).

59. 다만, 개인의 위치를 추적하여 수집한 개인데이터 문제와 해당 개인에게 제기된 형사절차에서 이 데이터의 사용을 재판소가 심리한 다른 사건에서는 제 8 조 위반이 아니라고 판단하였다(*Uzun v. Germany*, 2010, §§ 60-74). 사법심사 및 불법적인 GPS 감시로 획득한 증거를 배제할 가능성은, 수사 당국이 법에 어긋나는 수단으로 증거를 수집하지 못하게 억제하기 때문에 중요한 보호조치가 된다(*ibid.*, § 72). 또한, 문제 된 감시 조치 허가는 국내법상 매우 엄격한 조건을 따라야 한다는 점, 침해성이 덜한 수사 수단이 실효적이지 않다고 확인한 후 GPS 감시를 명령한 점, 그 명령도 비교적 짧은 기간에만 집행되었다는 점도 해당 제한의 비례성 심사에서 고려되었다(*ibid.*, §§ 77-81).

60. *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 사건 §§ 95-96 및 §§ 105-125 에서, 청구인의 고용주는 청구인의 업무 도중 이동 거리뿐만 아니라 필요하다면 사적 이동까지 점검·확인할 목적으로 회사 차량에 GPS 시스템을 설치하였다. 재판소는 해당 시스템으로 차량의 이동을 실시간 추적할 수 있었기 때문에, 차량을 사용하기로 되어 있던 사람의 지리적 위치를 원하는 시점에 또는 계속해서 특정할 수 있었다고 평하였다. 재판소의 견해에 따르면, 그러한 정보는 개인데이터가 된다. 또한, 직원은 시스템 비활성화 권한이 없어서 GPS 시스템이 주 7 일 하루 24 시간 내내 작동한 결과 상시적이고 체계적으로 감시하게 된 것은 명백히 청구인의 사생활을 제한하였다고 강조하였다. 한편, 재판소는 국내 법원들이 문제 된 상충하는 이해관계인 사생활을 존중받을 청구인의 권리와 회사의 원활한 운영을 보장받을 고용주의 권리를 회사가 추구한 정당한 목적(즉 지출 관리 권리)을 고려하여 신중하게 조화시켰다고 보았다. 따라서 재판소는 협약 제 8 조 위반이 아니라고 판단하였다.

vi. 사진

61. 자신의 초상을 보호할 권리는 인격 발달에 본질적 요소이고, 그 전제가 되는 권리는 초상 사용을 통제할 권리이다(*Reklos and Davourlis v. Greece*, 2009, §§ 40-43; *Margari v. Greece*, 2023, § 28; *Glukhin v. Russia*, 2023, § 66). 공개적으로 기록되거나 보도될 가능성이 있는 활동의 맥락에서, 개인이 의식적으로 또는 우연히 촬영 가능성에 스스로를

노출한 경우를 제외하고, 초상에 대한 실효적 보호는 원칙적으로 사진이 촬영되는 시점에 당사자의 동의를 얻는 것을 전제로 하며, 그저 사진이 출판될 때 동의를 받는 것만으로는 충분하지 않다(*Reklos and Davourlis v. Greece*, 2009, §§ 37, 40). 다만, 이 원칙은 절대적이지 않다. 특정 상황에서는, 공적 인물이나 보도 가치가 있는 인물의 지위 때문에, 공익에 의거하여 당사자의 인지나 동의 없이 초상을 기록하고 유포하는 것이 정당화될 수 있다[2].

62. 범죄 혐의로 체포된 개인의 경우, 당국이 촬영한 사진이 범죄 대응에 객관적으로 유용하다면, 그러한 사진의 보유는 범죄 대응 목적을 위하여 "민주사회에서 필요한" 것으로 인정될 수 있다(*Suprunenko v. Russia* (dec.), 2018, §§ 63-65). 피의자의 사진이 촬영되어 데이터베이스에 포함되었다는 사실만으로는 혐의나 유죄의 낙인을 찍을 수 없다(*ibid.*, § 64). *Murray v. the United Kingdom* [GC], 1994 사건 §§ 92-93 에서 재판소는 테러 범죄 혐의자를 동의 없이 촬영하고 보유한 사진이 민주사회에서 정당한 목적인 테러 방지에 비례하지 않는 것은 아니라고 보았다. 테러 범죄 수사 권한이 있는 당국이 체포된 자 또는 체포 당시 현장에 있던 다른 자들의 기본적인 개인정보를 기록하고 보유하는 것이 정당한 수사의 범위를 벗어난다고 간주할 수는 없었다(*ibid.*, § 93). 또한 재판소는, 청구인이 범죄 혐의로 경찰에 체포될 당시 당국이 촬영한 청구인의 사진을 내무부 컴퓨터 시스템에 보유한 것에 관한 청구를 명백히 근거 없는 것으로 선언하였다(*Suprunenko v. Russia* (dec.), 2018, § 65). 재판소의 견해에 따르면, 경찰 컴퓨터에 이렇게 수집·저장된 정보는 사적 성격을 띠고 있더라도 내밀하거나 민감하다고 볼 수 없다(*ibid.*, § 64).

63. 다만 재판소는 경찰이 체포되거나 기소된 개인의 사진을 사전 동의 없이 언론에 제공한 경우(*Sciacca v. Italy*, 2005, §§ 29-31; *Khuzhin and Others v. Russia*, 2008, §§ 115-118; *Margari v. Greece*, 2023, §§ 54-60), 경찰이 텔레비전 촬영팀을 경찰서로 불법 초청하여 청구인을 촬영하고 그 영상을 방송하게 한 경우(*Toma v. Romania*, 2009, §§ 90-93; *Khmel v. Russia*, 2013, § 41), 내무부가 경찰 구금 중에 촬영된 청구인들의 사진을, 신원을 가리지 않은 채 자국 웹사이트에 공개한 경우(*D.H. and Others v. North Macedonia*, 2023, §§ 63-65), 청구인의 사진을 수배자 게시판에 게시한 것이 법에 부합하지 않은 경우(*Guiorgui Nikolaïchvili v. Georgia*, 2009, §§ 129-131) 또는 기존 규칙과 절차가 "양질의 법률" 요건을 충족하지 못한 경우(*Negru v. the Republic of Moldova*, 2023, §§ 29-35) 제 8 조 위반이라고 판단하였다.

---

[2] 또한, 언론 보도를 목적으로 한 사진 출판인 경우 유럽인권협약 제 10 조에 대한 해설서 – 표현의 자유 참조

64. 재판소의 견해에 따르면, 유죄 판결을 받지 않은 범죄 혐의자의 사진을 무기한 보유하는 것은 범죄로 유죄 판결을 받은 개인의 자료를 보유하는 것보다 더 큰 낙인의 위험을 수반한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 122; *Gaughran v. the United Kingdom*, 2020, §§ 82-84). 개인데이터 보유 제도를 마련할 때 국가의 판단재량이 허용 범위를 넘었는지 평가하는 결정적인 요소는 개인데이터 보유 기간의 장단이라기보다는 특정한 보호조치의 존재와 작동 여부이다(*ibid.*, § 88).

65. 현재 사진에 적용할 수 있는 안면 인식 및 매핑 기술은 점점 더 복잡해지고 있으므로, 국내 법원은 당국이 촬영한 개인의 사진을 두고 사생활 존중권을 제한할 필요가 있는지 심리할 때 이러한 점을 고려해야 한다(*ibid.*, §§ 67-70; 또한, 공개된 텔레그램 채널에 게시된 사진이 청구인인지 파악하기 위하여 경찰이 안면인식 기술을 사용한 *Glukhin v. Russia*, 2023, §§ 64-91 참조).

66. 당국이 음주 운전으로 유죄 판결을 받은 개인의 사진을 DNA 프로필 및 지문과 함께 무기한 보유하기로 결정한 *Gaughran v. the United Kingdom*, 2020 사건 §§ 97-98 에서 재판소는 제 8 조 위반이라고 판단하였다. 범죄의 심각성을 고려하지도 않았고 이후 실질적인 재검토 가능성도 부재한 상태에서 개인데이터 보유를 결정하면서 당국은 상충하는 공익과 사익 사이에서 적절한 균형에 도달하지 못하였다. 국가가 사진을 보유하는 것은 DNA 프로필 보유에 비해 누릴 수 있는 판단재량의 범위가 넓다고는 하여도(*ibid.*, §§ 84, 96), 특히 관련 보호조치가 없거나 실질적인 재검토 가능성이 없는 상황에서 그러한 자료의 보유가 어떠한 경우라도 비례적이라고 볼 만큼 넓지는 않았다(*ibid.*, § 96).

67. *P.N. v. Germany*, 2020 사건 §§ 76-91 에서 재판소는 과거 유죄 판결을 받은 개인에 대한 새로운 형사절차가 개시된 후 신원 확인을 위하여 얼굴과 신체 사진(특히 문신), 지문, 장문(掌紋) 같은 정보를 경찰이 수집하게 한 조치와 관련하여 제 8 조 위반이 아니라고 판단하였다. 문제 된 신원 확인 자료 수집의 상대적으로 한정된 침해성과 기간, 데이터 보유가 청구인의 일상생활에 미친 한정적인 영향, 자료가 5 년 후 삭제된 점, 자료의 보관 장소가 보호조치와 개별 심사가 적용되는 경찰 데이터베이스인 점을 고려할 때, 문제 된 조치가 청구인의 사생활 존중권을 제한하는 정도는 비례성을 상실하지 않았다.

68. 맥락을 바꿔, *Reklos and Davourlis v. Greece*, 2009, §§ 41-43 에서 재판소는 사진작가가 병원에서 신생아 사진을 촬영하고 이후 사용할 가능성이 있는 상태에서 신원 파악이 가능한 형태로 보유한 것이 부모의 의사에 반하였음을 근거로 제 8 조 위반이 있었다고 판단하였다. 마찬가지로, 속임수로 비밀리에 촬영한 청구인의 이미지를 흐림 효과 처리 없이 언론에 공개한 *Hájovský v. Slovakia*, 2021 사건 §§ 46-49 및 남편이 청구인의 이름으로

허위 프로필을 만들고 내밀한 사진을 게시하는 방식으로 반복적인 사이버폭력을 가했지만, 당국이 청구인을 보호하지 못한 *Volodina v. Russia (no. 2)*, 2021 사건 § 68 에서도 위반이라고 판단하였다.

69. *Vučina v. Croatia* (dec.), 2019 사건 §§ 34-51 에서 재판소는 여성잡지의 사진 설명에 청구인의 이름이 아닌 다른 이름이 단순 실수로 기재되었고, 그 이름에 어떠한 부정적 의미도 없었던 사실만으로는 데이터 주체의 사생활 존중권에 대해 현저하게 중대한 제한이라고 간주할 수는 없다고 판단하였다.

70. *Von Hannover v. Germany (no. 2)* [GC], 2012 사건 §§ 114-126 에서 재판소는, 국내 법원이 당사자들의 동의 없이 촬영된 유명인 부부의 사진 게재 금지를 거부한 것은, 출판사 측의 표현의 자유와 청구인들 측의 사생활 존중권을 신중히 저울질하여 균형을 맞추었기 때문에 제 8 조 위반이 되지 않는다고 판단하였다. 그 과정에서 국내 법원은 동반 기사에 비추어 본 그 사진이 일반의 이익에 관한 공적 논의에 이바지하였는지를 대단히 중요하게 살펴보았다. 사진이 촬영된 상황도 심리하였다.

71. *Kahn v. Germany*, 2016 사건 §§ 63-76 에서 재판소는 전직 독일 국가대표 축구팀 골키퍼의 두 자녀가 찍힌 사진 게재 금지를 위반한 출판사에 어떠한 금전적 지급 명령도 내리지 않은 것과 관련하여 제 8 조 위반이 아니라고 판단하였다. 재판소는 출판금지명령을 위반한 출판사가 피해자에게 직접 금전을 지급하도록 명령해야만 개인의 사생활을 실효적으로 보호할 수 있다는 원칙을 협약 제 8 조에서 도출할 수는 없음을 명확히 하였다. 다만 이는 국가가 판단재량 범위 내에서 피해자에게 실효적일 다른 구제수단을 제공하고, 그러한 구제수단이 주장된 침해에 대한 권리구제 기회를, 비례성을 상실한 방식으로 제한하지 않는다는 것을 전제로 한다(*ibid.*, § 75).

B. 데이터 보호의 두 가지 측면(소극적 측면 및 적극적 측면)

39. 협약 제 8 조의 본질적 목적은, 개인이 사생활과 가족생활, 주거 및 통신 존중권을 향유하는 데 있어, 공권력 또는 국가가 권한을 위임한 민간단체의 자의적 제한을 받지 않도록 개인을 보호하는 것이지만, 국가는 이러한 권리에 대한 효과적인 존중을 보장할 특정한 적극적 의무를 국가에 부과할 수도 있다(*Bărbulescu v. Romania* [GC], 2017, § 108).

73. 개인데이터 보호를 제한하는 조치를 전적으로 사적 영역에 있는 개인 또는 단체가 취한 경우, 재판소는 국가의 적극적 의무 관점에서 사건을 심리한다(*Craxi v. Italy (no. 2)*, 2003, §§ 68-76; *Köpke v. Germany* (dec.), 2010; *Alkaya v. Turkey*, 2012, § 32; *Söderman v. Sweden* [GC], 2013, § 89; *Bărbulescu v. Romania* [GC], 2017, § 111; *López*

Ribalda and Others v. Spain [GC], 2019, § 111; *Buturugă v. Romania*, 2020, §§ 60-63; *Volodina v. Russia (no. 2)*, 2021, §§ 58-68; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, § 111; *Tena Arregui v. Spain*, 2024, § 35). 다만, 그 조치의 주체가 공공단체(*Copland v. the United Kingdom*, 2007, § 39; *Libert v. France,* 2018, § 41; *Drelon v. France*, 2022, § 85; *Cherrier v. France*, 2024, § 57), 국가가 의무를 위임한 민간단체(*Vukota-Bojić v. Switzerland*, 2016, § 47) 또는 법적 요건을 따르는 민간단체(*Podchasov v. Russia*, 2024, § 52)인 경우, 재판소는 국가의 소극적 의무 관점에서 사건을 심사한다. 재판소는 해당 제한이 협약 제 8 조제 2 항의 요건인 법에 따른 것인지, 정당한 목적을 추구하였는지 및 민주사회에서 필요한지 확인해야 한다. 이 문제는 아래 데이터 보호에 관한 세 가지 "심사 기준"에서 상세히 검토한다.

74. *Vukota-Bojić v. Switzerland*, 2016 사건 § 47 에서 재판소는, 국가는 의무를 민간단체나 개인에게 위임하는 방식으로 협약상 책임에서 벗어날 수는 없다고 강조하였다. 개인데이터를 수집·저장한 민간 보험회사가 국가 보험제도를 운영하고 있었고, 국내 법제가 공권력으로 간주하였으므로, 해당 회사는 공권력으로 간주되어야 했고, 회사의 행위는 피청구국에 귀속되었다(*ibid.*, § 47).

75. *Libert v. France,* 2018 사건 §§ 37-41 에서 재판소는, 개인용 파일을 업무용 컴퓨터에서 열었다는 혐의를 받은 청구인의 고용주인 국영철도공사(SNCF)가 제 8 조의 목적상 공권력을 간주될 수 없다는 정부의 이의를 기각하였다. 비록 직원들이 사법상 근로계약에 따라 고용되었다고 하더라도, 해당 회사는 공법상 법인이며 국가의 감독 대상이고 국가가 임명한 이사진이 운영하였으므로 사실상 국가가 보증하는 지위에 있었다.

76. 학교 직원의 전화 통화, 전자우편 및 인터넷 접속을 감시한 사건에서 재판소는, 학교가 협약의 목적상 정부가 책임지는 공적 기관이었으므로, 분석해야 할 쟁점은 국가가 청구인의 사생활 및 통신을 제한하지 않을 소극적 의무와 관련된 것이라고 보았다(*Copland v. the United Kingdom*, 2007, § 39).

77. *Liebscher v. Austria*, 2021 사건에서 청구인은 부동산 지분을 전 부인에게 이전하기 위하여 이혼 합의서의 (발췌본이 아니라) 전부를 제출해야 할 의무에 대하여 이의를 제기하였다. 해당 이혼 합의서에는 미성년 자녀들과 전 배우자의 이름 및 거주지, 양육비 지급액 및 양육권 합의, 부동산 이외의 재산분할 합의, 청구인의 소득과 재산 내역도 들어 있었다. 부동산 이전 및 그에 관한 확인 문서 전체(이혼 합의서 포함)는 공개된 등기부에 기록되어 누구든 제한 없이 열람할 수 있었다. 재판소는 이 사건을, 사생활 존중을 보장하기

위해 고안된 조치를 채택해야 할 국가의 적극적 의무(규제 체계 준비 및 적절한 경우 구체적인 조치 이행 포함) 관점에서 접근하였다(*ibid.*, §§ 60-61).

78. 협약상 국가의 적극적 의무와 소극적 의무 사이의 경계를 명확하게 정의하기는 어렵지만, 적용되는 원칙은 유사하다. 두 맥락 모두, 국가가 향유하는 판단재량의 범위에 따라 달라지기는 하지만, 개인의 이익과 공동체 전체의 이익 사이에서 적절한 균형에 도달해야 한다는 점을 특히 고려해야 한다(*Bărbulescu v. Romania* [GC], 2017, § 112; *Tena Arregui v. Spain*, 2024, § 32).

79. 개인데이터 보호 문제를 제기하는 사건에서, 유럽평의회 회원국 간 쟁점이 되는 이익의 중요성이나 이를 보호하는 최선의 수단에 관한 합의가 없는 경우(*Odièvre v. France* [GC], 2003, § 47; *Breyer v. Germany*, 2020, § 108; *Gauvin-Fournis and Silliau v. France*, 2023, § 111), 쟁점이 된 순수한 금융자료가 청구인의 신원과 밀접하게 관련되어 있지 않은 경우(*G.S.B. v. Switzerland*, 2015, § 93) 및 국가안보 사안인 경우(*Leander v. Sweden*, 1987, § 59), 재판소는 국가가 더 넓은 판단재량을 누린다고 판단하였다. 반대로, 개인데이터가 자동처리 대상이 되어 접근과 유포가 매우 쉬워지는 바람에 개인의 평판을 해치고 일상생활을 어렵게 할 수 있는 경우라면 국가 당국이 누릴 수 있는 판단재량의 범위가 좁아진다고 판단하였다(*Khelili v. Switzerland*, 2011, §§ 64, 70). 이는 특히 개인의 유전자 구성이 담겨 있고 본인과 그 가족에게 매우 중요한 DNA 정보 같은 민감한 데이터의 범주를 보호할 때도 똑같이 고려해야 한다(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 102-103).

80. 협약상 권리와 자유의 실효적 보호를 보장해야 하는 국가 고유의 적극적 의무로는, 구(舊) 국가 비밀 정보기관이 체계적으로 저장한 개인의 오랜 과거에 관한 정보에 합리적인 기간 내에 접근할 수 있도록 개인에게 보장할 의무(*Haralambie v. Romania*, 2009, § 79; *Jarnea v. Romania*, 2011, § 50; *Joanna Szulc v. Poland*, 2012, § 87), 이해관계자가 자신의 아동기 및 초기 발달 사항을 확인하고 이해하려면 필요한 정보를 수령할 수 있도록(*Gaskin v. the United Kingdom*, 1989, § 49) 또는 자신의 신원을 알 수 있도록(*Odièvre v. France* [GC], 2003, § 42; *Gauvin-Fournis and Silliau v. France*, 2023, § 110) 또는 자신이 노출된 건강상 위험을 파악할 수 있도록(*Guerra and Others v. Italy*, 1998, § 60; *McGinley and Egan v. the United Kingdom*, 1998, § 101; *Roche v. the United Kingdom* [GC], 2005, § 162) 공권력이 수집·저장한 "모든 적절한 유관 정보"에 접근할 "실효적이고 이용 가능한 절차"를 개인에게 보장할 의무 등이 있다.

81. 다만 재판소는, 국가 당국이 개인에 관하여 수집한 민감한 국가안보 정보의 맥락이라면, 이러한 적극적 의무가 당국에 부과되지 않는다고 보았다(*Leander v. Sweden*, 1987, § 51).

82. 따라서, 학교 총격 관련 *Kotilainen and Others v. Finland*, 2020 사건 § 83 에서 재판소는 당국에 청구인들 친족들의 생명을 보호할 적극적 의무가 있다고 하여도, 협약 제 2 조의 실체적 측면에 따라, 경찰이 총격 사건 이전에 의료기록과 군 관련 기록을 입수하여 가해자의 정신 건강에 관한 자료를 확인할 의무로 확장되는 것은 아니라고 보았다. 경찰이 개인 의료자료에 접근하는 것이 일상적인 조치가 될 수는 없으며, 반드시 구체적인 필요성과 정당화 요건에 따라야 한다.

83. 개인간 중대행위라는 맥락처럼 개인데이터 문제가 야기되는 상황에서 협약상 권리를 실효적으로 향유하려면 이러한 권리를 보호하는 구체적인 입법을 마련해야 한다. 따라서 *Söderman v. Sweden* [GC], 2013 사건 §§ 86-117 에서 재판소는, 나체 아동을 비밀리에 또는 동의 없이 동영상·사진 촬영한 단발적 행위가 처벌되지 않은 것은 명확한 입법 규정의 부재 때문이었으며, 그 당시 다른 형사법 규정으로도 보완되지 않았고 민사적 구제수단 또한 실효적이지 않았다는 점을 고려할 때, 제 8 조 위반이라고 판단하였다(*ibid.*, §§ 108-114). 마찬가지로 *K.U. v. Finland*, 2008 사건 §§ 49-50 에서는, 미성년자를 대상으로 한 외설적 광고를 데이트 사이트에 게시한 인물의 신원을 인터넷 접속 제공자에게 공개하도록 당국이 강제할 법적 근거가 부재하였다는 점에서 제 8 조 위반이라고 판단하였다. 입법자는 이러한 맥락에서 상충하는 다양한 보호 요구를 조정할 수 있는 체계를 제공해야 한다. *Khadija Ismayilova v. Azerbaijan*, 2019 사건 §§ 105-132 는 기자가 자택에서 비밀리에 촬영당하고 그 영상이 공개적으로 유포된 사안이었다. 이 사건에서 해당 행위는 형사법상 처벌 대상이었고 형사 수사가 개시되었다. 그런데도 재판소는, 사생활이 매우 심각하게 제한되었지만, 당국은 실효적인 형사 수사로 충분히 보호하지 못하였기 때문에 청구인의 사생활을 보호한다는 적극적 의무를 이행하지 않았다고 판단하였다(*ibid.*, §§ 119-131). *Volodina v. Russia (no. 2)*, 2021 사건 § 68 에서는, 배우자가 청구인의 이름으로 허위 프로필을 만들고 내밀한 사진을 게시하며 행방을 추적하고 소셜미디어를 통해 살해 위협을 보내는 방식으로 반복적인 사이버폭력을 가했지만, 당국이 보호하지 않았다고 청구인이 이의를 제기하였다. 재판소는 특히, 청구인의 배우자를 기소할 법적 수단이 있었던 당국은 실효적인 수사를 진행하지 않았고 어떠한 시점에서도 청구인을 보호하기 위한 적절한 조치를 고려하지 않았다고 판단하였다. 따라서 당국은 청구인이 심각한 학대를 당하지 않도록 보호할 의무를 다하지 못하였다.

84. 직장 내 근로자 점검·확인처럼 개인 간 심각성이 덜한 행위인 경우, 국가는 영상 감시(*López Ribalda and Others v. Spain* [GC], 2019, § 113; *Köpke v. Germany* (dec.), 2010)

또는 근로자의 비업무적 서신 및 통신 감시(*Bărbulescu v. Romania* [GC], 2017, § 119)에 관한 구체적 입법 마련 여부를 선택할 수 있다. 다만 입법 여부와 관계없이, 국내 법원은 고용주가 근로자의 사생활이나 통신 존중권을 제한하는 감시 조치를 시행할 때 그러한 조치가 비례성을 갖추고 남용을 방지할 적절하고 충분한 보호조치를 수반하도록 보장하여야 한다(*Köpke v. Germany* (dec.), 2010; *Bărbulescu v. Romania* [GC], 2017, § 120; *López Ribalda and Others v. Spain* [GC], 2019, § 116; 또한, 정당이 당원들의 전자 통신을 점검·확인한 맥락에서는 *Tena Arregui v. Spain*, 2024, § 38 참조).

85. 개인데이터 공개와 관련된 다른 여러 사건에서 재판소는, 제 8 조 위반 주체가 사인(私人)이든 공적 당국이든 관계없이, 위반 의혹이 있으면 조사할 적극적 의무가 국가에 있다고 판단하였다. 따라서, 부패 사건 형사 절차의 맥락에서 도청된 정치인의 전화 통화 녹취록이 법정에서 낭독되고 언론에 공개된 *Craxi v. Italy (no. 2)*, 2003 사건 §§ 68-76 에서 재판소는 이러한 사적 대화가 공적 영역으로 유출되는 것을 방지할 적극적 의무를 국가가 부담한다고 보았다. 통화 내용이 언론을 통해 폭로된 것은 검사의 행위에 따른 직접적 결과가 아니라, 국내 법원 등기과(登記課)의 기능 장애로 발생한 것으로 보였으므로, 재판소는 당국이 적절한 보호조치를 제공하고 실효적으로 조사하여 청구인의 권리를 실효적으로 보호하도록 조처하지 않았다는 점에서 제 8 조 위반이라고 판단하였다.

86. *Alkaya v. Turkey*, 2012 사건 §§ 30-40 에서 재판소는 유명 여배우의 자택 주소 전체가 공개된 사안에서 국내당국의 보호는 개인정보를 보호할 정도가 아니었다고 결론지었다. 재판소는, 신문사가 여배우의 주소를 공개하기로 한 결정이 공익을 근거로 정당화될 어떠한 증거도 발견하지 못하였고, 신문에 자택 주소가 게재되는 것이 청구인의 생활에 미칠 파급효과를 국내 법원이 고려한 것처럼 보이지 않는다고 평하였다. 국내 법원이 상충하는 이해관계를 평가하지 않았기 때문에 국가가 제 8 조에 따른 적극적 의무를 이행한 것으로 간주할 수 없다.

87. 가정 폭력의 맥락인 경우, 청구인의 전남편이 페이스북 등 청구인의 전자 계정을 무단으로 열람하고 사적 대화·문서·사진을 복사한 *Buturugă v. Romania*, 2020 사건 §§ 73-78 에서 재판소는, 청구인의 통신 비밀이 침해된 것을 조사해야 할 의무가 당국에 있었다고 판단하였다. 재판소는, 사이버 괴롭힘이 여성 및 여아에 대한 폭력의 한 측면으로 인정되고 그 형태는 사생활의 비밀에 대한 사이버 침해, 피해자의 컴퓨터 해킹, 데이터와 이미지(내밀한 세부 사항)의 절취·공유·조작 등 다양하게 나타날 수 있다는 점을 인정하면서, 배우자의 통신을 부적절하게 감시·접근·저장하는 행위는 가정폭력 사건을 수사할 때 국내 당국이 고려할 수 있음을 수용하였다. 통신의 비밀성 침해에 관한 주장이 제기되면, 당국은 가능한 모든 형태의 가정폭력 현상을 종합적으로 파악하기 위하여 본안을 심사하여야 한다(*ibid.*,

§§ 76-77). 그러한 본안 심사가 없었으므로 제 8 조가 위반되었다(또한, 맥락이 비슷한 *Volodina v. Russia (no. 2)*, 2021, §§ 48-68 참조).

C. 데이터 보호에 관한 세 가지 "심사 기준"

88. 제 8 조제 2 항에 따르면, 보호되는 권리의 향유에 제한을 가하려면 그러한 제한은 "법에 따른 것"이어야 하고, "정당한 목적"을 추구해야 하며, "민주사회에서 필요한 것"이어야 한다.

1. 법에 따른 제한인가

89. 재판소는 여러 사건에서, *협약 108* 제 5 조에 명시된 바와 같이 자동처리되는 개인데이터가 공정하고 적법하게 수집·처리되어야 한다는 요건이 충족되었는지 심사하였다. 다수의 사건에서 재판소는 유관 권리를 제한할 수 있는 조치를 승인할 국내법적 근거가 없다는 이유만으로 제 8 조 위반이라고 판단하였다(*Taylor-Sabori v. the United Kingdom*, 2002, §§ 17-19; *Radu v. Moldova*, 2014, § 31; *Mockutė v. Lithuania*, 2018, §§ 103-104; *M.D. and Others v. Spain*, 2022, §§ 61-64; *Kaczmarek v. Poland*, 2024, §§ 74-80).

90. 특히, *Mockutė v. Lithuania*, 2018 사건 §§ 103-104 에서 재판소는, 정신병원이 성인인 청구인의 건강 정보를 청구인의 어머니와 기자들에게 전달한 것과 관련하여, 정부도 국내 법원도 그에 대한 법적 근거가 될 수 있는 어떠한 규정도 제시하지 못했다고 하였다. 경찰이 청구인의 호출기를 "복제"하여 감시 대상으로 삼은 *Taylor-Sabori v. the United Kingdom*, 2002 사건 §§ 17-19 에서는 사설 통신망으로 전송된 호출기 메시지 가로채기를 규제하는 법률상 제도가 존재하지 않았다. *Radu v. Republic of Moldova*, 2014 사건 § 31 에서 공립병원이 청구인의 임신, 건강 상태, 치료에 관한 의료 정보를 청구인의 고용주에게 유포한 것은 "법에 따른 것"이 아니었다. *M.D. and Others v. Spain*, 2022 사건 §§ 61-64 에서는, 카탈루냐에서 직무를 수행하던 판사와 치안판사들이 이른바 "결정권"을 카탈루냐인들이 행사할 가능성을 지지하는 법적 견해를 밝히는 선언문에 서명한 것과 관련하여 경찰이 작성한 보고서에는 청구인 일부의 개인데이터, 사진, 직업 관련 정보 및 정치적 견해가 들어 있었다. 재판소는, 경찰의 보고서 작성이 법에 근거한 것이 아니었고, 공권력이 개인데이터를 수집 목적과는 다른 목적으로 사용하였으므로, 범죄와 아무 관련이 없는 행위를 한 개인들을 대상으로 작성한 경찰 보고서가 존재한다는 사실만으로도 협약 제 8 조 위반에 해당한다고 평하였다. 청구인의 전화 통화 녹음이 기자회견에서 공개된 *Kaczmarek v. Poland*, 2024 사건 §§ 74-80 에서 재판소는 주로 수사 과정에서의 기록 열람 및 사본 제작에 관한 형사소송법 규정은 그러한 공개의 법적 근거로 볼 수 없다고 판단하였다.

91. 다른 여러 사건에서 재판소는, 개인데이터를 보호해야 할 국내법이 접근 불가능하거나 비밀로 유지되었다는 이유로(*Vasil Vasilev v. Bulgaria*, 2021, §§ 169–170; *Nuh Uzun and Others v. Turkey*, 2022, §§ 80–99) 또는 충분히 명확하고 예측 가능하지 않다는 이유로(*Vukota-Bojić v. Switzerland*, 2016; *Ben Faiza v. France*, 2018, §§ 58–61; *Benedik v. Slovenia*, 2018*; Rotaru v. Romania* [GC], 2000; *Zoltán Varga v. Slovakia*, 2021, § 162; *Haščák v. Slovakia,* 2022, §§ 94–95; *Kaczmarek v. Poland*, 2024, §§ 93–96) 제 8 조 위반이라고 판단하였다. 예를 들어, *Nuh Uzun and Others v. Turkey*, 2022 사건 §§ 80–99 에서, 수용자(收容者)의 서신은 법무부가 검사와 교정당국을 직접적이고 구체적인 대상으로 지정하여 내린 지침에 따라 스캔 되어 국가사법망 서버에 업로드했는데, 그러한 지침은 일반 국민은 물론 청구인들에게도 공개되지 않았다. *Vukota-Bojić v. Switzerland*, 2016 사건 §§ 71–77 에서, 교통사고 이후 청구인이 가입한 보험회사가 청구인을 대상으로 실시한 비밀 감시의 근거가 된 법률 규정은, 보험 분쟁에서 공권력으로 기능하는 보험회사가 피보험자들을 비밀리에 감시하도록 부여된 재량의 범위와 행사 방식에 대하여 충분히 명확하게 규정하지 않았다. 루마니아 정보기관이 보유한 개인정보에 관한 *Rotaru v. Romania* [GC], 2000 사건 §§ 57–62 에서 국내법은 어떤 유형의 정보가 처리될 수 있는지, 어떤 범주의 개인을 대상으로 어떠한 상황에서 감시 조치할 수 있는지, 어떠한 절차가 뒤따라야 하는지 규정하지 않았다. *Benedik v. Slovenia*, 2018 사건 § 132 에서는 경찰이 동적 IP 주소와 연결된 가입자의 자료를 확보하기 위해 적용한 특정 법률 규정이 명확성을 결여하였고, 남용에 대한 보호조치나 해당 경찰 권한에 대한 독립적인 점검·확인이 존재하지 않아 자의적 제한에 대한 방어가 전혀 이루어지지 않았다. 마찬가지로 *Kaczmarek v. Poland*, 2024 사건 §§ 93–96 에서는, 청구인이 그 대상자가 아니었던 보안 작전 과정에서 수집된 청구인 관련 감시자료를 당국이 계속 보관한 것은 충분히 명확하지 않은 법률 규정에 근거하였고, 어떠한 절차적 보장도 마련되지 않아 청구인이 해당 자료의 폐기를 요구할 수 없게 된 결과를 낳았다.

92. 마찬가지로, *A.R. v. the United Kingdom*, 2025, § 54 에서, 청구인은 경찰이 강화된 고용 심사 과정에서 자신이 강간 혐의로 기소되었다가 재판에서 무죄 판결을 받았다는 정보와 혐의 범죄의 정황을 공개한 것에 대해 불만을 제기했다. 재판소는 관련 시점에 시행 중이던 법률 조항과 적용 가능한 지침을 고려할 때, 관할 당국에 지나치게 광범위한 재량권을 부여했다고 판단했다. 이러한 재량권의 자의적 행사를 방지할 충분한 법적 보호를 제공할 충분한 안전장치가 없었으므로, 해당 공개는 법률에 부합하지 않았다(*ibid.*, § 68).

93. 이와는 대조적으로, 국내법이 명확하고 예측할 수 있으며 잠재적 남용에 대한 보호조치가 충분하므로 제 8 조 위반이 아니라고 판단한 사건도 있다(*Satakunnan*

Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 2017, § 154; *Ben Faiza v. France*, 2018, § 75). *Ben Faiza v. France*, 2018 사건 §§ 70-76 에서, 이동통신 서비스 제공자로부터 청구인에 관한 개인정보(통화 내용 미포함)를 확보하기 위해 발부한 법원 명령은 "법에 따른 것"이었다. 이러한 법원 명령은 유관 법률상 제도로 승인하고 규율하였으며, 무효의 위험을 감수하고라도 사전에 검사의 승인을 받아야 했고 사법심사 대상이었으며 불법이 있으면 확보된 정보는 증거에서 배제될 수 있었다는 점에서 자의성을 방지하는 보호조치 또한 존재하였다(*ibid.*, § 73).

94. 재판소는, 데이터보호위원회의 결정(국내 법원이 승인함)으로 세금자료의 광범위한 공개를 금지한 *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 사건 § 154 에서 유사한 결론에 도달하였다. 유관 데이터보호법의 문언과, 그 법이 유럽연합사법재판소(CJEU)가 핀란드 법원에 제공한 지침에 따라 적용된 방식은 충분히 예측 가능하였다. 이 사건이 개인데이터법상 최초의 사례였고, 최고행정법원이 데이터보호지침에 규정된 이행정지의 해석에 관하여 CJEU 의 지침을 구하였다고 하더라도, 국내 법원이 언론 목적에 따른 이행정지를 해석·적용한 것이 자의적이거나 예측 불가능한 것이 되지는 않았다(*ibid.*, § 150). 청구인 회사들이 언론 전문기관이었으므로, 관련 핀란드 및 유럽연합 법령에 따라 데이터를 대량 수집하고 전면적으로 유포한 것이 "순전히" 언론목적의 처리로 보이지 않을 수도 있다는 점을 인식해야 했다(*ibid.*, § 151).

95. *Le Marrec v. France* (dec.), 2024 사건 §§ 72-75 에서 재판소는 특히 IP 주소 처리와 관련된 구체적 조항도 포함된 규정이 해당 사회보장 당국의 웹사이트에 게시되어 일반 대중도 접근할 정도였으므로, 협약 제 8 조의 "합법성" 요건을 충족한다고 판단하였다.

96. 마지막으로, 제한이 "법에 따른 것"이라는 요건과 "민주사회에서 필요한" 것이라는 기준은 매우 밀접하게 연결되어 두 가지 요건을 함께 논의해야 한다고 재판소가 판단한 사건도 있었다(*S. and Marper v. the United Kingdom* [GC], 2008, § 99; *Kvasnica v. Slovakia*, 2009, § 84; *Kennedy v. the United Kingdom*, 2010, § 155; *Glukhin v. Russia*, 2023, § 78).

97. 통신 가로채기 같은 비밀 감시 조치의 구체적인 맥락에서 재판소는 "예측가능성"을 다른 분야에서와 동일하게 이해할 수는 없다고 판단하였다. 재판소의 견해에 따르면, 당국이 언제 그렇게 조처할 가능성이 있는지 개인이 사전 예측하여 그에 따라 행위를 조정할 수 있어야 한다는 의미일 수는 없다(*Adomaitis v.Lithuania*, 2022, § 83; 또한, 사인(私人)이 비밀리에 영상을 녹화한 맥락에서 동일한 원칙을 적용한 *Sârbu v. Romania*, 2023, § 51 참조). 다만, 특히 행정부에 부여된 권한이 비밀리에 행사된다면, 자의적으로 제한할 위험이 명백히

존재한다. 따라서, 특히 사용할 수 있는 기술이 점점 정교해지고 있으므로, 비밀 감시 조치에 관한 명확하고 상세한 규정을 마련해야 한다. 국내법은 공권력이 언제, 어떠한 조건에서 그렇게 조처할 권한이 생기는지 시민들이 적절히 알 수 있을 정도로 명확해야 한다(*Malone v. the United Kingdom*, 1984, § 67; *Leander v. Sweden*, 1987, § 51; *Valenzuela Contreras v. Spain*, 1998, § 46; *Weber and Saravia v. Germany* (dec.), 2006, § 93; *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007, § 75; *Roman Zakharov v. Russia* [GC], 2015, § 229; *Denysyuk and Others v. Ukraine*, 2025, § 88). 또한, 관할 당국에 부여된 그러한 재량의 범위와 그 행사 방식을 법으로 명확히 규정하여 개인이 자의적으로 제한되지 않도록 적절히 보호하여야 한다(*Roman Zakharov v. Russia* [GC], 2015, § 230).

98. 형사수사 맥락의 통신 가로채기에 관한 판례에서 재판소는 권한 남용을 방지하기 위하여 법률에 최소한 규정되어야 하는 여섯 가지 요소를 ▲가로채기 명령을 내 수 있는 범죄의 성격 ▲가로채기 대상이 될 인물 범주의 정의 ▲조치 집행의 기간 제한 ▲수집된 자료의 심사·사용·저장 시 따라야 할 절차 ▲자료를 다른 당사자에게 전달할 때 주의사항 ▲가로챈 자료가 삭제 또는 폐기될 수 있거나 되어야 하는 상황이라고 결정하였다(*Huvig v. France*, 1990, § 34; *Valenzuela Contreras v. Spain*, 1998, § 46; *Weber and Saravia v. Germany* (dec.), 2006, § 95; *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007, § 76; *Denysyuk and Others v. Ukraine*, 2025, § 88). *Roman Zakharov v. Russia* [GC], 2015 사건 § 238 에서, 재판소는 이러한 최소한의 보호조치가 국가안보를 이유로 가로채기가 집행된 사건에도 동일하게 적용된다고 확인하였지만, 문제 된 입법이 제 8 조와 양립할 수 있는지 판단하기 위하여 비밀 감시 조치의 집행을 감독하는 장치, 통지 제도, 국내법상 제공되는 구제수단 등도 고려하였다[3].

99. 당국이 수집하고 범죄 예방·처벌 관련 목적으로 데이터베이스에 저장한 개인데이터라는 맥락에서 재판소는 이러한 조치의 범위와 적용을 규율하는 명확하고 상세한 규정을 반드시 마련하되, 최소한의 보호조치(기간, 저장, 사용, 제 3 자의 접근, 데이터의 무결성과 기밀성을 보존하는 절차 등)도 함께 마련하여 남용과 자의의 위험을 방지할 정도의 보장책을 제공해야 한다고 지적하였다(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 99, 103; *Nuh Uzun and Others v. Turkey*, 2022, § 86). 재판소는 국내법이 국내 당국에 부여된 재량의 범위와 행사 방식을 명확할 정도로 규정하지 않은 경우 제 8 조 위반이라고

[3] 또한, 통신 감청, 전화 감청 및 비밀 감시에 관한 법의 예측가능성 요건은 협약 제 8 조에 대한 해설서 – 사생활 및 가족생활을 존중받을 권리 참조.

판단하였다(*Shimovolos v. Russia*, 2011, § 70; *Dimitrov-Kazakov v. Bulgaria*, 2011, § 33; *Negru v. the Republic of Moldova*, 2023, § 34). *Shimovolos v. Russia*, 2011 사건 § 69 에서는, 인권운동가의 행방에 관한 데이터 등 개인데이터를 저장하는 감시 데이터베이스의 생성·유지와 운영 절차가 한 번도 공개되거나 일반에 제공된 적 없는 장관령으로 규율되었다. *Dimitrov-Kazakov v. Bulgaria*, 2011 사건 § 33 에서는 경찰 등록부에 개인을 "범법자"로 등록한 것이 당시 비공개 지침에 근거하였는데, 이 지침은 본질적으로 비밀성이 있었고 후에 비밀 해제 전까지 내무부 내부용으로만 사용되었다. *Negru v. the Republic of Moldova*, 2023 사건 § 24 에서는 청구인이 수배자 명단에 등록되었는데, 이는 범죄, 형사사건 및 범법자를 기록하는 국가 통합 전산정보시스템에서 개인데이터가 처리된 것을 의미하였고, 검사의 결정에 따라 절차적 명확성이 결여된 상태에서 사실상 무제한적 권한으로 평가된 재량이 행사된 결과 경찰서 공개 구역에 청구인의 사진이 게시되었다.

100. *Catt v. the United Kingdom*, 2019 사건 §§ 97, 106 에서 재판소는 개인데이터의 수집 및 보유를 위하여 당국이 사용한 법적 근거가 국내법상 모호하게 정의된 개념에서 비롯되어 모호성의 위험이 있다고 강조하였다.

101. 안면인식기술의 구현과 관련하여 재판소는 "양질의 법률" 요건에 부합하려면 조치의 범위와 적용을 규율하는 상세한 규정과 더불어 남용과 자의의 위험을 방지할 강력한 보호조치가 필수라고 강조하였다. 실시간 안면인식기술을 사용한다면 이러한 보호조치가 더 필요하다(*Glukhin v. Russia*, 2023, § 82). 재판소는 이 사건에서 처음으로 이러한 기술 사용 문제를 심리하면서, 안면인식기술을 포함한 개인 생체 데이터의 처리를 "사법행정과 관련하여" 허용하는 국내 법률 규정이 광범위하여 사실상 모든 형태의 사법절차와 관련하여 그러한 데이터처리를 허용하는 것처럼 보였기 때문에, "양질의 법률" 요건을 충족하는지 강하게 의문을 표시하였다. 국내법에는 안면인식기술 사용을 초래할 수 있는 상황의 성격, 그 목적, 대상이 될 수 있는 인물 범주 또는 민감한 개인데이터의 처리에 관한 어떠한 제한도 존재하지 않았다. 더욱이 안면인식기술 사용에 수반되는 절차적 보호조치(승인 절차, 확보된 데이터의 심사·사용·저장 절차, 감독 통제 장치 또는 가용 구제수단 등)도 존재하지 않는 것으로 보였다(*ibid.*, § 83).

2. 정당한 목적을 추구한 제한인가

102. 다수의 사건에서 재판소는 *협약 108* 제 5 조에 명시된 자동처리되는 개인데이터는 명시적이고 구체적이며 정당한 목적을 위하여 수집되어야 한다는 요건을 지켰는지 심사하였다. 이러한 여러 사건에서 제 8 조제 2 항에 열거된, 권리 행사 제한을 정당화할 수

있는 정당한 목적인지 심사하는 것은 비교적 간단하다. 정당한 목적으로는 국가안보, 공공의 안전 및 국가의 경제적 복리의 보호, 무질서 또는 범죄의 방지, 보건 또는 도덕의 보호, 타인의 권리와 자유의 보호가 있다. 재판소는 대체로 정부가 주장한 정당한 목적이 하나 이상 존재하는지 확인한다.

103. 재판소는 예를 들어, 개인의 사생활에 관한 데이터를 비밀경찰 등록부에 저장한 후 그 데이터를 국가안보상 요직 후보자에 대한 신원 심사에 사용하는 것은 협약 제 8 조의 목적상 정당한 목적인 국가안보의 보호를 추구한 것이라고 보았다(*Leander v. Sweden*, 1987, § 49). 또한, 테러 조직이 했다고 주장하는 여러 건의 살인미수 사건을 수사하고 추가 폭탄 테러를 방지하기 위해 검사가 명한 GPS 를 이용한 청구인 감시 역시, 국가안보와 공공의 안전, 범죄 예방 및 피해자 권리 보호라는 이익에 기여하였다고 보았다(*Uzun v. Germany,* 2010, § 77).

104. 재판소는 또한, 양자 협정에 따라 은행에서 얻은 데이터를 다른 국가 당국에 전달한 조치는 국가의 경제적 복리를 보호하는 역할을 했기 때문에 정당한 목적을 추구하였다고 판단하였다(*G.S.B. v. Switzerland*, 2015, § 83). 은행 부문은 피청구국에 매우 중요한 경제 분야였으므로, 문제 된 조치는 "스위스 경제에서 주요한 역할을 하며 다수의 인력을 고용하고 있는" 은행과 미국 세무당국 간 분쟁을 해결하기 위한 스위스 정보의 전방위적인 노력의 일환이었으므로, 국가의 경제적 복리 보호에 기여하였다고 보는 것이 정당할 수 있다(*ibid.*, § 83).

105. 재판소는, 도핑과의 싸움에서 근본을 이루는 것은 공정성과 기회 평등이라는 국제 규범을 참고하면서, 스포츠에서 도핑 문제에 대응할 필요성을 고려할 때 선수들의 소재를 파악할 의무는 보건 및 도덕의 보호라는 정당한 목적에 부합한다고 판단하였다(*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, 2018, §§ 164-166). 재판소의 견해에 따르면, 정부가 스포츠에서 공정하고 의미 있는 경쟁을 보장하려는 노력의 맥락에서 "도덕"이라고 설명한 것은 또한, 도핑을 사용하여 다른 선수보다 우위를 확보하려는 것은 아마추어 선수들과 특히 청소년이 경기력 제고를 위해 따라 하게 하는 위험한 유인을 제공하며 관중에게 기대할 권리가 있는 공정한 경쟁을 박탈하는 것이기 때문에, "타인의 권리와 자유의 보호"라는 정당한 목적과도 연결된다(*ibid.*, § 166).

106. *Ben Faiza v. France*, 2018 사건 § 77 에서 재판소는 이동통신 서비스 제공자로부터 청구인에 관한 개인정보(통화 내용 미포함)를 확보하려 발부된 법원 명령이, 조직범의 마약 밀수, 범죄단체 조직, 자금세탁과 관련한 형사절차의 맥락에서 진실을 규명하기 위한

것이라고 판단하였다. 따라서 이 조치는 무질서·범죄 예방 또는 공중보건 보호라는 정당한 목적을 추구하였다.

107. 교도소장이자 부패 혐의가 있는 청구인의 전화 통화를 감청하고, 그 정보를 보관하며, 이를 징계절차에서 공개한 조치로 결국 청구인이 해임된 것은 부패 성격의 행위를 방지하고 공공 서비스의 투명성과 개방성을 보장할 목적이었다고 판단되었고 따라서 무질서 또는 범죄 방지 및 타인의 자유와 권리 보호라는 정당한 목적을 추구하였다 *Adomaitis v. Lithuania*, 2022 (§ 84). 재판소는 또한 직업 수행 중 사인(私人)이 대화를 비밀리에 촬영한 후 당국이 이를 부패 유죄 판결의 증거로 사용한 사안에 대해서도 유사한 판단을 내렸다(*Sârbu v. Romania*, 2023, § 54).

108. *López Ribalda and Others v. Spain* [GC], 2019 사건 §§ 118, 123 에서 고용주가 회사 재산을 보호하고 원활한 운영을 보장하기 위하여 절도 혐의 책임자를 밝혀내고 처벌하는 조처를 하여 발생하는 정당한 이익은 직장 내 근로자에 대한 영상 감시를 수반하는 조처를 할 정당한 근거가 된다.

109. 청구인의 성명 전체와 자택 주소가 포함된 신원 데이터를 납세 의무 불이행을 이유로 세무 당국이 웹사이트에 공개한 것은 "국가의 경제적 복리 ... 의 이익"뿐만 아니라 "타인의 권리와 자유의 보호"를 추구한 것으로 판단되었다(*L.B. v. Hungary* [GC], 2023, §§ 111–13). 같은 맥락에서, 청구인의 IP 주소와 기타 "접속 데이터"를 처리하여 유관 사회보장 당국이 청구인을 특정하고 복지 사기를 방지할 수 있게 한 것은, 국가의 경제적 복리의 이익과 범죄 예방의 이익에 부합하였다(*Le Marrec v. France* (dec.), 2024, § 76).

3. "민주사회에서 필요한" 제한인가

110. 제 8 조에 따라 개인데이터 보호를 제한하는 조치가 민주사회에서 필요하다고 인정되려면, "강력한 사회적 필요"를 충족해야 하고, 추구되는 정당한 목적에 비추어 비례성을 상실해서는 안 된다(*Z v. Finland*, 1997, § 94; *Khelili v. Switzerland*, 2011, § 62; *Vicent Del Campo v. Spain*, 2018, § 46). 정보가 원용하는 사유는 관련성이 있고 충분해야 한다(*Z v. Finland*, 1997, § 94). 이러한 모든 측면에 대한 일차적 판단은 국내 당국에 속하지만, 그 제한이 필요한 것인지 최종적으로 평가하는 권한은 협약 요건과의 합치 여부를 심사하는 재판소에 있다(*S. and Marper v. the United Kingdom* [GC], 2008, § 101).

111. 개인 간 중대행위로 협약 제 8 조 권리를 제한할 수 있을 정도라는 맥락에서, "민주사회에서 필요한"이라는 요건 충족 여부에 대한 재판소의 심사는 국가가 그러한 권리를 충분히 보호하는 구체적 입법을 마련한 방식을 문제로 삼는다(*K.U. v. Finland*, 2008,

§§ 43-50; *Söderman v. Sweden* [GC], 2013, §§ 80-83). 반면, 직장 내 근로자에 대한 영상 감시처럼 심각성이 덜한 개인 간 행위인 경우, 재판소의 심사는 국내 법원이 재판소 판례에서 확립된 여러 기준을 고려하여 상충하는 이해관계를 균형 있게 평가하였는지 살펴본다(*López Ribalda and Others v. Spain* [GC], 2019, §§ 116-117, § 122). 이러한 여러 기준을 심사할 때, 하나의 기준이 결여되었다면 다른 기준에서 도출되는 보호조치에 중요성이 더해지고 그 결함을 충분히 보완할 수도 있다(*ibid.*, § 131).

112. 일반적으로, 제 8 조에 따른 개인데이터 보호를 제한하는 조치가 "민주사회에서 필요한"이라는 요건을 충족하는지 확인하려는 재판소는 그 조치가 *협약 108* 제 5 조에 열거된 요건 중에서 특히 수집되는 데이터의 양을 최소화할 요건, 데이터처리를 그 목적에 따라 정확하고 적절하며 관련성 있고 과도하지 않게 할 요건, 저장 기간 제한 요건, 데이터를 수집된 목적에 맞게 사용할 요건, 처리 시 투명성 보장 요건을 준수하였는지 심사하였다.

a. 수집·기록되는 데이터양 최소화 요건

113. 재판소는 여러 사건에서 자동처리된 개인데이터는 그 데이터를 기록한 목적에 적절하고 관련성이 있으며 과도하지 않았는지 심사하였다(*L.L. v. France*, 2006, §§ 45-46; *Vicent Del Campo v. Spain*, 2018, § 51; *Khadija Ismayilova v. Azerbaijan*, 2019, § 147; *Kruglov and Others v. Russia*, 2020, § 132 마지막 부분 참조; *L.F. v. France* (dec.), 2024, § 34).

114. 재판소는, 압수된 청구인들의 전자기기에 저장된 데이터와 관련하여, 압수수색 과정에서 그 데이터양을 최소화하기 위한 어떠한 선별 절차도 따르지 않은 것으로 보인 경우(*Kruglov and Others v. Russia*, 2020, § 132 마지막 부분 참조), 소송 당사자가 아니었던 청구인을 직장 내 괴롭힘 행위의 행위자로 특정한 법원의 결정에서, 판사가 청구인의 실명을 기재하지 않거나 머리글자로만 지칭하여 낙인을 찍지 않을 수도 있었던 경우(*Vicent Del Campo v. Spain*, 2018, § 51), 한 기자의 자택에서 자신도 모르게 촬영된 내밀한 공간에서의 영상에서 도출된 개인데이터가 수사 진행 보고서에 과도하고 불필요한 방식으로 공개된 경우(*Khadija Ismayilova v. Azerbaijan*, 2019, § 147), 제 8 조 위반이라고 판단하였다.

115. 재판소의 견해에 따르면, 특정 범죄의 예방과 처벌에 기여하기 위한 데이터베이스의 구축은 그 안에 저장되는 정보를 최대화하려고 과도하게 추진하는 방식으로는 실행될 수 없다(*B.B. v. France*, 2009, § 62; *Gardel v. France*, 2009, § 63; *M.B. v. France*, 2009, § 54). 이러한 제도적 장치에 부여된 정당한 목적에 따라 지켜야 하는 비례성을 존중하지

않는다면, 국가가 자국 관할권 내 개인들에게 협약에 따라 보장해야 하는 권리와 자유에 초래할 심각한 침해가 그 이점을 상쇄할 것이다(*M. K. v. France*, 2013, § 35; *Aycaguer v. France*, 2017, § 34). 무차별적으로 무기한 보유하는 제도라는 맥락에서, "더 많은 데이터를 보유할수록 범죄 예방이 강화된다"는 주장은 마치 산 사람도 모자라 죽은 사람의 정보까지 저장해야 한다는 말과 다름없이 과도하고 무의미하다(*Gaughran v. the United Kingdom*, 2020, § 89).

116. *Catt v. the United Kingdom*, 2019 사건 § 122 에서, 평화적 시위자의 정치적 의견을 드러내는 개인정보를 경찰 데이터베이스에 보유하면서, 비례성을 상실한 이후에는 보유한 정보를 파기하는 실효적인 보호조치가 결여된 것은 제 8 조 위반이 되었다.

117. 반면, *협약 108* 제 6 조의 의미에서 "민감한" 데이터에 해당하지 않고, 개인이 당사자로 참여한 법적 절차와 관련된 사실적·객관적 정보에 한정된 개인데이터가 법무부 내부 데이터베이스에서 처리되면, 제 8 조의 요건을 위반하지 않았다(*L.F. v. France* (dec.), 2024, §§ 34 및 40). 마찬가지로, *Le Marrec v. France* (dec.), 2024 사건 §§ 78–79 에서 재판소는 청구인의 IP 주소 및 사회보장 당국이 처리한 기타 "접속 데이터"로 인해 청구인이 "타국"에 거주하는 것이 특정된 사실에 대하여, 위 협약 제 6 조의 의미에서 "민감한" 데이터가 아니고, 청구인의 가장 내밀한 측면이나 존재 또는 정체성의 특별히 중요한 요소와 관련된 것도 아니라고 지적하였고, 해당 데이터는 청구인에 관해 매우 대략적인 정보를 담고 있었으므로 국내 당국에는 폭넓은 판단재량이 부여되었다.

b. 데이터의 정확성 및 갱신 요건

118. 재판소는 당국이 저장한 데이터의 부정확함이 드러났거나, 데이터 주체가 그 정확성을 다투는 경우와 관련된 여러 사건을 심리하였다(형사절차에서 부정확한 경찰 기록에 관한 *Cemalettin Canlı v. Turkey*, 2008, §§ 34–37; 과거 "철위대" 운동에 가담했다는 보안당국의 수집 정보에 대해 개인이 다툴 수 없는 상황에 관한 *Rotaru v. Romania* [GC], 2000, § 36).

119. 당국이 수집·보유한 허위 또는 불완전한 개인정보는 데이터 주체의 일상생활에 어려움을 더할 수 있고(*Khelili v. Switzerland*, 2011, § 64), 명예를 훼손할 수 있으며(*Rotaru v. Romania* [GC], 2000, § 44), 해당 데이터가 여러 당국 간 전달된다면 데이터 주체의 권리를 보호하려 법으로 정해진 절차적 보호조치를 무력화할 수 있다(*Cemalettin Canlı v. Turkey*, 2008, §§ 42–43). 재판소는 또한 아무런 증명된 사실적 근거 없이 단순한 추측이나 가정에 근거하여 개인데이터를 수집하는 것은 부적절하다고 강조하였다(*Drelon v. France*, 2022, § 97).

120. 재판소의 견해에 따르면, 저장된 데이터의 정확성을 증명할 의무는 당국에 있다. *Khelili v. Switzerland*, 2011 사건 §§ 66-70 에서, 당국이 기록한 불법 매춘에 관한 막연하고 일반적인 혐의를 둘러싸고 불확실성이 존재하였는데도 경찰 기록에 "성매매 종사자"라는 단어를 수년간 보유한 것은, 당국의 모순된 태도, 특정 데이터의 정확성을 입증해야 하는 책임은 당국에 있다는 원칙, 해당 분야에서 국내 당국이 누리는 판단재량의 폭이 좁다는 점, 청구인의 제 8 조상 사생활 존중권에 대한 제한의 심각성을 고려할 때, "민주사회에서 필요한" 것이 아니었다. 마찬가지로 프랑스 헌혈 서비스가 청구인의 동성애 성향을 추정하여 헌혈자로 받아들이기를 거부한 *Drelon v. France*, 2022 사건 §§ 95-97 에서 재판소는, 개인데이터의 수집은 적확하고 정확한 사실적인 근거가 있어야 하지만, 해당 사건에서는 사전 의료진 면담에서 청구인이 자신의 성생활에 관한 질문에 답변을 거부했다는 이유만으로 청구인의 성생활 방식에 관한 결론을 내렸다고 평하였다.

121. 청구인이 세 차례의 조사를 받았고, 구 공산정권과 협력한 공무원 공개에 관한 법률에 따라, 보관 자료를 근거로 하여 구 보안기관 협력자로 표시된 *Anchev v. Bulgaria* (dec.), 2017 사건 §§ 112-115 에서 재판소는 청구인이 해당 자료를 열람한 후 그 정확성을 구체적으로 다투어 공개적으로 문제를 제기할 수 있었다고 하면서 청구를 각하하였다.

122. 언론에 보도된 청구인의 범죄 혐의 관련 정보가 공소 내용을 부정확하게 반영한 *Margari v. Greece*, 2023 사건 § 59 에서 재판소는 계속 중인 형사절차 또는 범죄 혐의 수사 과정에서 공개되는 데이터는, 무죄 추정의 원칙이 준수되어야 한다는 점도 고려할 때, 무엇보다 상황과 피고인에 대한 공소 내용을 정확하게 반영해야 한다고 강조하였다.

c. 데이터가 기록된 목적 달성에 필요한 기간 이상 보유하지 않을 요건[4]

123. 재판소는 개인데이터 보유 기간을 제한할 필요성에 관한 문제를 여러 사건에서 검토하였다(*S. and Marper v. the United Kingdom* [GC], 2008; *B.B. v. France*, 2009; *Gardel v. France*, 2009; *M.B. v. France*, 2009; *M.K. v. France*, 2013; *J.P.D. v. France* (dec.), 2014; *Peruzzo and Martens v. Germany* (dec.), 2013; *W. v. the Netherlands* (dec.), 2009; *Brunet v. France*, 2014; *Drelon v. France*, 2022, § 98). 미성년자 강간 범죄로 5~15 년 사이 징역형을 선고받은 경우, 형 집행 종료 시점부터 국가 사법 데이터베이스에 최대 30 년간 성범죄자의 정보를 보유하는 것은 데이터 저장의 정당한 목적인 무질서나 범죄 예방이라는 목적에 비추어 비례성을 상실하지 않았다고 보았다(*B.B.*

[4] 또한 아래 데이터 보유 기간 참조.

v. France, 2009, §§ 67-68; *Gardel v. France*, 2009, §§ 68-69; *M.B. v. France*, 2009, §§ 59-60).

124. 다만, 범죄가 의심되었으나 유죄 판결을 받지 않은 사람들의 지문, 세포 검체, DNA 프로필을 국가 데이터베이스에 영구 보유하는 것은, 최초에 의심된 범죄의 성격·심각성과 관계없고 나이와도 무관하게 제 8 조 위반이라고 판단되었다(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 125-126). 특히 미성년자 사건에서는, 미성년자의 특수한 상황과 사회 안에서의 발달과 통합의 중요성을 고려할 때, 유죄 판결을 받지 않은 사람의 데이터를 영구 보유하는 것은 더욱 해로울 수 있다(*ibid.*, § 124).

125. 동시에, 특히 비밀 조치의 맥락에서 수집된 자료가 수집 목적과 관련이 없는 것으로 분류되는 즉시파기되는 것은 그 자체로 협약에 반하지 않는다(*Denysyuk and Others v. Ukraine*, 2025, § 108).

126. 개인데이터의 최대 보유 기간에 한도가 없으면 무조건 제 8 조와 양립 불가능한 것은 아니지만(*Gaughran v. the United Kingdom*, 2020, § 88; *Peruzzo and Martens v. Germany* (dec.), 2013, § 46), 데이터 저장 기간은 전적으로 당국의 주의 의무에 달려 있어 그 기간의 비례성을 보장해야 한다면 더욱더 절차적 보호조치가 필요하다(*ibid.*, § 46; *Aycaguer v. France*, 2017, §§ 44-46). *Grande Oriente d'Italia v. Italy*, 2024 사건 §§ 144-146 에서는, 범죄조직과 관련된 의회 조사의 일환으로 청구인 협회의 시설에서 시행된 수색 도중 압수된 다수의 문서에는 특히 협회 구성원들의 개인데이터도 들어 있었다. 재판소는 해당 의회조사위원회가 해산되어 기능이 종료되었는데도 압수된 문서의 사본이 여전히 관련 의회조사위원회 기록보관소에 보관되어 있다는 점과 국내법상 압수 문서는 조사 종료 시 반환되거나 사본이 파기되어야 한다는 점을 지적하였다. 이와 관련하여 재판소는 수색을 통해 입수한 문서의 사본을 파기하라는 규정의 부재는 협약 제 8 조와 양립할 수 없다고 재차 확인하였다.

d. 데이터를 그 기록 목적에 한정하여 사용할 요건

127. 재판소의 견해에 따르면, 데이터 사용은 데이터를 기록한 목적으로 한정해야 한다. 따라서 *Karabeyog˘lu v. Turkey*, 2016 사건 §§ 112-121 에서 형사 수사 과정에서의 전화 감청으로 수집된 데이터를 징계 조사에서 사용한 것은 수집을 정당화했던 목적과는 다른 목적으로 사용하여 제 8 조 위반이라고 판단하였다.

128. *Surikov v. Ukraine*, 2017 사건 §§ 83-95 에서는 개인의 정신 건강에 관한 데이터를 장기 보유하면서 최초의 수집을 정당화했던 사유와 무관한 목적으로 유포·사용한 것은, 데이터 주체의 사생활 존중권을, 비례성을 상실할 정도로 제한한 것이 되었다.

129. 개인정보의 부적절한 사용에 따른 위험 문제는, 병원 입원 중 불임수술을 당했을 것으로 의심되는 로마족 여성 8 명이 청구인으로서 본인의 진료기록 사본을 확보할 수 없었다고 주장한 *K.H. and Others v. Slovakia*, 2009 사건 §§ 45-57 에서도 제기되었다. 재판소는 제 8 조 위반이라고 판단하면서, 정부가 주장한 남용의 위험은 국내법에 적절한 보호조치를 도입하여 해당 데이터가 공개될 수 있는 상황과 그 기록에 접근할 수 있는 자의 범위를 엄격하게 한정하면 방지할 수 있었을 것이라고 지적하였다(*ibid.*, § 56).

130. 제 8 조가 보장하는 사생활의 내밀성에 대한 경계를 확립하기 위하여, 재판소는 보안을 목적으로 한 공공장소에서 개인 행위 감시와 그러한 행위의 녹화물이 당사자가 예상할 수 있는 범위를 벗어나 다른 목적으로 사용되는 경우를 구분하였다(보안상의 이유로 공공장소에서 청구인을 촬영한 영상이 언론에 공개된 *Peck v. the United Kingdom*, 2003, §§ 59-62; 경찰서 내 CCTV 의 통상적이고 예측 가능한 사용 범위를 벗어나, 영상 녹화로 청구인의 신원을 파악할 목적이었던 경찰의 기망행위에 관한 *Perry v. the United Kingdom*, 2003, §§ 41-42; 공공장소 감시를 위한 CCTV 카메라를 통해 안면인식기술을 사용한 *Glukhin v. Russia*, 2023, §§ 65-73).

e. 데이터처리 절차의 투명성 요건[5]

131. 공공당국이 수집·보관한 개인데이터와 관련된 일련의 사건들에서 재판소는, 이해관계자가 자신의 아동기 및 초기 발달 사항을 확인하고 이해하려면 필요한 "관련성 있고 적절한 모든 정보"에 접근할 수 있거나(*Gaskin v. the United Kingdom*, 1989, § 49), 개인의 정체성을 발견할 수 있으며(*Odièvre v. France* [GC], 2003, §§ 41-49), 자신이 노출된 건강상 위험을 확인할 수 있거나(*Roche v. the United Kingdom* [GC], 2005, § 162; *Guerra and Others v. Italy*, 1998, § 60; *McGinley and Egan v. the United Kingdom*, 1998, § 101), 과거 전체주의 정권 시기 개인사를 추적할 수 있도록(*Haralambie v. Romania*, 2009, § 93), 당국이 이해관계자에게 "실효적이고 이용 가능한 절차"를 제공할 적극적 의무가 있다고 판단하였다.

[5] 또한 아래 자기 데이터에 접근할 권리 참조.

132. 이러한 투명성 요건은 국가안보와 관련하여 민감한 정보의 맥락에서는 그 강도가 완화된다(*Leander v. Sweden*, 1987, § 51; *Segerstedt-Wiberg and Others v. Sweden*, 2006, § 102; *Dalea v. France* (dec.), 2010).

II. 데이터 보호와 사생활 존중권(협약 제 8 조)

협약 제 8 조약

"1. 모든 사람은 그의 사생활과 가족생활, 주거 및 통신을 존중받을 권리를 가진다.

2. 공권력은 국가 안보, 공공의 안전, 국가의 경제적 복리를 위해, 무질서 또는 범죄의 방지를 위해, 보건 또는 도덕의 보호를 위해, 또는 타인의 권리와 자유를 보호하기 위해 민주사회에서 필요하고 법에 따라 이루어지는 경우를 제외하고는 이 권리의 행사를 제한할 수 없다."

133. 재판소는 지금까지 당국이나 다양한 민간 기관이 수행한 다수의 개인데이터 운용을 대상으로 데이터 주체의 "사생활", "주거" 및/또는 "통신"이 제 8 조와 양립할 수 없는 방식으로 침해되었는지 심리하였다. 재판소는 서로 다른 맥락에서 법인과 자연인이 각자의 개인데이터를 보호하기 위하여 원용할 수 있는 여러 권리의 범위를 구체화하였다.

A. 사생활 존중권을 침해할 수 있는 데이터 운용

134. 기술의 발전과 함께, 데이터의 수집·저장·공개는 매우 다양한 형태를 띠게 되었다. 재판소는 여러 사건에서, 이러한 데이터 운용 중 하나 이상이 데이터 주체의 사생활 존중권에 대해 정당화되지 않은 제한을 초래하였는지 심리하였다.

1. 개인데이터 수집

135. 재판소는, 당국이 구축한 여러 비밀 감시 시스템을 통해 조직범죄와 테러를 방지하기 위한 조치의 맥락, 증거 사용을 위해 당국이 수집한 개인데이터와 관련된 사법적 맥락, 보건 맥락, 공공부문과 민간 부문 고용주를 모두 포괄하는 직장 내 데이터 수집 맥락, 공익 보호를 위하여 공적·사적 기관이 보유한 개인데이터를 당국에 전달하도록 하는 법적 의무 맥락이라는 다양한 맥락에서 개인데이터 수집 행위를 심리하였다.

a. 비밀 감시를 통한 당국의 데이터 수집[6]

136. 재판소는 다양한 비밀 감시 방법을 통한 개인데이터 수집 문제와 관련하여 상당수의 사건을 심리하였다. 당국이 어떤 감시 시스템을 사용하든 상관없이 남용을 방지하는 적절하고 충분한 보장책이 존재하여야 한다. 재판소는 시민을 비밀 감시할 권한은 민주 제도를 보호하기 위하여 엄격하게 필요한 범위에서만 허용될 수 있다고 본다(*Klass and Others v. Germany*, 1978, § 42; *Szabó and Vissy v. Hungary*, 2016, §§ 72-73). 이러한 제한은 관련 적절하고 충분한 사유로 뒷받침해야 하고, 추구하는 정당한 목적에 비례하여야 한다(*Segerstedt-Wiberg and Others v. Sweden*, § 88). 국내 법률은 감시 조치 명령과 실행 및 잠재적 구제 수단 확보에 관하여 적확하고 실효적이며 포괄적인 수준에 이른 보호조치를 제공하여야 한다(*Szabó and Vissy v. Hungary*, 2016, § 89).

i. 전화 감청 및 통화내역 기록

137. 사법 체계 내에서 재판소가 제 8 조 위반이라고 판단한 영역으로는, 경찰에 전화 감청 및 통화내역 기록(발신 전화 목록) 제공(*Malone v. the United Kingdom*, 1984, §§ 63-89), 청구인의 업무상 또는 사적 통화를 모두 점검·확인 및 전사(*Huvig v. France*, 1990, §§ 24-35), 제 3 자의 전화선을 감청하여 청구인의 통화를 여러 차례 점검·확인 및 전사(*Kruslin v. France*, 1990, §§ 25-36), 제 3 자의 전화선을 통해 특정인 감청(*Lambert v. France*, 1998, §§ 21-41), 당시 베른 주재 소련 대사관 소속 인물이 특정인에게 걸어온 전화를 검사가 자신의 사무실에서 점검·확인 및 녹취(*Amann v. Switzerland* [GC], 2000, §§ 45-62), 예비조사 단계에서 전화 감청(*Prado Bugallo v. Spain,* 2003, §§ 28-33), 형사소추 맥락에서 감청된 전화 통화가 이후 언론에 보도(*Craxi v. Italy (no. 2)*, 2003, §§ 57-84), 청구인이 당사자가 아닌 절차에서 감청한 전화 녹취록을 청구인의 사건기록 편입(*Matheron v. France*, 2005, §§ 27-44), 피의자 명의의 검사 승인도 없고 자의적 행위를 막을 정도의 보호조치를 규정한 입법도 없는 상황에서 당국의 전화 통화 점검·확인(*Dumitru Popescu v. Romania (no. 2)*, 2007, §§ 61-86), 형사 수사를 위한 변호사의 전화 감청(*Kvasnica v. Slovakia*, 2009, §§ 80-89), 전화 감청에 관한 국내 규정에 자의적 행위를 막기에는 부족한 보호조치 (*Dragojević v. Croatia*, 2015, §§ 85-102; *Liblik and Others v. Estonia*, 2019, §§ 132-143; *Denysyuk and Others v. Ukraine*, 2025, §§ 93-135), 적절한 사법적 보장책 결여(*Moskalev v. Russia*, 2017, §§ 35-45), 형사절차 맥락에서 전화 녹취에 대한 실효적 감독 결여(*Pruteanu v. Romania*, 2015, §§ 41-58), 휴대전화 통화

[6] 또한, 유럽인권협약 제 8 조에 대한 해설서 – 사생활 및 가족생활을 존중받을 권리 참조.

점검·확인(*Šantare and Labazņikovs v. Latvia*, 2016, §§ 56-63), 휴대전화 감청 조치에 대한 사후 통보를 정당한 근거 없이 미이행(*Cevat Özel v. Turkey,* 2016, §§ 29-37), 예방적 전화 통화 점검·확인(*Mustafa Sezgin Tanrıkulu v. Turkey,* 2017, §§ 45-66), 정보기관이 충분한 법적 보호조치 없이 개인과 개인 소유 아파트에서 열린 회의를 감시하는 사실상 무제한인 권한 행사(*Zoltán Varga v. Slovakia*, 2021, §§ 170-171) 및 그러한 감시가 아무런 국내법상 보호도 없이 또 다른 사람에게 무작위적으로 영향을 미친 경우(*Haščák v. Slovakia,* 2022, § 95), 변호사와 의뢰인(전 국방장관)이 형사 수사와 관련하여 비밀 감시를 받던 도중 이들의 전화 통화를 감청·녹음·전사(*Vasil Vasilev v. Bulgaria*, 2021, §§ 167-181)가 있다.

138. 재판소는 전화 감청이 사법 결정으로 승인되었고, 감청의 필요성을 법원이 심사한 상황이라면 제 8 조 위반이 아니라고 판단하였다(*İrfan Güzel v. Turkey*, 2017, §§ 78-89).

139. 마찬가지로 재판소가 제 8 조 위반이 아니라고 판단한 사건으로는, 경찰이 개인의 사적 통화의 내역을 기록하는 방식(metering)으로 발신 전화번호를 확보한 사건(*P.G. and J.H. v. the United Kingdom*, 2001, §§ 42-51), 청구인인 판사가 불법 조직의 구성원·기여자·지지자라고 의심되어 형사 수사 과정에서 전화선을 감청한 사건(*Karabeyog˘lu v. Turkey*, 2016, §§ 74-111) 및 교도소장이 교도소 내에서 사익을 위한 부패 관련 활동을 했다는 의혹에 따라 형사 수사(결국 증거 부족을 이유로 중단됨) 맥락에서 전화 통신을 감청한 사건(*Adomaitis v. Lithuania*, 2022, §§ 81-90)이 있다.

140. 명백히 근거가 없다고 보아 심리부적격으로 선언된 청구로는, 예방적 정보활동 체계에서 경찰의 전화 감청(*Deveci v. Türkiye* (dec.), 2022), 예비조사 체계에서 전화 감청(*Greuter v. the Netherlands* (dec.), 2002), 주요 마약 밀매 조직에 특정한 개인들의 가담 사실 증명에 사용된 주요 수사 기법의 하나인 전화 감청(*Coban v. Spain* (dec.), 2006) 및 회사 자산 횡령 혐의로 기소된 유럽의회 의원의 전화 통신 점검·확인 및 그 사건에서 국내 국회의원에게 적용하는 특별 대우 미적용(*Marchiani v. France* (dec.), 2008)이 있다.

141. 교정시설 맥락인 경우, *Doerga v. the Netherlands*, 2004 사건 §§ 43-54 에서 교정 당국이 수용자의 전화 통화를 불법 녹음·저장한 후 추가 범죄로 유죄 판결을 내리는 증거로 사용한 것은 제 8 조 위반이다.

142. 재판소가 제 8 조 위반을 인정한 영역으로는 교정 기숙학교에 수용된 미성년자들의 서신과 전화 통화를 모두 자동으로 점검·확인하여 감시 대상이 교류하는 유형으로는 어떠한 비밀성도 배제되게 한 경우(*D.L. v. Bulgaria*, 2006, §§ 100-116), 국방부가 시민의 자유 분야에서 활동하는 여러 단체가 발신한 통신을 영장에 따라 감청한 경우(*Liberty and Others v. the United Kingdom*, 2008, §§ 56-70), 재판소에서 청구인을 대리하는 전문성을 갖춘

몰도바 비정부기구에 대해 통신 점검·확인을 허용하는 입법이 존재한다는 사실만으로 문제가 된 경우(*Iordachi and Others v. Moldova*, 2009, §§ 29-54), 수사 중인 정치인의 전화회선에서 당국의 승인을 받아 녹음된 사적인 대화가 언론에 유출되어 방송된 경우(*Drakšas v. Lithuania*, 2012, § 62), 이동통신 사업자가 마련한 휴대전화 통화의 비밀 점검·확인에 관한 법적 체계에 결함이 있어 연방보안국(FSS)은 사전에 법원의 승인을 받지 않아도 모든 종류의 전화 통신을 감청할 수 있었던 경우(*Roman Zakharov v. Russia* [GC], 2015, §§ 163-305), 형사 수사 과정에서 감청된 전화 자료를 징계조사에서 사용한 경우(*Karabeyog˘lu v. Turkey*, 2016, §§ 112-121) 및 감청된 고객과의 대화 녹취록이 변호사에 대한 징계절차에 사용된 경우(*Versini-Campinchi and Crasnianski v. France*, 2016, §§ 49-84)가 있다. 반면, 교도소장이 교도소 내 부패혐의로 형사 수사를 받던 맥락에서 감청을 통해 얻은 정보를 징계절차에서 사용한 것은 비례적이라고 판단되었다(*Adomaitis v. Lithuania*, 2022, § 87).

ii. 호출기 메시지 가로채기

143. *Taylor-Sabori v. the United Kingdom*, 2002 사건 §§ 18-19 에서는 사법 절차 체계에서 경찰이 청구인의 호출기 메시지를 가로채 유죄 판결의 근거로 삼은 것은 가로채기에 관한 법규가 전혀 존재하지 않았기 때문에 제 8 조에 반한다고 판단되었다.

iii. 음성·영상 감시

144. 재판소는 비밀경찰의 작전 도중 무전 송신 장치를 사용하여 대화를 녹음하면서 적절한 절차적 보호조치가 수반되지 않은 경우, 제 8 조 위반이라고 판단하였다(*Bykov v. Russia* [GC], 2009, §§ 81, 83; *Oleynik v. Russia*, 2016, §§ 75-79).

145. 재판소는 국가 당국의 비밀 감시 조치 및 통신 가로채기 영역에서, 협약 제 8 조가 보장하는 사생활의 엄격한 경계를 확립하기 위하여, 보안 목적으로 공공장소에서 개인의 행위를 점검·확인하는 것과 당사자가 예측할 수 있는 범위를 벗어나 다른 목적으로 그 행위를 녹화하는 것을 구별하였다(*Peck v. the United Kingdom*, 2003, §§ 59-62; *Perry v. the United Kingdom*, 2003, §§ 41-42). 재판소는 또한 공공장소에서 CCTV 점검·확인에 사용된, 특히 실시간 안면 인식 기술을 사용하여 경찰이 사전 통보 없이 단독 시위에 가담하고 지하철로 이동 중이던 청구인을 특정하여 체포한 점을 들어, 그 침해성이 상당하다는 점을 강조하였다. 재판소는 이러한 조치가 "민주사회에서 필요"하다고 보려면 정당한 근거를 갖추어야 하고, 특히 실시간 안면 인식 기술의 경우 가장 철저히 근거를 갖추어 정당화되지 않으면 안 된다고 강조하였다(*Glukhin v. Russia*, 2023, § 86).

146. 사법 체계에서 재판소가 제 8 조 위반이라고 판단한 사건으로는, 경찰서에서 청구인들이 기소될 때와 유치장에 유치되어 있을 때 음성을 녹음한 사건(*P.G. and J.H. v. the United Kingdom*, 2001, §§ 56-63), 경찰서에서 피의자 신원 확인을 목적으로 비밀 폐쇄회로 카메라를 사용해 촬영한 사건(*Perry v. the United Kingdom*, 2003, §§ 36-49), 청구인이 방문한 제 3 자의 주거지에 설치된 청취 장치를 통해 경찰이 청구인의 자발적이고 즉흥적인 대화를 녹음하였고, 그 대화에서 청구인이 마약 밀수에 가담했다고 인정한 사건(*Khan v. the United Kingdom*, 2000, §§ 25-28), 사법 조사 단계에서 경찰이 사유 시설을 도청한 사건(*Vetter v. France*, 2005, §§ 20-27), 경찰 당국이 청구인의 신체에 청취 장치를 달아 대화를 녹음하고 그 녹음이 유죄 증명 증거의 유일한 항목은 아니었다고는 하여도 재판에서 사용한 사건(*Heglas v. Czech Republic*, 2007, §§ 71-76) 및 국가 수사당국의 협력과 기술 지원을 받아, 형사 또는 다른 성격의 공식 조사 단계에서 그 목적을 위하여 개인이 통신을 녹음한 사건(*Van Vondel v. the Netherlands*, 2007, §§ 47-55)이 있다. 반면, 사인(私人)이 업무상 청구인과의 대화를 스스로 주도하여 은닉 카메라로 촬영하고, 그 기록이 저장된 다른 사람의 컴퓨터를 당국이 검사하는 과정에서 발견된 해당 영상을 형사절차에서 사용한 경우에는 위반이 아니라고 판단하였다(*Sârbu v. Romania*, 2023, §§ 48-59).

147. 교정시설 맥락에서 재판소가 제 8 조 위반을 인정한 사건으로는, 당국이 청구인의 수용실, 교도소 접견실 및 동료 수용자의 신체에 은밀히 설치한 영상·음성 기록 장치를 이용하여, 청구인이 자발적이지 않은 유도된 발언을 하게 한 사건(*Allan v. the United Kingdom*, 2002, §§ 35-36), 교도소 접견실에서 수감자와 가족 간 대화를 녹음한 사건(*Wisse v. France*, 2005, §§ 28-34), 수용자와 변호인 간 상담을 비밀리에 감시한 사건(*R.E. v. the United Kingdom*, 2015, §§ 115-143), 수용실 내 수용자를 비밀 폐쇄회로 카메라로 하루 24 시간 영상 감시한 사건(*Gorlov and Others v. Russia*, 2019, §§ 83-100)이 있다.

148. 재판소는 취약자가 체포된 후 자신을 보조하도록 지정된 자와 상담하는 장면을 비밀리에 감시한 것과 관련하여 제 8 조 위반이 아니라고 판단하였다(*R.E. v. the United Kingdom*, 2015, §§ 154-168). 수용자와 "적절한 성인(취약자를 보조하는 성인 보호자)" 간 상담의 감시를 가능하게 하는, 지시에 따른 감시 활동에 관한 규정에는 남용을 방지하기 위한 적절한 보호조치가 수반되어 있었다.

149. 쟁점이 된 데이터를 은닉된 카메라로 수집한 다양한 맥락에서 재판소가 제 8 조 위반을 인정한 사건으로는, 공공장소에서 자살을 시도하는 사람을 촬영한 은닉된 폐쇄회로 카메라 영상을 언론에 전송한 사건(*Peck v. the United Kingdom*, 2003, §§ 57-87), 은닉된 카메라로 개인을 촬영한 영상을 모자이크 또는 흐림 효과 처리 없이 TV 로 방송한

사건(*Bremner v. Turkey*, 2015, §§ 71-85), 언론인을 자택에서 은밀히 영상 녹화하고 이를 공중파에 방송한 사건(*Khadija Ismayilova v. Azerbaijan*, 2019, §§ 108-132)이 있다.

iv. GPS 차량 위치 추적[7]

150. *Uzun v. Germany*, 2010 사건 §§ 49-81 에서, 테러 혐의가 있는 개인에 대한 GPS 감시는 제 8 조 위반에 해당하지 않았다. 반대로, *Ben Faiza v. France*, 2018 사건 §§ 53-61 에서는, 차량에 위치추적 장치를 설치하고 확보한 데이터를 사용하여 수사관들이 청구인의 이동 경로를 실시간으로 파악하고 체포할 수 있었던 것은 제 8 조에 반한다고 판단하였다.

v. 사설탐정의 감시

151. *Vukota-Bojić v. Switzerland*, 2016 사건 §§ 52-78 에서 재판소는 논란이 된 사회보장급여를 수령하던 개인의 활동을 사설탐정이 불법적으로 감시한 것과 관련하여 제 8 조 위반이라고 판단하였다. 국내법은 보험 분쟁에서 공권력을 행사하는 보험회사에 부여된 재량의 범위와 그 행사 방식, 즉 피보험자에 대한 비밀 감시를 수행할 수 있는 권한이 어떠한지에 관해 명확하게 규정하지 않았다.

vi. 서신 감시

152. 교정시설 맥락에서, 재판소가 제 8 조 위반이라고 판단한 경우는, 수용자의 서신 가로채기 및 개봉(*Lavents v. Latvia*, 2002, §§ 136-137), 교정시설 내 우편 서비스가 정상 작동하지 않는 상황 등에서 수용자의 서신 개봉(*Demirtepe v. France*, 1999, §§ 26-28; *Valašinas v. Lithuania*, 2001, §§ 128-130), 수용자의 서신을 가로채고 검열(*Silver and Others v. the United Kingdom*, 1983, §§ 84-105; *Labita v. Italy* [GC], 2000, §§ 176-184; *Niedbała v. Poland*, 2000, §§ 78-84; *Messina v. Italy (no. 2)*, 2000, §§ 78-83), 수용자가 변호사에게 보내는 편지 가로채기(*Ekinci and Akalın v. Turkey*, 2007, §§ 37-48), 수용자와 변호사 및 유럽인권위원회 간 서신 가로채기(*Campbell v. the United Kingdom*, 1992, §§ 32-54; *A.B. v. the Netherlands*, 2002, §§ 81-94), 유럽인권위원회가 수용자에게 보낸 편지 개봉(*Peers v. Greece*, 2001, §§ 81-84), 수용자와 고문 간 주고받은 서신 감시(*Szuluk v. the United Kingdom*, 2009, §§ 47-55), 수용자의 사적인 서신(수신·발신 모두) 스캔 후 국가사법네트워크 서버에 업로드(*Nuh Uzun and Others v. Turkey*, 2022, §§ 80-99)한 경우가 있다. 반면, *Erdem v. Germany*, 2001 사건 §§ 53-

[7] 또한 상기 GPS 위치 데이터 참조.

70 에서는 테러 혐의 수용자와 변호사 간 서신을 가로챈 것과 관련하여 제 8 조 위반이 아니라고 판단하였다.

153. 다른 맥락에서, 파산자의 서신을 파산관재인이 개봉하고 복사하여 기록에 편철한 경우에는 제 8 조 위반이 있다고 판단되었다(*Foxley v. the United Kingdom*, 2000, §§ 27-47).

vii. 비밀 감시, 간첩 활동 및 대규모 감시 작전

154. *Roman Zakharov v. Russia* [GC], 2015 사건 §§ 171-172 에서, 재판소는 특정 조건이 충족된다면, 청구인은 단순히 비밀 감시 조치가 존재하거나 조치를 허용하는 입법이 존재한다는 사실만으로도 위반의 피해자임을 주장할 수 있고, *Kennedy v. the United Kingdom*, 2010 사건 § 124 에서 취한 접근 방식이, 감시 조치의 비밀성이 그 조치를 사실상 다툴 수 없게 하거나 국내 사법 당국 및 재판소의 감독 밖에 두는 결과로 이어지지 않도록 할 필요성에 가장 잘 부합한다고 결정하였다. *Ekimdzhiev and Others v. Bulgaria*, 2022 사건 § 262-277 및 371-384 에서 재판소는 *Roman Zakharov v. Russia* [GC], 2015 사건 § 171 에서 발전된 원칙을 기준으로 하여, 청구인들(두 명의 변호사 및 이들과 관련된 두 개의 비정부기구)이, 비밀 감시를 허용하는 국내법이나 관행의 단순한 존재 및 당국의 보유된 통신 데이터 열람을 규율하는 법률 때문에, 제 8 조에 따른 권리 제한의 피해자임을 주장할 수 있다고 인정하였다(또한, 인터넷 통신 서비스 제공자에게 인터넷 통신 내용과 통신사실 확인자료를 저장하고, 법집행 당국과 보안기관이 요청할 경우 접근을 허용하며, 암호화된 전자 메시지 해독을 요구하는 법적 요건과 관련하여 유사한 접근 방식을 취한 *Podchasov v. Russia*, 2024, §§ 54-55 참조).

155. 재판소가 제 8 조 위반이라고 판단한 사건으로는, 특별감시장치법에 따라 청구인 협회가 언제든지 통보 없이 감시 조치 대상이 될 수 있었던 사건(*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2007, §§ 69-94), 비밀경찰 작전의 단계에서 절차적 보호조치 없이 무전 송신 장치를 통해 대화를 가로채고 녹음한 사건(*Bykov v. Russia* [GC], 2009, §§ 72-83), 러시아 연방보안국(FSB)의 주도로 수행된 "작전 실험" 맥락에서 대화가 녹음되었으나 법에 따른 것이 아니었던 사건(*Oleynik v. Russia*, 2016, §§ 74-79), 국방부가 시민 자유 분야에서 활동하는 단체들의 발신 통신을 영장에 따라 감청한 사건(*Liberty and Others v. the United Kingdom*, 2008, §§ 55-70), 청구인이 인권 단체의 구성원이라는 이유로 기록이 저장되고 경찰이 감시한 사건(*Shimovolos v. Russia*, 2011, §§ 64-71), 남용 방지를 위한 적절한 보호조치 없이 특별 대테러 기구를 설치한 비밀 감시 입법(*Szabó and Vissy v. Hungary*, 2016, §§ 52-89), 비밀 감시를 통해 수집된 정보의

저장(*Rotaru v. Romania* [GC], 2000, §§ 45-63; *Association « 21 December 1989 » and Others v. Romania*, 2011, §§ 169-177), 이동전화 통신의 비밀 감시를 규율하는 국내 법체계의 여러 결함(*Roman Zakharov v. Russia* [GC], 2015, §§ 163-305) 및 강력한 보호조치는 존재했지만, 자의와 남용의 위험에 맞서 적절하고 실효적인 보장을 제공할 충분한 "종단 간" 보호조치를 담고 있지 않았던 대규모 통신 가로채기 제도(*Centrum för rättvisa v. Sweden* [GC], 2021, §§ 365-374 및 *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 424-427)가 있다. 재판소는 또한 *Ekimdzhiev and Others v. Bulgaria*, 2022 사건 §§ 356-359 및 419-421 에서, 비밀 감시 관련 법률은 *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2007 사건에서 검토된 이후 상당한 개선이 있었다고는 하지만, 실제 적용된 법률은 여전히 여러 측면에서 자의와 남용에 대한 최소한의 보호조치가 되기에는 부족하다고 하면서 제 8 조 위반이라고 판단하였다. 통신 데이터의 보유 및 그에 대한 당국의 사후 접근을 규율하는 법률에도 유사한 판단을 내렸다. 같은 맥락에서, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, 2024 사건 §§ 195-278 에서도 재판소는 비밀 감시와 통신 데이터 보유 및 처리를 허용하는 두 가지 폴란드 법률에 자의를 방지할 정도의 보장책이 결여되어 있다고 판단하였다.

156. *Denysyuk and Others v. Ukraine*, 2025 사건 §§ 93-135 및 148-50 에서, 세 명의 청구인은 형사절차 과정에서 수행된 경찰 작전 과정에서 비밀 감시를 받았고, 이 과정에서 네 번째 청구인인 변호사와의 통신이 가로채져서 번호사와 의뢰인 간 비밀 특권이 침해될 수 있었다. 재판소는 (i) 청구인들이 비밀 감시를 승인한 사법 결정에 접근하는 것이, 관련된 이해관계의 균형을 전혀 고려하지 않은 채 단지 "기밀로 분류되었다"는 이유만으로 거부된 점 (ii) 변호사와 의뢰인 간 비밀 통신이 우연히 가로채어진 경우 식별하고 처리하는 절차를 규정하는 상세한 국내 규칙과 지침이 부재하였고, 개인 통신의 가로채기를 감독하는 독립적인 감독기구도 존재하지 않았던 점 (iii) 사후적으로 해당 제한의 적법성과 필요성을 검증하고 제 8 조 권리 침해 주장 발생 시 구제할 수 있을 정도의 절차적 보호조치가 부재하였던 사정을 근거로, 다툼이 된 제한이 "법에 따른 것"이 아니라고 보아 협약 제 8 조 위반이라고 판단하였다.

157. 재판소가 제 8 조 위반이 아니라고 판단한 사건으로는, 마약 밀매 혐의로 기소된 청구인의 전화선을 감청하는 동시에 위장 잠입 요원을 투입한 사건(*Lüdi v. Switzerland*, 1992, §§ 38-41), 일반 대중의 서신, 우편 및 전화 통신을 비밀리에 감시하도록 승인하는 제도(*Klass and Others v. Germany*, 1978, §§ 39-60) 및 테러와 중대한 범죄에 대응하기 위해 국내 통신을 가로채도록 승인한 입법 체계(*Kennedy v. the United Kingdom*, 2010, §§ 151-170)가 있다.

158. 재판소는 *Klass and Others v. Germany*, 1978 사건의 후속으로, 통신에 대한 전략적 감시를 문제 삼은 *Weber and Saravia v. Germany* (dec.), 2006 사건 §§ 143–153 에서 명백한 근거가 없다고 선언하였다.

b. 직장에서 고용주의 데이터 수집

159. 재판소는 공공부문 고용주(*Halford v. the United Kingdom*, 1997, §§ 49, 45; *Antović and Mirković v. Montenegro*, 2017, § 58; *Libert v. France*, 2018, § 41) 또는 민간 부문 고용주(*Köpke v. Germany* (dec.), 2010; *Bărbulescu v. Romania* [GC], 2017, § 109; 및 *López Ribalda and Others v. Spain* [GC], 2019, § 109)에 의한 직장 내 개인데이터 수집 문제를 제 8 조에 따라 심리하였다. 일부 사건에서는 데이터 주체의 인지 없이, 완전히 비밀리에(*Halford v. the United Kingdom*, 1997, § 49; *Copland v. the United Kingdom*, 2007, § 45; *Bărbulescu v. Romania* [GC], 2017, § 78), 또는 부분적으로 비밀리에(*López Ribalda and Others v. Spain* [GC], 2019, § 93) 유지된 감시를 통해 데이터를 수집·운용하였지만, 해당 직원들이 알고 있는 상태에서 데이터가 수집된 사건도 있었다(*Antović and Mirković v. Montenegro*, 2017, § 44).

160. 수집 대상이 된 개인데이터가 도출된 상황으로는, 직장에서 사적인 전화 감시(*Halford v. the United Kingdom*, 1997, § 44), 전화, 전자우편, 인터넷 사용 점검·확인(*Copland v. the United Kingdom*, 2007, §§ 44–49), 인터넷 및 인스턴트 메시징(야후) 사용의 점검·확인(*Bărbulescu v. Romania* [GC], 2017, § 74), 고용주가 업무용으로 제공한 컴퓨터에 직원이 저장한 파일 열람(*Libert v. France*, 2018, § 25), 근무지에서 신원이 확인되었거나 확인할 수 있는 직원의 행위를 보여주는 영상 녹화 장면에서 촬영된 사진(*Köpke v. Germany* (dec.), 2010; *Antovic and Mirkovic v. Montenegro*, 2017, § 44; *López Ribalda and Others v. Spain* [GC], 2019, § 92) 또는 GPS 시스템을 통해 직원이 회사 차량을 운전하며 근무 중 이동한 거리, 해당되는 경우 사적인 이동 거리까지 점검·확인(*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, §§ 94–96)이 있다.

161. 이 분야 최초의 두 가지 판결(*Halford v. the United Kingdom*, 1997, § 44 및 *Copland v. the United Kingdom*, 2007, § 41)에서 재판소는, 업무 장소에서 비업무용 전화는 제 8 조 목적상 “사생활”과 “통신”의 개념에 일응 포함된다고 판결하였다. 또한 직장에서 발송된 전자우편 역시 제 8 조에 따라 동일하게 보호되어야 하고, 개인적 인터넷 사용을 점검·확인하여 파생된 정보 역시 마찬가지라고 보았다(*Copland v. the United Kingdom*, 2007, § 41). 이어서, 고용주가 업무 목적으로 제공한 컴퓨터에 저장하였으나 명백히 개인적인 것이라고 알 수 있는 직원의 데이터 역시 “사생활” 개념에 포함될 수 있다고

명기하였다(*Libert v. France*, 2018, § 25). 나아가, 사전 통보 없이 직장에서 직원의 행동을 보여주는 은밀한 영상 녹화 역시 직원의 "사생활"에 영향을 미친다(*Köpke v. Germany* (dec.), 2010). 이후 재판소는, 직장에서의 직원을 영상으로 비밀리에 감시하였든 공개적으로 감시하였든 이러한 결론에서 벗어날 이유를 찾지 못하였다(*Antovic and Mirkovic v. Montenegro*, 2017, § 44; *López Ribalda and Others v. Spain* [GC], 2019, § 93).

162. *Halford v. the United Kingdom*, 1997 사건 §§ 50-51 및 *Copland v. the United Kingdom*, 2007 사건 § 48 에서, 재판소는 문제 된 시점에 각각 직원의 비업무용 전화 통화로부터 개인데이터 수집과 직장에서 발송된 전자 메시지로부터 개인데이터 수집을 승인하는 국내법이 부재하였기 때문에, 그 결과 초래된 사생활 존중권에 대한 제한은 "법에 따른 것"이 아니라고 판단하였다. *Köpke v. Germany* (dec.), 2010 사건에서 재판소는 고용주가 도난 혐의를 받은 슈퍼마켓 계산원을 대상으로 사설탐정 회사를 동원하여 은밀한 영상 감시를 통해 데이터를 수집한 것과 관련된 청구를 명백히 근거 없다고 선언하였다. 당시에는 고용주가 직원에 대한 영상 감시에 의거할 수 있는 조건이 입법으로 규정되어 있지 않았지만, 연방노동법원의 판례가 이미 직원의 사생활 존중권에 대한 자의적 제한을 방지하는 주요 보호조치를 제시하고 있었다.

163. 현 사안에서 중대한 위법 행위가 있었다는 합리적 의심이 존재하고 확인된 손실의 규모는, 고용주가 직장 내에서 개인데이터를 수집하는 행위를 정당화하는 중대한 근거가 될 수 있다(*López Ribalda and Others v. Spain* [GC], 2019, § 134). 반대로, 직원의 횡령이나 기타 위법행위에 대한 단순한 의심만으로는 고용주가 은밀하게 영상 감시 장치를 설치하는 것을 정당화할 수 없다(*ibid.*, § 134).

164. *Bărbulescu v. Romania* [GC], 2017 사건 § 121 에서 재판소는 직장에서 직원의 서신 및 통신을 감독하기 위한 조치가 제 8 조에 위반되지 않기 위한 여러 기준을 제시하였다. 이 맥락에서 국내 당국은 ▲고용주가 직원의 서신 및 기타 통신을 점검·확인할 가능성과 그러한 조치의 시행에 관하여 직원에게 통보하였는가? ▲고용주의 점검·확인 범위와 직원의 사생활 비밀을 침해하는 정도는 어떠하였는가? ▲고용주가 직원의 통신을 점검·확인하는 것을 정당화할 합법적인 이유를 제시하였는가? ▲직원의 통신 내용에 직접 접근하는 것보다 침해성이 낮은 방법과 조치에 기반한 점검·확인 시스템을 구축하는 것이 가능하였는가? ▲점검·확인이 대상 직원에게 미친 결과는 무엇이었는가? ▲특히 고용주의 점검·확인 운용이 침해성격을 띠는 경우, 직원에게 적절한 보호조치가 제공되었는가?와 같은 질문에 대답하여야 한다. 마지막으로, 국내 당국은 통신 점검·확인의 대상이 된 직원이 사법기관에서, 최소한 본안 차원에서 위 기준이 어떻게 준수되었는지 및 다툼이 된 조치가 합법적인지를 판단받을 수 있는 구제수단에 접근하도록 보장해야 한다(*ibid.*, § 122).

165. 이후 *López Ribalda and Others v. Spain* [GC], 2019 사건 § 116 에서 재판소는 그러한 기준을 직장에서 고용주가 시행하는 영상 감시 조치에도 적용할 수 있다고 지적하였다. 이어서 *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 사건 § 115 에서 재판소는 동일한 기준을 고용주가 회사 차량으로 이동한 직원의 주행 거리를 GPS 시스템을 통해 점검·확인하는 상황에 적용하였다.

166. 재판소는, 국내 법원이 고용주의 감시 조치가 비례적이고 적절하며 충분한 보호조치를 수반하였다고 보장하지 못한 경우, 제 8 조 위반이라고 판단하였다. *Bărbulescu v. Romania* [GC], 2017 사건 §§ 108-141 에서 국내 법원은 감시 조치 이행을 정당화하는 구체적 사유, 직원의 사생활 및 통신에 침해성이 낮은 조치가 가능했는지 여부 또는 고용주가 사전에 직원에게 통신 점검·확인 가능성을 통보했는지 여부를 판단하지 못하였다. 반대로 *Libert v. France*, 2018 사건 §§ 37-53 에서 재판소는, 직원이 업무용 컴퓨터에 저장한 개인 파일을 열람하여 파일에 담긴 음란물이 해고의 근거가 된 것에 대해 제 8 조 위반이 아니라고 판단하였다. 재판소는, 국내 법원이 해석·적용한 국내법이 자의 방지를 위한 적절한 보호조치를 포함하고 있었음을 지적했는데, 특히 "개인용"이라고 표시된 파일은 직원이 입회한 경우에만 고용주가 열도록 허용되었다는 점이 그러한 보호조치에 해당하였다.

167. 재판소의 견해에 따르면, 중대한 공적 또는 사적 이익의 보호와 관련된 압도적 필요 요건이 있어야만 고용주가 직원의 개인데이터 보호를 침해할 수 있는 조치에 대해 사전 정보를 제공하지 않아도 정당화될 수 있다(*López Ribalda and Others v. Spain* [GC], 2019, § 133). 고용주는 통상적인 데이터 수집이라 하더라도 해당 직원에게 그러한 데이터 수집 조치의 존재와 조건을 알려야 한다(*ibid.*, § 131). 투명성 요구와 그에 따른 정보 제공권은 기본적인 사항이며, 특히 고용관계의 맥락에서는 고용주가 직원에 대하여 상당한 권한이 있고 그러한 권한은 남용이 방지되어야 한다는 점에서 더욱 중요하다. 다만, 점검·확인 대상이 되는 개인에게 정보를 제공하는 것과 그 범위는, 개별 사건에서 이와 같은 조치의 비례성을 평가할 때 고려해야 할 기준 중 하나일 뿐이다. 다만 그러한 정보를 제공하지 않은 경우, 다른 기준에서 파생되는 보호조치가 그만큼 더 중요해진다(*ibid.*, § 131).

168. 사전에 정보가 제공되지 않은 경우, 감시 대상이 된 직원들이 사생활 존중권의 실효적인 보호를 보장하기 위하여 특별히 마련된 국내 구제수단을 이용할 수 있었는지 확인하여야 한다. 직장에서 직원에게 부과되는 조치라는 맥락에서, 이러한 보호는 고용법뿐만 아니라 민사법, 행정법 또는 형사법에 속할 수 있는 다양한 수단으로 보장될 수 있다(*ibid.*, § 136).

169. 직원을 대상으로 한 영상 감시를 조금 더 구체적으로 살펴보면, *López Ribalda and Others v. Spain* [GC], 2019 사건 § 125 에서 재판소는 영상 감시 조치의 비례성을 분석할 때, 직원이 합리적으로 기대할 수 있는 사생활의 비밀 보호 수준에 비추어 점검·확인이 이루어진 장소를 구분할 필요가 있다고 지적하였다. 화장실, 탈의실 등 본질적으로 사적인 공간에서는 그 기대 수준이 매우 높아, 보호 강화뿐만 아니라 영상 감시의 전면적 금지까지도 정당화된다(*ibid.*, §§ 125, § 61, § 65, 관련 국제 문서 인용). 사무실처럼 폐쇄적 근무 공간에서도 기대 수준은 여전히 높지만, 동료나 일반 대중이 볼 수 있거나 접근할 수 있는 장소에서는 그 기대 수준이 현저히 낮아진다(*ibid.*, § 125).

170. 이와 관련하여 *Köpke v. Germany* (dec.), 2010 사건에서 재판소는, 슈퍼마켓 계산원인 청구인이 고용주가 사설탐정 회사를 동원하여 시행한 은밀한 영상 감시 조치에 대해 제기한 청구를 명백한 근거가 없어 심리부적격이라고 선언하였다. 재판소는 특히, 문제 된 조치가 기간적으로 한정되어 있었고(2 주), 계산대 주변 일반인 출입이 가능한 구역만을 대상으로 하였으며, 확보된 영상 데이터는 탐정 회사 직원과 고용주의 직원 등 한정된 인원만이 처리하였고, 해당 자료는 오직 청구인의 해고 절차와 노동법원 절차 단계에서만 사용되었다고 평하였다.

171. 반대로, *Antovic and Mirkovic v. Montenegro*, 2017 사건 §§ 55-60 에서 재판소는, 대학교수인 두 명의 청구인이 강의하던 대학 강의실에 영상 감시 시스템을 설치한 결과 사생활이 침해되었다는 주장과 관련하여, 그 조치가 법에 규정된 것이 아니었으므로 제 8 조 위반이라고 판단하였다.

172. *López Ribalda and Others v. Spain* [GC], 2019 사건 § 137 에서 재판소는, 슈퍼마켓 계산원과 판매원을 대상으로 일부는 공개적이고 일부는 은밀하게 영상으로 감시한 건과 관련하여, 스페인 입법이 제공한 실질적인 보호조치(청구인들이 이용하지 않았던 구제수단 포함)를 고려할 때 제 8 조 위반이 아니라고 판단하였다.

173. 마찬가지로, *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 사건 §§ 105-125 에서는 고용주가 회사 차량에 설치한 GPS 시스템에 기록된 주행거리 데이터를 근거로 청구인을 해고하였다. 재판소는 국내 법원들이 쟁점이 된 상충하는 이해관계인 청구인의 사생활 존중권과 회사의 원활한 운영을 보장하려는 고용주의 권리를, 회사가 추구한 정당한 목적인 비용 지출을 관리할 권리를 고려하여 신중히 비교형량하였다고 보아, 제 8 조 위반이 아니라고 판단하였다.

174. 유사한 여러 원칙은 다른 맥락에서도 적용될 수 있는데, 특히 정당이 당원의 전자 통신을 점검·확인하는 경우, 정당의 내부 조직 구조는 사기업과 다르고, 고용주와 직원 간

법적 관계와 정당과 당원 간 법적 관계도 본질적으로 다르다 하더라도 적용할 수 있다(*Tena Arregui v. Spain*, 2024, §§ 38 및 41).

c. 법원 절차에서 증거로 사용하기 위한 데이터 수집

175. 법원 절차 단계에서 물적 증거를 수집하는 것은, 절차에서의 지위가 당사자이든, 증인이든, 제 3 자이든 상관없이 개인데이터 보호와 관련된 문제를 야기한다.

i. 수색 및 압수

176. 재판소는 여러 사건에서, 체약국이 특정 범죄의 물적 증거를 확보하기 위하여 수색 및 압수와 같은 조치에 의거할 필요가 있다고 판단할 수 있음을 강조하였다(*Vasylchuk v. Ukraine*, 2013, § 79; *K.S. and M.S. v. Germany*, 2016, § 43). 이러한 경우, 조치에 대한 심사는 조치를 정당화하기 위해 제시된 이유의 관련성과 타당성 및 추구된 목적에 대한 비례성 원칙 준수 여부를 대상으로 한다(*Smirnov v. Russia*, 2007, § 44). 수색 및 압수를 유발한 범죄의 심각성, 영장이 발부된 상황(특히 당시 다른 증거 존재 여부), 영장의 내용과 범위, 수색된 시설의 성격 및 그 영향력을 합리적 범위로 제한하기 위해 시행된 보호조치, 수색한 방식과 그로 인해 해당인의 사생활 존중에 미칠 수 있는 잠재적 파급 효과 등은, 서로 상충하는 여러 이해관계를 비교형량할 때 고려해야 할 중요한 기준이다(*ibid.*, § 44; *Modestou v. Greece*, 2017, § 42 및 이 조항에서 관련 판례 다수 참고). 재판소에 따르면 국내법에는 자의성을 방지할 수 있을 정도로 적절하고 충분한 보호조치도 있어야 한다(*Vinci Construction and GTM Génie Civil and Services v. France*, 2015, § 66; *Modestou v. Greece*, 2017, § 43; *Reznik v. Ukraine*, 2025, § 58). 해당하는 보장책으로는 제 8 조를 침해하는 조치에 대한 "실효적인 심사"의 존재도 있다(*Modestou v. Greece*, 2017, § 42).

177. *Trabajo Rueda v. Spain*, 2017 사건 §§ 44-47 에서, 아동 음란물이 포함되어 있다고 주장하면서 경찰이 청구인의 개인용 컴퓨터를 압수하여 저장된 모든 개인 파일에 접근할 수 있게 한 것은 제 8 조에 반한다고 간주되었다. 재판소는 경찰이 청구인의 개인용 컴퓨터에서 파일을 압수하고 저장된 모든 데이터에 접근하기 위해, 통상 요구되는 사전 법원 영장을 상당히 신속하게 받을 수 있었는데도 받지 않은 채 긴급히 조처할 필요가 있었다는 점을 확신하지 못하였다.

178. *K.S. and M.S. v. Germany*, 2016 사건 §§ 32-58 에서 재판소는, 은행 직원이 불법 복사한 뒤 정보기관에 판매한 해외 은행 내 청구인들의 자산 관련 개인데이터에 기초하여 발부된 영장에 따른 청구인들의 자택 수색과 관련하여, 제 8 조 위반이 아니라고 판단하였다. 독일의 법률과 실무는 남용 방지에 적절하고 실효적인 보장책을 제공하고 있었다. 또한 국내

법원은 해외에서 가져온 데이터에 근거하여 수색영장을 발부하면서 판단재량의 범위를 벗어나지 않았다. 특히 재판소는, 수색영장이 발부될 당시 문제 된 데이터 세트 이외에 독일 당국이 구매한 관련 데이터 세트는 거의 없었거나 전혀 없었다는 사실에 특히 비중을 두었다(*ibid.*, § 51). 나아가 절차 규칙을 위반하여 획득한 증거는 형사절차에서 사용될 수 없다는 절대적 규칙이 존재하지 않는다는 사실만으로 당국이 국제법이나 국내법을 위반하여 고의로 데이터를 확보했다고 할 수는 없다(*ibid.*, § 51). 또한 데이터 저장 매체에는 청구인들이 국내 세무 당국에 제출해야 했던 재정 상황에 관한 정보가 담겨 있었으나, 청구인들의 신원과 밀접하게 연관된 데이터는 포함되지 않았다(*ibid.*, § 53; 양자 협정에 따라 다른 국가의 세무 당국에 은행 정보를 제공한 사건인 *G.S.B. v. Switzerland*, 2015, § 93 과 비교).

179. 물적 증거를 수집하기 위한 목적으로 사업장을 수색하는 것은, 협약 제 8 조가 보장하는 "통신"과 "주거" 존중권의 관점에서 데이터 보호 문제를 야기한다. 예를 들어, *Bernh Larsen Holding AS and Others v. Norway*, 2013 사건 §§ 104-175 에서 재판소는 회사가 다른 회사들과 공유하던 컴퓨터 서버의 모든 데이터에 대한 백업 사본을 제출하도록 명령한 결정과 관련하여 제 8 조 위반이 아니라고 판단하였다. 비록 사전 법원 영장 요건은 적용되지 않았으나, 재판소는 남용을 방지하기 위한 실효적이고 적절한 보호조치, 회사 및 그 직원들의 이익, 실효적인 세무조사의 공익을 고려하였다(*ibid.*, §§ 172-175). 반대로, 경쟁법 규칙을 위반한 가격 담합 존재의 증거 확보를 목적으로 한 사업장 검사에 관한 *DELTA PEKÁRNY a.s. v. Czech Republic*, 2014 사건 §§ 92-93 에서 재판소는 제 8 조 위반이라고 하였다. 재판소는 판사의 사전 승인 부재, 조치의 필요성에 대한 실효적인 사후 심사의 결여, 확보된 데이터의 파기 가능성에 관한 규정 부재를 언급하였다.

180. *Buck v. Germany*, 2005 사건 §§ 30-53 에서, 제 3 자가 저지른 도로교통 위반과 관련하여 청구인의 사업장과 주거 시설을 수색한 것은 제 8 조 위반에 해당하였다. 재판소는 특히 문제 된 수색 및 압수가 제 3 자가 저질렀다고 주장된 경미한 법규 위반과 관련한 명령이었고, 청구인의 사적 주거 시설을 포함하였다는 점 등 사건의 특수한 상황을 고려하여, 그러한 제한은 추구된 정당한 목적에 비례하는 것으로 간주할 수 없다고 결론 내렸다(*ibid.*, § 52).

181. 출처 확인을 목적으로 언론인의 직업 관련 시설, 주거, (일부 사건에서) 개인 차량을 수색하고 대규모 압수를 진행한 것을 두고 재판소는 *Ernst and Others v. Belgium*, 2003 사건 §§ 110-117 에서 제 8 조 위반이라고 판단하였다. 사법 수사의 비밀 위반에 대응하기 위한 조치와 관련하여, 체약국의 입법과 실무는 주거 수색 및 압수를 규정할 수 있지만, 남용을 방지하는 적절하고 충분한 보장책을 제공해야 한다. 그러나 본 사건에서는 청구인들에 대해

어떠한 기소도 없었고, 다양한 수색영장은 포괄적으로 기재되어 문제 된 수사, 수색 대상이 된 특정 시설, 압수 대상 물품에 관한 정보가 포함되지 않아, 수사관들에게 광범위한 재량권을 남겨두었기 때문에 상황이 달랐다. 또한 청구인들은 수색의 실제 이유에 대한 통보를 전혀 받지 못하였다(본 사건에서 제 10 조 위반에 관한 **오류! 참조 원본을 찾을 수 없습니다.** 참조).

182. 법률사무소를 대상으로 한 압수는, 변호사와 의뢰인 간 신뢰관계의 기초가 되는 데이터의 비밀성을 보호하기 위하여 항상 특별한 절차적 보호조치를 수반해야 한다[8]. *Kırdök and Others v. Turkey*, 2019 사건 §§ 52–58 에서, 사법 당국이 해당 변호사들과 사무실을 공유하던 변호사에 대한 형사절차를 목적으로 여러 변호사의 전자 데이터를 압수한 후 반환하거나 파기하기를 거부한 것은 제 8 조 위반에 해당하였다. 재판소는 수색 과정에서 직업상 비밀유지 원칙의 적용을 받는 전자문서나 데이터에 대해 비밀 자료 선별 절차가 하나도 마련되지 않았다는 점에 비중을 두었다. 또한 압수된 데이터가 아직 전사되지 않았으므로 소유자를 확인할 수 없다는 이유로 반환을 거부한 것은 법에 명확히 규정되어 있지 않았으며, 데이터의 비밀성을 요구하는 직업상 비밀유지의 본질에 배치되었다.

183. *Kruglov and Others v. Russia*, 2020 사건 §§ 123–138 에서 재판소는 경찰이 청구인들의 주거와 사무실을 수색하는 과정에서, 변호사인 청구인들이나 그 의뢰인들에게 속하는 개인 정보 및 직업상 비밀유지 대상 문서도 들어 있는 컴퓨터와 하드디스크를 비밀 자료 선별 절차 없이 압수한 것은 제 8 조에 반한다고 결정하였다. 특히, 사전 법원 영장이 존재하기는 하였지만, 국내 법원이 범죄 수사의 필요성과 데이터 비밀성 보호 의무를 비교형량하기 위하여 다른 출처에서 정보를 확보할 가능성을 고려하는 등의 시도를 전혀 하지 않았기 때문에, 그 효과가 한정적이었다(*ibid.*, §§ 126–129). 일반화하자면, 재판소는 변호사의 전자기기에는 직업상 비밀유지 원칙의 적용을 받는 자료(비밀유지 특권 대상 자료)가 들어있을 수 있는데도, 외부 감독이나 다른 보호조치 없이 압수·반출·열람된다는 사실 그 자체가 해당 변호인 청구인의 제 8 조 권리에 대한 비례성을 상실한 제한이 된다고 본다(인용된 당국 포함 *Reznik v. Ukraine*, 2025, § 76).

184. 재판소가 제 8 조 위반을 인정한 다른 사건으로는, 정당한 이유나 보장책 없이 변호사의 주거지에서 대량의 문서와 컴퓨터 본체를 수색·압수한 사건(*Smirnov v. Russia*, 2007, §§ 36–49), 법률이 규정한 절차적 보호조치를 위반하여 변호사의 전자 데이터를 수색·압수한 사건(*Wieser and Bicos Beteiligungen GmbH v. Austria*, 2007, §§ 42–68), 법률사무소에 저장된 모든 전자 데이터를 수색·압수하도록 승인하면서 승인 사유가 불충분하게 제시된

[8] 또한, 법률사무소 대상 압수에 적용되는 절차적 보장책에 관한 추가 사항은 유럽인권협약 제 8 조에 대한 해설서 – 사생활 및 가족생활을 존중받을 권리 참조.

사건(*Robathin v. Austria*, 2012, § 52), 변호사의 컴퓨터와 휴대전화가 압수 후 검사되는 과정에서 직업상 비밀유지 대상 데이터 보호를 위해 마련된 절차적 보호조치가 불충분하다고 평가된 사건(*Särgava v. Estonia*, 2021, §§ 107–108) 및 변호사인 청구인의 주거지가 그의 의뢰인에 대한 형사절차의 맥락에서 수색되고, 이 과정에서 여러 데이터 저장 장치가 압수되어 이후 전문가 검사를 거쳤으나, 제 8 조 권리를 보장하기 위한 절차적 보호조치가 부족했던 사건(*Reznik v. Ukraine*, 2025, §§ 73–77)도 있다.

185. *Vinci Construction and GTM Génie Civil and Services v. France*, 2015 사건 §§ 69–81 에서 재판소는 변호사의 비밀유지의무에 해당하는 전자 메시지를 포함하여 회사에 속한 컴퓨터 데이터를 수색·압수한 것에 대해 제 8 조 위반이라고 판단하였다. 하급심 법원은 수사관들이 압수한 여러 문서 중 변호사가 발신한 서신도 있다고 인정하면서도, 문제 된 압수에서 형식상의 합법성만을 평가했을 뿐, 세부적인 심사 요건을 수행하지 않았다.

186. *André and Others v. France*, 2008 사건 §§ 37–49 에서, 의뢰 회사 중 한 곳에 대한 증거를 확보하기 위하여 세무 당국이 "주거" 수색 형식으로 법률사무소에서 문서를 수색·압수한 것은 제 8 조 위반에 해당하였다. 문제 된 수색의 목적은, 단지 해당 회사의 변호사 자격으로 있던 청구인들의 사무실에서, 회사 측 사기의 존재를 입증할 수 있는 문서를 찾아내어 회사에 대한 증거로 사용하는 것이었다. 청구인들에게는 어느 시점에서도 범죄 혐의가 제기된 적이 없었고, 의뢰 회사의 사기에 연루되었다는 의심을 받은 적도 없었다(*ibid.*, § 46).

187. *Visy v. Slovakia*, 2018 사건 §§ 33–47 에서, 불법 압수된 자료가 반환된 후 5 분 만에 진행된 두 번째 압수는 제 8 조 위반에 해당하였다. 청구인은 두 번째 압수와 관련하여 자의와 남용을 방지하는 실효적인 보장을 전혀 제공받지 못하였다.

188. *Sher and Others v. the United Kingdom*, 2015 사건 §§ 171–176 에서 재판소는 테러 사건의 맥락에서, 테러 활동 혐의가 있는 경우 연장 가능한 수색영장 문제를 심리하였다. 재판소는 그러한 사건에 내재하는 복잡성이, 일반적으로 허용될 수 있는 범위보다 더 넓은 조건에 근거한 수색을 정당화할 수 있다고 판결하였다. 제 8 조에 따라 수색영장이 압수 대상 물품의 구체적 성격을 상세히 특정하도록 요구하는 것은, 수많은 생명이 위태로울 수 있는 상황에서 수사의 실효성을 심각하게 저해할 수도 있다. 이러한 성격의 사건에서 경찰은 수색 도중 직면한 정황에 근거하여 어떤 물품이 테러 활동과 관련이 있을 수 있는지를 평가한 후 추가 조사를 위해 압수할 수 있는 일정한 재량이 있어야 한다(*ibid.*, § 74).

189. *Ivashchenko v. Russia*, 2018 사건 §§ 59–95 에서 합리적인 범법 의심이 없는 상황에서 세관 당국이 개인의 전자 데이터를 열람·복사할 권한을 행사한 것은 제 8 조 위반에

해당하였다. 청구인의 개인적·직업적 데이터를 복사한 후 전문가 평가를 위해 전달하고 약 2 년간 보유한 것은, 일반적으로 동의하는 비침해적인 "통상적" 절차라고 볼 수 있는 범위를 벗어났다. 청구인은 세관에 출석하고 소지품을 제출하거나 세관 검사를 받을지 여부를 선택할 수 없었다(또한, 합리적 근거 없이 개인을 정지·수색하여 제 8 조 위반에 해당할 수 있는 권한에 관한 *Gillan and Quinton v. the United Kingdom*, 2010, §§ 61-67 참조. 재판소는, 공개 수색으로 개인 정보가 타인에게 노출되어 당혹감을 초래하는 사실은, 굴욕감과 수치심이라는 요소 때문에 때 따라 개인의 사생활에 대한 제한의 심각성을 더욱 가중할 수 있다고 지적하였다. 경찰관이 누리는 재량도 문제가 되었는데, 경찰은 합리적 의심이 존재함을 입증할 필요가 없었을 뿐 아니라, 심지어 무슨 짓이라도 저질렀다는 주관적인 의심조차 없어도 대상자를 정지·수색할 수 있었다).

ii. 세포 검체 채취를 위한 강제 의료 행위

190. 일반적으로 세포 검체 채취 목적으로 혈액 검사나 구강 면봉 채취와 같은 다양한 강제 의료 행위를 하는 것은, 민사 또는 형사 절차에서 증거를 수집한다는 맥락에서 그 자체로 금지되는 것은 아니다(*Jalloh v. Germany* [GC], 2006, § 70; *Caruana v. Malta* (dec.), 2018, § 41; *D.H. and Others v. North Macedonia*, 2023, § 52).

191. 특히, *D.H. and Others v. North Macedonia*, 2023 사건 §§ 52-53 에서 재판소는, 성병 전염 범죄 혐의로 청구인들(모두 성매매 종사자)의 혈액을 채취한 것은, 해당 의료 행위는 판사가 명령하였고, 클리닉에서 의사가 집행하였으며, 과도한 물리력 사용이 있었거나 건강에 해로웠다고 청구인들이 주장한 적도 없었기 때문에, 제 8 조 요건에 위반되지 않는다는 의견이었다. 관련 청구는 명백히 근거 없다고 보아 각하되었다.

192. *Mikulić v. Croatia*, 2002 사건 § 64 에서 재판소는, 친부로 추정되는 자에게 DNA 검사를 강제할 절차적 수단이 없다면, 친자관계 청구를 결정할 대체적 수단이 제공되는 경우에만 비례성 원칙에 부합한다고 보았다. 그러나 국내법상 그러한 수단이 부재하였기 때문에, 친부로 추정되는 자가 DNA 검사를 거부함에 따라 청구인은 오랫동안 정체성이 불확실한 상태로 방치되었으므로, 재판소는 제 8 조 위반이라고 판단하였다(*ibid.*, §§ 65-66).

193. *Mifsud v. Malta*, 2019 사건 §§ 61-78 에서는 부친 확인 소송에서 몰타 법률에 따라 청구인에게 본인의 의사에 반해 유전자 검사를 받게 하는 법원의 결정은 제 8 조에 반하지 않았다. 국내 법원은 청구인에게 DNA 검사를 받도록 명령하기 전에, 청구인이 스스로 선택한 변호인의 대리하에 참여하였고 청구인의 절차적 권리가 상대방과 동등하게 보장된 사법 절차 체계 안에서, 사건에서 상충하는 이해관계에 대해 필요한 이익 형량을 하였다. 따라서 국내

법원은 청구인의 딸로 추정되는 자의 부친 관계를 확정할 권리와 청구인이 DNA 검사를 받지 않을 권리 사이에서 적절한 균형을 달성하였다(*ibid.*, § 77). 종합적으로 볼 때, 해당 의사결정 절차는 공정하였고, 제 8 조가 보장하는 청구인의 이익을 적절히 보호하였다.

194. *Boljević v. Serbia*, 2020 사건 §§ 50–56 에서 재판소는 41 년 전 확정판결(남성이 친자관계를 다투는 소송에서 DNA 검사가 존재하지 않던 시기에 인용된 판결)에 대한 재심 청구를 시효 만료를 이유로 국내 법원이 각하한 것이 제 8 조에 반한다고 결정하였다. 재판소는 법적 안정성의 유지만으로는 청구인이 본인의 인격적 정체성에서 중요한 측면에 관한 진실을 알 권리를 박탈할 근거가 될 수 없으며, 반드시 사건 내 상충하는 이해관계를 형량해야 한다고 보았다. 그러나 국내법상 재심 청구의 시효 제한 규정 때문에 당국은 청구인의 사건에서와 같이 특별한 사정을 고려한 이익형량을 할 수 없었고, 청구인은 부친으로 추정되는 남성이 사망한 후 친자관계에 관한 확정판결이 있었다는 사실을 알게 되었다. 재판소는, 망인의 DNA 시료 채취를 위한 요청은 망인의 사생활을 해칠 수 없다고 보았다. 재판소는 이미, 유전자 검사 목적의 유해 발굴에 관한 *Succession Kresten Filtenborg Mortensen v. Denmark* (dec.), 2006 사건과 사망인의 추정상 아들이 생부의 신원을 확인하기 위하여 DNA 검사를 요청한 청구를 법원이 기각하여 제 8 조 위반에 해당한 *Ja¨ggi v. Switzerland*, 2006 사건 § 42 에서도 동일한 결론에 도달하였다(*ibid.*, §§ 34–44).

195. *Caruana v. Malta* (dec.), 2018 사건 §§ 28–42 에서 재판소는 살인범으로 추정되는 자의 아내에게 구강 점막 시료를 제공하게 한 의무에 관한 청구는 명백히 근거가 없다고 선언하였다. 재판소는 구강 면봉 채취는 경미한 개입으로서 신체적 상해나 신체적·정신적 고통을 거의 유발하지 않는다고 판결하였다. 살인은 중대한 형사범죄이므로 가능한 한 많은 증거를 수집하는 것이 합리적이고 필요하였다(*ibid.*, § 41). 나아가 재판소는 증인의 지위와 피고인의 지위를 구별하였는데, 후자의 경우 형사절차에서 그러한 조치를 거부하는 것은 최종적인 유죄 판단 및 관련 제재에 영향을 미칠 수 있는 상황이라는 점을 지적하였다(*ibid.*, § 40).

196. *Dragan Petrovic v. Serbia*, 2020 사건 §§ 79–84 에서, 살인사건 수사 과정에서 구강 면봉 채취는 법의 예측가능성이 결여되어 있었기 때문에 제 8 조 위반에 해당하였다. 청구인이 경찰관들에게 자발적으로 타액 검체를 제공하기로 동의하였다는 사실은, 그렇지 않으면 강제로 타액이나 혈액 검체를 채취당할 것이라는 위협 아래 동의한 것에 불과하였기 때문에, 사생활에 대한 제한을 받았는지와 무관하다고 보았다(*ibid.*, § 79).

197. 재판소는 또한 수혈을 거부한 여호와의 증인들을 대상으로 의료 데이터를 수집한 사건에서 제 8 조 위반이라고 판단하였다(*Avilkina and Others v. Russia*, 2013); 또한, 위 188 참조.

198. 또한 이식 목적으로 적법한 절차에 따라 유족에게 알리거나 동의를 받지 않고 망자의 시신에서 장기를 적출한 경우(*Petrova v. Latvia*, 2014, §§ 87-98) 및 망자의 신체 조직 적출 시 유족 동의 사안에서 국내법의 불명확성에 관한 사건(*Elberte v. Latvia*, 2015, §§ 105-117)도 제 8 조 위반으로 판단되었다.

d. 의료 맥락에서 개인데이터 수집

199. 재판소는 의료 분야에서 민감한 데이터 수집 문제도 살펴보았다. *L.H. v. Latvia*, 2014 사건 §§ 47-60 에서, 공공병원 환자의 의료 데이터를 의료서비스의 품질 관리를 책임지는 국가 기관("기관")이 수집한 것은 자의성을 방지하도록 법적으로 보호하는 명확하게 규정된 법률의 부재로 인하여 제 8 조에 부합하지 않는다고 판단되었다. 해당 기관은 7 년에 걸쳐 문제 된 데이터를 무차별적으로 수집하였고, 수집된 데이터가 조사의 목적에 비추어 "잠재적 결정성"이 있거나 "관련성"이 있거나 "중요성"이 있는지 사전에 평가한 적이 없었다. 또한 기관은 청구인의 데이터 수집을 위해 동의를 요청하거나 받을 의무도 없었다(*ibid.*, § 53). 수집될 수 있는 개인데이터의 범위는 어떠한 방식으로도 제한되지 않았다(*ibid.*, § 57). 나아가 정보 수집 사유의 관련성과 충분성이 국내 절차 단계에서 단 한 번도 심사되지 않았다(*ibid.*, § 57). 이와 같은 맥락에서 재판소는 기관이 개인데이터의 비밀을 유지할 법적 의무가 있었는지는 관련성이 낮다고 보았다(*ibid.*, § 58).

200. *Surikov v. Ukraine*, 2017 사건 §§ 75-95 에서, 정신 건강에 관한 개인데이터의 장기간 수집·보유하고 최초 수집 목적과 무관한 사유로 전달하고 사용한 것은 비례성을 상실한 제한으로서 데이터 주체의 사생활 존중권 침해에 해당하므로 제 8 조를 위반하였다. 특히 특정 기술·책임·역량과 관련된 직무에 배정하는 맥락에서 근로자의 정신적·신체적 건강에 관한 정보에는 고용주에게 정당한 이해관계가 있을 수 있지만, 관련 정보의 수집과 처리는 합법적이어야 하고 고용주의 이익과 해당 직위 지원자의 사생활 비밀 관련 관심사 사이에는 적절한 균형이 유지되어야 한다(*ibid.*, § 91).

201. *Z v. Finland*, 1997 사건 §§ 106-110 에서, 재판소는 청구인의 남편에 대한 형사절차 단계에서 환자의 사전 동의 없이 의료기록을 압수하고 이를 수사기록에 편철한 것과 관련하여 제 8 조 위반이 아니라고 판단하였다. 의사결정 과정에는 어떠한 절차적 하자도 없었으며,

압수 조치를 다투거나 비밀유지명령에 규정된 기간을 무효로 할 수 있는 구제수단도 존재하였다.

202. *Drelon v. France*, 2022 사건 §§ 79-100 에서 청구인은 프랑스 혈액기증서비스의 채혈 장소에서 헌혈하려 하였으나, 동성애적 성향으로 추정된다는 이유로 받아들여지지 않았다. 청구인은 헌혈 전 의료 면담에서 성생활에 관한 질문에 답변하기를 거부하였지만, 수집된 데이터에는 남성이 다른 남성과 성관계를 가진 경우에 적용되는 헌혈 부적격 사유가 기재되어 있었다. 재판소는 해당 데이터의 민감한 성격을 지적하면서, 그 데이터의 수집과 저장은 특히 보건 보호 및 혈액 안전 확보의 중요성 등 적절하고 충분한 사유에 근거하였음을 받아들였다. 동시에 재판소에 따르면 수집된 데이터는 증명된 사실적 근거 없이 단순한 추측에 기반한 것이었다. 또한 데이터 보유 기간이 과도하게 길어, 청구인에게 반복적으로 불리하게 사용될 수 있었고, 그 결과 헌혈에서 자동 배제되었다고 하였다. 재판소는 이러한 여러 요소를 참고하여 협약 제 8 조 위반이라고 판단하였다.

e. 개인데이터 강제 제출

203. 재판소는 여러 차례, 이동통신사업자, 인터넷 서비스 제공자, 은행, 엘리트 운동선수, 병원이 법률 또는 당국의 명령에 따라 보유하고 있는 개인데이터를 당국에 제출해야 하는 의무를 심사하였다.

204. 조직범죄 및 테러리즘 대응과 관련하여, 재판소는 수사 기법이 현대 통신 기술에 맞게 조정되어야 한다는 점을 받아들였다. *Breyer v. Germany*, 2020 사건 §§ 81-110 에서, 선불심카드 이용자의 개인데이터를 기록하고 이를 당국에 제출하도록 이동통신사업자에게 부과된 법적 의무는 사법적 결정이나 당사자에 대한 통지 없이도 여러 공공 당국이 그러한 데이터의 검색 및 제출을 요청할 수 있도록 허용한 전기통신법에 근거하였으며 제 8 조에 반한다고 간주하지 않았다. 한정된 데이터만 저장되었고, 개별 통신 사건과 관련된 데이터는 저장되지 않았으므로, 제한은 비교적 경미하였다(*ibid.*, §§ 92-95). 기술적 보안 보장, 제한된 보유 기간, 가입자를 명확히 식별하는 데 필요한 정보로 한정된 데이터, 향후 조회 및 사용을 위한 규제된 절차, 독립 기관에 의한 감독, 권리 침해를 주장하는 사람이 제기할 수 있는 불복 절차 등 여러 보호조치도 마련되어 있었으며, 이렇게 한정된 데이터 세트의 수집·저장에 대한 비례성 심사에서 검토·감독 수준은 결정적 요소가 아니었다(*ibid.*, §§ 96-107).

205. 반대로, 재판소는 인터넷 서비스 제공자에게 저장된 접속 데이터나 가입자 중 한 명의 접속 데이터를 검색하여 경찰에 제출하게 하는 법적 의무를 부과한 것은, 경찰이 근거로 삼은 법적 규정이 불명확하였고, 특히 문제 된 경찰 권한에 대한 독립적 감독이 부재한 상황에서

자의적 제한을 받지 않도록 보호하지 않았기 때문에, 제 8 조 위반에 해당한다고 보았다(*Benedik v. Slovenia*, 2018, §§ 132–134).

206. *Sommer v. Germany*, 2017 사건 § 63 에서, 변호사인 청구인의 은행 계좌를 조회하는 기준이 지나치게 낮았고, 정보 요청의 범위가 넓으며, 그 후 청구인의 개인정보가 공개되고 계속 저장되었으며 절차적 보호조치가 불충분했기 때문에, 청구인의 은행 계좌에 대한 조회는 제 8 조 위반에 해당하였다.

207. 수혈을 거부한 여호와의 증인들을 대상으로 의료 데이터를 수집한 *Avilkina and Others v. Russia*, 2013 사건 § 54 에서 재판소는 검찰이 청구인들을 진료한 의료기관으로부터 청구인들에 관한 데이터를 수집하면서 데이터 주체에게 알리거나 이의를 제기할 기회를 부여하지 않은 것은 제 8 조에 부합하지 않는다고 판결하였다. 검찰청은 문제 된 종교단체를 대상으로 제기된 이의를 처리하기 위해, 해당 개인들을 직접 조사하거나 동의를 구하는 등 다른 선택지가 있었음에도 불구하고 그러한 절차를 거치지 않았다(*ibid.*, § 48).

208. *National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, 2018 사건 §§ 155–191 에서, 반도핑 정책의 일환으로 불시 도핑검사를 실시하기 위하여 엘리트 선수 "검사 대상 집단"에 부과된 소재지를 보고할 법적 요건은, 연속 18 개월 동안 세 번째 불이행 시 중대한 제재가 따르도록 규정되어 있었으나, 제 8 조에 반한다고 간주하지 않았다. 재판소는 소재지 보고 의무가 청구인들의 사생활에 미치는 영향을 과소평가하지 않으면서도, 엘리트 선수들에게 부과된 의무를 완화하거나 폐지할 경우 도핑이 선수들의 건강 및 전체 스포츠 공동체의 건강에 미치는 위험성을 높이고, 불시검사의 필요성에 관한 유럽 및 국제적 합의에도 배치된다고 보았다(*ibid.*, § 191).

209. *Aycaguer v. France*, 2017 사건 §§ 45–47 에서 재판소는 청구인이 국가 전산 전과자 DNA 데이터베이스에 DNA 프로필을 기록하기 위한 강제 생물학적 검사를 거부하여 유죄판결을 받은 것은 민주사회에서 필요한 조치로 간주할 수 없으므로 제 8 조 위반이라고 판단하였다. 청구인이 강제 DNA 검사 명령을 받게 된 행위는 정치·노동조합적 맥락에서 발생한 것으로, 신원이 확인되지도 않은 군사경찰들을 향해 우산을 휘두르기만 한 행위에 불과하였고, 이에 대해 청구인은 징역 2 월에 집행유예 판결을 받았다. 청구인의 상황이 보여주듯 발생할 수 있는 상황이 서로 현저하게 다를 수 있는데도, 전산 DNA 데이터베이스에는 범죄의 성격과 심각성에 따라 차등을 두는 규정이 없었다(*ibid.*, § 43). 마지막으로, 청구인은 저장된 데이터를 삭제할 수 있는 어떠한 절차에도 접근할 수 없었는데, 그러한 절차는 범죄 혐의자에게만 부여되었고 이미 유죄판결을 받은 자에게는 적용되지 않았다(*ibid.*, § 43).

2. 개인데이터 보유

210. 공공 당국이 개인의 사생활과 관련된 정보를 어떠한 방식으로 획득하였든 이를 저장하는 행위는, 그 정보가 이후 실제로 사용되는지 여부와 무관하게, 협약 제 8 조의 의미에서 데이터 주체의 사생활 존중권에 대한 제한에 해당한다(*Amman v. Switzerland* [GC], 2000, § 69; *Rotaru v. Romania* [GC], 2000, § 46; *S. and Marper v. the United Kingdom* [GC], 2008, § 67; *M.K. v. France*, 2013, § 29; *Aycaguer v. France*, 2017 § 33). 이러한 정보는 본질적으로 사적인 성격이므로, 재판소는 당사자의 동의 없이 당국이 보유와 사용을 승인하는 국가 조치를 엄격하게 심사해야만 한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 104).

a. 범죄 대응 목적의 개인데이터 저장

211. 지문, DNA 정보 등 개인데이터 보호와 관련된 데이터 주체와 공동체 전체의 이익보다 범죄 예방이라는 정당한 이익이 우선할 수도 있다(*S. and Marper v. the United Kingdom* [GC], 2008, § 104). 국가 당국은 국민을 보호하기 위하여, 성범죄 같은 중대범죄를 포함하여 특정 범죄의 처벌과 예방에 이바지하는 실효적인 수단으로 데이터베이스를 정당하게 구축할 수 있다(*B.B. v. France*, 2009, § 62; *Gardel v. France*, 2009, § 63; *M.B. v. France*, 2009, § 54; *N.F. and Others v. Russia*, 2023, § 44). 이러한 정보를 처음 수집하는 목적은 특정인과 의심되는 범죄를 연계하는 것이지만, 이 정보를 보유하는 것은 미래의 범죄자 신원 파악에 활용하는 것으로 목적의 범위를 넓어진다(*S. and Marper v. the United Kingdom* [GC], 2008, § 100). 재판소는 이러한 등록부의 예방적 목적 자체를 문제 삼을 수 없다(*Gardel v. France*, 2009, § 63; *B.B. v. France*, 2009, § 62; *M.B. v. France*, 2009, § 54). 오늘날 유럽 사회가 직면한 과제 중 하나인 범죄와 특히 조직범죄 및 테러리즘과의 싸움은 현대 과학적 수사·신원 확인 기법의 활용에 상당 부분 의존한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 105). 동시에, 개인데이터의 보호는 협약 제 8 조가 보장하는 사생활 및 가족생활 존중권의 향유에 근본적인 요소이므로, 국내법은 이 조항의 보장과 양립할 수 없는 방식으로 개인데이터가 사용되는 것을 방지하는 적절한 보호조치를 마련해야 한다(*ibid.*, § 103; *Glukhin v. Russia*, 2023, § 75).

212. 재판소는 범죄의 처벌 및 예방을 목적으로 한 데이터베이스에 경범죄(*M.K. v. France*, 2013, §§ 6, 8, 41; *Aycaguer v. France*, 2017, §§ 8, 43), 중범죄(*B.B. v. France*, 2009, §§ 6, 62; *Gardel v. France*, 2009, §§ 8, 9, 63; *M.B. v. France*, 2009, §§ 6, 54; *Peruzzo and Martens v. Germany* (dec.), 2013, §§ 6, 12, 37–38; *Trajkovski and Chipovski v. North Macedonia*, 2020, §§ 6, 12) 또는 경범죄도 중범죄도 아닌 일련의 범죄(*P.N.*

v. Germany, 2020, §§ 6, 81)로 유죄 판결을 받은 자의 개인데이터가 기록된 사건을 살펴보았다. 범죄의 처벌 및 예방을 목적으로 한 데이터베이스에 범죄 혐의를 받았으나 결국 불기소 처분된 자(*S. and Marper v. the United Kingdom* [GC], 2007, §§ 10, 11, 113; *M.K. v. France*, 2013, §§ 7, 9, 42; *Brunet v. France*, 2014, §§ 6, 7, 40), 무죄 판결을 받은 자(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 10, 113) 또는 재판 후 단순히 경고 처분만 받고 유죄판결은 받지 않은 자(*M.M. v. the United Kingdom*, 2012, §§ 7-9)의 개인데이터가 저장된 사안에 관한 사건도 있었다. 한 사건에서는 청구인들의 개인데이터가 단지 여러 차례 형사소추를 당했다는 이유만으로 내무부 데이터베이스에 수집·저장되었다. 당시의 기록 시스템은 범죄의 성격과 중대성에 관계없이, 그러한 유죄판결이 소멸하였거나 실효되었더라도 형사 유죄판결뿐만 아니라, 개인이 형사소추를 당했다가 이후 "비갱생 사유"로 절차가 종결된 경우까지 포함하였다(*N.F. and Others v. Russia*, 2023, § 49). 마지막으로, 단순한 혐의에 근거하여 경찰 파일에 개인데이터를 저장하는 예방적 조치와 관련된 사건도 있었다(*Shimovolos v. Russia*, 2011, § 16; *Khelili v. Switzerland*, 2011, §§ 8, 9, 59; *Catt v. the United Kingdom*, 2019, §§ 6, 14, 119).

213. 경찰 목적을 위한 개인데이터 저장의 필요성을 심사할 때 아래에 제시되는 여러 요소를 중요하게 고려한다.

i. 저장된 데이터의 무차별·비차별적 성격

214. 재판소는 여러 사건에서, 당국이 설치한 데이터 저장 시스템이 유죄판결에 이르게 된 범죄의 성격이나 심각성에 따른 구별을 하지 않았거나(*M.K. v. France*, 2013, § 41; *Aycaguer v. France,* 2017, § 43; *Gaughran v. the United Kingdom*, 2020, § 94; *N.F. and Others v. Russia*, 2023, § 49) 데이터 주체가 유죄판결을 받았는지, 무죄 판결을 받았는지, 불기소 처분을 받았는지, 아니면 단순히 범죄 혐의만을 받고 경고 처분에 그쳤는지에 따라 구별하지 않은 점(*S. and Marper v. the United Kingdom* [GC], 2008, § 119; *M.M. v. the United Kingdom*, 2012, § 198; *M.K. v. France*, 2013, § 42; *Brunet v. France*, 2014, § 41; *N.F. and Others v. Russia*, 2023, § 49)을 문제 삼았다. 재판소는 특정 범죄의 처벌과 예방을 지원하기 위해 마련된 제도가 저장되는 정보의 양을 극대화하려는 남용적 경향의 일환으로 시행되어서는 안 된다고 본다(*M.K. v. France,* 2013, § 35; *Aycaguer v. France,* 2017, § 34). 실제로 이러한 제도가 추구하는 정당한 목적에 비례성을 유지하지 못한다면, 그 장점은 국가가 협약에 따라 관할권 내의 사람들에게 보장해야 할 권리와 자유에 대한 중대한 침해로 상쇄되고 말 것이다(*M.K. v. France,* 2013, § 35; *Aycaguer v. France,* 2017, § 34).

215. *S. and Marper v. the United Kingdom* [GC], 2008 사건 §§ 119, 125 에서, 범죄 혐의를 받았으나 유죄판결을 받지 않은 모든 사람으로부터, 연령이나 범죄의 성격·심각성과 무관하게 지문·생물 검체·DNA 프로필을 수집·저장할 수 있도록 한 데이터베이스는, 데이터 보유의 정당성을 명확한 기준에 따라 심사하는 독립적 검토 절차나 보유 기간의 제한 없이 운영되었으며, 그 결과 제 8 조 위반으로 판단되었다. 이러한 제도의 포괄적이고 무차별적인 성격은 상충하는 공익과 사익 간 적절한 균형을 반영하지 못하였다.

216. 범죄로 유죄판결을 받지 않았고, 무죄추정의 원칙을 보장받아야 할 사람들이 유죄판결을 받은 자와 동일하게 취급되는 경우 낙인효의 위험이 존재한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 122). 범죄 혐의를 받았다가 무죄 판결이나 불기소 처분을 받은 자의 개인데이터를 보유하는 것을 혐의를 제기하는 것과 동일시할 수는 없으나, 유죄판결을 받은 자의 데이터와 동일하게 무기한 보유된다는 사실은 범죄 혐의를 받은 적 없는 자의 데이터는 폐기된다는 규정과 대비되어 무죄로 대우받지 못하고 있다는 인식을 강화한다(*ibid.*, § 122). 따라서 범죄 혐의를 받은 후 불기소 처분을 받은 자라는 사실은 유죄판결을 받은 자와 달리 대우할 정당한 근거가 된다(*ibid.*, § 122; 또한, 같은 취지에서 *M.K. v. France*, 2013, § 42; *Brunet v. France*, 2014, § 40 참조). 그러므로 청구인이 조정 후 불기소 결정을 받은 *Brunet v. France*, 2014 사건 § 40 에서 재판소는 당국의 기록에 개인데이터가 무차별적으로 등재되어 유죄판결을 받은 자와 절차가 종결된 자 사이에 어떠한 구별도 두지 않은 점을 문제 삼았다. 중범죄가 아닌 범죄로 유죄판결을 받은 후 개인데이터가 수집·보유된 *Aycaguer v. France*, 2017 사건 §§ 42-43 에서 재판소는, 법 적용 단계에서 발생할 수 있는 상황은 매우 다양한데도, 당국이 범죄의 심각성 수준에 따른 구별 없이 광범위하게 개인데이터를 수집한 범위를 문제 삼았다. 재판소의 견해에 따르면, 청구인에게 유죄판결을 이끌었던 행위인 정치·노동조합 맥락에서 군사경찰을 향해 우산으로 몇 차례 휘두르기만 한 것은 성범죄, 테러, 반인도범죄, 인신매매 같은 중대범죄에 해당하는 행위와 비교할 수 없는 것이었다.

217. *M.M. v. the United Kingdom*, 2012 사건 §§ 187-207 에서, 아들의 결혼 파탄 이후 손자의 호주 출국을 막기 위해 영아였던 손자와 함께 청구인이 하루 동안 실종되었던 사건과 관련하여, 경찰 기록에 경고 처분이 평생 기록되는 것은 제 8 조 위반이라고 판단되었다. 재판소는, 유죄판결은 물론 주의, 경고 처분, 견책 같은 비(非)유죄 처분뿐만 아니라, "데이터 주체가 100 세에 이를 때까지 데이터를 보유해야 한다"라는 일반 지침에 따라 경찰이 기록한 대량의 보충적 데이터까지도 포함하는, 지나치게 포괄적인 데이터 보유 제도의 범위를 문제 삼았다(*ibid.*, § 202). 재판소는 기록 제도의 범위가 넓어지면서 보유·공개되는 데이터의 양과 민감성이 커질수록, 이후 데이터가 처리되는 여러 핵심 단계에서 적용될 보호조치의 내용이

더욱 중요해진다고 보았다(*ibid.*, § 200). 음주 운전으로 유죄판결을 받은 청구인의 생체 데이터와 사진을 무기한 저장한 것이 제 8 조 위반에 해당한 *Gaughran v. the United Kingdom*, 2020 사건 §§ 94–97 에서도 동일한 원칙이 적용되었다.

218. *N.F. and Others v. Russia*, 2023 사건 §§ 49–55 에서는 개인이 형사소추를 당하면 자동으로 형사절차 관련 정보가 수집·저장되는 데이터 저장 시스템을 살펴보았다. 이 시스템은 범죄의 성격이나 중대성과 무관하게 모든 형사 유죄판결 정보를 포함하였고, 그 유죄판결의 실효 여부도 상관하지 않았으며, 나아가 "비갱생 사유"로 종결된 형사절차에 관한 정보까지 포함하였다. 재판소는 이 시스템의 범위와 적용이 과도하다고 판단하였다. 또한 재판소는 유죄판결을 받은 적이 없는 개인의 경우 데이터가 계속 처리되는 것이 특히 침해적이라는 점을 강조하였다. 유죄판결을 받은 개인이라 하여도, 그 판결이 이미 실효되었거나 법원에 의해 취소된 이후라면 사생활을 제한하는 것은 여전히 침해적일 수 있었다. 남용에 대한 충분한 보장과 검토 가능성이 결여된 상태였으므로, 비례성을 상실한 처리라고 판단되었다.

219. 유죄판결을 받지 않은 자의 데이터를 보유하는 것은, 미성년자의 특수한 상황과 발달 및 사회 통합의 중요성을 고려할 때 특히 해로울 수 있다. 그러한 유형의 불이익으로부터 미성년자를 보호하도록 각별히 주의해야 한다(*S. and Marper v. the United Kingdom* [GC], 2008, § 124).

ii. 데이터 보유 기간

220. 당국이 개인의 개인데이터를 얼마나 오랫동안 보유할지는, 해당 데이터를 경찰 목적을 위해 기록이나 데이터베이스에 저장하는 것이 추구되는 정당한 목적에 비례하는지 평가할 때 결정적이라고 할 수 없지만 중요한 요소이다. 재판소는 다음과 같은 사건에서 제 8 조 위반이라고 판단하였다.

- 범죄 혐의를 받았으나 불기소 처분 또는 무죄판결로 절차가 종결된 자의 지문 및 DNA 데이터를 무기한 보유한 경우(*S. and Marper v. the United Kingdom* [GC], 2008)
- 유죄판결이 법정 기간 만료로 경찰 기록에서 삭제된 이후에도 개인의 DNA 프로필, 지문 및 사진을 무기한 보유한 경우(*Gaughran v. the United Kingdom*, 2020)
- 개인에 관한 모든 유죄판결, 무죄판결, 경고처분, 주의, 견책을 평생 경찰 기록에 보유하는 경우(*M.M. v. the United Kingdom*, 2012)

- 가중절도죄로 유죄판결을 받은 자의 DNA 프로필을 무기한 보유한 경우(*Trajkovski and Chipovski v. Macédoine du Nord*, 2020)
- 비교적 경미한 범죄로 유죄판결을 받은 자의 개인데이터를 최대 40 년간 보유한 경우(*Ayçaguer v. France*, 2017)
- 도서 절도 혐의를 받았으나 유죄판결을 받지 않은 자의 지문을 최대 20 년간 보유한 경우(*M. K. v. France*, 2013)
- 배우자에 대한 폭력 혐의로 고소를 당하였으나 조정(mediation)으로 종결된 사건에서 개인데이터를 최대 20 년간 보유한 경우(*Brunet v. France*, 2014)
- 청구인의 대체적 행정벌에 관한 데이터를 무기한 보유한 경우(*Tonchev v. Bulgaria*, 2024)

221. 반대로, 재판소는 성폭행으로 유죄판결을 받은 자의 개인데이터를 최대 30 년간 보유한 후 자동으로 삭제하도록 규정된 여러 사건에서는, 데이터가 더 이상 관련성이 없게 되면 즉시 삭제할 수 있게 하는 절차가 도입되었기 때문에, 제 8 조 위반이 아니라고 판단하였다(*B.B. v. France*, 2009, § 67; *Gardel v. France*, 2009, § 69; *M.B. v. France*, 2009, § 59). 또한 재판소는 중대범죄로 유죄판결을 받은 자의 개인데이터를 무기한 보유하되, 그 보유의 필요성을 판단하기 위해 10 년 간격을 넘지 않는 정기적인 검토가 수반된 사건에 대해서는, 그 청구를 명백히 근거 없다고 선언하였다(*Peruzzo and Martens v. Germany* (dec.), 2013, §§ 44–49). *P.N. v. Germany*, 2020 사건 §§ 87–90 에서 재판소는 상습범의 개인데이터를 새로운 형사절차 개시 이후 신원을 확인하기 위해 5 년간 보유하도록 한 조치에 대해, 적절한 보장과 개별적 검토가 수반된다는 점에서 제 8 조 위반이 아니라고 판단하였다.

222. 유죄판결을 받은 자의 생체 데이터 보유 제도와 관련하여, 국가가 해당 제도를 마련할 때 허용할 수 있는 판단재량의 한계를 벗어났는지 평가하는 결정적 요소가 되는 것은 보유 기간의 길이 자체가 아니라 특정한 보호조치의 존재와 작동 여부이다(*Gaughran v. the United Kingdom*, 2020, § 88). 국가가 유죄판결을 받은 자의 생체 데이터 보유 기간에 제한을 두거나, 데이터 보유를 무기한으로 정할 경우, 그 자체로 판단재량의 한계에 도달하게 되므로 반드시 실효적인 보호조치를 확보하여야 한다(*ibid.*, § 88). 특히, 범죄의 심각성, 개인 혐의의 강도, 전과, 그 밖의 특별한 사정과 같은 명확한 기준에 따라 데이터 보유의 정당성을 독립적으로 심사할 수 있는 절차의 존재 여부는 데이터 보유 기간의 비례성을 보장하는 중대한 보호조치이다(*ibid.*, § 94; *S. and Marper v. the United Kingdom* [GC], 2008, § 119; *B.B. v. France*, 2009, § 68; *Gardel v. France*, 2009, § 69; *M.B. v. France*, 2009, § 60).

223. 개인데이터 보유 기간에 상한이 없다고 해서 반드시 제 8 조에 어긋나는 것은 아니지만(*Peruzzo and Martens v. Germany* (dec.), 2013, § 46; *Gaughran v. the United Kingdom*, 2020, § 88), 데이터 보유가 전적으로 당국이 보유 기간의 비례성을 보장하기 위하여 주의 의무를 얼마나 다하느냐에 달려 있다면, 절차적 보호조치가 특히 필요한 경우가 된다(*Peruzzo and Martens v. Germany* (dec.), 2013, § 46; *Ayçaguer v. France*, 2017, § 38).

224. 중대범죄로 유죄판결을 받고 재범 위험이 있는 자의 생체 데이터를 무기한 보유한 *Peruzzo and Martens v. Germany* (dec.), 2013 사건 § 44 에서 재판소는, 국내법에 따라 연방형사청이 사건별로 데이터 보유 목적과 개인데이터가 기록된 사안의 성격 및 중대성을 고려하여, 10 년을 초과하지 않는 정기적 간격으로 데이터 보유의 필요성과 삭제 여부를 점검하게 되어 있다는 사실을 긍정적으로 평가하였다(*ibid.*, § 46). 재판소는 구체적인 심각성의 기준선에 도달하는 범죄로 유죄판결을 받은 자의 DNA 프로필만 채취될 수 있다는 점을 고려할 때 그러한 점검 간격의 길이가 불합리하다고 볼 수는 없다고 판결하였다(*ibid.*, §§ 48-49).

225. *Gaughran v. the United Kingdom*, 2020 사건 § 96 에서, 음주 운전으로 유죄판결을 받은 개인의 지문, DNA 프로필 및 사진을 무기한 저장한 것은 제 8 조 위반이라고 판단하였다. 당국은 범죄의 심각성이나 해당 데이터를 계속해서 무기한 보유할 필요성을 고려하지 않았고, 실질적인 검토 절차도 제공하지 않았다(*ibid.*, § 96).

226. 국내법에 규정된 개인데이터의 최대 저장 기간은, 법이 정한 기간 만료 전에 데이터 삭제를 요청하더라도 그것이 받아들여질 가능성이 단순히 가정에 불과하다면, 실제로는 진정한 상한이라기보다 하나의 규범에 가까운 것으로 볼 수 있다(*M. K. v. France*, 2013, §§ 44-47; *Brunet v. France*, 2014, §§ 41-45; *Ayçaguer v. France*, 2017, §§ 44-46). 재판소는 국내 제도가 절차가 종결된 범죄에 대해 20 년 또는 25 년의 최대 저장 기간을 규정한 경우(*M. K. v. France*, 2013, §§ 44-47; *Brunet v. France*, 2014, §§ 41-45) 및 중대범죄가 아니었지만, 유죄판결로 이어진 사건에 대해 최대 40 년의 저장 기간을 규정한 경우(*Ayçaguer v. France*, 2017, § 42) 제 8 조 위반이라고 판단하였다.

227. *Catt v. the United Kingdom*, 2019 사건 § 120 에서, 청구인의 개인데이터가 극단주의 관련 국가 경찰 데이터베이스에 최소 6 년간 보유된 후 예정된 검토를 거치도록 한 것은 제 8 조 위반이라고 판단되었다. 청구인은 데이터 보유 기간의 비례성을 보장하기 위하여 유관 실무준칙에 규정된 매우 유연한 보호조치의 이행 여부를 당국의 주의 의무에 전적으로 의존할 수밖에 없었다. 데이터 보유가 비례성을 상실하는 즉시 삭제하게 하는 보호조치가

결여된 점은 재판소가 보호 수준을 높인 영역인 정치적 견해를 드러내는 데이터가 무기한 보유되고 있었기 때문에 특히 문제가 되었다(*ibid.*, §§ 122-123).

228. *M.M. v. the United Kingdom*, 2012 사건은 범죄기록에 관한 개인데이터 보유 기간에 대한 정책 변경이 데이터 주체의 취업 전망에 미친 결과와 관련된 것이었다(§ 204). 재판소는, 적용될 보호조치를 명확히 하고, 그러한 데이터의 보유 기간 등을 규율하는 규칙을 명시한 명확하고 상세한 법률 규정이 존재하지 않는 한, 범죄기록 데이터의 무차별적이고 무기한적인 수집은 제 8 조의 요건을 충족하기 어렵다고 보았다(*ibid.*, § 199).

229. 또한, 맥락을 달리하여, *Z v. Finland*, 1997 사건 §§ 111-113 에서 개인의 신원과 HIV 양성 여부를 드러내는 의료 데이터가 포함된 절차에서 제출된 증거에 대해, 법원이 그 비밀유지 기간을 10 년으로 제한한 사례 참조. 이 사건에서 10 년의 비밀유지 기간은 소송 당사자들의 의사 및 이익과 상충하였으며, 청구인의 동의 없이 문제 된 정보가 제출된 사실만으로도 이미 사생활 및 가족생활 존중권에 대한 심각한 제한을 초래하였다. 만약 10 년 후 해당 의료 정보에 대중이 접근할 수 있게 된다면 청구인에게 추가로 가해질 제한은 아무리 중대한 사유가 있다고 해도 정당화되지 않는다.

iii. 저장된 데이터 파기·삭제에 관한 보호조치[9]

230. 재판소의 견해에 따르면, 경찰 목적을 위하여 저장된 데이터베이스에서 데이터를 삭제하는 것은 특별히 부담스러운 일이 아니었다(*Catt v. the United Kingdom*, 2019, § 127). 만약 정부가 데이터베이스를 구축하면서 그 안의 데이터를 쉽게 검토하거나 수정할 수 없게 한 다음 해당 데이터베이스에서 정보를 삭제하지 않겠다는 정당화의 근거로 삼는다면, 이는 제 8 조에 따른 사생활 보호 필요성과 정면으로 배치된다(*ibid.*, § 127).

231. 국내 차원에서, 특정 기준에 따라 정보 보유의 정당성을 독립적으로 심사하고, 데이터 주체의 사생활 존중권을 적절하고 실효적으로 보장하는 데이터 삭제를 위한 사법 절차가 마련되어 있는지는, 상충하는 다양한 이해관계 사이에서 균형을 이루는 데 중요한 요소이다(*S. and Marper v. the United Kingdom* [GC], 2008, § 119; *Gardel v. France*, 2009, § 69).

232. 재판소는 데이터가 최대 30 년까지 "장기간" 보유된 경우이거나(*B.B. v. France*, 2009, §§ 66, 68; *Gardel v. France*, 2009, §§ 67, 69; *M.B. v. France*, 2009, §§ 58, 60), 심지어 무기한 보유된 경우에도(*Peruzzo and Martens v. Germany* (dec.), 2013, § 46) 데이터 주체가 특정 기준에 따라 데이터 보유의 정당성을 독립적으로 심사받을 수 있는 사법

[9] 또한, 상기 데이터 삭제권 참조.

절차를 통해 구제받고, 이를 통해 법에 규정된 최대 보유 기간 만료 전에 데이터를 삭제할 수 있었거나, 무기한 보유의 경우에는 그 관련성을 상실하는 즉시 삭제할 수 있었던 상황이라면 제 8 조 위반이 아니라고 판단하였다(상반되는 취지로, *S. and Marper v. the United Kingdom* [GC], 2008, § 119 참조).

233. 따라서 *B.B. v. France*, 2009 사건 § 68, *Gardel v. France*, 2009 사건 § 69 및 *M.B. v. France,* 2009 사건 § 60 에서 재판소는 데이터 주체가 단순히 검찰에 신청함으로써 개시할 수 있고, 그 결정에 대해 사법적 항고가 가능한 데이터 삭제를 위한 사법 절차가, 명확한 기준에 따라 정보 보유의 정당성을 독립적으로 심사하며, 적절하고 실효적인 보호조치를 제공한다고 결정하였다. 또한, *Peruzzo and Martens v. Germany* (dec.), 2013 사건 § 44 에 관한 204 참조.

234. 경범죄자도 중범죄자도 아니었던 성인 범죄자의 개인데이터 보유에 관한 *P.N. v. Germany*, 2020 사건 §§ 81, 88 에서, 해당 데이터 주체에 대해 새로운 형사 수사가 개시되지 않은 상태로 5 년이 경과하면 데이터가 삭제되도록 한 규정은 제 8 조에 반한다고 판단하지 않았다. 그동안 경찰 당국이 데이터 추가 보유의 필요성을 심사할 수 있었고, 그 결정은 사법 심사 대상이었으므로, 청구인은 해당 데이터가 경찰 목적으로는 더 이상 필요하지 않다는 것을 행실로 보여준다면 데이터를 삭제할 수 있었다(*ibid.,* § 88).

235. 초기 목적에 더 이상 관련되지 않는 개인데이터를 삭제할 수 있도록 하는 실효적 보호조치가 부재한 것은, 보호 수준을 높여야 하는 민감한 범주의 개인데이터와 관련하여 특히 문제가 된다(*Catt v. the United Kingdom*, 2019, § 123).

236. 국내법상 데이터 삭제 가능성은, 언제든지 그러한 삭제를 요청할 권리가 가능한 한 자료가 많은 파일을 보유하려는 수사기관의 이익과 충돌할 수 있고, 그 과정에서 대립하는 이해관계가 부분적으로라도 모순될 수 있는 경우에는, "실질적이고 실효적인" 보호조치라기보다는 "이론적이고 허구적인" 보장에 불과하다(*M.K. v. France,* 2013, § 44). 또한, 데이터 주체가 자신의 데이터 삭제를 요청한 후에도 당국이 이를 거부하거나 계속 보유하는 이유에 대해 아무런 설명도 제공하지 않는다면, 데이터 삭제에 관한 보호조치의 효과는 제한적일 수밖에 없다(*Catt v. the United Kingdom*, 2019, § 122). 마찬가지로, 삭제 요청이 극히 예외적인 경우에만 허용되거나, 데이터 주체가 범죄를 저질렀음을 인정하고 데이터가 정확하다는 이유로 기각되는 경우에도 동일하다(*M.M. v. the United Kingdom*, 2012, § 202).

237. 재판소는 범죄로 유죄판결을 받은 개인 역시 무죄 판결이나 불기소 처분을 받은 자와 마찬가지로, 등록된 데이터의 삭제를 요청할 수 있는 실질적인 수단이 있어야 한다고

본다(*B.B. v. France*, 2009, § 68; *Brunet v. France*, 2014, §§ 41-43; *Ayçaguer v. France*, 2017, § 44). 데이터 삭제 절차가 범죄 혐의자에게만 제공되고 유죄판결을 받은 자에게는 제공되지 않았던 *Ayçaguer v. France*, 2017 사건 § 44 에서 재판소는 제 8 조 위반이라고 판단하였다. 재판소는 DNA 프로필을 국가 데이터베이스에 보유하도록 한 규정이, 그 기간과 삭제 가능성의 부재로 인해 상충하는 공익과 사익 사이에서 적절한 균형에 도달하지 못한다고 평하였다(*ibid.*, § 45).

238. *Khelili v. Switzerland*, 2011 사건 §§ 68-70 에서, 재판소는 불법 성매매 혐의로 유죄판결을 받은 적도 없던 청구인이 경찰 기록의 "직업"란에 기재된 "성매매 종사자" 항목을 삭제하려던 과정에서 마주한 불확실성과 어려움을 지적하면서, 제 8 조 위반이라고 판단하였다. 재판소는 문제 된 경찰 기록의 항목 삭제가 기술적 사유로 불가능하거나 어렵다고 주장된 바는 전혀 없었다고 하였다(*ibid.*, § 68).

iv. 제 3 자의 접근을 규율하고 데이터의 무결성과 기밀을 보호하는 보장책

239. 재판소는 적용할 수 있는 국내법에 공식 데이터베이스에 저장된 개인데이터를 오용과 남용으로부터 실효적으로 보호할 수 있는 보장 장치가 있는지 여러 차례 심사하였다(*S. and Marper v. the United Kingdom* [GC], 2008, § 103; *B.B. v. France*, 2009, § 61; *Gardel v. France*, 2009 § 62; *M.M. v. the United Kingdom*, 2012, § 195; *M.K. v. France*, 2013, § 35; *Brunet v. France*, 2014, § 35; *Ayçaguer v. France*, 2017, § 38). 재판소는 다음과 같은 경우에 그러한 보장 장치가 마련되어 있다고 하였다.

- 등록된 데이터를 열람할 수 있는 기관은 비밀유지 의무를 지닌 기관으로 한정된 경우(*B.B. v. France*, 2009, § 69; *Peruzzo and Martens v. Germany* (dec.), 2013, § 47)
- 등록된 데이터는 데이터베이스를 열람할 수 있는 권한이 부여된 사람을 특정하는 등, 열람 절차와 관련하여 충분히 명확하게 규정된 절차의 적용을 받는 경우(*M.K. v. France*, 2013, § 37; 상반되는 취지로는 *Khelili v. Switzerland*, 2011, § 64 참조)
- DNA 검체를 채취한 개인의 신원이 DNA 프로파일링을 담당하는 전문가에게 공개되지 않았고, 전문가들에게는 검체의 무단 사용을 방지하기 위한 적절한 조처를 할 의무가 부과된 경우(*Peruzzo and Martens v. Germany* (dec.), 2013, § 45), DNA 프로필을 확립하는 목적에 더 이상 필요하지 않은 세포 물질은 즉시 파기되어야 했으며, 그러한 세포 물질로부터 추출된 DNA 프로필만이 연방범죄수사청 데이터베이스에 보존될 수 있는 경우(*ibid.*, § 45), 또한 보존된 DNA 프로필은

형사절차 목적이나 범죄 예방 목적에 필요한 경우에 한해 관련 당국에만 공개될 수 있었던 경우(*ibid.*, § 47).

240. 등록부의 사용 규칙과 접근할 수 있는 공공 당국의 범위가 여러 차례 확대되어 더 이상 사법 당국과 경찰에만 한정되지 않고 행정기관도 접근할 수 있게 된 *Gardel v. France*, 2009 사건 § 70 에서 재판소는 해당 등록부가 오직 비밀유지 의무를 지닌 당국에 의해, 명확하게 규정된 상황에서만 열람될 수 있다는 점을 확인하고 이를 긍정적으로 평하였다.

241. *P.N. v. Germany*, 2020 사건 § 89 에서는 성인 범죄자로부터 채취하여 경찰이 최대 5 년간 보유한 신원 확인용 데이터가 무단 접근이나 유포와 같은 남용을 방지할 정도로 보호되지 않았다는 점을 시사하는 어떠한 정황도 없었다.

242. 반대로, 한 개인의 경찰 기록에 경고 처분을 평생 보유하고 구직 과정에서 그 데이터를 장래 고용주에게 공개한 *M.M. v. the United Kingdom*, 2012 사건 § 204 에서 재판소는 구직자의 범죄기록에 대한 제 3 자 접근을 규율하는 절차에 결함이 있어, 중앙기록에 보유된 데이터가 지원 직무와 관련성이 있는지 또는 데이터 주체가 여전히 위험을 초래할 수 있다고 인식될 정도인지를 어떠한 단계에서도 평가할 수 없게 되어 있던 점을 문제 삼았다. 마찬가지로, "비갱생 사유"로 종결되었거나 유죄판결로 끝난 형사절차에 관한 정보를 포함한 데이터베이스와 관련된 *N.F. and Others v. Russia*, 2023 사건 § 51 에서 재판소는 해당 데이터 처리의 목적이나 다른 중요한 기능에 대한 구별이 규정상 전혀 존재하지 않아, 제 3 자의 접근 가능성과 관련하여 협약 제 8 조의 요건에 부합하는 비례성 심사를 실질적으로 할 수 있는 여지가 없다고 평하였다.

b. 의료 맥락에서 개인데이터 보유

243. 재판소는 건강과 관련된 민감한 데이터의 저장 문제를 살펴보았다. *Malanicheva v. Russia* (dec.), 2016 사건 §§ 13, 15–18 에서 재판소는 보건의료기관의 효율적 운영과 사법적 의사결정 과정에서 관련 데이터를 저장하고 공유할 필요가 있다고 판결하였다. 또한, 청구인의 이름이 정신질환자 병원 등록부에 기재된 것과, 그 이후 보건의료기관 간의 내부 교신 및 법원에 제출된 의견서에서 청구인의 정신 건강상 여러 측면이 잘못 언급되었다는 청구는 명백히 근거 없다고 보아 기각하였다. 문제 된 등록 정보가 대중에게 공개되었거나, 데이터 주체에게 가장 적합한 의료적 처치를 결정하는 것 외의 목적으로 사용되었다는 정황은 전혀 없었다.

244. 2004 년에 수집된 청구인의 동성애적 성향에 관한 개인데이터를 2278 년까지 보유하게 한 *Drelon v. France*, 2022 사건 § 98 에서 재판소는 그 기간이 과도하다고 보았다.

245. 과거에 위원회는, 국내 법원에서 위법으로 선언된 환자의 강제입원에 관한 데이터가 정신병원 기록에 기재된 사건에서, 그 청구를 명백히 근거 없다고 선언하며 각하하였다 (*Yvonne Chave née Jullien v. France*, 1991). 위원회는 정신질환자와 관련된 정보를 기록하는 것은 공립병원 서비스의 효율적 운영을 보장하는 정당한 이익뿐 아니라, 자의적 입원의 위험을 예방하고 정신병원 감독을 담당하는 행정 당국이나 사법 당국이 사용할 수 있는 조사 수단이 되므로 환자 자신의 권리를 보호하는 정당한 이익에도 부합한다고 판결하였다. 이 사건에서 청구인의 개인데이터는 정신병원 등록부에 기록되었으나, 적절한 비밀유지 규칙으로 보호되고 있었다.

246. 또한, *Surikov v. Ukraine*, 2017 사건 § 75-95 에서 제 8 조 위반이 문제 된 사안은 182 참조.

c. 언론 목적의 개인데이터 온라인 저장

247. 재판소는 언론이 과거에 보도된 뉴스를 보관하는 기사 보관소를 유지하고 이를 대중이 이용할 수 있도록 하는 데 있어, 부차적이지만 여전히 중요한 역할을 수행한다고 강조하였다. 이와 관련하여, 온라인 기사 보관소는 교육과 역사 연구를 위한 중요한 자료원이 되며, 특히 대중이 쉽게 접근할 수 있고 일반적으로 무료로 제공되기 때문에 뉴스와 정보의 보존과 공개에 실질적으로 이바지한다(*Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, 2009, §§ 27 및 45; *Węgrzynowski and Smolczewski v. Poland*, 2013, § 59; *M.L. and W.W. v. Germany*, 2018, § 90; 또한, 제 10 조와 관련하여 심리된 *Hurbain v. Belgium* [GC], 2023, § 180 참조).

3. 개인데이터 공개

248. 여러 사건에서 재판소는 데이터 처리자가 개인의 개인데이터를 공개하는 조치에 대해 심사하였다. 그 공개 대상은 다음과 같다.

- 다른 개인이나 법인(병원이 환자의 건강 상태에 관한 정보를 가족과 언론인에게 전달한 *Mockutė v. Lithuania*, 2018, §§ 99-100, 구급대원이 환자의 HIV 양성 여부를 병원 직원에게 알린 *Y. v. Turkey* (dec.), 2015, §§ 70-72, 병원이 환자의 의료 정보를 환자의 고용주에게 제공한 *Radu v. Republic of Moldova*, 2014, § 27, 당국이 청구인의 범죄경력 정보를 장래 고용주에게 공개한 *M.C. v. the United Kingdom*, 2021, § 46)

- 공공 당국(부인과 병동이 환자의 의료 정보를 사회보장기금에 제공한 *M.S. v. Sweden*, 1997, § 35, 각종 상황에서 제출될 증명서에 불필요하게 민감한 의료 데이터가 기재된 *P.T. v. Republic of Moldova*, 2020, §§ 5-6, 29-31)
- 대중(TV 뉴스 보도에서 은밀히 촬영된 개인의 식별 가능한 정보와 흐림 효과 처리되지 않은 사진이 방송된 *Hájovský v. Slovakia*, 2021 §§ 46-49, 공공장소에서 자살을 시도하는 장면이 담긴 CCTV 영상이 언론에 전송된 *Peck v. the United Kingdom*, 2003, § 63, 숨겨진 카메라로 촬영된 개인의 흐림 처리되지 않은 영상이 방송된 *Bremner v. Turkey*, 2015, §§ 71-85, 자택에서 은밀히 촬영된 언론인의 동영상이 대중에게 방송된 *Khadija Ismayilova v. Azerbaijan*, 2019, §§ 108-132, 판결문이 언론에 전달되는 과정에서 개인의 신원과 건강 상태가 공개된 *Z v. Finland*, 1997, §§ 70-71, 수사기록의 증거가 언론에 공개된 *Apostu v. Romania*, 2015, §§ 121-132, 국회 위원회 보고서에서 판사의 사생활 및 직업윤리에 관한 내용이 공개된 *Montera v. Italy* (dec.), 2002, 왕녀의 사생활과 관련된 사진이 타블로이드 신문에 게재된 *Von Hannover v. Germany*, 2004, §§ 61-81, 회계사의 진술에 기초해 고위 판사의 아내가 특정 기업과의 불법 거래에 연루되었다고 보도한 언론 기사에 관한 *Polanco Torres and Movilla Polanco v. Spain*, 2010, §§ 44-54, 대중 일간지가 유명 여배우의 상세 주소를 공개한 *Alkaya v. Turkey*, 2012, §§ 30-31, 피의자의 사진이 다양한 범죄 혐의를 언급하는 진술과 함께 언론에 유포된 *Mityanin and Leonov v. Russia*, 2018, §§ 111-121, 아동의 사진이 「가정이 필요한 아이들」이라는 소책자 표지에 게재된 *Bogomolova v. Russia*, 2017, §§ 54-58, 세무 당국이 청구인의 이름과 주소를 포함한 개인데이터를 주요 체납자 명단에 기재하여 웹사이트에 의무적으로 공개한 *L.B. v. Hungary* [GC], 2023).

a. 사전 동의의 영향

249. 데이터 주체가 데이터 전송, 공개 또는 게재에 사전에 동의했는지는, 특정 사건에서 그러한 조치가 사생활 존중권에 대한 제한에 해당하는지(*M.S. v. Sweden*, 1997, §§ 31, 35; *M.M. v. the United Kingdom*, 2012, §§ 186, 189) 또는 협약 제 8 조제 2 항의 의미에서 "법에 따른 것"으로 볼 수 있는지(*Radu v. the Republic of Moldova*, 2014, § 27; *Mockutė v. Lithuania*, 2018, § 101) 판단하는 데 결정적인 정도는 아니라 해도 중요한 요소이다. 재판소는 데이터 주체의 동의 없이 데이터 처리자가 개인데이터를 공개한 여러 사건에서 제 8 조 위반이라고 판단하였다(*Radu v. the Republic of Moldova*, 2014, §§ 30, 32;

Mockutė v. Lithuania, 2018, §§ 103, 106; *Peck v. the United Kingdom*, 2003, §§ 85-87; *Sõro v. Estonia*, 2015, §§ 17-19, 64).

250. 데이터 주체의 동의가 유효하려면 설명을 충분히 듣고 동의해야 하고 모호하지 않아야 한다(*M.S. v. Sweden*, 1997, § 32; *Konovalova v. Russia*, 2014, §§ 47-48). 한 공공기관(병원의 산부인과)이 다른 공공기관(사회보장부)에 개인의 의료기록을 데이터 주체의 동의 없이 전달한 사건에서, 데이터 주체가 손해배상 청구를 제기하여 다투게 된 쟁점은 데이터 비밀성에 관한 권리를 스스로 포기했는지 여부였다(*M.S. v. Sweden*, 1997, §§ 31-32). 재판소는, 데이터 공개가 청구인이 손해배상 청구를 제기한 사실에만 의거한 것이 아니라 청구인의 통제 범위를 벗어난 여러 요인에도 좌우되었으므로, 단지 손해배상 청구를 했다는 이유만으로 청구인이 의료기록과 관련하여 사생활 존중권을 명확히 포기한 것으로 추론할 수는 없다고 결정하였다. 이에 따라 제 8 조가 적용되었다.

251. 개인데이터가 본인의 요청이나 동의에 따라 공개되었다고 하더라도, 개인에게 실질적인 선택권이 없다면(예: 구직자의 범죄기록에 저장된 개인데이터 공개를 고용주가 강제하는 경우), 제 8 조가 보장하는 보호를 상실하지 않는다(*M.M. v. the United Kingdom*, 2012, § 189). 예시로 든 바로 그 사건인 *M.M. v. the United Kingdom*, 2012 사건 §§ 187-207 에서 청구인은 자신의 범죄기록에 등록된 경고처분 정보를 잠재적 고용주에게 공개해 달라고 요청하였고, 재판소는 범죄기록 데이터의 보유 및 공개 제도의 어느 단계에서도 해당 데이터가 지원 직무와의 관련성 여부나, 데이터 주체가 여전히 위험을 초래할 수 있다고 인식될 수 있는 정도를 평가하지 못하여 충분한 보호조치가 결여되어 있었기 때문에 제 8 조 위반이라고 판단하였다(*ibid.*, § 204). *M.C. v. the United Kingdom*, 2021 사건 §§ 47-57 에서 재판소는 *M.M. v. the United Kingdom* 사건 이후 도입된 입법적 변화를 지적하며, 새로 마련된 범죄기록 정보 공개 제도는 범죄의 유형을 여러 방식으로 구별하였고, 어떤 전과가 어느 시점에 공개될지 명확하게 하였으며, 범죄자의 연령과 범죄의 심각성에 따라 달라지는 명확하고 제한된 공개 기간을 규정하였으므로 제 8 조의 관련 요건과 합치한다고 판단하였다.

252. 범죄자 식별 및 범죄 예방을 위해 당국이 거리에 설치한 CCTV 에 수많은 사람의 영상이 포함되는 경우처럼 데이터 주체의 동의를 얻는 것이 항상 가능한 것은 아니다(*Peck v. the United Kingdom*, 2003, § 81). 재판소의 견해에 따르면, CCTV 영상의 공개가 동의에 근거하는 경우, 이는 범죄 탐지와 예방에서 CCTV 시스템의 실효성을 제고하려는 모든 조치를 사실상 무력화할 수 있으며, CCTV 시스템과 그 이점에 대한 홍보를 통해 그 기능은 더욱 강화된다(*ibid.*, § 81). 이러한 상황에서, 또는 CCTV 영상에 포함된 개인이 자신의 영상 공개에 동의하지 않는 경우, 데이터 처리자는 영상 유포 이전에 영상 일부를 가리거나(*ibid.*,

§ 82) 영상을 수신하는 측이 적절하고 충분한 방식으로 영상을 가리도록 보장하는 등의 대안을 고려해야 한다(*ibid.*, § 83).

253. *Peck v. the United Kingdom*, 2003 사건 § 87 에서 자치단체가 언론에 배포한 보도 자료를 통해 공공장소에서 자살을 시도하는 개인을 촬영한 CCTV 영상을 공개한 것은 제 8 조 위반에 해당하였다. 재판소는 문제 된 영상이 명백히 한 개인만을 집중적으로 촬영한 것이었으므로, 경찰에 알려 개입하는 것을 지켜본 CCTV 운영자는 경찰에 문의하여 청구인의 신원을 확인한 뒤, 공개에 대한 동의를 요청할 수 있었을 것이라고 판결하였다(*ibid.*, § 81).

254. *Bremner v. Turkey*, 2015 사건 §§ 71-85 에서, 숨겨진 카메라로 촬영된 텔레비전 다큐멘터리에서 개인의 영상이 흐림 처리나 모자이크 없이 방송된 것은 제 8 조에 반하는 것으로 판단되었다. 특히 청구인이 잘 알려진 인물이 아니었다는 점과 관련하여, 문제 된 방송에 내재된 정보 가치가 있었다거나 적절하고 충분한 방식으로 사용되었다고 볼 만한 정황은 없었다.

255. 나아가 재판소는 사전 통지 의무로 초래될 위험이 있는 위축 효과, 사전 통지 의무의 실효성에 대한 중대한 의문 및 이 영역에서 국가 당국이 누리는 광범위한 판단재량을 고려하여, *Mosley v. the United Kingdom*, 2011 사건 § 132 에서 제 8 조가 사생활에 관한 정보를 공개하기 전에 당사자에게 통지할 법적 의무의 근거가 되지 않는다고 판단하였다.

256. 어떤 상황에서는 개인의 정신 건강에 관한 데이터를 본인의 동의 없이 가까운 친족에게 공개하는 것도 사생활 존중권을 침해할 수 있다. *Mockutė v. Lithuania*, 2018 사건 § 100 에서 재판소는 성인 환자의 건강 정보를 그 동의 없이 어머니에게 공개한 것은, 두 성인 간의 긴장된 관계를 고려할 때, 협약 제 8 조가 보장하는 권리에 부합하지 않는다고 판단하였다.

257. 체포되었거나 기소된 사람들과 관련하여, 재판소가 제 8 조 위반이라고 판단한 사건으로는, 경찰이 청구인의 동의 없이 그들의 사진을 언론에 제공한 사건(*Sciacca v. Italy*, 2005, §§ 29-31; *Khuzhin and Others v. Russia*, 2008, §§ 115-118; *Margari v. Greece*, 2023, §§ 54-60), 경찰이 청구인의 동의 없이 TV 촬영팀을 경찰서로 불러들여 그 영상을 텔레비전 방송용으로 촬영하게 한 사건(*Toma v. Romania*, 2009, §§ 90-93; *Khmel v. Russia*, 2013, § 41), 내무부가 경찰 구금 중 촬영된 청구인들의 사진을, 신원을 가리지 않은 채 웹사이트에 게시한 사건(*D.H. and Others v. North Macedonia*, 2023, §§ 63-65), 청구인의 사진을 "수배자" 게시판에 게시하는 조치가 법률에 규정되어 있지 않은 사건(*Guiorgui Nikolaïchvili v. Georgia*, 2009, §§ 129-131) 또는 기존 규정과 절차가 "양질의 법률" 요건을 충족하지 못한 사건(*Negru v. the Republic of Moldova*, 2023, §§ 29-35)이 있다.

258. 데이터 주체의 사전 동의를 얻지 않고 데이터를 전송, 공개 또는 게재한 경우라 하더라도, 범죄 수사의 필요성과 재판 절차의 공개 보장(*Avilkina and Others v. Russia*, 2013, § 45; *Z v. Finland*, 1997, § 97) 및 보건(*Y. v. Turkey* (dec.), 2015, § 74), 국가 안보(*Anchev v. Bulgaria* (dec.), 2017, § 100) 또는 국가의 경제적 복리(*M.S. v. Sweden*, 1997, § 38)를 보호할 필요와 같은 정당한 고려사유가 있다면 반드시 제 8 조 위반에 해당한다고 볼 수 없다.

b. 사법 절차 맥락에서 데이터 공개

259. 재판소는 사법 절차의 맥락에서 당국이 채택한 조치가 당사자나 제 3 자의 개인데이터 공개로 이어진 여러 사건을 심사하였다.

- 이혼 판결문에서 개인 의료기록의 일부를 인용한 경우(*L.L. v. France*, 2006, § 46) 및 의료 데이터가 포함된 증거에 대해 비밀유지를 10 년으로 제한한 명령(*Z v. Finland*, 1997, §§ 112-113)
- 공개 변론 중 청구인의 비밀인 정신과 자료를 공개한 경우(*Panteleyenko v. Ukraine*, 2006, § 57) 및 기일 연기 요청을 뒷받침하기 위해 제출된 진단서를 확인한 경우(*Stokłosa v. Poland* (dec.) 2021, §§ 43-44
- 판결문이 언론에 전달되는 과정에서 개인의 신원과 HIV 양성 여부를 공개한 경우(*Z v. Finland*, 1997, § 113)
- 사전 통지 없이 판결문에 제 3 자의 신원을 전부 공개한 경우(*Vicent Del Campo v. Spain*, 2018, §§ 47-51)
- 판결문에서 피해자의 개인데이터를 공개하고 여성의 역할에 관한 고정관념을 전달하는 표현과 논거를 사용하여, 입법 체계가 충분히 마련되어 있었음에도 불구하고 성폭력 피해자 보호의 실효성을 저해할 수 있었던 경우(*J.L. v. Italy*, 2021, §§ 136-142)
- 형사절차 피고인의 사진과 개인데이터를 언론(*Margari v. Greece*, 2023, § 54) 또는 경찰서 공개구역의 수배자 명단에 게재한 경우(*Negru v. the Republic of Moldova*, 2023, § 24)
- 성폭력 피해에 대한 민사 손해배상 청구를 기각한 판결 전문과 함께 청구인의 성명과 주소 전체를 누구나 접근할 수 있는 공식 온라인 사법 데이터베이스에 공개한 경우(*A.P. v. Armenia*, 2024, § 159)

260. 재판소의 의견에 따르면, 개인데이터 중 특정 유형의 비밀성을 보호할 필요성은 때로 범죄 수사 및 소추의 필요성과 재판 공개의 필요성보다 순위에 놓일 수 있다(*Avilkina and Others v. Russia,* 2013, § 45; *Z v. Finland*, 1997, § 97). 관할 국가 당국은, 법원에 대한 신뢰를 유지하기 위해 필요한 재판 공개 원칙의 보호와 당사자 또는 제 3 자의 데이터 기밀성 유지 이익 사이에서 적절한 균형에 도달하도록 어느 정도 재량이 있어야 한다(*C.C. v. Spain*, 2009, § 35). 사법절차의 당사자이든 제 3 자이든 상관없이 개인데이터를 공개할 수 있는 조치는 무엇이든 압도적인 사회적 필요 요건을 충족해야 하고(*Vicent Del Campo v. Spain*, 2018, § 46), 절차의 특수성으로 인해 엄격히 필요한 범위 내에서 가능한 한 제한되어야 한다(*L.L. v. France*, 2006, § 45; *Margari v. Greece*, 2023, § 47).

261. 특정 사건에서 판결문 본문에 개인의 신원과 그 밖의 개인데이터를 공개할 정도의 사유가 존재하였는지 판단하려면, 국내법과 실무상 침해성이 덜한 다른 조치가 가능했는지 살펴야 한다. 판결문에 데이터 주체를 식별할 수 있는 이름을 언급하지 않는 가능성(*Z v. Finland*, 1997, § 113; *Vicent Del Campo v. Spain*, 2018, § 50), 전체 이유를 일정 기간 비공개로 유지하고 대신 축약된 이유, 주문 및 적용 법률을 표시한 판결문을 공개하는 방법(*Z v. Finland*, 1997, § 113) 또는 판결문 전체나 그 일부 사항에 대한 접근을 제한하는 방법(*Vicent Del Campo v. Spain*, 2018, § 50) 등이 있다. 재판소는 이러한 여러 조치가 일반적으로 판결이 데이터 주체의 사생활 보호권에 미치는 영향을 줄이는 적절한 수단이 될 수 있다고 평하였다.

262. *Panteleyenko v. Ukraine,* 2006 사건 § 82 에서 재판소는 정신병원에서 확보한 개인의 정신 건강 및 치료에 관한 비밀 정보가 공개 변론 과정에서 공개되는 것을 방지하기 위하여 비공개 심리를 이용한다면, 그 정보가 당사자들의 주지사항이 되고 기록에 포함되는 것까지는 막을 수는 없을지라도, 도움이 되었을 것이라고 판결하였다.

263. *Frâncu v. Romania*, 2020 사건 §§ 72-73 에서, 항소심 법원이 시장에 대한 부패 사건에서 청구인의 비공개 심리 요청을 기각하여 청구인의 의료 정보의 기밀성을 보장하지 못한 것은 제 8 조에 반하는 것으로 판단되었다. 재판소의 견해에 따르면, 항소심 법원이 단순히 청구인의 사건이 형사소송법상 비공개 심리에 해당하는 "어느 경우에도 해당하지 않는다"고만 선언하고 추가 설명을 하지 않은 것은, 재판의 투명성을 보장하려는 일반의 이익과 건강 상태에 관한 데이터의 비밀성을 유지하려는 청구인의 이익 사이에서 적절한 균형에 도달하지 못한 것이다. 피고인의 높은 공적 지위가 비공개 심리 요청의 비례성을 심사하는 과정에서 고려 요소가 될 수 있다고 가정하더라도, 이 사건에서 항소심 법원은 그러한 조치의 비례성에 대한 개별적 심사를 전혀 하지 않았다.

264. *Khadija Ismayilova v. Azerbaijan*, 2019 사건 §§ 105-132 에서 재판소는 직업 언론인인 청구인의 이름과 주소 등 민감한 개인데이터와 친구, 친척, 동료들의 이름을 포함한 사적 정보를, 검찰 당국이 형사 수사 진행 상황 보고 형식의 보도 자료에서 공개한 것이 제 8 조 위반에 해당한다고 결정하였다(*ibid.*, §§ 142-150).

265. *M.P. v. Portugal*, 2021 사건 §§ 48-49 에서 청구인의 전남편이, 청구인에게 접근 권한을 받은 것으로 보이는 데이트 사이트에서 교환된 전자 메시지를 청구인의 동의 없이 이혼 소송에 제출한 행위는, 가정법원이 결국 그 메시지를 고려하지 않았고, 이러한 유형의 절차에서 데이터에 대한 공적 접근은 어차피 제한되어 있었기 때문에, 제 8 조 위반에 해당하지 않았다.

266. *J.S. v. the United Kingdom* (dec.), 2015 사건 §§ 71-73 에서 재판소는 검찰청의 보도 자료에 포함된 개인 정보 공개와 관련한 청구에서, 해당 보도 자료는 법원 절차에 관한 언론 문의에 통상적으로 제공되는 범위를 넘지 않았고, 청구인의 이름, 나이, 학교(청구인은 교사 폭행 혐의를 받던 미성년자)나 다른 어떠한 개인정보도 공개하지 않았으므로 명백히 근거 없다고 보아 각하하였다.

267. 이혼 소송 과정에서 판사가 보조적·부차적 근거로, 의료 자문가와 청구인의 주치의 간 개인 서신에 포함된 비밀 의료 문서를 참조한 *L.L. v. France*, 2006 사건 §§ 46 에서 판사나 수사판사가 문제 된 의료 데이터를 판결 이유에서 제외하더라도 동일한 결론에 이를 수 있었던 사실은 반드시 고려해야 할 중요한 요소였다. 누구나 특정한 이해관계를 증명하지 않고도 판결 이유 부분의 사본을 입수할 수 있었으므로, 당사자 간 이혼 소송이 비공개로 진행되었고 제 3 자에 대하여 효력이 있는 판결문에는 주문만 포함되어 있었다 하더라도, 개인데이터 보호의 근본적 역할을 고려할 때, 청구인이 사생활 존중권에서 겪은 제한은 정당화될 수 없었다(*ibid.*, §§ 47, 33).

268. *Vicent Del Campo v. Spain*, 2018 사건 §§ 53, 56 에서, 사법 절차의 제 3 자인 청구인이 판결 선고 전에 법원에 자신의 신원 공개를 자제해 달라고 요청할 기회가 전혀 없었던 사실은 제 8 조 위반에 해당하였다. 청구인은 어떠한 방식으로도 통지받거나, 심문받거나, 출석을 요구받거나, 통보받지 못하였다.

269. 국내 법원이 청구인의 신원과 HIV 양성 여부를 드러내는 기록에 대한 비밀유지 기간을 10 년으로 제한한 사건에서, 재판소는 사법 당국이 당사자와 제 3 자의 개인데이터 보호 이익에 충분한 비중을 두지 않았다는 이유로 제 8 조 위반이라고 판단하였다(*Z v. Finland*, 1997, §§ 111-112). 재판소는 청구인의 동의 없이 건강 상태에 관한 정보가 사법 절차에서 제출됨으로써 사생활 존중권에 심각한 제한이 발생하였으며, 그 의료 정보가 10 년 후

대중에게 공개될 경우 이러한 제한은 더욱 심화될 것이라고 보았다(*ibid.*, § 112). 반대로, *Y. v. Turkey* (dec.), 2015 사건 §§ 81-82 에서는 행정법원이 관할권 부인을 선언한 단일 결정에서만 청구인의 신원과 HIV 양성 여부가 언급되었고, 그 결정은 공표되거나 대중에게 공개되지 않았으며, 동일한 절차에서 내려진 다른 어떠한 결정에서도 해당 정보가 언급되지 않았기 때문에, 데이터 주체의 사생활 존중권을 침해할 소지가 있다고 보지 않았다.

270. *Drakšas v. Lithuania*, 2012 사건 § 60 에서, 청구인(저명한 정치인)과 탄핵 심판을 받던 대통령 사이의 전화 통화를 비밀 정보기관이 가로채어 녹음 내용을 헌법재판소 공개 변론에서 공개하고, 전국 텔레비전 방송으로 생중계한 것은 제 8 조 위반에 해당하지 않았다. 재판소는 청구인이 공적 인물로서 피할 수 없음을 알면서도 자신의 모든 언행이 기자들과 일반 대중의 면밀한 검증 대상이 되는 상황에 스스로를 노출하였다고 보았다. 따라서 헌법재판 절차에서 법률에 근거해 청구인의 사적 영역에 속하지 않는 정치적 또는 업무상 전화 통화를 공개한 것은 타인의 권리 보호를 위해 필요한 조치였다.

271. *A.P. v. Armenia*, 2024 사건 §§ 159-162 에서 청구인의 개인데이터를 성폭력에 대한 민사 손해배상 청구를 기각한 판결 전문과 함께 공개한 것은 청구인의 사생활 존중권에 대한 제한에 해당하였다. 해당 정보는 청구인이 비공개를 구체적으로 요청하였는데도, 누구나 접근할 수 있는 공식 온라인 사법 데이터베이스에 공개되었다. 재판소는 그러한 공개가 국내법상 법적 근거가 없었다고 판단하였고, 따라서 그 제한은 협약 제 8 조의 의미에서 "법에 따른 것"이 아니라고 결론지었다.

272. 또한, 경찰이 체포되거나 기소된 개인의 동의 없이 사진을 언론에 공개한 경우에 관한 **오류! 참조 원본을 찾을 수 없습니다.** 및 사인(私人)에 의한 개인데이터 공개 사건에서 국가의 적극적 의무와 관련된 80-82 참조.

c. 공중보건 보호를 위한 데이터 공개

273. 의료 비밀을 존중받을 개인의 권리는 절대적인 것이 아니며, 고용주의 당사자주의 절차 보장 권리 같은 다른 정당한 권리 및 이익과 연결하여 고려하여야 한다(*Eternit v. France* (dec.), 2012, § 37). 이러한 권리보다 병원 직원의 안전이나 공중보건의 보호 같은 공익의 근본적 요소를 보호할 필요가 우선할 수 있다(*Y. v. Turkey* (dec.), 2015, § 74).

274. 병원 및 보건 체계 내 환자 진료와 관련된 사건에서, 환자의 상태에 관한 정보의 전달은 특정한 상황에서 환자에게 적절한 의료 처치를 보장할 뿐 아니라, 해당 진료에 관여하는 의료진과 다른 환자들의 권리와 이익의 보호에 필요한 예방 조처를 할 수 있게 하는 데 관계가 있고 필요하다고 인정될 수 있다(*Y. v. Turkey* (dec.), 2015, § 74). 의료 종사자가 업무 도중

감염 위험에 노출되는 경우, 병원 직원의 안전과 공중보건의 보호는 질병의 병원 내 전파를 방지하기 위하여 진료에 관여하는 의료진 사이에서 환자의 건강 상태에 관한 정보를 전달하는 것을 정당화할 수 있다(*ibid.*, § 78).

275. 환자의 건강 상태에 관한 데이터 같은 민감한 정보는 데이터 주체가 어떤 형태로든 낙인찍히는 것을 방지하고, 남용의 위험을 제거할 수 있도록 충분한 보호조치를 제공하는 방식으로 전달되어야 한다(*Y. v. Turkey* (dec.), 2015, § 79). 정보를 수신하는 자에게는 의료 전문가에게 적용되는 구체적인 비밀유지 규칙이나 이와 유사한 비밀유지 의무가 적용되어야 한다(*ibid.*, § 74).

276. *Y. v. Turkey* (dec.), 2015 사건 §§ 78–79 에서 재판소는 환자가 치료를 받은 병원 내 여러 의료 제공자 사이에서 HIV 양성 상태에 관한 정보가 교환된 사안과 관련하여 제기된 청구에 대해, 환자가 동의하지는 않았지만 해당 정보 공유는 병원 직원의 안전과 공중 보건 보호로 정당화된다는 이유로 명백히 근거 없다고 보아 각하하였다. 재판소는 국내법상 모든 의료 제공자가 자신의 지위나 직무와 관련하여 전달받은 모든 데이터의 비밀을 존중할 의무가 있으며, 이를 위반할 경우 징계 또는 형사 제재를 받을 수 있다는 점을 중요하게 보았다.

d. 국가안보 보호를 위한 데이터 공개

277. 과거 공산주의 정권의 유산을 해체하는 과정과 관련된 일련의 사건에서, 재판소는 국가안보 보호 목적을 위해 수집·저장된 개인의 오랜 과거와 관련된 데이터의 공개 문제를 검토하였다(*Sõro v. Estonia*, 2015, § 58; *Anchev v. Bulgaria* (dec.), 2017, § 100). 재판소는 해체 절차를 위해 시행된 개별적 조치와 규율 및 제공된 보호조치의 중요성을 강조하였다.

278. 따라서 *Sõro v. Estonia*, 2015 사건 §§ 56–64 에서 청구인이 과거 보안기관에서 운전사로 근무했다는 내용의 정보 공개는 제 8 조 위반에 해당하였다. 청구인이 사전에 해당 데이터가 공개될 것임을 통보받았고 데이터 공개에 이의를 제기할 수 있기는 하였지만, 과거 보안기관 직원들이 각자 수행한 구체적 업무를 평가하여 그들이 직업 활동을 마치고 수년 후 민주주의 체제에서 잠재적으로 초래할 수 있는 위험을 구별할 수 있는 절차는 마련되어 있지 않았다(*ibid.*, § 61). 재판소는 에스토니아가 독립을 회복한 시점과 문제의 개인데이터가 공개된 시점 사이에 흐른 시간의 경과에 따라, 청구인이 새로 수립된 민주주의에 가했을지도 모르는 초기 위협은 상당히 줄어들었음에 틀림없다고 판결하였다(*ibid.*, § 62). 또한, 공개법 자체가 청구인이 새로 고용되는 것에 어떤 제한을 부과한 것은 아니었지만, 동료들의 태도로

인해 청구인이 직위를 내놓을 수밖에 없었다는 것은 청구인의 사생활 존중권에 대한 제한이 심각하다는 점을 보여주었다(*ibid.*, § 63).

279. 반대로, *Anchev v. Bulgaria* (dec.), 2017 사건 §§ 92-116 에서는 공개 절차가 엄격히 규율되었고, 특별 독립위원회에 그 권한이 위임되었으며 그 결정이 두 단계의 사법심사에 회부되는 등 자의적·남용적 적용을 방지하기 위한 여러 보호조치가 수반된 경우로, 이러한 맥락에서 청구인의 오랜 과거와 관련된 데이터의 공개는 제 8 조와 양립할 수 없는 것으로 간주되지 않았다. 해당 공개가 어떠한 제재나 법적 불이익을 수반하지 않았기 때문에, 그 제한은 당국이 누리는 폭넓은 판단재량의 범위를 벗어나는 것이 아니었다(*ibid.*, §§ 106-113). 재판소는 만약 국가가 근로 금지나 선거권 일부 박탈과 같이 데이터 주체의 개인적 영역에 더 심각하게 개입하는 조치를 시행했다면 결론이 달라질 수도 있었을 것이라고 밝혔다(*ibid.*, § 113).

e. 국가의 경제적 복리 보호를 위한 데이터 공개

280. 국가의 경제적 복리를 보장하기 위한 조치로서, 당국이 수집하거나 저장한 데이터의 비밀을 침해하는 경우라 하더라도, 실효적이고 만족스러운 보호조치가 수반된다면 반드시 제 8 조에 위반되는 것은 아니다(*M.S. v. Sweden*, 1997, § 41). 상충하는 여러 이해관계를 균형 있게 고려할 때, 국내법이 데이터 처리자가 취할 수 있는 조치를 규율하는지 여부, 법적 요건 불이행 시 그 책임이 문제 되는지 여부, 데이터 수령자가 유사한 규칙과 보장을 준수할 의무 및 특히 비밀유지 의무를 부담하는지 여부는 반드시 고려해야 할 중요한 요소이다(*ibid.*, § 43).

281. *M.S. v. Sweden*, 1997 사건 §§ 31-44 에서 한 공공기관(병원의 부인과 부서)이, 청구인이 직접 신청한 급부 수급 자격의 법적 요건 충족 여부를 심사할 책임이 있는 다른 공공기관(사회보장부)에 청구인의 진료기록을 전달한 행위는 제 8 조 위반이 되지 않았다. 재판소는 해당 데이터 전달이 자격을 갖춘 청구인들에게 공적 자금을 배분하는 데 결정적일 잠재력이 있으므로, 국가의 경제적 복리 보호라는 목적을 추구한 것으로 볼 수 있다고 판결하였다(*ibid.*, § 38). 청구인의 비밀 데이터 공개에는 남용을 방지할 수 있는 실효적이고 기준을 충족하는 보호조치가 수반되었는데, 관련 국내법상 해당 데이터를 전달하기 위해서는 그 정보가 직무상 장애보험법 적용에 중요해야 한다는 조건이 있었고(*ibid.*, §§ 18, 43), 부인과 부서 직원들이 그 조건을 준수하지 않았다면 민사상 및/또는 형사상 책임을 질 수 있었으며(*ibid.*, §§ 22, 43), 데이터 수령자 역시 그 비밀을 존중할 유사한 의무를 부담하고 있었다(*ibid.*, §§ 20, 22, 43).

282. *L.B. v. Hungary* [GC], 2023 사건 §§ 20-29 에서는 청구인의 개인데이터(이름과 자택 주소 포함)가 국세청 웹사이트에 주요 체납자 명단으로 공개되었다. 해당 입법은 세법 위반에 대응하기 위한 수단으로 이러한 명단 공표를 도입하였으며, 분기 말 기준으로 180 일 이상 연속하여 다액의 세금을 체납한 모든 납세자에게 데이터의 체계적이고 의무적인 공개가 적용되었다. 재판소는 입법부가 이러한 일반 제도를 선택한 것이 그 자체로 문제 되는 것은 아니며, 납세자 데이터의 공개 자체도 문제 되지 않는다고 하였다. 또한 재판소는 체약국들이 세금 납부 의무를 이행하지 않은 납세자의 개인데이터를 유포하는 제도를 마련할 필요성을 평가할 때, 세수 제도의 원활한 작동을 보장하는 수단 중 하나로서 폭넓은 판단재량을 누린다고 판단하였다. 그러나 재판소는 이러한 재량에 제한이 없는 것은 아니라고 강조하면서, 이러한 맥락에서 입법부·행정부·사법부 등 국내 권한 있는 당국이 상충하는 이해관계 사이에서 적절한 균형을 이루었고 그 과정에서 (i) 문제 된 정보 유포에 따른 공익뿐만 아니라 (ii) 공개된 정보의 성격 (iii) 해당인의 사생활 향유에 미치는 파급효과와 위험 및 (iv) 특히 인터넷을 통한 정보 유포가 잠재적으로 미치는 범위 (v) 목적 제한, 저장 제한, 데이터 최소화, 데이터 정확성 등 기본적인 데이터 보호 원칙을 고려하였는지 면밀히 심사할 것이라고 지적하였다. 또한 재판소는 절차적 보호조치의 존재 역시 위와 같은 맥락에서 중요한 역할을 할 수 있다고 강조하였다(*ibid.*, § 128).

283. 사건의 사실관계에서, 재판소는 문제 된 공표 제도의 두 가지 특징으로 첫째, 납세자의 개인데이터 중 자택 주소가 의무적 공개 대상에 포함된 점, 둘째, 국세청이 개별적 비례성 평가를 할 재량이 전혀 부여되지 않은 점을 지적하였다. 이를 전제로 재판소는 의회 심사의 질을 분석하며 확인한 결함으로는 (i) 동일한 억지 목적을 지닌 기존 수단들이 존재하는 상황에서, 문제 된 일반적 조치(특히 세금 체납자의 자택 주소 공개 요구)의 필요성과 보완적 가치에 대한 평가가 이루어지지 않았던 점 (ii) 사생활의 비밀에 대한 영향, 특히 세금 체납자의 자택 주소가 일반 대중에 의해 오용될 위험에 대한 고려가 이루어지지 않았던 점 (iii) 문제 된 정보 유포에 사용된 매체(인터넷)의 잠재적 파급 범위에 대한 고려가 없었던 점(민감한 정보인 이름과 자택 주소에 대한 무제한적 접근을 의미하며, 최초 공개의 자연스럽고 개연적이며 예측 가능한 결과로 재유포의 위험이 뒤따른다는 점을 내포함) (iv) 국내법 및 EU 법에 따른 데이터 보호 요건, 데이터 최소화 원칙에 비추어 적절히 맞춤화된 대응을 고안할 가능성에 대한 고려가 이루어지지 않았던 점이 있다. 이러한 배경을 종합하여, 재판소는 피청구국이 폭넓은 판단재량을 누린다고는 하지만, 문제 된 제한은 "민주사회에서 필요한" 제한이 아니라고 결론지었다(*ibid.*, §§ 129-40).

f. 개인데이터의 대량 공개

284. 대량의 과세 데이터에 대한 접근을 제공하고 수집을 허용하는 데 공익이 존재한다고 해서, 곧바로 어떠한 분석적 가공도 없이 원자료를 그대로 대량 유포하는 데에도 공익이 있다는 의미는 아니다. *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 사건 § 175 에서 재판소는 언론 목적의 데이터 처리와 언론인에게 특권적으로 제공된 원자료의 대량 유포는 구별해야 한다고 강조하였다. 과세 관련 개인데이터의 대량 공개를 국내 규정 및 EU 데이터 보호 규정과 양립할 수 없는 절차에 따라 금지하는 것은 그 자체로 제재가 되는 것은 아니며, 설령 공개되는 정보의 양이 제한되어 실무적으로 일부 청구인 회사들의 사업 활동 수익성이 떨어지게 되었더라도 마찬가지이다(*ibid.*, § 197).

B. 데이터 주체의 권리

285. 재판소의 판례는 개인데이터 주체가 협약상 권리를 향유하도록 보장하기 위하여 여러 가지 구체적 권리를 부여한다.

1. 자기 데이터에 접근할 권리

286. 당국의 개인데이터 수집·보유의 대상이 된 개인은 제 8 조가 보호하는 이익으로서, 전체주의 정권하에서 과거 비밀기관이 자신에 대해 수집하여 국가 기록보관소에 저장한 정보(*Haralambie v. Romania*, 2009, § 79; *Jarnea v. Romania*, 2011, § 50; *Joanna Szulc v. Poland*, 2012, § 87), 자신이 노출된 건강상 위험이나 건강과 관련하여 필요한 정보(*Roche v. the United Kingdom* [GC], 2005, § 155; *K.H. and Others v. Slovakia*, 2009, § 44; *Yonchev v. Bulgaria*, 2017, § 46), 자신의 어린 시절과 초기 발달 과정을 알거나 이해하는 데 필요한 정보(*Gaskin v. the United Kingdom*, 1989, § 41), 자신의 출신을 추적하기 위한 정보와 특히 부모의 신원에 관한 정보(*Odièvre v. France* [GC], 2003, §§ 43-44; *Godelli v. Italy*, 2012, §§ 62-63; *M.G. v. the United Kingdom*, 2002, § 27)를 제공받을 권리가 있다.

287. 이러한 다양한 맥락에서, 당국은 제 8 조가 보장하는 사생활의 실효적 존중에 내재된 적극적 의무로서, 청구인이 특정 목적을 위해 필요한 관련되고 적절한 모든 정보에 접근할 수 있도록 하는 실효적이고 이용 가능한 절차를 제공하여야 한다(*Roche v. the United Kingdom* [GC], 2005, § 162; *Haralambie v. Romania*, 2009, § 86; *Joanna Szulc v. Poland*, 2012, §§ 86, 94).

288. 반대로, 국가가 국가안보 보호나 테러 대응을 위해 설계된 비밀 감시제도의 실효성을 위태롭게 할 수 있다고 정당하게 우려하는 경우에는, 비밀 등록부에 수집·보관된 정보에 대한 접근을 거부하더라도 제 8 조상 당국의 적극적 의무를 위반한 것이 아니다(*Leander v. Sweden*, 1987, § 66; *Segerstedt-Wiberg and Others v. Sweden*, 2006, § 102). 보안기관이 개인에 관하여 어느 정도까지 정보를 보유하고 있는지 통지받을 개인의 이익보다 국가안보 및 테러 대응의 이익이 우위에 있다고 간주할 권한이 국가에 있는지 판단하려면 재판소는 자의성을 방지할 정도의 보호조치가 존재하는지 확인하여야 한다. 양질의 법률(*ibid.*, §§ 79-80)과 마련된 보장 및 특히 문제 된 조치에 대한 심사 가능성과 데이터 주체가 국내에서 이용할 수 있는 구제수단(*ibid.*, §§ 52-68)은 상충하는 이해관계를 균형 있게 조정할 때 고려해야 할 중요한 기준이다(*ibid.*, § 103). 유사한 원칙은 외국인 추방의 맥락에서도 적용된다. *Hassine v. Romania*, 2021 사건 §§ 55-69 에서, 루마니아 정보기관은 루마니아에 합법적으로 거주하던 튀니지 국적 청구인이 국가안보를 위협할 수 있는 활동에 가담했다는 의혹을 시사하는 비밀 분류 자료에 근거하여, 국가안보를 이유로 루마니아에서 추방하였고 5 년간 불법체류자로 선언하였다. 청구인도 변호인도 해당 문서를 열람할 권한이 없었다. 재판소는 청구인의 추방에 관한 행정절차에 필요한 절차적 보호조치가 결여되어 있었다고 판단하였고, 제 7 의정서 제 1 조 위반이라고 판결하였다.

289. 특히 은밀한 조치의 맥락에서, 수집 목적상 관련성이 없다고 판단된 즉시 수집된 자료를 파기하여 데이터 주체가 그 자료에 접근할 수 없게 되는 경우라 하더라도, 그 자체로 협약에 위반되는 것은 아니다. 동시에, 데이터 주체는 가로챈 자료의 파기를 명한 관련 당국의 결정 사본과 실제 파기 "행위"에 관한 자료 제공을 요구할 정당한 근거가 있다(*Denysyuk and Others v. Ukraine*, 2025, §§ 108-109). 나아가, 관련 절차에 대한 독립적 기관의 감독 규정을 포함하여, 가로챈 자료의 선별 및 파기에 관한 명확한 공개 규칙과 지침이 마련되어야 한다(*Denysyuk and Others v. Ukraine*, 2025, §§ 110-113).

290. 청구인의 개인데이터가 셍겐 정보시스템(SIS)에 장기간 등록된 사건에서, 재판소는 청구인이 요청한 정보 전체에 개인이 충분히 접근할 수 없었다고 해도, 국가안보를 보호해야 하는 압도적 필요 요건을 고려할 때, 사생활 존중권을 침해한 것이 될 수는 없다고 결정하였다(*Dalea v. France* (dec.), 2010). 청구인은 셍겐 데이터베이스에 자신이 포함된 구체적 사유에 대해서는 다툴 수 없었지만, 자신과 관련된 다른 모든 데이터에 접근할 수 있었고, 국가안보·국방·공공 안전과 관련된 고려 사항 때문에 보고되었다는 통보를 받았다(*ibid.*, *Leander v. Sweden*, 1987, § 66 참조).

291. 개인데이터가 포함된 개인에 관한 서류철 중 일부 문서만이 국가 기밀 목적상 비밀로 분류된 경우, 당국은 청구인에게 해당 서류철에 부분적으로 접근하도록 허용할 수도

있었다(*Yonchev v. Bulgaria*, 2017, §§ 55-59). 따라서 청구인(전직 경찰관)이 자신의 개인 서류철 중 심리 평가서와 같은 특정 문서를 열람하는 것을 당국이 거부한 사건에서, 재판소는 서류철 내 문서 중 하나라도 기밀로 분류되면 나머지도 자동으로 기밀로 간주되어 기밀정보 보호 규정의 적용을 받도록 한 지나치게 형식적인 국내 규정 때문에 제 8 조 위반이라고 판단하였다(*ibid.*, § 60).

292. 구 공산주의 국가의 전체주의 정권하에서 과거 보안기관이 기록·보관한 개인 서류철에 대한 접근권을 국내법이 명시적으로 규정한 경우, 국가는 데이터 주체가 모든 관련 정보에 합리적으로 신속히 접근할 수 있도록 실효적이고 이용 가능한 절차를 마련해야 한다(*Haralambie v. Romania*, 2009, § 86; *Jarnea v. Romania*, 2011, § 50; *Antoneta Tudor v. Romania*, 2013, § 34; *Joanna Szulc v. Poland*, 2012, §§ 86, 94). 재판소는 청구인이 자신의 이름으로 보관된 서류철 중 일부에만 접근을 허용받은 사건(*Jarnea v. Romania*, 2011, §§ 54-60)과 청구인들이 최초 요청으로부터 10 년이 지난 후에야 자신들의 문서에 접근을 허용받은 두 사건(*Joanna Szulc v. Poland*, 2012, §§ 93-95; *Antoneta Tudor v. Romania*, 2013, §§ 34-40)에서 제 8 조 위반이라고 판단하였다. 보관 시스템의 결함이나, 청구인의 개인 서류철에 잘못된 생년월일이 기재된 사실과 같은 오류가 있었다 하더라도, 개인데이터에 대한 접근을 6 년간 지연시킬 정당한 사유가 될 수는 없다(*Haralambie v. Romania,* 2009, § 95). 이 유형의 정보에 대한 접근을 요청하는 사람이 고령일 경우, 전체주의 정권 시기의 개인사를 추적하려는 이해관계에는 한층 더 긴급성이 부여된다(*ibid.*, § 93 마지막 부분 참조).

293. 건강 또는 건강 위험에 관한 정보와 관련하여, 개인데이터에 대한 접근권은 데이터 주체에게 자신의 데이터 파일 사본을 제공받을 권리까지 확장된다(*K.H. and Others v. Slovakia*, 2009, § 47). 데이터 파일 사본의 복제 방식과 그 비용을 데이터 주체가 부담해야 하는지 결정하는 것은 파일 보유자의 몫이다(*ibid.*, § 48). 데이터 주체가 자신의 개인데이터 파일 사본 제공을 요청하면서 구체적 정당화를 제시하도록 강제되어서는 안 된다. 오히려 이를 거부할 중대한 사유가 있음을 보여줄 책임은 당국에 있다(*ibid.*, § 48). *K.H. and Others v. Slovakia*, 2009 사건 §§ 50-58 에서, 전직 입원 환자들은 공립병원에 보관된 원본 의무기록을 복사할 수 없었으며, 그 의무기록에는 자신들의 도덕적·신체적 완전성의 관점에서 중요하다고 여긴 정보가 포함되어 있었다. 재판소는 병원이 원본 파일에서 손으로 발췌할 수 있도록 한 단 하나의 가능성만을 제공한 것은 청구인들이 본인의 건강 관련 문서에 실효적으로 접근할 수 있도록 보장하지 못했다고 판단하였다.

294. 정부가 위험한 활동에 관여하여 그 활동에 참여한 사람들의 건강에 은폐된 부정적 결과를 초래할 수 있는 경우, 당국은 청구인이 자신이 노출된 위험을 평가할 수 있도록

“관련성 있고 적절한 모든정보”에 접근할 수 있는 “실효적이고 이용 가능한 절차”를 제공해야 하는 적극적 의무를 부담한다(*McGinley and Egan v. the United Kingdom*, 1998, § 101; *Roche v. the United Kingdom* [GC], 2005, § 161-162). 예컨대 청구인이 문제 된 문서의 공개를 요구하기 시작한 지 거의 10 년이 지나서야 보건 정보 및 연구 기관이 해당 문서의 검색과 공개 절차를 개시한 경우와 같은 불합리한 대기 기간은, 문서가 오래된 점이나 분산된 특성과 관련된 어려움이 있다고 하더라도, 제 8 조에 위반하여 데이터 주체의 사생활 존중과 관련된 국가의 적극적 의무를 이행하지 못한 것이 된다(*ibid.*, § 166).

295. 부모의 사망이나 양육 불능으로 보호조치에 편입된 아동인 경우 개인데이터에 대한 접근과 관련하여, 해당 문서를 작성한 “기록 작성자”가 동의해야 접근할 수 있게 하는 제도는 원칙적으로 국가가 누리는 판단재량의 범위 내에서 제 8 조와 양립할 수 있다. 다만, 그러한 제도는 자신의 사생활 및 가족생활과 관련된 문서를 열람하려는 사람의 이익을 보호해야 하며, 기록 작성자가 응답하지 않거나 동의를 거부하는 경우에도 독립적 기관이 최종적으로 접근 허용 여부를 결정하도록 규정되어 있는 경우에만 비례성 원칙에 부합한다(*Gaskin v. the United Kingdom*, 1989, § 49). 사회복지 당국이 특정 서류철 전체에 대한 접근을 거부한 경우(그 정보와 관련된 제 3 자 또는 그 정보를 작성·제공한 제 3 자가 공개에 동의하지 않는 경우 포함), 국내 제도에 이러한 독립적 기관에 대한 불복 절차가 마련되어 있지 않았다면, 재판소는 제 8 조 위반이라고 판단하였다(*ibid.*, § 49; *M.G. v. the United Kingdom*, 2002, §§ 30-32).

296. 재판소의 견해에 따르면, 혼외출생아가 생물학적 아버지와의 법적 친자관계를 확인하고자 하는 경우, 자신의 개인적 정체성의 중요한 측면에 관한 진실을 알기 위해 필요한 정보를 얻는 것은 협약에 의해 보호되는 중대한 이익에 해당한다(*Mikulić v. Croatia*, 2002, § 64; *Boljević v. Serbia*, 2020, § 50). 법원이 DNA 검사를 명령해도 친부로 추정된 자가 이에 따르도록 강제할 수단이 없는 제도라 하더라도, 국가의 판단재량을 고려할 때 원칙적으로 제 8 조에서 도출되는 의무와 양립한다고 볼 수 있다(*Mikulić v. Croatia*, 2002, § 64). 다만, 친부로 추정된 자가 법원 명령에 따르도록 강제할 절차적 수단이 전혀 없는 경우, 독립적 기관이 친자 확인 청구를 신속히 판단할 수 있는 대체적 수단을 마련한 경우에만 비례성 원칙에 부합한다(*ibid.*, § 64). 재판소는 친부로 추정된 자가 의학적 절차에 참여하기를 거부했을 때, 국내 제도상 DNA 검사를 강제하거나 독립적 기관이 친자 확인 청구를 신속히 판단할 수 있는 대체적 수단이 전혀 마련되어 있지 않았던 사건에서 제 8 조 위반이라고 판단하였다(*ibid.*, § 64). 개인이 자신의 출생 배경을 밝히려는 이익은 나이가 든다고 사라지는 것이 아니라 오히려 그 반대이다(망자에 대한 DNA 검사를 허용해 달라는

아들로 추정된 자의 요청을 거부한 *Ja¨ggi v. Switzerland*, 2006, § 40; *Boljević v. Serbia*, 2020, § 54).

297. 익명으로 출생한 아동의 경우, 자신의 출신과 생물학적 부모의 신원에 관한 정보에 접근하는 문제는, 보호조치에 편입된 아동의 사건기록에 대한 접근이나 친자 확인 증거에 대한 접근 문제와는 다르다(*Odièvre v. France* [GC], 2003, § 43; *Godelli v. Italy*, 2012, § 62). 다양한 법체계와 전통을 고려할 때, 국가는 생물학적 부모의 신원 비밀을 보존하는 데 있어 일정한 판단재량을 누려야 했다(*Odièvre v. France* [GC], 2003, § 46; *Godelli v. Italy*, 2012, § 65). 한 국가 제도가 청구인에게 어머니와 생물학적 가족에 관한 비식별 정보에 접근을 허용하여 청구인이 자신의 과거사를 일부 확인할 수 있도록 하고, 제 3 자의 이익을 해치지 않는 범위 내에서, 최근 제정된 법률에 따라 개인이 자신의 생물학적 출신을 찾을 수 있도록 지원할 권한을 부여받은 독립 기관의 서비스를 통해 어머니의 동의를 조건으로 어머니의 신원 공개를 요청할 가능성을 보장한 경우, 이는 제 8 조와 양립할 수 있다고 평가되었다(*Odièvre v. France* [GC], 2003, § 49; 또한 제 3 자 기증자를 통한 보조생식술으로 태어난 사람이 해당 기증자에 관한 정보에 접근하는 문제에 관한 *Gauvin-Fournis and Silliau v. France*, 2023, §§ 113-33). 반대로, 어머니의 익명 유지 의사에 맹목적으로 우선권을 부여하고, 출생 시 법적 인정을 받지 못한 입양아에게 자신의 출신에 관한 개인 신원을 특정할 수 없는 정보에 접근하거나 어머니의 신원 공개를 신청할 수단을 전혀 제공하지 않은 제도는 제 8 조 요건과 양립할 수 없는 것으로 판단되었다(*Godelli v. Italy*, 2012, §§ 70-72).

2. 정정권

298. 재판소는 당국이 거짓 데이터나 청구인이 그 정확성을 다투는 데이터를 저장한 사건들을 여러 차례 검토하였다(보안기관이 작성한 서류철에 청구인이 루마니아 군단주의 운동에 참여했다는 자료가 기재되어 있었으나 이를 반박할 수 없었던 *Rotaru v. Romania* [GC], 2000, §§ 42-44, 55-63; 경찰이 수집한 불완전한 개인데이터를 사법절차에 포함시킨 *Cemalettin Canlı v. Turkey*, 2008, §§ 34-37; 경찰 기록에 청구인이 계속 부인해 온 "성매매 종사자"라는 직업이 기재된 *Khelili v. Switzerland*, 2011, § 56).

299. 셰겐 데이터베이스에 자신과 관련된 보고서를 정정할 수 없었던 경우(*Dalea v. France* (dec.), 2010) 및 개인의 민족 출신을 공식 기록에 등록한 경우(*Ciubotaru v. Moldova*, 2010, § 59)는 사생활 존중권에 대한 제한에 해당한다. 국가안보, 국방, 공공 안전과 같은 고려사항이 문제 되는 상황에서는 이러한 제한이 반드시 제 8 조와 양립할 수 없는 것은 아니다(*Dalea v. France* (dec.), 2010). 문제 된 조치의 합법성을 판단하고 당국의 남용

가능성을 시정하기 위해, 자의성을 방지하는 보장책과 사실 및 법률의 모든 쟁점을 심사할 권한을 가진 독립적이고 공정한 기관에 의해 그 조치가 심사될 가능성은 필수적이다(*ibid.*, *Leander v. Sweden*, 1987, § 66 참조).

300. 당국이 수집·보유한 거짓되거나 불완전한 개인정보는 데이터 주체의 일상생활을 어렵게 만들 수 있고(*Khelili v. Switzerland*, 2011, § 64), 명예를 훼손할 수 있거나(*Rotaru v. Romania* [GC], 2000, § 44) 데이터 주체의 권리를 보호하기 위해 법에서 보장하는 중요한 절차적 보호조치를 제거할 수 있다(*Cemalettin Canlı v. Turkey*, 2008, §§ 35, 40-42). 경찰의 "기타 범죄에 관한 정보 메모"라는 제목의 파일이 국내 법원에 제출되어, 피고인이 과거 불법단체 가입으로 두 차례 형사소추를 받았다는 사실을 언급한 사건에서, 재판소는 제 8 조 위반이라고 판단하였다. 이 사건에서 해당 파일에 기재된 정보는 거짓일 뿐 아니라, 첫 번째 형사소송에서 청구인이 무죄 판결을 받았고 두 번째 소송에서는 절차가 중단되었다는 사실도 기재되지 않았다(*ibid.*, § 42). 두 차례 절차의 결과를 기재하지 않은 것은 국내 규정에 명백히 규정된 의무에 반하는 것이었으므로 청구인의 권리를 보호하기 위해 법에서 정한 중요한 절차적 보호조치들이 제거되었다(*ibid.*, 2008, § 42).

301. 공식 국가 등록부에 기재된 개인데이터의 정정을 요청하는 개인에게 극복할 수 없는 장벽을 초래하는 요건을 부과하는 것은, 국가가 개인의 사생활을 실효적으로 존중할 의무와 양립할 수 없는 것으로 판명될 수 있다(*Ciubotaru v. Moldova*, 2010, §§ 51-59). 청구인이 공식 등록부에 기재된 자신의 민족 출신 등록을 변경할 수 없었던 사건에서, 부모가 특정 민족 집단에 속했음을 증명해야 한다는 요건은 청구인이 당국에 의해 부모에 관하여 기록된 것과 다른 민족 정체성을 등록하는 데 극복할 수 없는 장벽이 되었다(*ibid.*, § 57).

302. 수술한 상태인 성별전환자임을 감안하여 가족관계등록부 정정을 요청하는 맥락에서, 국내 제도 내 행정적·법적 실무의 일관성은 제 8 조에 따른 이러한 요청의 심사에서 중요한 요소로 간주되어야 한다(*Christine Goodwin v. the United Kingdom* [GC], 2002, § 78). 출생 등록부의 수정을 당국이 거부한 사건에서, 재판소는 성별전환자가 겪어온 길고도 어려운 전환 과정에서 최종이자 절정에 해당하는 단계로 여겨질 수 있는 합법적인 젠더 재지정이 법적으로 전면 인정되지 않는다는 사실에 주목하였다(과학과 사회의 발전을 반영하여 *Rees v. the United Kingdom*, 1986, §§ 42-44, *Cossey v. the United Kingdom*, 1990, §§ 39-40 및 *Sheffield and Horsham v. the United Kingdom* [GC], 1998, §§ 60-61 과 같은 과거 판례를 변경한 *ibid.*, § 78). 국가가 성별전환자의 성별 불일치 상태를 완화하는 치료와 수술을 승인하고, 수술 비용을 지원하거나 공동 부담하며, 심지어 여성에서 남성으로 성별 정정을 한 개인과 함께 사는 여성이 인공수정을 받는 것을 허용하는 상황에서, 그 치료가 가져온 결과의 법적 효과 인정을 거부하는 것은 비합리적으로 보이며(*Christine Goodwin*

v. the United Kingdom [GC], 2002, § 78), 특히 출생 등록부에 최초로 기재된 젠더 항목을 정정하는 데 따르는 어려움은 극복할 수 없는 것이 아니기 때문에 그러하다(*ibid.*, § 91).

303. *S.V. v. Italy*, 2018 사건 § 72 에서, 성별전환자가 젠더 전환 과정 중이었고 성별 재지정 수술을 완료하기 이전에 이름 변경을 당국이 허용하지 않은 것은, 청구인을 비합리적으로 오랜 기간(2 년 6 개월) 취약성을 느낄 수밖에 없는 비정상적 상황에 두게 한 경직된 사법절차에 근거한 것이었다.

304. *Hämäläinen v. Finland* [GC], 2014 사건 §§ 87-89 에서, 재판소는 후천적 젠더의 법적 인정을 위한 전제조건으로서 청구인의 혼인을 등록파트너십으로 전환하도록 요구한 것은, 동성 결혼이 핀란드에서 불법인 상황에서 혼인과 거의 동일한 수준의 법적 보호를 제공하는 실제적인 선택지였기 때문에, 비례성 원칙에 반하지 않는다고 판단하였다. 따라서 이 두 법적 개념 간의 사소한 차이점은 국가의 적극적 의무 관점에서 현재의 핀란드 제도를 결함 있는 것으로 만들지는 않았다. 또한, *A.P., Garçon and Nicot v. France*, 2017 사건에서는 외모 변경의 불가역성(§§ 116-135), 젠더 정체성 장애의 현실성(§§ 138-144), 의료 검진을 받아야 하는 의무(§§ 149-154) 등 트랜스젠더 개인의 가족관계등록부 변경을 위한 법적 조건이 문제 되었다.

3. 데이터 삭제권

305. 재판소는 일정 기간이 지난 후 개인데이터를 삭제할 권리문제를 다양한 맥락에서 다루었으며, 특히 다음과 같은 경우와 관련하여 검토하였다.

- "잊힐 권리": 과거에 공개된 개인의 성, 이름, 사진 등이 포함된 정보나 정보의 보관소를 언론이 재게시하거나 웹사이트에 계속 남겨두는 선택 또는 관행과 관련된 사안(*Węgrzynowski and Smolczewski v. Poland*, 2013; *M.L. and W.W. v. Germany*, 2018; *Biancardi v. Italy*, 2021; *Mediengruppe Österreich GmbH v. Austria*, 2022; *Hurbain v. Belgium* [GC], 2023)
- 범죄를 저질렀다고 기소되었거나 단순히 의심만 받은 개인의 경우: 범죄 예방 및 대응을 목적으로 한 데이터베이스에 당국이 수집한 DNA 프로파일, 신원 사진, 지문 등 개인데이터를 일정 기간이 지난 후 삭제할 수 있는 권리(*B.B. v. France*, 2009; *Gardel v. France*, 2009; *M.B. v. France*, 2009; *M. K. v. France*, 2013; *Brunet v. France*, 2014; *Ayçaguer v. France*, 2017; *Catt v. the United Kingdom*, 2019; *Gaughran v. the United Kingdom*, 2020)

- 전과 삭제 불가: 일정 기간이 지난 후에도 경찰 기록에서 자신의 전과를 삭제할 수 없었던 경우(*M.M. v. the United Kingdom*, 2012)
- 보안기관 기록보관소에 장기간 보유된 청구인들의 개인데이터: 그 성격과 보관 기간을 고려할 때 "민주사회에서의 필요성" 요건에 더 이상 부합하지 않는 경우(*Segerstedt-Wiberg and Others v. Sweden*, 2006)

a. "잊힐 권리"

306. "잊힐 권리(right to be forgotten)"라는 개념은 비교적 최근에 등장했으며 아직 형성 중지만, 실제 적용에서는 이미 여러 가지 뚜렷한 특징을 보여주고 있다(*Hurbain v. Belgium* [GC], 2023, §§ 191 및 194). 이 개념은 처음에는 언론이 과거에 공개된 사법적 성격의 정보를 재게시하는 맥락에서 국내 사법 관행에 등장했는데, "잊힐 권리"를 주장하는 사람은 사실상 정보를 재게시한 사람을 상대로 판결을 받아내고자 하였다(*ibid.*, § 194). 이후 이 "잊힐 권리"의 새로운 측면이, 뉴스 기사 디지털화의 맥락에서 국내 사법 관행에 나타났는데, 이로 인해 해당 신문사의 웹사이트에서 기사가 광범위하게 유포되었다. 이러한 유포 효과는 동시에 검색엔진에 의한 웹사이트 색인으로 인해 한층 증폭되었다. 이 측면은 "온라인상 잊힐 권리"로 알려져 있으며, 인터넷에 공개된 데이터의 삭제, 수정 또는 접근 제한을 요구하는 청구와 관련되어 있고, 이러한 청구는 뉴스 발행사나 검색엔진 운영자를 상대로 제기된다. 이러한 사건에서 문제 되는 것은 정보가 다시 떠오르는 것이 아니라, 그것이 온라인상에 계속 남아 있다는 점이다(*ibid.*, § 195). 일반적으로, "잊힐 권리"는 실제로 검색엔진 운영자나 뉴스 발행사가 취할 수 있는 다양한 조치로 이어질 수 있다. 이는 보관소에 보관된 기사의 내용(예컨대 기사 삭제, 수정 또는 익명화)이나 정보 접근 가능성의 제한과 관련된다. 후자의 경우, 검색엔진과 뉴스 발행사 모두 접근에 제한을 둘 수 있다(*ibid.*, § 175).

307. 재판소는 개인의 개인데이터를 공개하는 뉴스 기사에 대한 삭제, 수정, 익명화 또는 검색 목록 제거 요청과 관련된 여러 사건을 살펴보았다. 이러한 사건들은, 사생활 존중권을 주장한 개인이 제기한 경우에는 제 8 조에 따라(*Węgrzynowski and Smolczewski v. Poland*, 2013; *M.L. and W.W. v. Germany*, 2018), 언론인·편집자·언론사 소유자가 표현의 자유를 근거로 제기한 경우에는 제 10 조에 따라(*Biancardi v. Italy*, 2021; *Mediengruppe Österreich GmbH v. Austria*, 2022; *Hurbain v. Belgium* [GC], 2023) 심사되었다.

308. 구체적으로 살펴보면, *Biancardi v. Italy,* 2021 사건은, 사인에 대한 형사절차와 관련된 민감한 정보를 인터넷에 게시하고도 이를 검색 목록에서 제거하지 않은 것과 관련자들의 반대에도 불구하고 해당 정보를 쉽게 접근할 수 있도록 그대로 둔 기자의 결정에 대한 민사판결이 제 10 조와 양립할 수 있는지 재판소가 처음으로 판결할 기회가 된

사건이었다. 이 사건에서는 온라인 기사에서 신원 익명화 문제는 제기되지 않았다. 재판소는 관련자들의 공식적인 삭제 요청 이후에도 해당 기사가 8 개월 동안 온라인에서 쉽게 접근 가능했던 점을 지적하였다. 제재의 강도(형사책임이 아닌 민사책임이 부과된 점과 배상액의 수준)는 과도한 것으로 보이지 않았다

309. 개인의 과거와 관련된 정보를 최초로 공개하는 맥락에서 재판소는, 대통령 선거를 앞둔 시기에 한 후보자의 선거운동과 간접적으로 연결된 개인에 관한 특정 정보를 게시하지 말라는 법원 명령과 관련된 *Mediengruppe Österreich GmbH v. Austria*, 2022 사건을 심리하였다. 해당 신문은 후보자의 사무실 관리자 동생의 사진을 "우익 현장"에서 촬영된 것으로 게재하고, "유죄 판결을 받은 네오나치"라고 밝혔다. 문제의 기사 게시 시점은 유죄판결을 받은 지 20 년 이상, 출소한 지 약 17 년이 지난 뒤였으며, 문제의 기사 게시 당시 해당 전과는 이미 범죄기록에서 삭제된 상태였다. 국내 상급법원은 시간적 연계의 부재를 지적하면서, 청구인 회사가 관리자의 동생 사진을 동의 없이 게재하면서 그를 "유죄 판결을 받은 네오나치"라고 동일 기사에서 보도하는 것을 금지하였다. 재판소는 제 10 조 위반이 없다고 판단하면서, 특히 유죄 판결·출소·문제의 기사 게시 사이의 시간 경과, 관련인의 악명 상실, 추가 형사 유죄 판결이 없었던 점, 형을 마친 사람들의 사회 복귀의 중요성, 일정한 시간이 흐른 후 더 이상 자신의 유죄 판결에 직면하지 않을 정당하고 매우 중대한 이익 등을 강조하였다.

310. 과거에 기사화된 개인의 개인데이터를 포함하는 언론사 온라인 기사 보관소와 관련하여, 재판소는 이 맥락이 최초 공개와 관련된 상황과는 다르다고 지적하였으며(*Hurbain v. Belgium* [GC], 2023, § 205), 해결해야 할 주요 쟁점은 정보의 최초 공개가 아니라 그러한 정보가 온라인상에 계속 존재하는 것이라고 규정하였다(*ibid.*, § 174).

311. 이와 같은 맥락에서, 변호사의 평판을 훼손하는 기사가 신문의 온라인 기사 보관소에 남아 있음에도 그 기사를 삭제하라는 명령을 법원이 거부한 것은 *Węgrzynowski and Smolczewski v. Poland*, 2013 사건 §§ 60-70 에서 제 8 조 위반이 아니라고 판단되었다. 재판소는 사법 당국이 과거 최종 판결에서 개인의 명예를 부당하게 침해한다고 인정된 출판물의 모든 흔적을 공적 영역에서 제거하도록 명령하여 역사를 다시 쓰는 역할을 담당하는 것은 아니라는 점을 받아들였다(*ibid.*, § 65). 나아가 언론의 공적 온라인 기사 보관소에 접근할 수 있게 되어 대중에게 발생하는 정당한 이익은 제 10 조에 의해 보호된다(*ibid.*, § 65). 주목할 만한 점은, 폴란드 법원이 해당 신문 웹사이트의 기사에 첫 번째 소송의 결과를 알리는 주석을 추가하는 것이 바람직하다고 평하였다는 것이다. 재판소는 이를 통해 국내 법원은 인터넷상에서 일반 대중이 접근할 수 있는 출판물이 개인 권리의 실효적 보호에 미칠 수 있는 중요성을 인식하였고, 해당 기사에 관한 사법적 결정에 대한 충분한 정보를 신문 웹사이트에

제공하는 것의 가치를 평가하였음을 보여준다고 보았다. 해당 변호사는 자신에게 유리한 이전 판결이 기사에 언급되도록 요청하지는 않았다(*ibid.*, §§ 66-67).

312. *M.L. and W.W. v. Germany*, 2018 사건에서, 살인죄로 유죄 판결을 받고 14 년간의 형기를 마친 후 석방된 두 청구인은, 대중의 시선 밖에서 새로운 삶을 시작할 수 있게 하려고 신문사의 온라인 기사 보관소에 있는 사진과 전체 신원(성 및 이름)이 기재된 보도를 삭제해 달라고 요청했으나 받아들여지지 않았다. 재판소는, 정확하고 객관적인 보관소에 대한 접근에의 공익이 우선해야 한다는 이유로 제 8 조 위반이 아니라고 판단하였다(*ibid.*, § 116). 특히 재판소는 첫째, 청구인들이 익명화를 요청했을 당시 문제 된 보도가 여전히 공익적 논쟁에 기여하고 있었다는 점, 둘째, 청구인들이 단순히 대중에게 알려지지 않은 사인이 아니었다는 점, 셋째, 청구인들이 유죄 판결 이후 언론에 접근하여 재심을 요청하려 했던 언론과의 관계, 넷째, 해당 보도들이 사실을 객관적으로 전달하였고 청구인들을 비방하거나 명예를 훼손할 의도는 없었다는 점, 마지막으로 그 정보의 접근 가능성이 제한적이었다는 점을 고려하였다(*ibid.*, §§ 98-115).

313. *Hurbain v. Belgium* [GC], 2023 사건에서, 재판소는 한 개인의 개인데이터를 공개하는 기사의 전자 아카이브 버전이 계속 온라인상에서 존속하는 문제와 관련하여, 제 8 조와 제 10 조 각각의 권리를 균형 있게 조정하기 위해 적용해야 할 기준에 관한 기존 판례를 재검토하고 조정하였다. 이 사건은 약 20 년 전 사망 사고를 일으킨 운전자의 "잊힐 권리"에 근거하여 그 사건을 정확히 보도한 기사의 온라인 보관본을 익명화하라는 명령을 국내 법원으로부터 받은 신문사 발행인이 제기하였다.

314. 재판소는 판결에서, 특정 정보가 인터넷상에 계속 존속하는 것이 초래하는 부정적 효과, 특히 해당인에 대한 대중의 인식 방식에 미치는 중대한 영향, 해당인의 프로필 형성과 현실을 단편적·왜곡적으로 제시할 위험을 인정하였다. 그러나 재판소는 잊힐 권리를 주장할 권원이 협약에 의해 독립적으로 보호되는 권리에 해당하는 것은 아니며, 제 8 조에 의해 보호되는 범위 내에서만 특정 상황이나 특정 정보 항목에 한정된다고 설명하였다(*ibid.*, § 199).

315. 재판소는 이어, 온라인 기사 보관본의 내용 변경 요청과 관련하여 동일한 가치를 지니는 권리들 사이의 균형을 도모할 때 고려해야 할 기준으로 (i) 보관된 정보의 성격 (ii) 사건 발생 이후 및 최초 공개·온라인 공개 이후 경과한 시간 (iii) 해당 정보의 현시점에서의 공익성 (iv) 잊힐 권리를 주장하는 사람의 공인 여부 및 사건 이후 그 행위 (v) 해당 정보가 온라인상 계속 존속함으로써 발생하는 부정적 영향 (vi) 디지털 보관소에서의 정보 접근 가능 정도 (vii) 표현의 자유와 특히 언론의 자유에 조치가 미치는 영향을 들었다(*ibid.*, § 205).

316. 재판소는 또한, 대부분의 경우 사생활 보호가 쟁점이 된 다른 이익들과, 특정 사건에서 그 보호를 실현하기 위해 동원된 수단을 비교하여 어떠한 보호를 부여할지를 판단하기 위해서는 여러 기준을 동시에 고려해야 한다고 강조하였다. 따라서 잊힐 권리 주장의 맥락에서 사생활 보호는 실제로 그것이 실행된 수단과 분리하여 고립적으로 평가될 수는 없다. 이러한 관점에서 보면, 이는 상충하는 이해관계의 각각의 무게와 특정 사건에서 사용된 수단의 범위를 고려하여, 사생활 존중권을 통한 "잊힐 권리"에 부여된 비중이나 표현의 자유에 부여된 비중이 과도했는지 여부를 가리는 균형 검토의 문제이다. 또한 적용될 기준이 모두 같은 무게를 지니는 것은 아니다. 조치를 요청하는 개인의 이익과 그러한 요청이 발행인에게 미치는 영향 사이에서 균형을 제대로 맞추도록 특별히 주의해야 한다. 언론 보관소의 온전성을 유지해야 한다는 원칙에 따라 언론이 정보 전달과 보관소 유지라는 임무를 수행하는 데 위축 효과가 생기지 않도록, 콘텐츠의 수정은 물론 삭제는 반드시 엄격하게 필요한 범위로 제한하여야 한다(*ibid.*, § 206 및 211).

317. 사건 심사 과정에서 위에서 언급된 기준들을 적용하면서, 재판소는 국내 법원이 문제된 기사에 보도된 사법적 사실의 성격과 중대성, 해당 기사가 시사적·역사적·과학적 관심을 가지지 않았다는 점, 관련 개인이 잘 알려진 인물이 아니었다는 점을 일관되게 고려하였다고 평하였다. 또한, 국내 법원은 해당 개인이 입은 중대한 피해에 주목했는데, 이는 기사가 제한 없는 접근이 가능한 상태로 온라인상에 계속 존속한 결과로, 특히 최초 공개 이후 상당한 시간이 흘렀다는 점을 고려할 때 "가상의 범죄기록"을 형성할 수 있는 것이었다. 나아가 국내 법원은 쟁점이 된 권리들을 균형 있게 조정하기 위해 고려할 수 있는 여러 조치를 검토한 끝에, 기사 익명화가 신청인에게 과도하거나 실행 불가능한 부담을 부과하지 않으면서도 해당 개인의 사생활을 보호하는 가장 효과적인 수단이라고 판결하였다(*ibid.*, § 255). 따라서 재판소는 국내 법원이 적절한 균형 검토를 수행하였다고 확신하였으며, 제 10 조 위반이 아니라고 판단하였다(*ibid.*, § 256).

b. 기타 맥락

318. *M.M. v. the United Kingdom*, 2012 사건 §§ 187–207 에서, 한 개인의 경찰기록에 경고처분을 평생 등록해 둔 것은 제 8 조 위반이라고 판단되었다. 재판소는 과거 개인에게 내려진 유죄 판결이나 경고처분은 시간이 지남에 따라 그 개인의 사생활의 불가분한 일부가 되어 존중되어야 한다고 보았다. 범죄기록에 포함된 데이터가 어떤 의미에서는 공적 정보라 하더라도, 그것이 중앙 파일에 체계적으로 보관되면, 사건 당사자를 제외한 모든 사람이 그 사건을 잊었을 시점에도 오랫동안 공개될 수 있음을 의미한다. 재판소는 데이터 삭제를

가능하게 하는 심사 기준이 매우 제한적이었고, 삭제 요청이 극히 예외적인 경우에만 허용되었다는 사실을 불안한 것으로 간주하였다(*ibid.*, § 202).

319. 재판소는 국가가 데이터 보유 영역에서 권한을 극대화하여 사실상 무기한으로 데이터를 저장함으로써 판단재량을 극단적으로 밀어붙이는 경우, 그 데이터의 계속된 보유가 비례성을 상실했을 때 개인데이터를 삭제할 수 있도록 하는 실효적 보호조치가 마련되어 있는지가 결정적이라고 판결한다(*Catt v. the United Kingdom*, 2019, § 119; *Gaughran v. the United Kingdom*, 2020, § 94). 음주 운전으로 유죄 판결을 받은 청구인의 생체 데이터와 사진이, 모든 형사 유죄 판결자들의 개인데이터를 무기한 보관하는 정책에 따라 보유된 사건에서, 재판소는 제 8 조 위반이라고 판단하였다(*ibid.*, § 98). 해당 범죄의 성격, 당사자의 연령, 경과된 시간, 당사자의 현재 인격을 고려할 때 데이터 보관이 더 이상 필요하지 않아 보이는 경우에도, 청구인이 자신의 데이터 삭제를 신청할 수 있는 규정은 존재하지 않았다. 경찰은 유죄 판결을 받은 사람들의 생체 데이터와 사진을 극히 예외적인 경우에만 삭제할 수 있었다. 심사 가능성은 거의 형식적 수준에 불과하였다(*ibid.*, § 94).

320. 저장 목적과 관련하여 더 이상 필요하지 않은 개인데이터를 삭제할 수 있는 실효적 보호조치가 없는 것은, 특히 더 높은 수준의 보호를 요구하는 민감한 데이터의 특별 범주에 있어서는 심각한 우려를 낳는다(*Catt v. the United Kingdom*, 2019, § 112). 평화적 시위자의 정치적 견해를 드러내는 민감한 데이터가 경찰 데이터베이스에 보관된 사건에서, 재판소는 제 8 조 위반이라고 판단하였다(*ibid.*, § 128). 이러한 데이터의 최대 보관 기간에 관한 규정이 부재한 상황에서, 청구인은 자신의 데이터 보유 기간의 비례성을 보장하기 위해 적용되는 실무준칙이 매우 유연한 탓에, 당국의 주의 의무에 전적으로 의존할 수밖에 없었다. 재판소는, 데이터 주체가 삭제를 요청한 후에도 당국이 해당 데이터를 삭제하지 않거나 그 보유 결정을 설명하지 않는다면, 데이터 삭제 보장의 효과는 제한적이라고 판결하였다(*ibid.*, §§ 118 및 122).

321. 성범죄 유죄 판결을 받은 개인들의 개인데이터 보유와 관련된 여러 사건에서, 재판소는 청구인들이 자신의 데이터 보유가 더 이상 필요하지 않은 것으로 보이는 경우(유죄 판결 이후의 시간 경과 등을 고려하여) 삭제를 요청할 수 있었음을 확인하고 제 8 조 위반이 아니라고 판단하였다(*B.B. v. France*, 2009, §§ 66–68; *Gardel v. France*, 2009, §§ 67–69; *M.B. v. France*, 2009, §§ 58–60). 동시에, 데이터 삭제를 요청할 가능성이 전혀 없다고 해서 반드시 제 8 조 위반에 해당하는 것은 아니며, 그러한 데이터 보유의 목적, 데이터의 성격, 자의성 및 남용 위험에 맞서 당사자에게 제공된 보장을 종합적으로 고려해 평가해야 한다. 특히, 법무부 내부 데이터베이스에 보관된 관련 데이터가 *협약 108* 제 6 조의 의미에서 "민감한" 데이터가 아니고, 개인이 당사자로 참여한 사법절차와 관련된 사실적이고 객관적인

정보로 한정되어 있으며, 그 처리가 사법의 적정한 운영과 관련 공공서비스의 원활한 기능 보장을 목적으로 하고, 또한 (데이터의 정확성을 확보할 가능성과 제한된 보관 기간이라는) 적절한 보장이 수반된 경우라면, 그러한 데이터의 사전 삭제 절차가 마련되지 않았더라도 비례성에 반한다고 볼 수는 없다(*L.F. v. France* (dec.), 2024, §§ 44-47).

322. *Peruzzo and Martens v. Germany* (dec.), 2013 사건 § 46 에서, 마약 밀매와 관련된 중대한 범죄로 유죄 판결을 받은 후 개인데이터가 기록부에 보관된 사안과 관련하여, 재판소는 비록 법률이 DNA 프로파일 보관의 최대 기간을 규정하지는 않았더라도, 연방범죄수사청이 각 사안의 데이터 보유 목적과 정황의 성격 및 중대성을 고려하여 10 년을 넘지 않는 정기적인 간격으로 데이터 보유의 필요성을 점검하도록 규정되어 있었다는 점을 고려하였다.

323. *Ayçaguer v. France*, 2017 사건 § 44 에서 재판소는, DNA 프로필을 국가 데이터베이스에 보관하도록 한 현행 규정이 그 보관 기간과 삭제 불가능성 때문에 검체 채취를 반대한 청구인에게 충분한 보호를 제공하지 못하였으므로 제 8 조 위반이라고 판단하였다(*ibid.*, § 45). 재판소는 유죄 판결을 받은 자도, 범죄 혐의를 받았거나 불기소 처분되었거나 무죄 판결을 받은 자와 마찬가지로, 데이터 보유 기간이 범죄의 성격과 제한의 목적에 비례하도록 보장하기 위해 저장된 데이터 삭제를 요청할 수 있는 구체적 기회를 부여받아야 한다고 강조하였다(*ibid.*, § 45; *B.B. v. France*, 2009, § 68; *Brunet v. Francee*, 2014, §§ 41-43).

324. 개인데이터 삭제 가능성과 관련하여, 언제든 법원에 삭제 요청을 제출할 권리는 가능한 한 많은 자료에 접근해야 하는 수사 당국의 이익과 충돌할 수 있다. 따라서 쟁점이 된 이익들이 적어도 부분적으로는 상충하므로, 삭제는 "실질적이고 실효적인" 보장이 아니라 "이론적이고 허구적인" 보장에 불과하다(*M.K. v. France*, 2013, §§ 44-47).

325. *Segerstedt-Wiberg and Others v. Sweden*, 2006 사건 §§ 73-92 에서, 국가 보안기관의 파일에 청구인들이 정치 집회에 참석한 사실, 시위 중 경찰 검문에 대한 폭력적 저항을 옹호한 사실, 특정 정당의 당원이었다는 사실 등 매우 오래된 개인데이터를 보관한 것은 제 8 조 위반에 해당하였다. 재판소는 국가안보 보호와 테러 대응이라는 국가의 이익이 문제 된 정보의 수집 및 보관을 정당화한다 하더라도, 이는 청구인 각자가 사생활 존중권을 행사하는 데에 대한 제한의 심각성과 균형을 이루어야 한다고 보았다. 청구인들에 관한 정보의 성격과 오랜 경과 기간을 고려할 때, 그 보관의 이유가 관련성은 있다고 하더라도 30 년이 지난 시점에는 충분하다고 볼 수 없었다(*ibid.*, § 90).

4. 자신의 권리를 보장할 특수한 절차적 보호조치 및 실효적 절차 제도를 누릴 권리

326. 제 8 조에는 명시적 절차 요건이 포함되어 있지 않지만, 이 조항에 의해 보장되는 권리를 실효적으로 향유하기 위해서는 관련 의사결정 과정이 공정하고, 해당 권리가 보호하는 이익을 적절히 존중할 수 있어야 한다. 이러한 과정은 청구인이 증명 및 증거 문제를 포함한 공정한 조건하에서 제 8 조에 따른 권리를 주장할 수 있도록 하는 실효적 절차 제도가 존재해야 할 수 있다(*I. v. Finland*, 2008, § 44; *Ciubotaru v. Moldova*, 2010, § 51). 공식 국가 등록부에 기재된 신원 데이터를 정정하려는 사람에게 극복할 수 없는 장벽을 초래하는 요건을 부과하는 것은, 사생활 존중권에 대한 실효적 준수를 보장할 국가의 적극적 의무와 양립할 수 없다(*ibid.*, §§ 51-59). 청구인의 HIV 양성 상태가 공개된 사건에서, 재판소는 제 8 조 위반이라고 판단하면서, 국가가 민사절차의 틀 내에서, 청구인이 자신의 건강 상태 정보 유포에 따른 손해배상을 청구하는 과정에서 청구인에게 지나치게 무거운 입증책임을 부과하였다는 점에 중점을 두었다(*I. v. Finland*, 2008, § 44).

327. 특정인의 건강에 관한 기밀정보가 언론에 의해 공개되어 발생한 피해에 대해 국내 법원이 손해배상을 명하거나 그러한 남용의 재발을 방지할 권한을 법률이 제한하는 경우, 이는 항소 절차의 실효성을 저해할 수 있으며, 따라서 청구인들이 정당하게 기대할 수 있었던 사생활 보호를 제공하지 못하게 된다. 따라서 *Armonienė v. Lithuania*, 2008 사건 §§ 47-48 및 *Biriuk v. Lithuania*, 2008 사건 §§ 46-47 에서 재판소는 문제 된 시점에 시행 중이던 공중 정보 제공법이, 전국 일간지에 청구인들의 동의 없이 HIV 양성 상태가 공개되고 신원이 밝혀진 이후 국내 법원이 청구인들에게 지급한 손해배상액에 상한선을 두고 있었기 때문에 제 8 조 위반이라고 판단하였다. 나아가, 국가 데이터베이스(납세자 정보 서비스)에 보관된 개인데이터의 불충분한 보호라는 계속적 상황, 그 데이터베이스 접근 맥락에서 남용을 방지하지 못한 당국의 장기간의 태만에 대해 청구인이 불만을 제기한 사건에서, 단순한 금전적 배상만을 제공하는 구제수단은 실효적이지 않은 것으로 판단되었다(*Casarini v. Italy* (dec.), 2024, § 89).

328 . 형사절차의 틀 안에서 또는 피고인이 무죄 판결이나 불기소 처분, 유죄 판결을 받은 후 수집된 개인데이터의 보유 정당성에 대해 국가 차원에서 독립적 심사를 제공하지 않는 것은, 그러한 데이터 보유가 제 8 조와 양립할 수 있는지 여부를 판단할 때 고려해야 할 중요한 요소이다(*S. and Marper v. the United Kingdom* [GC], 2008, §§ 119, 125). 형사절차가 각각 무죄 판결과 불기소 처분으로 종결된 두 개인으로부터 채취한 세포 검체, DNA 프로파일 및 지문을 무기한 보유한 사건에서, 재판소는 청구인들이 국가 데이터베이스에서 해당

데이터를 삭제하거나 샘플을 파기할 가능성이 거의 없었다는 점을 지적하며 제 8 조 위반이라고 판단하였다.

329. *Vicent Del Campo v. Spain*, 2018 사건 §§ 39, 53 에서, 사법절차의 제 3 자였던 청구인이 판결 선고 전에 자신의 신원이나 자신과 관련된 개인정보의 공개를 막아 달라고 국내 법원에 신청할 수 없었던 것은, 자신의 권리를 방어할 수 있는 실효적 절차 제도를 박탈당한 것이었다.

330. 쟁점이 된 상충하는 이해관계에 대한 비례성 분석을 수행하지 않고, 청구인의 사생활 비밀권과 데이터 보호 문제를 고려하지 않은 당국의 태도는 협약 제 8 조 요건을 위반한다(*Liebscher v. Austria*, 2021, §§ 64-69).

331. *M.D. and Others v. Spain*, 2022 사건 §§ 65-72 에서, 당국만 접근할 수 있는 경찰 데이터베이스에서 청구인들의 개인데이터가 언론에 유출된 사안과 관련하여, 재판소는 공적 기관이 보유한 사적 데이터의 불법적 공개와 관련해 제 8 조상의 적극적 의무에는 기자들이 해당 데이터에 접근한 경위를 규명하고, 필요하다면 발생한 결함에 책임이 있는 자를 처벌하기 위한 실효적 조사 실시 의무가 포함된다고 판결하였다. 당국이 이러한 조사를 수행하지 않은 것은 제 8 조 위반에 해당하였다. 마찬가지로, *Y.G. v. Russia*, 2022 사건 §§ 46-53 에서, 청구인은 자신의 건강 상태 정보를 포함한 개인데이터가 시장에서 판매 가능한 상태였다고 주장했는데, 재판소는 이러한 중대한 사생활 침해 상황에서, 공식 조사의 형태로 국가의 지원을 받지 못한 채 홀로 행동해야 했던 청구인에게는 가해자를 특정할 실효적 수단이 없었으므로, 형사법적 고소가 당시 상황에서 부적절한 수단이 아니었다고 보았다. 당국이 조사를 수행하지 않은 것은 청구인의 사생활 존중권을 적절히 보호할 국가의 적극적 의무를 위반한 것이다.

332. 청구인의 개인데이터가 납세자 정보 서비스 데이터베이스에 보관되어 있었는데, 세무경찰관이 이를 여러 차례 불법적으로 열람한 뒤 기자에게 제공하여 보도에 사용되도록 한 *Casarini v. Italy* (dec.), 2024 사건 §§ 92-105 에서 재판소는 데이터보호당국(DPA)에 제기하는 청구가 실효적 구제수단에 해당하므로 이를 모두 거쳐야 한다고 판단하였다. 데이터보호당국은 사법기관은 아니지만, 외부 압력으로부터 자유로운 독립적이고 완전히 자율적인 행정기관이었으며, 그 절차는 당사자주의적 성격을 지니고 구속력 있는 결정을 내렸다. 또한 그 결정은 관할 사법당국에 항소할 수 있었고, 후자의 결정은 파기원에 법률심으로 상고할 수 있었다.

333. 국내 구제수단이 실효적이기 위해서는 자신의 개인데이터에 접근하고자 하는 데이터 주체가 제출한 신청은 합리적인 기간 내에 처리되어야 한다. *Roche v. the United Kingdom*

[GC], 2005 사건 §§ 166-167, 169 에서 재판소는 청구인이 군 가스 실험에 참여한 결과 자신의 건강에 발생할 수 있는 잠재적 위험을 평가할 수 있었던 개인데이터가 포함된 문서에 접근하는 데 부당하게 오랜 기간을 기다려야 했다는 이유로 제 8 조 위반이라고 판단하였다.

334. 엄격한 기한이나 절차적 제한도 심사의 대상이 된다. *Moldovan v. Ukraine*, 2024 사건 §§ 52-53 에서, 청구인은 생물학적 아버지와의 친자관계 인정을 구하는 청구를 심리하던 국내 법원이, DNA 검사가 가능했는데도 동거 사실 증명을 친자관계 인지의 필수 요건으로 규정한 구법 조항을 적용했다고 주장하였다. 재판소는 이러한 국내 법원의 접근 방식의 효과가 경직된 시한이나 다른 절차적 제한의 효과와 유사하다고 보았다. 재판소는 이와 같은 접근 방식과 더불어, 국내 법원이 제출된 DNA 증거를 면밀할 정도로 심리하지 않은 것이 결합되어, 협약 제 8 조상 국가의 적극적 의무 위반에 해당한다고 결론 내렸다.

335. 인터넷 이용자의 트래픽 데이터에 대한 비밀 유지 요건에 국내 당국이 지나치게 큰 비중을 두는 것은, 범죄자를 특정하고 처벌하기 위한 형사 수사의 실효성을 저해하는 경우, 특정 상황에서 제 8 조를 위반할 수 있다(*K.U. v. Finland,* 2008, § 49). *K.U. v. Finland*, 2008 사건 §§ 49-50 에서 재판소는 미성년자를 소아성애자의 접근 대상으로 삼는 인터넷 광고를 게시한 사람을 특정하고 사법적 책임을 묻도록 하는 절차 제도가 부재하여 피해자가 그 사람을 상대로 금전적 배상을 청구할 수 없었던 점을 이유로 제 8 조 위반이라고 판단하였다. 때로는 전기통신 및 인터넷 서비스 이용자가 사생활 비밀권과 관련하여 누리는 보장보다 사회 불안과 범죄 예방 또는 타인의 권리와 자유 보호와 같은 다른 정당한 고려 사항이 우선할 수 있다.

336. 국가안보 영역에서, 위와 같은 이유로 조치의 대상이 된 사람은 누구든지 문제 된 조치에 대해 모든 관련 사실적·법적 쟁점을 심리하고 필요하다면 당국의 남용을 처벌할 권한을 가진 독립적이고 공정한 기관에 의한 심사를 받을 수 있어야 한다. 그러한 심사기관 앞에서 관련인은 자신의 입장을 제시하고 당국이 제시한 논거를 반박할 수 있도록 하는 당사자주의 절차의 보장을 받아야 한다. 따라서 *Dalea v. France* (dec.), 2010 사건에서 재판소는 청구인의 개인데이터가 셍겐 데이터베이스에 장기간 등록된 것이, 문제 된 조치에 대한 심사를 청구인이 보장받았다는 점에서 “민주사회에서의 필요성”에 해당할 수 있다고 보았다. 비록 청구인이 자신의 데이터 등록의 구체적 사유에는 이의를 제기할 수 없었더라도, 셍겐 데이터베이스에 자신과 관련된 다른 모든 데이터를 열람할 수 있었다.

337. 국가안보 사유로 조치의 대상이 된 사람은 누구든지 문제 된 조치의 심사를 청구할 수 있어야 하는데, 그 심사를 담당하는 독립적이고 공정한 기관은 반드시 사법적 지위를 가질 필요는 없다. *Leander v. Sweden*, 1987 사건 § 59 에서, 비밀경찰 파일을 이용하여 목수를

채용한 사안과 관련하여, 청구인이 사법적 구제수단을 가질 권한은 없었더라도(*ibid.*, §§ 62, 67), 관련 국내 당국이 개인에 관한 정보를 비밀 파일에 수집·보관하고 이를 활용하도록 허용하는 작용에 대해 의회와 독립기관이 심사를 수행할 가능성을 포함한 보장 장치가 존재했기 때문에(*ibid.*, § 65) 재판소는 제 8 조 위반이 아니라고 판단하였다. 국가안보를 이유로 한 조치를 심사하는 국내 기관에 대한 구제수단의 실효성을 평가하기 위해서는, 해당 기관이 보유한 절차적 권한과 보장에 주목해야 한다(*ibid.*, §§ 77, 80, 83–84). 또한, 다투어진 조처를 한 당국의 직속 상급자에게 제기하는 상급자에 대한 불복신청은 권한 남용에 맞설 정도의 보호를 구성하는 데 필요한 독립성 요건을 충족하지 못한다(*Roman Zakharov v. Russia* [GC], 2015, § 292).

338. 비밀 감시 조치와 관련하여, 그 심사와 감독은 감시를 처음 명할 때, 수행되는 도중 및 종료된 이후라는 세 단계에서 진행될 수 있다. 첫 두 단계와 관련해서는, 비밀 감시의 본질과 논리에 따라 감시 자체뿐 아니라 그에 수반되는 심사 역시 대상자의 인지 없이 이루어져야 한다. 따라서 개인이 스스로 실효적 구제를 구하거나 심사 절차에 직접 참여하는 것이 필연적으로 차단되는 만큼, 마련된 절차 자체가 권리를 보호하는 충분하고 동등한 보장을 제공해야 한다. 개별 사건에서 남용이 매우 쉽게 발생할 수 있고, 그러한 남용이 민주사회 전체에 심각한 결과를 초래할 수 있는 영역에서는, 감독 통제를 법관에게 부여하는 것이 원칙적으로 바람직하며, 사법적 통제는 독립성·공정성·적정 절차에 대한 최상의 보장을 제공한다(*ibid.*, § 233; *Klass and Others v. Germany*, 1978, §§ 55–56; *Denysyuk and Others v. Ukraine*, 2025, § 88).

339. 세 번째 단계인 감시가 종료된 이후와 관련해서는, 사후 통지 여부가 법원에서 구제수단의 실효성과 불가분하게 연결되므로 감시장악권 남용에 대한 실효적 보호조치의 존재와도 직결된다(*Roman Zakharov v. Russia* [GC], 2015, § 234). 원칙적으로, 당사자가 자신도 모르게 취해진 감시 조치에 대해 사후 통지를 받아 그 적법성을 다툴 수 있거나(*Klass and Others v. Germany*, 1978, §§ 57–59; *Weber and Saravia v. Germany* (dec.), 2006, §§ 135–137) 통신이 가로채기 되었을 가능성을 의심하는 누구든 법원에 제소할 수 있는 제도가 마련되어 있지 않다면(*Kennedy v. the United Kingdom*, 2010, §§ 167, 169; *Roman Zakharov v. Russia* [GC], 2015, § 234) 법원에 의한 구제 가능성은 거의 없다.

340. *Klass and Others v. Germany*, 1978 사건 §§ 57–59 및 *Weber and Saravia v. Germany* (dec.), 2006 사건 §§ 135–137 에서, 재판소는 국내 차원에서 가용한 구제수단이 적절하다고 판단하였다. 통신이 점검·확인된 개인들은 감시 목적을 해치지 않는 범위에서 가능한 한 신속하게 통지를 받았다. 또한 구제수단은 독립적 기관이 감시 대상자에게 해당 조치를 통지해야 하는지를 결정할 권한을 부여받는 등 실효적 보호조치로

보완되어 있었다. 그러한 통지에 근거하여, 당사자는 손해배상을 청구하는 민사소송이나 기본법 위반 여부에 대한 판결을 구하기 위한 연방헌법재판소 제소 등 다양한 사법적 수단을 선택할 수 있었다(*Klass and Others v. Germany*, 1978, §§ 57, 24).

341. 조치의 대상자가 자신에 대한 조치에 관해 통지를 받지 못하는 제도의 경우에도, 비밀 감시 조치로 사생활 존중권이 침해되었다고 생각하는 개인이 사전에 자신의 통신이 가로채졌다는 사실을 통지받지 못했더라도 독립적이고 공정한 기관에 제소할 가성은, 재판소가 제 8 조 위반이 아니라고 판단한 사건에서 중요한 보호조치로 평가되었다(*Kennedy v. the United Kingdom*, 2010, §§ 167, 169). 반대로, 국내 제도상 가용한 구제수단이 문제된 조치에 관한 최소한의 정보만을 가진 사람에게만 열려 있는 경우, 재판소는 당사자에게 비밀 감시 조치에 대항할 실효적 구제가 없었다고 판결하였으며, 이는 제 8 조 위반에 해당한다(*Roman Zakharov v. Russia* [GC], 2015, §§ 293–298, 305; *Denysyuk and Others v. Ukraine*, 2025, §§ 116–32).

III. 협약 및 의정서 내 다른 여러 조항과의 상호작용

342. 협약 체계에서 개인데이터 보호의 주요 근거가 되는 협약 제 8 조가 보장하는 사생활과 가족생활, 주거 및 통신의 존중권 외에도, 그 보호와 관련된 쟁점은 협약 및 그 의정서의 다른 조항에서도 문제 될 수 있다. 이러한 경우 재판소의 주요 임무는 이 보호를 다른 권리 및 정당한 이익과 비교형량하여 조화시키는 것이다. 때로는 개인데이터 보호 문제가 제기됨으로써, 재판소가 협약 및 그 추가 의정서가 보장하는 다른 권리의 범위를 확정할 수 있게 되었다.

A. 데이터 보호와 실체적 권리[10]

협약 제 9 조

"1. 모든 사람은 사상, 양심 및 종교의 자유에 대한 권리를 가진다. 이 권리는 자신의 종교 또는 신념을 변경할 자유와, 예배, 선교, 행사, 의식을 통해 혼자서 또는 다른 사람들과 함께 그리고 공개적으로 또는 개인적으로 자신의 종교 또는 신념을 표명할 자유를 포함한다.

2. 종교 또는 신념을 표명할 자유는 공공의 안전을 위해, 공공질서, 보건, 도덕 또는 타인의 권리와 자유의 보호를 위해 민주사회에서 필요한 경우 법이 정하는 바에 따라서만 제한될 수 있다."

협약 제 10 조

"1. 모든 사람은 표현의 자유에 대한 권리를 가진다. 이 권리는 의견을 가질 자유와 공권력의 제한을 받지 않고 국경과 관계없이 정보와 사상을 주고받을 자유를 포함한다. 이 조항은 방송, 텔레비전 또는 영화 사업에 대한 국가의 허가 제도를 금지하지 아니한다.

2. 이러한 자유의 행사에는 의무와 책임이 따르므로 국가안보, 영토보전 또는 공공의 안전을 위해, 무질서나 범죄의 방지를 위해, 보건이나 도덕의 보호를 위해, 타인의 명예나 권리의 보호를 위해, 비밀리에 얻은 정보의 공개를 방지하기 위해 또는 사법부의 권위와 중립성의 유지를 위해 민주사회에서 필요한 경우 법이 정하는 형식과 조건에 따라야 하고, 제한과 처벌의 대상이 될 수 있다."

협약 제 14 조

"본 협약에서 명시된 권리와 자유의 향유는 특히 성별, 인종, 피부색, 언어, 종교, 정치적 또는 그 밖의 견해, 출신 국가 또는 사회계층, 소수민족과의 연계, 재산, 출생 또는 기타 신분을 포함하여 어떠한 사유로 인한 차별 없이 보장된다."

제 1 의정서 제 1 조

"모든 자연인 또는 법인은 자신의 재산을 평화적으로 향유할 권리를 가진다. 어느 누구도 공익을 위하여 그리고 법률 및 국제법의 일반원칙에 의하여 규정된 조건을 따르는 경우를 제외하고는 자신의 재산을 박탈당하지 아니한다.

단 위의 규정은 국가가 일반의 이익에 따라 재산의 사용을 규제한다거나, 세금이나 기타의 부담금 또는 벌금을 확보하기 위하여 필요하다고 보는 법률을 시행할 권리를 결코 해하지 아니한다."

제 4 의정서 제 2 조

"1. 합법적으로 국가의 영토 내에 있는 모든 사람은 그 영토 내에서 이동의 자유와 주거선택의 자유에 관한 권리를 가진다.

2. 모든 사람은 자국을 포함하여 어떠한 국가로부터도 자유롭게 떠날 수 있다.

3. 공공질서의 유지, 범죄의 예방, 위생 및 도덕의 보호, 또는 타인의 권리 및 자유의 보호를 위하여 민주사회에 있어서 국가 안보 또는 공공의 안전에 필요한 것으로서 법률에 의하지 아니하고는, 이러한 권리의 행사에 관하여 어떠한 제한도 부과하지 아니한다.

4. 특정한 분야에서는 제 1 항에 규정된 권리들이 민주사회에서 공익에 의하여 정당화되고 법률에 의하여 부과되는 제한을 받을 수 있다."

1. 데이터 보호와 사상, 양심, 종교의 자유(협약 제 9 조)

343. 재판소는 개인데이터 보호 문제도 제기된 일부 사건에서는 제 9 조 위반이라고 판단한 반면, 위반이 아니라고 판단한 사건도 있었다.

344. *Sinan Işık v. Turkey*, 2010 사건 §§ 37-53 에서 재판소는 청구인의 신분증에 종교란을 기재하도록 하는 것이 의무적이든 임의적이든 간에 그 자체가 문제 되는 상황에 직면하였다. 재판소는, 종교 등록부 및 신분증의 종교란 기재를 변경하기 위해 당국에 서면으로 신청해야 하는 사실 자체와 단순히 신분증의 종교란을 공란으로 두는 것만으로도 개인이 자신의 의사에 반하여 종교의 한 측면이나 가장 내밀한 신념에 관한 정보를 공개하도록 강제된다고 보았다. 재판소는, 종교나 신념을 외부에 드러낼 자유에는 부정적 측면, 즉 개인이 자신의 종교를 공개하도록 강제되거나 자신에게 특정한 신념이 있거나 없다는 결론을 낳을 수 있는 방식으로 행동하도록 강제되지 않을 권리도 포함된다는 점을 다시 강조하면서, 제 9 조 위반이라고 판단하였다. 종교란을 공란으로 둘 수 있더라도, 그렇게 하는 사실 자체가 특정한 의미를 지니며, 결국 해당 정보를 기재한 신분증 소지자와 이를 표시하지 않기로 한 소지자를 구별할 수 있게 하기 때문이다(*ibid.*, § 51).

345. *Alexandridis v. Greece*, 2008 사건 § 41 에서, 변호사가 자신이 정교회 신자가 아님을 법원에 밝히고 종교적 선서 대신 엄숙한 선언을 하겠다고 표명하도록 요구한 것은 그의 제 9 조상 권리에 대한 제한이었다. 국가 당국은 개인의 양심 영역에 개입하여 그 종교적

[10] 이 장은 협약 제 9 조에 대한 해설서, 협약 제 10 조에 대한 해설서, 협약 제 14 조와 제 12 의정서 제 1 조에 대한 해설서 및 제 1 의정서 제 1 조에 대한 해설서를 고려하고 이와 결합하여 읽어야 한다.

신념을 확인하거나 영적 사안에 관한 신념을 공개하도록 강제할 권한이 없다. 이러한 원칙은 무엇보다 특정한 직무를 수행하기 위해, 특히 선서할 때 개인이 그러한 행위를 강요당하는 경우에 더욱 그러하다(*ibid.*, § 38). *Dimitras and Others v. Greece*, 2010 사건 § 88 에서도, 형사절차에서 증인으로서 종교적 선서를 하지 않기 위해 청구인들이 자신의 종교적 신념을 밝히도록 요구한 것이 제 9 조 위반이라고 판단되었다. 재판소는 모든 증인이 신원 확인을 위해 진술 전에 다른 정보들과 함께 자신의 종교를 밝혀야 한다고 규정한 형사소송법 조항은 종교의 자유와 조화시키기 어렵다고 보았다(*ibid.*, § 88).

346. *Mockutė v. Lithuania*, 2018 사건 § 129 에서 재판소는 정신과 치료의 필요가 정신과 의사가 환자와 종교를 포함한 여러 사안을 논의하도록 요구할 수 있다는 점은 수용할 준비가 되어 있었다. 그러나 그러한 논의가 환자의 신념을 "교정"하기 위해 캐묻는 형태가 되어서는 안 되며, 그러한 신념이 환자 자신이나 타인에게 위험한 행위로 드러날 명백하고도 긴급한 위험이 없는 한 그러하다. 국가는 개인이 무엇을 믿을지를 규정하거나 그가 신념을 바꾸도록 강제하는 조처를 수 없으며, 국가의 판단재량의 범위가 종교적 신념의 성격에 따라 더 넓어지거나 좁아질 수도 없다.

347. *Jehovah's Witnesses v. Finland*, 2023 사건 §§ 80–99 에서 재판소는 청구인 종교단체의 방문 전도 활동 맥락에서, 그 단체의 종교의 자유와 방문 대상자(데이터 주체)의 사생활 비밀권 사이에서 적절한 균형에 도달하였는지 판단하여야 했다. 국내 차원에서 관할 당국은, 개인적·민감한 데이터(이름과 주소)가 수집·처리되는 이러한 활동에서 데이터 주체의 명확한 동의 또는 명시적 동의가 요구된다고 보았다. 재판소는 청구인 종교단체의 방문 전도라는, 신앙을 드러내고 전파하려는 종교 활동 맥락에서 동의 요건을 적용한 것이 그 단체의 제 9 조상 권리에 대한 제한을 구성한다고 인정하였다(§ 81). 동시에 재판소는 문제된 제한이 특히 최고행정법원이 해당 국내 법률을 EU 사법재판소의 해석과 일치하게 해석했음을 고려할 때 "법에 따른 것"이라고 보았다(§§ 84–88). 문제 된 조치는 또한 "타인의 권리와 자유"를 보호한다는 정당한 목적을 추구했으며(§ 89), "민주사회에서 필요한" 것에도 부합하였다. 이와 관련하여 재판소는, 동의 요건이 청구인 단체의 방문 전도 활동 맥락에서 개인적·민감한 데이터의 전달이나 공개를 방지하기 위한 적절하고 필요한 보호조치라는 점을 지적하면서, 청구인 단체가 그러한 요건이 종교의 자유의 본질을 침해한다고 입증하지 못했다고 평하였다(§ 95). 나아가 해당 요건은 모든 종교단체와 종교 활동에 동일하게 적용되었으며(§ 96), 청구인 단체에 대해 요청된 제재는 실제로 부과되지 않았다(§ 97).

2. 데이터 보호와 표현의 자유(협약 제 10 조)[11]

348. 일반적으로, 재판소가 협약 제 8 조에 의해 보장되는 개인데이터 보호권과 제 10 조상의 표현의 자유를 비교형량하여 조화시켜야 했던 여러 사건에서, 원칙적으로 그 결과는 청구가 제 8 조에 근거하든 제 10 조에 근거하든 달라지지 않아야 한다고 보았다. 재판소의 견해에 따르면, 두 권리는 동등하게 존중받을 가치가 있다(*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 163; *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, 2018, § 46).

349. 국가가 보관하고 있는 개인데이터가 포함된 특정 정보에 비정부기구가 접근하는 것을 당국이 거부한 것은 다음 여러 사건에서 제 10 조 위반이라고 판단되었다.

- *Centre for Democracy and the Rule of Law v. Ukraine*, 2020 (§§ 120–121): 중앙선거위원회가, 요청된 정보가 기밀이며 당사자의 동의 없이는 전부 공개할 수 없다는 이유로, 의회 선거에 입후보한 정당 지도자들의 이력서 사본을 NGO 에 제공하는 것을 거부한 사건
- *Magyar Helsinki Bizottság v. Hungary* [GC], 2016 (§§ 195–197, 200): 당국이 조사 수행 중인 NGO 에 국선변호인 명단과 각자의 선임 횟수 제공을 거부한 사건
- *Youth Initiative for Human Rights v. Serbia*, 2013 (§§ 24–26): 정보기관이 법원의 제공 명령에도 불구하고 NGO 에 정보를 제공하지 않은 사건

350. 인쇄 매체나 시청각 매체에서 개인데이터가 공개된 것과 관련하여, 재판소는 다음과 같은 여러 사건에서 제 10 조 위반이라고 판단하였다.

- *N. Š. v. Croatia*, 2020 (§§ 92–117): 청구인이 아동 양육권에 관한 행정절차 중 입수한 기밀로 여겨진 정보를 텔레비전에서 공개한 혐의로 유죄 판결을 받은 사건. 재판소는 아동의 취약성을 고려할 때 아동의 개인데이터 보호가 필수적이라고 판결하였다(*ibid.*, § 99). 다만, 국내 법원이 취한 과도하게 형식주의적 접근은 공개의 배경, 특히 해당 정보가 이미 공공 영역에 속해 있었다는 사실을 고려하지 않았으므로 제 10 조와 양립할 수 없다고 보았다(*ibid.*, §§ 115–116);
- *Gîrleanu v. Romania*, 2018 (§§ 68–100): 청구인이 언론 조사 과정에서 군사 기밀을 공개한 혐의로 행정벌금을 부과받은 사건

[11] 이 장은 협약 제 10 조에 대한 해설서를 고려하고 이와 결합하여 읽어야 한다(특히, pp. 26–47; 58–60 및 62–65 참조).

- *Couderc and Hachette Filipacchi Associés v. France* [GC], 2015 (§§ 94–153): 주간지 발행인과 출판사가 군주의 비밀 아들의 존재를 밝히는 기사와 사진을 게재한 것에 대해 유죄 판결을 받은 사건
- *Axel Springer AG v. Germany* [GC], 2012 (§§ 75–111): 잘 알려진 배우의 체포와 유죄 판결 보도를 금지한 사건
- *Dupuis and Others v. France*, 2007 (§§ 30–32, 39–49): 피고인들의 개인데이터를 포함한 진행 중인 사법수사 사건 기록에서 정보를 입수하여 책에서 사용·재생산한 혐의로 언론인들이 유죄 판결을 받은 사건

351. 반대로, 재판소는 다음과 같은 여러 사건에서 제 10 조 위반이 아니라고 판단하거나, 심리부적격이라고 선언하였다.

- *Hurbain v. Belgium* [GC], 2023 (§§ 167–257): 수년 전 발생한 치명적 교통사고 운전자의 실명을 언급한 기사의 온라인 전자판을 익명화하라는 민사 판결이 문제 된 사건
- *Biancardi v. Italy*, 2021 (§§ 67–71): 민간인을 대상으로 한 형사절차와 관련된 민감한 정보를 인터넷에 게재한 후, 당사자가 반대했음에도 불구하고 해당 정보를 쉽게 접근 가능하도록 유지한 신문 편집인에 대해 비식별 처리를 하지 않은 책임을 인정한 민사 판결이 문제 된 사건
- *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 (§§ 139–199): 개인 세금 데이터의 대량 공개를 금지한 사법 결정이 문제 된 사건
- *Bédat v. Switzerland* [GC], 2016 (§§ 44–82): 형사 수사의 비밀에 속하는 정보를 보도한 혐의로 언론인이 유죄 판결을 받은 사건
- *Mediengruppe Österreich GmbH v. Austria*, 2022 (§§ 44–73): 대통령 선거를 앞두고 특정 후보 캠프와 간접적으로 관련된 개인에 대해 "유죄 판결을 받은 네오나치"라는 설명과 함께 사진을 게재하지 말라는 법원 명령이 문제 된 사건. 유죄 판결 후 20 년이 지난 시점에 보도되었다.
- *Gafiuc v. Romania*, 2020 (§§ 85–90): 공산주의 체제 아래 루마니아 스포츠에 관한 연구라는 연구 주제와의 관련성이 평가되지 않은 채, 잘 알려진 스포츠 인사들의 개인데이터를 "원자료" 형태로 여러 기사에서 공개한 뒤, 언론인의 세쿠리타테(루마니아 비밀경찰) 기록 열람 권한이 취소된 사건

- *Giesbert and Others v. France*, 2017 (§§ 77-103): 형사절차 기록에서 가져온 문서를 공개재판에서 낭독되기 전에 신문사가 게재한 것에 대해 법원이 위법하다고 판단한 사건
- *Verlagsgruppe Droemer Knaur GmbH & Co. KG v. Germany*, 2017 (§§ 36-62): 출판사가 철저한 사전조사를 하지 않고 개인의 인격권을 심각하게 침해한 것에 대해 손해배상 책임을 명한 사건
- *Kurier Zeitungsverlag und Druckerei GmbH v. Austria*, 2012 (§§ 47-56): 성적 학대 피해 아동의 신원을 기사에서 공개한 것에 대해 배상 책임을 명한 사건. 재판소는 범죄 피해자의 취약성을 고려할 때 그들의 신원은 특별한 보호를 받아야 한다고 보았다.
- *MGN Limited v. the United Kingdom*, 2011 (§ 152): 언론에 유명인의 약물중독 치료 과정 세부 사항이 공개된 것이 유해하며 회복에 심각한 지장을 초래할 수 있다는 점이 고려된 사건
- *Editions Plon v. France*, 2004 (§§ 22-55): 사망한 국가원수와 관련된 의료 비밀에 속하는 정보를 담은 책의 배포를 최종적으로 금지한 사건
- *Mitov and Others v. Bulgaria* (dec.), 2023 (§§ 30-41): 최고행정법원장이 제정한 익명화 규칙과 특정 형사판결의 공개를 지연하는 법률에 따라, 탐사보도 기자들인 청구인들이 법원 데이터베이스에 있는 모든 스캔된 사건 자료를 자유롭게 열람하지 못한 사건
- *Ramadan v. France* (dec.), 2024 (§§ 28-46): 성폭행 혐의로 진행 중인 형사절차에서, 청구인이 자신의 책과 두 개의 다른 매체에서 피해자의 동의 없이 피해자의 신원을 공개한 사건. 피해자의 신원은 이미 제 3 자에 의해 언론에 공개된 상태였다.

352. 언론이나 방송매체에서 개인의 초상을 배포하거나, 그러한 개인데이터의 배포를 금지하는 법원 명령과 관련하여, 재판소가 제 10 조 위반이라고 판단한 사건으로는, 기자가 법원 심리를 허가 없이 녹음·방송한 혐의로 유죄 판결을 받은 사건(*Pinto Coelho v. Portugal (no. 2)*, 2016, §§ 31-56), 공익적 목적을 추구하던 네 명의 기자가, 민간 보험중개인과의 인터뷰를 몰래카메라로 촬영·방송한 혐의로 유죄 판결을 받은 사건(*Haldimann and Others v. Switzerland*, 2015, §§ 63-68), 정치인의 사진을 게재하지 말라는 금지명령이 문제 된 사건(*Krone Verlag GmbH & Co. KG v. Austria*, 2002, §§ 21-39), 형사절차 피의자의

사진을 신문에 게재하지 말라는 법원 명령이 문제 된 사건(*News Verlags GmbH & Co. KG v. Austria*, 2000, §§ 37-60) 등이 있다.

353. 다만, 이러한 이미지의 배포나 배포 금지 명령이 제 10 조를 위반하지 않은 것으로 판단된 사건으로는 감금과 고문을 당했던 사람의 사진이 이미 판매 중인 잡지에 게재된 것과 관련하여, 사진을 지우도록 한 법원 명령이 문제 된 사건(*Société de Conception de Presse and d'Édition v. France*, 2016, §§ 32-54), 살인 혐의로 재판을 받는 사람을 식별할 수 있는 초상을 게재하지 못하도록 한 결정이 문제 된 사건(*Axel Springer SE and RTL Television GmbH v. Germany*, 2017, §§ 43-59), 장기형 집행을 시작하기 위해 교도소로 압송되는 사람의 사진을 게재한 혐의로 두 신문사의 편집국장이 유죄 판결을 받은 사건(*Egeland and Hanseid v. Norway*, 2009, §§ 56-65)이 있다. 또한, *Vučina v. Croatia* (dec.) 2019 사건에 관하여 위 17 및 65 참조.

354. *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, 2018 사건 §§ 59-69, 77-78 에서, 공적 인물에 대한 비밀 감시의 일환으로 은닉된 카메라로 촬영된 여러 영상을 보도 목적으로 배포한 것이, 녹화가 공적 공간에서 이루어졌는지 사적 공간에서 이루어졌는지에 따라 제 10 조 위반이라고 본 경우와 위반이 아니라고 본 경우가 있었다.

355. 사적 개인이 당사자의 동의 없이 다른 사람을 몰래 촬영한 이미지를 인터넷에 게시한 것과 관련하여, 재판소는 *Khadija Ismayilova v. Azerbaijan*, 2019 사건 §§ 158-166 에서, 자 아파트에 설치된 은닉된 카메라로 정체불명의 개인들에 의해 촬영된 바 있는 언론인인 청구인을 피청구국이 보호하지 못했다고 판단하였다. 당국이 형사 수사 진행 상황을 알린다는 명목으로 보도 자료를 통해 청구인의 이름, 친구 및 동료의 주소 등 개인정보를 부당하게 공개한 것은 상황을 더욱 악화시켰으며, 언론 활동을 보호하는 환경의 정신에 반하는 것이었다(*ibid.*, § 165).

356. 내부고발자의 표현의 자유 보호와 국가안보에 영향을 미치는 기밀정보의 공개와 관련하여, 재판소는 청구인이 직무 수행 과정에서 정보기관의 개인데이터 수집과정에서 발견한 여러 불규칙 사항을 공개한 혐의로 유죄 판결을 받은 것에 대해 제 10 조 위반이라고 판단하였다(*Bucur and Toma v. Romania*, 2013, §§ 95-120). 또 다른 내부고발 사건에서, 한 공립병원의 부진료과장은 자신의 상급자가 안락사를 시행하고 있다는 의심을 보고한 후(이 의심은 후에 근거 없는 것으로 밝혀졌다) 해임되었다. 재판소는 제 10 조 위반이 아니라고 보았다. 청구인은 모든 정보를 담고 있는 종이 의무기록이 아니라, 환자의 건강에 관한 모든 정보를 담고 있지 않음을 알고 있던 전자 의무기록에 기초하여 의심을 제기하였다. 따라서

청구인이 선의로 행동했음에도 불구하고, 공개한 정보의 정확성과 신뢰성을 신중하게 확인하지 못한 것이다(*Gawlik v. Liechtensten*, 2021, §§ 74-78).

357. 언론인의 개인데이터 또는 그 소지 데이터가 출처의 신원을 밝히는 데 이용될 수 있는 경우의 보호 문제는 재판소가 여러 사건에서 심리하였다.

- *Sedletska v. Ukraine*, 2021 (§§ 59-60 및 64-73): 수사 당국이 16 개월 동안 특정 거리와 장소 인근에서 언론인의 휴대전화 위치·일시·통신기록 등 통신데이터를 수집·열람하도록 한 법원 허가가, "공익상 압도적 필요 요건"으로 정당화되지 않았고 절차적 보호조치가 결여되었다는 이유로 제 10 조 위반이라고 판단된 사건
- *Jecker v. Switzerland*, 2020 (§§ 37-43): 검찰이 마약 거래상 신원을 특정하기 위해 언론인에게 자신의 취재원 중 한 명의 신원을 공개하라는 명령을 내린 사건에서, 쟁점이 된 구체적 이익에 대한 비교형량이 이루어지지 않았으므로 제 10 조에 반한다고 본 사건
- *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, 2012 (§ 102): 독립적 기관의 사전 심사 없이 언론인들을 감시하고, 그들의 출처를 특정할 수 있는 문서 제출을 명한 것이 제 8 조와 제 10 조를 결합하여 위반한 것으로 판단된 사건. 사후 심사만으로는 충분하지 않은데, 언론 취재원의 비밀은 일단 파괴되면 회복될 수 없기 때문이다(*ibid.*, §§ 100-101)
- *Financial Times Ltd and Others v. the United Kingdom*, 2009 (§ 63): 재판소는 취재원의 행위가 공개명령을 내려야 하는지 여부를 결정하는 데 있어 결코 결정적일 수 없으며, 고려해야 할 여러 요소 중 하나(비록 중요한 요소이긴 하지만)에 불과하다고 명시한 사건
- *Weber and Saravia v. Germany* (dec.), 2006 (§§ 143-153): 통신 전략 감시를 허용하는 법률 규정으로 인해 언론인이 업무 과정에서 입수한 정보의 비밀을 보장할 수 없게 되었다는 표현의 자유 침해 주장에 대해, 재판소가 이를 명백히 근거 없다고 선언하며 심리부적격으로 본 사건
- *Ernst and Others v. Belgium*, 2003 (§§ 94-105): 언론인들의 출처를 특정하기 위해 언론사 사무실에 대한 대규모 압수수색이 제 10 조 위반이라고 판단된 사건(또한, 언론인의 자택 수색을 통한 취재원 특정이 문제 된 *Roemen and Schmit v. Luxembourg*, 2003, §§ 47-60, 진행 중인 유럽기관 조사와 관련해 비밀정보를 얻기 위해 유럽 공무원에게 뇌물을 제공했다는 의심을 받은 언론인의 자택·사무실 압수수색이 문제 된 *Tillack v. Belgium*, 2007, §§ 56-68, 언론 취재원의 신원을

특정할 수 있는 문서를 경찰이 압수한 *Sanoma Uitgevers B.V. v. the Netherlands* [GC], 2010, §§ 64-100, 언론인의 자택에 대한 긴급 수색과 취재원 정보가 담긴 저장장치 압수가 문제 된 *Nagla v. Latvia*, 2013, §§ 78-102, 로펌 사무실에서 컴퓨터 파일과 이메일이 대규모 압수된 *Sérvulo & Associados – Sociedade de Advogados, RL and Others v. Portugal*, 2015, §§ 101-120 및 군사 기밀과 관련된 맥락에서 직장 내 불합리한 관행을 폭로한 국가 공무원들을 보호하기 위한 언론인의 출처 보호가 문제 된 *Görmüş and Others v. Turkey*, 2016, §§ 32-77 참조)

- *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, (§§ 442-458): 대규모 통신 가로채기 과정에서 정보기관이 부수적으로 대량의 언론인 관련 기밀 자료에 접근할 수 있게 된 사건. 재판소는 협약 제 10 조 위반이라고 판단하였다.

3. 데이터 보호와 차별 금지(협약 제 14 조)

358. 남성에서 여성으로의 젠더 재지정 수술을 받은 청구인 두 명의 새로운 젠더 정체성을 피청구국이 법적으로 인정해야 할 의무가 있는지가 쟁점인 *Sheffield and Horsham v. the United Kingdom* [GC], 1998 사건 §§ 51-61, 76-77 에서 재판소는 제 8 조 단독으로 보아도 제 14 조와 결합하여 보아도 위반이 없다고 판결하였다. 재판소의 견해에 따르면, 청구인들이 개인데이터를 공개해야 할 상황이 그들의 사생활 존중권을 과도하게 침해할 정도로 빈번하게 발생한다고 볼 수는 없었다. 또한 피청구국이, 트랜스젠더의 젠더 지위에 관한 침해적 조사를 어느 정도 최소화하기 위해, 새로운 이름과 젠더가 기재된 운전면허증·여권 및 기타 유형의 공식 문서를 발급하도록 허용하고, 출생증명을 신원확인 수단으로 사용하는 것을 공식적으로 억제하려고 노력하였다고 평하였다(*ibid.*, § 59; *Cossey v. the United Kingdom*, 1990, §§ 36-42).

359. 재판소는 제 8 조 또는 제 9 조에 따른 개인데이터 보호와 밀접하게 관련된 쟁점을 심리한 몇 가지 사건에서, 제 14 조와 관련한 별도의 문제는 없다고 판단하였다(청구인의 신분증에 종교를 기재하도록 하는 것이 의무적이든 임의적이든 문제가 된 *Sinan Işık v. Turkey*, 2010, § 57, 수혈을 거부한 여호와의 증인 여러 명의 의료기록이 공개된 *Avilkina and Others v. Russia*, 2013, § 61, 개인의 젠더 재지정의 법적 인정과 관련된 *Christine Goodwin v. the United Kingdom* [GC], 2002, §§ 92-93, 108 및 *I. v. the United Kingdom* [GC], 2006, §§ 72-73, 88).

4. 데이터 보호와 평화적 재산향유권(제 1 의정서 제 1 조)

360. 재판소는 압수·수색의 맥락에서 개인데이터 보호와 평화적 재산향유권을 살펴보았다.

361. *Smirnov v. Russia*, 2007 사건 §§ 53–59 에서 재판소는 국내 당국이 공동체의 일반적 이익 요구와 청구인의 평화적 재산향유권 보호 요건 사이에서 “적절한 균형”에 도달하지 못하였다고 판결하였다. 따라서 변호사인 청구인의 자택에서 이루어진 수색과, 그 뒤에 청구인의 개인데이터가 들어 있는 하드디스크를 포함한 컴퓨터 본체를 압수한 조치로 인해 제 1 의정서 제 1 조 위반이 있었다. 실물 증거의 보관이 사법의 적정한 운영을 위해 필요할 수는 있었으나, 해당 컴퓨터 자체는 어떠한 범죄의 물건·도구·산물도 아니었다. 수사관이 하드디스크에 저장된 정보를 조사·출력하여 기록에 편철한 이상, 컴퓨터 본체를 계속 압수해 둘 이유는 없었다. 더욱이 해당 컴퓨터는 청구인의 업무 도구였을 뿐 아니라 의뢰인의 데이터도 보관되어 있었다.

362. *Kruglov and Others v. Russia*, 2020 사건 §§ 145–146 에서 변호사인 청구인들과 그 의뢰인의 자택 및 사무실에 대한 경찰 수색과, 직업상 비밀에 해당하는 개인 정보와 문서가 저장된 컴퓨터 및 하드디스크 압수는(그 자체가 범죄의 물건·도구·산물은 아니었음에도 불구하고) 제 1 의정서 제 1 조 위반이라고 판단되었다.

363. *Pendov v. Bulgaria*, 2020 사건 §§ 43–51 에서 재판소는 제 3 자에 대한 형사절차의 맥락에서 청구인의 컴퓨터 서버를 불필요하게 장기간 보관한 것이 제 1 의정서 제 1 조 위반에 해당한다고 판결하였다. 해당 서버는 형사 수사의 목적상 단 한 번도 조사되지 않았으며, 그 수사는 전적으로 제 3 자에게만 관련된 것으로, 필요한 정보는 복사가 가능했고, 서버는 청구인의 직업 활동에 필수적이었으며, 검찰의 부분적인 부작위 상태까지 고려할 때, 청구인의 서버를 7 개월 반 동안 보관한 것은 비례성을 상실한 것이었다(*ibid.*, § 51).

5. 데이터 보호와 이동의 자유(제 4 의정서 제 2 조)

364. 재판소는 당국이 보관한 개인데이터 때문에 개인 이동의 자유가 제한된 여러 사건을 살펴보았다. 재판소는 제 8 조에 따라 사건을 심리하였다.

365. 이와 관련하여 *Dalea v. France* (dec.), 2010 사건에서는, 경찰이 셍겐 정보시스템에 청구인이 그 정확성을 다투던 데이터를 보관한 결과, 청구인은 셍겐 지역 내에서 자유롭게 이동할 수 없게 되었다. 청구인은 데이터베이스에 포함된 개인데이터에 접근하거나 정정할 수 없었다. 재판소는 제 8 조가 그 자체로 외국인이 특정 국가에 입국하거나 거주할 권리를 보장하는 것은 아니라는 점을 거듭 확인하였다. 본 사안에서 프랑스 당국이 청구인을 셍겐 데이터베이스에 포함시킨 조치는 법에 따른 것이었고, 국가안보 보호라는 정당한 목적으로 추구하였다. 추구된 목적에 비례하고 민주사회에 필요하였다. 청구인은 제 4 의정서 제 2 조를 원용하지 않았다.

366. *Shimovolos v. Russia*, 2011 사건 §§ 64-71 에서, 청구인은 인권단체의 회원이라는 이유로 기차 및 항공 여행 정보가 "감시 데이터베이스"에 기록되었다. 해당 명단에 이름이 오른 사람이 기차표나 항공권을 구입할 때마다 교통부 소속 내무부는 자동으로 통보를 받았다. 그 결과 청구인이 EU-러시아 정상회의와 관련해 사마라로 가는 기차에 탑승하여 그 도시에서 열리는 시위에 참가하려 했을 때, 경찰관 세 명이 신분증을 확인하고 여행 목적을 물었다. 재판소는 공표되지 않았고 대중이 접근할 수 없었던 부처 명령에 따라 청구인의 이동 데이터를 수집·보관한 것은 제 8 조가 보장하는 권리에 부합하지 않는 방식으로 사생활에 제한을 가한 것으로 판단하였다. 또한 재판소는 제 4 의정서 제 2 조와 관련해서는 별도의 문제는 발생하지 않았다고 보았다(*ibid.*, § 73).

367. 테러리스트의 국제적 이동을 점검하는 중요성과 관련된 쟁점을 제기한 *Beghal v. the United Kingdom*, 2019 사건 §§ 89-109 에서 재판소는 제 8 조 위반이라고 판단하기에 앞서, 항구·공항·국제철도 터미널에서 승객을 정지·수색·심문할 수 있도록 경찰·출입국관리관·세관지정관에게 부여된 권한이 테러방지법에 근거하고 있었지만, 그 권한이 충분히 한정되지 않았고, 남용을 방지할 적절한 법적 보호조치도 없었다고 보았다. 특히, 해당 법률은 사전 승인 요건을 두지 않았으며, 테러와의 관련성에 대한 의심이 없는 경우에도 정지와 심문 권한이 행사될 수 있었다.

368. 회원국이 발급하는 여권과 여행문서의 보안요소 및 생체정보 기준에 관한 EU 규정을 국내법에 편입하면서(국가 당국에 아무런 재량을 남기지 않은 채) 도입된 여권법에 따라 여권을 신청할 때 지문을 채취하도록 한 의무와 그러한 지문을 전자칩에 저장하도록 한 조치가 문제 된 *Willems v. the Netherlands* (dec.), 2021 사건에서 재판소는 EU 법상 "동등한 보호의 추정"에 의거하여 명백히 근거 없다고 보아 청구를 각하하였다(*ibid.*, §§ 26-36).

B. 데이터 보호와 절차적 권리

협약 제 6 조

"1. 모든 사람은 민사의 권리와 의무 또는 자신을 상대로 제기된 형사소추의 결정을 위하여 법에 따라 설립된 독립적이고 공평한 법원에 의하여 합리적인 기간 내에 공정한 공개 심리를 받을 권리를 가진다. 판결은 공개적으로 선고되며, 다만 민주사회의 도덕, 공공질서 또는 국가안보를 위한 경우, 미성년자의 이익이나 당사자들의 사생활 보호를 위하여 필요한 경우 또는 공개가 정의의 이익을 해할 특별한 사정이 있다고 법원이 판단하는 경우 엄격히 필요한 한도 내에서 언론 또는 대중에 대하여 재판의 전부 또는 일부가 공개되지 아니할 수 있다.

2. 모든 형사피의자는 법에 따라 유죄가 입증될 때까지는 무죄로 추정된다.

3. 모든 형사피의자는 다음과 같은 최소한의 권리를 가진다.

(a) 그에 대한 기소의 성격 내지 이유를 그가 이해하는 언어로 신속하고 상세하게 통보받을 권리

(b) 자신의 변호 준비를 위하여 충분한 시간과 편의를 가질 권리

(c) 직접 또는 본인이 선택한 법적 조력을 통하여 자신을 변호하거나 법적 조력을 위한 충분한 지불수단이 없다면, 정의의 이익을 위하여 필요한 경우에는 무료로 법적 조력을 받을 권리

(d) 자기에게 불리한 증인을 심문하거나 심문받도록 할 권리 및 자기에게 불리한 증인과 동일한 조건으로 자신을 위한 증인을 출석시키고 심문받도록 할 권리

(e) 법정에서 사용되는 언어를 이해하지 못하거나 말할 수 없는 경우에는 무료로 통역의 조력을 받을 권리."

협약 제 13 조

"본 협약에 규정된 권리와 자유를 침해당한 모든 사람은 그 침해가 공무집행 중인 자에 의하여 자행된 것이라 할지라도 국가당국 앞에서의 실효적인 구제조치를 받아야 한다."

1. 공정한 재판을 받을 권리(협약 제 6 조)[12]

369. 사법절차 맥락에서 개인데이터가 자동처리되는 모든 개인은, 절차에서의 지위(청구인, 피고, 증인, 피고인 또는 제 3 자)와 무관하게 협약 제 6 조의 보장을 누려야 한다.

a. 일반적 보장(협약 제 6 조제 1 항)

370. 재판소는 여러 사건에서, 사법절차의 공정성을 보장하기 위해 마련된 다양한 일반적 보장 속에서 당사자나 제 3 자의 개인데이터를 보호할 필요성을 협약 제 6 조제 1 항의 관점에서 심사하였다. 여기에는 특히 무기대등과 당사자주의 절차의 권리, 공개 심리 및 판결의 공개 선고에 대한 권리, 증거조사, 합리적인 기간 내에 재판을 받을 권리, 사법적 결정에 이유를 제시해야 할 의무가 포함된다.

i. 민감한 정보 또는 비밀 정보가 포함된 절차에서의 무기대등과 당사자주의 원칙의 존중

371. *Eternit v. France* (dec.), 2012 사건 §§ 35-42 에서, 고용주는 근로자의 질병을 직업병으로 인정한 건강보험공단의 결정을 다투는 소송을 제기하였다. 사용자가 공단 소속 의학자문관이 작성한 의견서 사본을 제공받지 못했음에도 불구하고, 재판소는 해당 절차가 협약 제 6 조제 1 항을 위반한 것으로 보지 않았다. 근로자의 진료기록을 사용자에게 제공하지 않은 것은 근로자의 의료데이터 기밀을 보호할 필요에 의해 정당화되었으며, 법원은 이를 청구인 회사의 당사자주의 절차 보장권과 동등한 수준으로 고려하여 어느 쪽에서도 그 권리의 본질이 훼손되지 않도록 해야 했다. 법원에 독립적인 의학 전문가를 지정해 근로자의 진료기록을 검토하고, 그 기밀성을 존중하는 보고서를 작성하여 법원과 당사자들을 안내하도록 요청할 수 있었던 점에서 필요한 균형을 달성하였다(*ibid.*, § 37). 법원이 사용자의 요청이 있을 때마다 전문가 감정을 의뢰한 것은 아니고, 법원이 보유한 정보가 불충분하다고 판단한 경우에만 감정을 실시한 사실도 협약 제 6 조제 1 항에 따른 공정한 재판의 요건에 반하지 않았다(*ibid.*, §§ 35-39).

372. *Kennedy v. the United Kingdom*, 2010 사건 §§ 184-191 에서 당국이 개인의 통신을 불법적으로 가로챘다고 의심하는 사람이 제기한 불만을 심리하기 위해 설립된 독립기구인 조사권한재판소(IPT)에서, 무기대등 원칙과 당사자주의 원칙에 대한 제한이 협약 제 6 조제 1 항과 양립할 수 있는 것으로 보았다. 국가안보의 이익과 특정 수사기법을 비밀에

[12] 이 장은 협약 제 6 조에 대한 해설서 민사 영역(pp. 60-91) 및 형사 영역(pp. 32-100)을 고려하고 이와 결합하여 읽어야 한다.

부쳐야 할 필요성은 당사자주의 절차 보장권과 비교형량되어야 했다. 재판소의 견해에 따르면, 공개될 경우 추구된 목적 달성을 불가능하게 만들 수 있는 민감하고 기밀성 있는 자료를 비밀로 유지할 필요가 있었다(*ibid.*, §§ 186-187).

373. 일반화하자면, 재판소는 당사자주의 절차의 권리는 형사사건에서 검찰과 변호인 양 측 모두 상대방이 제출한 의견서와 증거(피고인에 대한 비디오 녹화물과 같이 피고인에게 불리한 증거 포함)에 대해서도 알 권리와 반박할 권리를 보장받아야 함을 의미한다고 강조하였다(*Murtazaliyeva v. Russia*, [GC], 2018, §§ 90-95).

ii. 사법적 결정의 이유 제시와 데이터 보호

374. *Surikov v. Ukraine*, 2017 사건 §§ 102-103 에서 재판소는 국내 법원이 제기된 여러 구체적이고 중요한 쟁점을 다루지 않았다는 이유로 협약 제 6 조제 1 항 위반이 있었다고 판단하였다. 청구인은 사용자가 자신의 정신 건강과 관련된 민감하고 오래된 정보를 자의적으로 수집·보관하였고, 이를 자신의 승진 신청 심사 과정에서 이용하였으며, 동료들과 법원에 불법적으로 공개하였다고 주장하였다. 재판소는 제 6 조가 법원에 판결 이유를 제시할 의무를 부과한다고 거듭 확인하였다. 그 의무가 모든 주장에 대해 상세히 답변할 것을 요구하는 것으로 이해될 수는 없지만, 국내 법원이 청구인이 제기한 구체적이고 중요하며 관련성 있는 쟁점을 무시한다면 공정성의 원칙이 훼손된다고 보았다(*ibid.*, § 101 및 이 조항에서 인용된 판례).

375. 청구인의 정확한 주소, 납세자 번호, 시골집 내부 사진을 담은 텔레비전 보도와 관련된 *Samoylova v. Russia*, 2021 사건 §§ 50-52 에서, 재판소는 국내 법원이 청구인이 제기한 쟁점 중 사건 결과에 결정적인 영향을 미칠 수 있는 주장에 대해 구체적이고 명시적인 답변을 제공하지 않았다고 보았으며, 이는 협약 제 6 조제 1 항이 보장하는 공정한 심리를 받을 권리를 무시한 것으로 판단했다.

376. *Kennedy v. the United Kingdom*, 2010 사건 §§ 185-191 에서, 당국이 통신 가로채기 조치가 수행되었는지 여부를 "긍정도 부정도 하지 않는다"는 방침은 협약 제 6 조 제 1 항과 양립할 수 없는 것으로 보지 않았다. 따라서, 당국이 통신을 불법적으로 가로챘다고 의심하는 사람들이 제기한 불만을 심리하기 위해 설립된 조사권한재판소가 청구인에게 단순히 그들의 청구에 유리한 결정이 내려지지 않았다고 통보하는 것만으로도 충분하였는데, 이는 해당 재판소에 제소한 결과 청구인이 실제 감청 여부를 통지받게 된다면 정부의 '긍정도 부정도 하지 않는다'는 방침이 우회될 수 있었기 때문이다(*ibid.*, § 189).

iii. 불법으로 또는 제 8 조를 위반하여 수집된 개인데이터를 증거로 사용

377. 국내법이나 협약 제 8 조의 요건에 반하는 방식으로 수집된 개인데이터를 사법절차에서 실물 증거로 사용하는 문제를 재판소가 살펴본 사건은 행정절차(공적 보험 제도 하에서 보험회사가 권한 범위 내에서 은밀히 수집한 정보를 피보험자와의 분쟁에서 사용한 *Vukota-Bojic v. Switzerland*, 2016, § 77), 민사절차(사용자가 직장에서의 인터넷 사용과 관련해 수집한 데이터를 해고 사유로 사용한 *Bărbulescu v. Romania* [GC], 2017, §§ 140-141, 제약영업사원의 회사 차량에서 기록된 GPS 주행 데이터를 해고 사유로 사용한 *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, §§ 130-140), 형사절차(은밀한 경찰 작전의 일환으로 대화를 가로채어 이를 유죄 판결의 근거로 사용한 *Bykov v. Russia* [GC], 2009, §§ 80-83)의 맥락이었다.

378. 재판소는 이러한 성격의 증거가 사법절차에서 인정·사용되더라도, 절차 전체가 공정하게 진행되었다면 절차가 불공정하다고 판단되는 결과로 자동으로 이어지지는 않는다고 판결하였다(*Bykov v. Russia* [GC], 2009, §§ 89-91; *Vukota-Bojic v. Switzerland*, 2016, §§ 91-100).

379. 재판소는 경찰의 정보원이 청구인의 수용실 안 대화를 녹음하기 위해 은밀한 장치를 사용하여 얻은 정보와 관련된 사건에서, 그러한 조치가 "법에 따른 것"이 아니었으므로 제 6 조제 1 항 위반이 있었다고 판단하였다(*Allan v. the United Kingdom*, 2002, §§ 45-53). 청구인의 자백은 자발적인 것이 아니었고, 경찰의 지시에 따라 제 3 자가 지속적으로 질문을 하여 대화를 유도한 결과였는데, 이는 사실상 심문과 동일한 상황이었음에도 형식적 경찰신문에 수반되는 보호조치가 전혀 없었다. 청구인과 제 3 자 사이에 특별한 관계가 없었고 직접적인 강제도 식별되지 않았으나, 청구인은 자백의 자발성을 침해하는 심리적 압박을 받았을 것이다. 이러한 상황에서 획득된 정보는 청구인의 의사에 반하여 얻어진 것으로 간주될 수 있으며, 이를 재판에서 사용한 것은 묵비권과 자기부죄금지 특권을 침해한 것이었다.

iv. 공개 심리 및 판결의 공개 선고와 데이터의 비밀성[13]

380. *P. and B. v. the United Kingdom*, 2001 사건 §§ 38-41, 46-49 에서는 아동 거주 지정 사건에서 공개 심리가 아니라 비공개 심리실에서 판결이 선고된 것이 협약 제 6 조제 1 항에 위반되지 않는다고 판단되었다. 재판소의 견해에 따르면, 아동 양육권 관련

[13] 또한, 협약 제 8 조의 관점에서 사법 절차 맥락에서 데이터 공개에 관한 본 해설서 상단 부분 참조.

절차는 해당 아동과 당사자들의 개인데이터를 보호하고 정의의 이익을 해치는 결과를 피하고 언론 및 일반인의 출석을 배제하는 것이 정당화될 수 있는 전형적인 사례이다(*ibid.*, § 38). 이해관계를 입증할 수 있는 사람이라면 누구든지 결정과 판결의 전문을 열람하거나 사본을 교부받을 수 있었고, 법원의 판결이 통상적으로 당사자의 이름을 밝히지 않고 공표되었다는 사실은 공개 선고의 부재를 보완하기에 충분하였다(*ibid.*, § 47).

381. *Kennedy v. the United Kingdom*, 2010 사건 § 188 에서, 재판소는 협약 제 6 조 제 1 항에 따라 국가안보가 심리에서 일반인의 배제를 정당화할 수 있음을 재확인하였다. 재판소는 통신의 불법 가로채기와 관련된 수사권재판소에 제기된 쟁점의 성격이 공개 심리의 부재를 정당화한다고 판결하였다.

382. *Vasil Vasilev v. Bulgaria*, 2021 사건에서 재판소는 청구인이 범죄사건에서 비밀감시 대상이 된 의뢰인과의 전화 통화가 감청·녹음·필사된 데 따른 손해배상을 청구하기 위해 제기한 절차에서 모든 심리에 일반인의 출입이 배제되고 판결이 공개 선고되지 않은 전면적인 공개 접근 부재와 관련하여 협약 제 6 조가 이중으로 위반되었다고 판단하였다. 모든 심리와 판결 선고에서 일반인을 배제한 것은 전적으로 기록에 포함된 기밀정보(청구인의 전화 통화에 대한 비밀 감청에서 나온 증거)의 존재만을 근거로 한 것이었다. 재판소의 견해에 따르면 사건의 대상이 된 기밀정보를 보호할 필요성으로는 전면적인 공개 접근 부재가 정당화될 수 없었다. 절차에서 제기된 쟁점의 성격은 국가 당국이 협약 제 8 조상의 권리를 침해했다는 주장에 대한 책임 여부였으며, 고도의 기술적 성격을 띠는 것이 아니었고 청구인은 공개 심리에 대한 권리를 포기하지도 않았다(*ibid.*, §§ 107–111). 국가 당국에 의한 기본권 침해 주장과 관련된 사건에서는 절차에 대한 공적 감시가 법치주의에 대한 신뢰를 유지하기 위해 필수적이다. 사건 기록에 기밀정보가 포함되어 있다는 사실만으로는 판결 전체를 일반인에게 공개하지 않을 근거가 될 수 없다. 만약 사건에 기밀정보가 포함된다면 민감한 정보의 비밀성을 유지하면서도 판결에 일정 정도의 공개 접근을 허용할 수 있는 기법이 존재한다(*ibid.*, §§ 116–118).

v. 데이터 보호와 관련된 사법절차의 기간

383. *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 사건 § 215 에서 재판소는 청구인 회사들이 개인의 과세 데이터를 대량으로 공개한 것이 국내법 및 유럽연합법과 양립 가능한지 여부와 관련된 절차가 두 단계의 사법심을 거쳐 6 년 6 개월 동안 진행된 것이 협약 제 6 조 제 1 항의 합리적인 기간 요건을 충족하지 못한다고 판결하였다. 유럽연합사법재판소에 제기된 선결문제 회부 요청과 관련된 절차는 국내 당국에 귀속되는 절차 기간을 산정할 때 고려될 수 없었다(*ibid.*, § 208).

384. 이에 반해, *Surikov v. Ukraine*, 2017 사건 §§ 104-106 에서, 재판소는 사용자가 직원의 정신 건강에 관한 민감하고 오래된 정보를 보관하고 그것을 승진 신청 심사에 사용한 것과 관련된 절차의 기간에 관한 청구를 명백히 근거 없다고 선언하였다. 재판소는 세 단계의 사법심을 거쳐 6 년 미만의 기간이 협약 제 6 조제 1 항의 합리적인 기간 요건과 관련하여 문제를 제기하지 않는다고 판단하였다(*ibid.*, § 101).

b. 구체적 보장(협약 제 6 조 제 2 항 및 제 3 항)

385. 형사 사안에서 개인데이터를 근거로 기소된 개인은 누구든지 구체적인 보장이 부여되어야 한다.

i. 데이터 보호와 무죄추정의 권리(협약 제 6 조제 2 항)

386. *Batiashvili v. Georgia*, 2019 사건 §§ 87-97 에서, 재판소는 당국이 한 개인의 체포 이전에 그의 전화 대화를 조작하여 텔레비전에서 방송한 상황에서 협약 제 6 조제 2 항이 적용된다고 판단하였다. 재판소의 견해에 따르면, 당국의 개입은 청구인이 법정에서 유죄가 입증되기 전에 이미 유죄로 인식되도록 하는 데 기여하였으므로 이는 협약 제 6 조제 2 항 위반에 해당하였다. 사건의 전 과정을 전체적으로 고려하면, 청구인의 상황은 수사 당국의 행위로 인해 실질적으로 영향을 받았다는 점이 드러났다(*ibid.*, § 94). 범죄를 신고하지 않았다는 혐의는 제 1 심 절차 진행 중에 철회되었으나, 녹취가 대중에게 공개된 지 약 4 개월 뒤에 공판에 회부된 공소장에는 여전히 문제 된 혐의가 기재되어 있었으며, 검찰 당국은 그 혐의의 근거가 된 증거가 허위라는 점을 충분히 인식하고 있었음에 틀림없었다(*ibid.*, § 95).

387. *Y.B. and Others v. Turkey*, 2004 사건 §§ 43-51 에서, 경찰청사에서 열린 기자회견에서 기자들에게 촬영된 피의자들과 관련하여 경찰이 언론에 한 발언은 협약 제 6 조제 2 항을 위반하는 것으로 판단되었다. 형사절차 진행 중에 피의자의 사진이 공개되는 것만으로는 무죄 추정권 침해에 해당하지는 않았다. 국내 당국은 최대한 신중하고 절제한다는 조건을 지킨다면 진행 중인 형사 수사에 관해 대중에게 알릴 권한이 있다. 그러나 형사절차에 관한 객관적 정보를 공개할 때는 그 정보에 어떠한 평가나 유죄에 대한 예단이 담겨서는 안 된다(*ibid.*, §§ 47-48). 이 사건에서 경찰 당국의 태도는 청구인들이 직면할 수 있는 혐의에 대한 사전 평가를 포함하고 언론은 청구인들을 쉽게 알아보게 하는 물리적 수단을 제공한 만큼 무죄 추정 원칙과 양립할 수 없는 것이었다(*ibid.*, § 50).

388. *Panteleyenko v. Ukraine,* 2006 사건 § 68-71 에서 청구인에 대한 형사절차를 종결한 법원 결정은 법관들이 기소된 범죄를 청구인의 범행으로 본다는 점을 분명히 드러내는 표현으로 되어 있었으므로, 재판소는 협약 제 6 조제 2 항 위반이라고 판단하였다. 무죄에

해당하지 않는 사유를 이유로 절차를 종결한 결정은, 직업상 공증인이었던 청구인과 관련된 개인데이터를 담은 증거에 기초한 것이었는데, 이는 관련 건물을 점유하는 사람에게 압수수색영장을 사전에 교부해야 한다는 법적 요건과 수사 중인 사건과 직접 관련이 없는 문서 및 물품의 압수를 금지하는 규정을 위반한 사무실 수색을 통해 확보된 것이었다(*ibid.*, § 70)[14].

ii. 데이터 보호와 방어권(협약 제 6 조제 3 항제 b 호)

389. *Rook v. Germany*, 2019 사건 § 69 에서 재판소는 전기통신 감시를 통해 확보된 청구인에 관한 대량의 데이터와 전자 파일을 검토하는 데 3 개월 반이 주어진 것이 변호인이 방어 준비를 할 수 있도록 하는 데 있어 협약 제 6 조제 3 항제 b 호의 관점에서 충분하다고 결정하였다. 형사절차의 복잡성을 고려할 때, 청구인의 변호인에게 수사 과정에서 수집된 4 만 5,000 건의 전화 통화와 3 만 4,000 건의 기타 데이터 세트 및 경찰이 청구인의 아파트 및 다른 장소에서 압수한 1,400 만 개의 전자 파일을 모두 읽고 청취할 기회를 제공할 필요는 없었다(*ibid.*, §§ 7–8, 67–71).

390. 일반화하자면, 재판소는 현대적 수사 기법이 실제로 방대한 양의 데이터를 산출할 수 있으며, 이를 형사절차에 통합하는 것이 절차에 불필요한 지연을 초래해서는 안 된다고 강조하였다. 청구인의 공개할 권리는 당국이 이미 관련성이 있다고 본 모든 자료에 대한 접근권과 혼동되어서는 안 되며, 후자는 일반적으로 당사자가 그 자료 전체를 이해할 수 있어야 한다는 것을 의미한다(*ibid.*, § 67). 법원 절차가 이미 시작된 뒤에 변호인이 기록의 완전한 사본을 확보했다고 해서 방어 준비를 할 충분한 시간이 없었다는 의미는 아니다. 협약 제 6 조제 3 항제 b 호는 일정 기간 이상 계속되는 재판의 준비가 첫 공판기일 이전에 모두 완료되어야 한다는 의미는 아니다(*ibid.*, § 72)[15].

391. *Sigurður Einarsson and Others v. Iceland*, 2019 사건 §§ 88–93 에서 재판소는 검찰이 수집하였으나 수사기록에 포함하지 않은 방대한 데이터에 변호인이 접근할 수 없었던 점과, 검찰이 수사와 관련된 정보를 식별하기 위해 해당 데이터를 전자적으로 분류하는 과정에서 변호인이 관여할 수 없었던 점과 관련하여 협약 제 6 조 제 1 항 및 제 3 항제 b 호 위반이 없다고 판단하였다. “수집된 데이터 전체”와 관련하여, 검찰은 그 방대한 데이터의

---

[14] 또한, 사법결정의 사유 제시에 관하여는 협약 제 6 조에 대한 해설서 – 공정한 재판을 받을 권리(형사 영역)(pp. 168–176) 참조.

[15] 또한, 피고인의 변호 준비에 필요한 편의와 관련하여 협약 제 6 조에 대한 해설서– 공정한 재판을 받을 권리(형사 영역) 참조.

내용이 무엇인지 알지 못했으므로 그 점에서 변호인보다 유리하지 않았다. "표시된" 데이터와 관련해서는, 원칙적으로 변호인에게 잠재적으로 면책적 증거를 탐색할 수 있는 기회를 보장하는 것이 적절하였을 것이다. 다만, 청구인들은 어느 단계에서도 그러한 취지의 법원 명령을 공식적으로 신청하지 않았고 찾고자 하는 증거의 유형을 특정하지도 않았다.

2. 실효적 구제를 받을 권리(협약 제 13 조)[16]

392. *Anne-Marie Anderson v. Sweden*, 1997 사건 §§ 41-42 에서, 재판소는 의료 당국이 사회복지 당국에 개인적이고 비밀스러운 의료데이터를 전달하기 전에 환자가 그 조치를 다툴 가능성이 없었던 것과 관련하여, 의료기록 공개에 관한 사안에서 협약 제 8 조와 결합한 협약 제 13 조 위반이 없다고 판단하였다. 그 밖에도, 해당 조치는 청구인에게 통지되었고, 문제 된 정보는 공개되지 않았으며 정신과 진료기록에 적용되는 것과 동일한 수준의 비밀보호가 유지된 만큼 조치의 성격은 제한적이었다.

393. *Mik and Jovanović v. Serbia* (dec.) 사건에서 청구인들은 출생 직후 사망했다고 주장되었으나 청구인들이 시신을 본 적 없는 영아 아들들의 행방에 관해 국가가 신뢰할 만한 정보를 제공하지 않는 상황이 계속되는 것과 관련하여, 협약 제 8 조 단독으로도 제 13 조와 결합하여서도 위반이라고 주장하였고, 재판소는 청구인들 외 여러 사람이 마주한 상황과 관련하여 최근 제정된 입법으로 제도적 장치(DNA 데이터베이스 포함)를 마련하였다고 밝혔다. 특히 새로운 법적 체계는 국립 산부인과 병원에서 실종된 것으로 의심되는 신생아들의 실제 상태를 밝혀내고 부모를 구제하기 위한 사법적 절차와 사법 외 절차 모두를 규정하였다. 또한 판사들에 대한 광범위한 교육, 사법 외 절차의 맥락에서 광범위한 조사·데이터 수집·보고 권한을 가진 위원회 위원(등록된 부모 단체 대표들이 그 다수를 차지)의 임명 등, 해당 체계를 실행할 중요한 조치가 마련되었다. 재판소는 청구인들 스스로가 새로운 제도적 장치를 이용하기로 선택하였다고 하면서, 협약 제 37 조제 1 항제 c 호의 의미에서 청구 사건의 심사를 계속하는 것은 더는 정당화되지 않는다고 결론지었다.

394. *Panteleyenko v. Ukraine*, 2006 사건 §§ 82-84 에서 재판소는 청구인의 정신 건강에 관한 비밀 정보가 공개 심리에서 드러난 것과 관련하여 청구인이 이에 대해 문제를 제기할 수 있는 실효적 구제수단이 부재했다는 점에서 협약 제 8 조와 결합하여 읽은 제 13 조 위반이라고 판단하였다. 재판소의 견해에 따르면, 기존의 법적 구제수단은 비밀 정신과 데이터가 법원 사건기록에서 공개되는 것을 중단시키지도 못했고 청구인의 사생활을 제한하여 발생한

[16] 이 장은 협약 제 13 조에 대한 해설서를 고려하고 이와 결합하여 읽어야 한다(실효적 구제를 받을 권리, 특히 pp. 49-51 참조).

손해에 대해 배상을 인정하지도 못했으므로 실효성이 없었다. 비공개 심리가 이루어졌더라면 정보가 일반 대중에게 공개되는 것은 막을 수 있었겠지만, 당사자들이 알게 되거나 사건기록에 포함되는 것을 막지는 못했을 것이다.

395. 청구인들의 자녀 입양과 관련된 정보를 공개한 사법결정이 인터넷에 게시된 것과 관련하여, 재판소는 *X and Others v. Russia*, 2020 사건 §§ 73-79 에서 사법제도의 오작동으로 인해 발생한 비재산적 손해에 대한 배상을 제공하는 사법적 구제수단이 부재했으므로 협약 제 8 조와 결합하여 읽은 제 13 조 위반이 있었다고 판결하였다.

396. 강간 사건과 관련하여 조사를 받은 뒤 경찰 등록부에 "범죄자"로 기재되고 그 후 공소장이 제출되지 않았음에도 불구하고 해당 기재가 계속 보존된 사안에서, 재판소는 청구인이 문제 된 조치에 대해 불복할 수 있는 구제수단을 당시 보유하지 못했다는 점을 지적하면서, 협약 제 8 조와 결합하여 읽은 제 13 조 위반이 있었다고 판단하였다(*Dimitrov-Kazakov v. Bulgaria*, 2011, §§ 37-39).

397. *Nada v. Switzerland* [GC], 2012 사건 §§ 209-214 에서, 청구인이 탈레반 규정 부속 명단에서 자신의 이름 삭제를 요청할 수 있는 실효적 구제수단이 부재한 것은 협약 제 8 조와 결합하여 읽은 제 13 조 위반에 해당하였다. 청구인은 국내 법원에 청구할 수 있었지만 법원은 그 청구를 본안에서 심리하지 않았다.

398. 직업적 맥락에서의 개인데이터 사용과 관련하여, 재판소는 동성애자의 사생활에 대한 침해적 조사가 이루어지고 그 결과 군에서 전역 조치가 내려진 *Smith and Grady v. the United Kingdom*, 1999 사건 §§ 136-139 에서 청구인들의 사생활 침해에 관한 실효적 구제수단이 부재했다는 이유로 협약 제 8 조와 결합하여 읽은 제 13 조 위반이라고 판단하였다.

399. *Karabeyog˘lu v. Turkey*, 2016 사건 §§ 128-132 에서, 형사 수사 도중 전화 도청으로 확보된 데이터를 징계절차에서 사용한 것에 대해 법원의 심사를 구할 수 있는 국내 구제수단이 부재하였으므로, 재판소는 협약 제 8 조에 비추어 읽은 제 13 조 위반이라고 판단하였다.

400. *Peck v. the United Kingdom*, 2003 사건 §§ 101-114 에서 재판소는 청구인이 공공장소에서 자살을 시도하는 장면이 담긴 CCTV 영상이 언론에 공개된 것에 대해 불복할 수 있는 실효적 구제수단을 보유하지 못했다고 결정하였다. 사법심사의 가능성과 관련하여, 국내 법원에서 유일한 쟁점은 공공장소에서 CCTV 카메라로 촬영된 영상과 관련된 정책이 "불합리하다"고 할 수 있는지 여부였으므로, 청구인의 권리 제한이 긴급한 사회적 필요에 부응했는지, 비례적인지 여부에 관한 심사는 사실상 배제되었다(*ibid.*, §§ 106-107). 언론위원회와 관련해서는, 손해배상 판결 권한이 없었으므로 실효적 구제수단을 제공할 수 없었다(*ibid.*, §§ 108-109). 비밀유지 의무 위반 소송과 관련해서는, 해당 시점에 법원이

영상에 “비밀의 본질적 성격”이 있었다거나 정보가 “비밀유지 의무를 수반하는 상황에서 전달되었다”고 인정할 가능성은 낮았다(*ibid.*, § 111).

401. 비밀감시와 관련하여, 이러한 조치의 비밀성은 특히 감시가 진행 중일 때는 당사자가 구제수단을 행사하는 것을 어렵게 하거나 사실상 불가능하게 한다. 협약 제 13 조의 목적상 “실효적 구제수단”이란 모든 감시제도에 내재하는 제한된 구제 범위를 고려할 때 가능한 효과적인 구제수단을 의미해야 한다(*Klass and Others v. Germany*, 1978, §§ 68-69). 조치가 비밀로 유지된다면, 객관적인 감독 장치만으로도 충분할 수 있다. 조치가 공개된 경우에만, 합리적인 기간 내에 당해 개인이 이용할 수 있는 법적 구제수단이 제공되어야 한다(*Rotaru v. Romania* [GC], 2000, § 69).

402. 표적화된 비밀감시 조치와 관련하여, 개별 사건에서 남용이 매우 쉽게 이루어질 수 있고 민주사회 전체에 해로운 결과를 초래할 수 있으므로, 감독 통제를 판사에게 맡기는 것이 원칙적으로 바람직하며, 사법적 통제가 독립성·공정성·적절한 절차에 대한 최고의 보장책을 제공한다. 감시 조치가 해제된 후에는 제한의 목적을 해치지 않고 통지가 가능해지는 즉시 당사자에게 정보가 제공되어야 한다. 자신의 사생활권 행사를 제한한 절차에 대한 심사를 당사자가 받을 수 있도록, 원칙적으로 그 개인에게 다툴 수 있는 결정에 관한 최소한의 정보(결정이 내려진 날짜와 결정을 내린 법원 명칭 등)가 제공되어야 한다(*Roman Zakharov v. Russia* [GC], 2015, §§ 233, 287, 294; *İrfan Güzel v. Turkey*, 2017, §§ 96, 98-99).

403. *Klass and Others v. Germany*, 1978 사건 §§ 65-72 에서 “G10”법은 국가를 “임박한 위험”으로부터 방어하기 위하여 당국이 우편물과 소포를 개봉·검사하고, 전보를 열람하며, 전화 통화를 청취·녹음할 수 있게 하였다. 재판소는 독일법상 마련된 구제수단의 총합이 해당 사건의 구체적 상황에서 사생활 및 통신의 존중과 관련된 협약 제 8 조에 비추어 협약 제 13 조의 요건을 충족한다고 판결하였다. 비록 같은 법에 따르면 제한 조치의 명령 및 집행은 법원에서 다툴 수 없었지만, 자신이 감시 대상이라고 믿는 개인들은 여러 다른 구제수단을 이용할 수 있었다. 1970 년 연방헌법재판소 판결에 따르면, 권한 있는 당국은 감시 조치가 중단되면 지체 없이, 통지가 제한의 목적을 해치지 않는 한도 내에서, 당사자에게 통지해야 했다. 이러한 통지가 이루어진 시점부터 개인들은 법원에서 여러 가지 법적 구제수단을 이용할 수 있었다. 행정법원에 확인소송을 제기하여 G10 법이 자기 사건에 적법하게 적용되었는지, 명령받은 감시 조치가 법에 합치하는지 심사를 받을 수 있었고, 손해를 입은 경우 민사법원에 손해배상청구를 제기할 수 있었으며, 문서의 파기 또는 경우에 따라 반환을 구하는 소송을 제기할 수도 있었다. 마지막으로, 이러한 구제수단이 모두 성공하지 못할 경우, 연방헌법재판소에 기본법 위반 여부에 관한 판단을 청구할 수 있었다. 또한, 유사한 취지의 판례로, 국가안보상 중요 직위에 지원한 후보자들에 대한 비밀 심사 제도와 관련된 *Leander*

v. Sweden, 1987 (§§ 78-84), 정보기관이 전화 통화를 가로채기·녹음하고 개인데이터를 보관한 것과 관련된 *Amann v. Switzerland* [GC], 2000 (§§ 89-90) 참조.

404. 피고인이 자신의 전화 도청의 적법성에 대해 제기한 의문에 당국이 응답하지 않은 점을 고려하여, 재판소는 *İrfan Güzel v. Turkey*, 2017 사건 §§ 100-109 에서 협약 제 8 조와 결합하여 읽은 제 13 조 위반이라고 판단하였다.

405. *Allan v. the United Kingdom*, 2002 사건 § 55 에서, 재판소는 청구인의 수용실에서 대화를 녹음하기 위해 사용된 비밀장치의 사용과 경찰에 의한 그 이용을 규율하는 법제도가 해당 시점에 존재하지 않았다는 이유로, 협약 제 8 조와 결합하여 읽은 제 13 조 위반이라고 판단하였다.

406. 국가안보 보호를 위한 특별 감시수단 사용 요청에 직접 관여한 내무장관에게만 비밀감시 제도에 대한 전반적 통제를 맡기고 독립적 기관에는 맡기지 않은 사안에서, 재판소는 실효적 구제수단이 부재했다는 이유로 협약 제 8 조에 비추어 제 13 조 위반이라고 판단하였다(*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2007, §§ 98-103).

407. 개인의 사생활에 관한 데이터의 보관이나 그 정보의 진실성에 대해 국가 기관을 상대로 다툴 수 있는 구제수단이 부재했다는 점을 고려하여, 재판소는 *Rotaru v. Romania* [GC], 2000 사건 §§ 68-73 에서 협약 제 8 조와 결합하여 읽은 제 13 조 위반이라고 판단하였다. 재판소는 *Segerstedt-Wiberg and Others v. Sweden*, 2006 사건 §§ 116-122 에서도, 청구인들에 관한 보안경찰 기록을 전체적으로 열람하고, 보안경찰이 보관한 기록의 파기 및 그 기록에 포함된 개인데이터의 삭제나 정정을 모색할 수 있는 청구인들의 구제수단이 부재한 경우에 대해 동일한 결론에 도달하였다.

3. 신체의 자유와 안전에 대한 권리(협약 제 5 조)

408. 청구인의 최초의 미결구금 당시 협약 제 5 조제 1 항제 c 호의 목적상 테러 조직 가입이라는 죄를 지었다고 의심할 만한 근거를 정당화하기 위해 제출된 유일한 증거가 청구인이 암호화된 바이록(ByLock) 메신저 시스템을 사용했다는 판단뿐이었던 *Akgün v. Turkey*, 2021 사건 §§ 178-181 에서 재판소는 협약 동조항 위반이라고 판단하였다. 청구인의 범죄 혐의는 조직범죄와 관련된 것이었다. 특정 범죄조직의 내부 통신을 위한 목적으로 특별히 설계되어 해당 조직만이 독점적으로 사용한 암호화 메신저 서비스를 개인이 이용했다는 전자 증거는 조직범죄 대응에서 중요한 수단이 될 수 있다. 따라서 그러한 증거는 개인이 해당 조직에 속한다는 강력한 정황을 제공할 수 있으므로, 피의자는 절차 초기에

그러한 증거를 근거로 구금될 수 있다. 그러나 그러한 증거가 개인에 대한 혐의의 유일하거나 배타적 근거를 이루는 경우, 국내 법원이 그 증거의 잠재적 증거 가치를 국내법에 따라 신중히 심사하기 전에 문제 된 자료에 관한 충분한 정보를 확보해야 한다. 이 사건에서 정부는 청구인이 미결구금에 처한 시점에 치안법원이 보유한 증거가 협약 제 5 조제 1 항제 c 호에 따른 “합리적 의심”의 기준(청구인의 범행 사실을 객관적 관찰자에게 납득시킬 수 있는 기준)을 충족하였다고 증명하지 못하였다. 재판소의 견해에 따르면, 청구인이 바이록 메신저를 사용했다는 결론에 도달한 문서는 추정된 활동의 날짜나 빈도를 특정하지 않았고 추가적인 관련 세부 사항도 포함하지 않았기 때문에 그 자체로 청구인의 불법 활동을 특정하거나 제시하지 못하였다. 나아가 이 문서도 미결구금 명령도 청구인의 추정된 활동이 테러 조직 가입을 시사한다는 점을 설명하지 못하였다.

IV. 데이터 보호의 현대적 난제

A. 기술 발전, 알고리즘 및 인공지능[17]

409. 범죄 예방 목적으로 당국이 범죄 혐의자나 유죄 확정자의 지문, 생물학적 검체, DNA 프로필을 채취·보관하는 사건과 관련하여, 재판소는 현대 과학 기법의 사용이 어떠한 대가를 치르더라도, 그러한 기법의 광범위한 사용으로부터 얻을 수 있는 잠재적 이익을 사생활의 중요한 이익과 신중하게 비교형량하지 않은 채 허용될 수는 없다고 명확히 밝혔다(*S. and Marper v. the United Kingdom* [GC], 2008, § 112; *Podchasov v. Russia*, 2024, § 62). 새로운 기술의 발전에서 선구자적 역할을 주장하는 국가는 이러한 균형을 적절히 달성할 특별한 책임을 진다(*S. and Marper v. the United Kingdom* [GC], 2008, § 112). 유전학과 정보기술 분야의 급속한 발전을 고려한다면, 향후 유전정보와 밀접하게 엮인 사생활적 이해관계가 새로운 방식이나 지금으로서는 정밀하게 예측할 수 없는 방식으로 부정적인 영향을 받을 가능성을 배제할 수 없다(*ibid.*, § 71).

410. 재판소의 견해에 따르면, 개인의 사진에 얼굴 인식과 얼굴 매핑 기법 등을 적용할 수 있는 점점 더 정교한 기술이 빠르게 발전함에 따라, 사진을 촬영하고 그 결과 데이터의 보관 및 잠재적 유포 문제가 발생한다. 국내 법원은 해당 당사자의 사생활을 제한할 필요성을 평가할 때 이러한 여러 요소를 고려해야 한다(*Gaughran v. the United Kingdom*, 2020, § 70). 이 사건에서(*ibid.*, §§ 96-98), 재판소는 현대 기술이 더 복잡해졌다는 점을 강조하면서, 경미한 범죄 이후 청구인의 사진을 당국이 촬영하고, 법정 기간이 만료되어 유죄판결이 기록에서 말소된 뒤에도 계속 보관한 사안에서, 국내 법원이 청구인의 사생활 존중권을 제한할 필요성을 심사할 때 이 측면을 충분히 고려하지 않았다고 평하였다.

411. *Breyer v. Germany*, 2020 사건 § 88 에서 재판소는 조직범죄 및 테러 대응 맥락에서 현대적 전기통신 수단과 의사소통 행태가 변하면서 수사 수단도 이에 적응해야 한다는 점을 인정하였다. 재판소의 견해에 따르면, 이동통신사업자에게 가입자 정보를 보관하고 당국의 요청 시 제공하게 하는 의무는 일반적으로 의사소통 행태 및 전기통신 수단의 변화에 대한 적절한 대응이다. 반면 *Podchasov v. Russia*, 2024 사건 §§ 70-79 에서, 국내법은 인터넷 통신서비스 제공업자가 모든 인터넷 통신의 내용은 6 개월간, 통신사실확인자료는 1 년간 보관·저장하게 하였고, 수사당국이나 보안기관이 요청하면 저장된 데이터(암호화된 경우

[17] 이 장은 본 해설서 중 범죄 대응 목적의 개인데이터 저장 및 비밀 감시를 통한 당국의 데이터 수집 부분과 함께 읽어야 한다.

해독용 정보 포함)에 대한 접근권을 부여하도록 규정하였으며, 재판소는 이러한 보관 의무가 극도로 광범위하다는 점에 주목하면서, 그러한 제한이 예외적으로 광범위하고 심각하다고 보았다. 재판소는 또한 국내법상 수사당국이나 보안기관이 특정인의 통신에 접근하기 전에 해당 통신서비스 제공업자에게 사전 법원 영장 제시할 필요가 없었다고 평하였다. 실제로 통신서비스 제공업자는 당국이 저장된 데이터에 직접 접근할 수 있도록 장비를 설치해야 할 의무가 있었다. 이러한 제도에서는 무엇보다도 자의적 권한 행사와 남용에 대한 안전장치가 필요하지만, 국내법은 그러한 안전장치를 규정하지 않았다. 통신 해독에 관한 법정 요건과 관련하여, 그러한 조치는 특정 개인에게 한정되지 않고 모든 이용자의 암호화를 약화시켜, 정당한 이익에 아무런 위협을 가하지 않는 사람들도 포함된 모든 사람에게 무차별적으로 영향을 미칠 수 있는 것이므로, 비례적인 조치라고 간주할 수 없었다(§§ 77-79).

412. 통신의 대규모 감시에 관한 *Szabó and Vissy v. Hungary*, 2016 사건 § 68 에서 재판소는 오늘날 테러리즘의 형태로부터 임박한 공격을 예방하기 위해 정부가 대규모 통신 감시를 포함한 최첨단 기술에 의존하는 것이 자연스러운 귀결이라는 점을 인정하였다. 재판소는 이 사건에서 당국은 새로운 기술로 당국이 당초 작전의 목표가 아니었던 사람들까지 포함된 대량의 데이터를 손쉽게 가로챌 수 있었기 때문에, 대규모 감시를 허용한 입법이 남용 방지에 필요한 안전장치를 마련하지 않았다고 판단하였다. 또한 이러한 조치는 어떠한 통제도 없이 행정부가 명령할 수 있었고, 엄격히 필요한지 평가도 하지 않았으며, 실효적인 사법적 또는 기타 구제수단도 부재하였다(*ibid.*, §§ 73-89).

413. *Roman Zakharov v. Russia* [GC], 2015 사건 §§ 302-305 에서 재판소는 비밀감시 제도라면 본질적으로 남용의 위험이 따르지만, 특히 비밀정보기관과 경찰이 기술적 수단을 통해 모든 이동통신에 직접 접근할 수 있는 구조에서는 그 위험이 매우 크다고 판결하였다. 재판소는 통신의 일반적 가로채기를 허용한 러시아 법제가 자의적 권한 행사와 남용의 위험을 방지하기 위한 적절하고 실효적인 보장을 제공하지 못했다고 판단하면서, 협약 제 8 조 위반을 인정하였다.

414. 청구인의 최초 미결구금 당시 협약 제 5 조제 1 항제 c 호의 목적상 범죄 혐의를 정당화하기 위해 제출된 유일한 증거는 청구인이 암호화 메신저인 바이록을 사용했다는 점뿐이었던 *Akgün v. Turkey*, 2021 사건 §§ 178-181 에서 재판소는, 증거를 수집하는 절차와 기술이 본질적으로 복잡하여 국내 법원이 그 진정성·정확성·무결성을 평가하는 능력을 약화시킬 수 있기 때문에, 그러한 증거를 의심의 유일한 근거로 삼는 것은 여러 민감한 문제를 야기할 수 있다고 강조하였다(373 참조).

415. *Centrum för rättvisa v. Sweden* [GC], 2021 사건 § 261 및 *Big Brother Watch and Others v. the United Kingdom* [GC], 2021 사건 §§ 322-323 에서 재판소는 국제 행위자들의 네트워크가 인터넷을 이용해 의사소통을 하고, 탐지를 회피할 수 있는 정교한 기술이 존재하며, 현재 국가들이 직면하고 있는 위협이 급증하고 있다는 점을 고려할 때, 대규모 감시 제도의 사용이 그 자체로 협약 제 8 조에 위반되는 것은 아니라고 명시적으로 인정하였다. 그러나 재판소는 현대 통신기술이 끊임없이 발전하고 있다는 점을 고려할 때, 대규모 감시 권한의 남용 위험과 이러한 조치에 내재하는 정당한 비밀 유지 필요성 때문에, 표적 감시 제도에 관한 기존 접근 방식을 대량 감시 제도의 특수성을 반영하도록 조정할 필요가 있다고 강조하였다. 특히 대규모 감시 절차는 "종단 간 보호조치"의 적용을 받아야 하는데, 이는 국내 차원에서 절차의 각 단계별 조치의 필요성과 비례성이 심사되어야 하고, 대규모 감시는 그 목적과 범위가 정해지는 초기 단계에서 독립적인 인가를 받아야 하며, 나아가 그 집행은 감독과 독립적인 사후 심사의 대상이 되어야 한다는 의미이다.

416. *Glukhin v. Russia*, 2023 사건에서 재판소는 처음으로 경찰의 안면인식기술 사용 문제를 심사하였다. 이 기술은 첫째, 공개 텔레그램 채널에 게시된 사진과 영상을 통해 청구인을 특정하는 데 사용되었고, 둘째, 청구인이 도시 지하철로 이동하는 동안 추적·체포하는 데 사용되었다. 재판소는 이러한 조치의 침해성이 매우 높다고 지적하면서, "민주사회에서 필요한" 것으로 보려면 정당한 근거를 갖추어야 하고, 특히 실시간 안면인식기술을 사용하려면 가장 철저히 근거를 갖추어 정당화되지 않으면 안 된다고 강조하였다(*ibid.*, § 86). 이와 관련하여, 재판소는 청구인이 사전에 통보하지 않고 1 인 시위를 했다는 경미한 범죄로 기소되었을 뿐임을 지적하였다. 시위 과정에서 교통 방해, 재산 손괴, 폭력 행위와 같은 비난받을 행위를 했다고 기소된 적도 없었다. 또한 청구인의 행위가 공공질서나 교통 안전에 위험을 초래했다는 주장도 제기되지 않았다. 이러한 사정에서, 재판소는 청구인을 특정하기 위해 안면인식기술을 사용하고, 추적·체포하기 위해 실시간 안면인식기술까지 사용한 것은 "강력한 사회적 필요"에 부합하지 않았으므로 "민주사회에서 필요한" 것으로 간주할 수 없다고 보았다(*ibid.*, §§ 88-90).

B. 인터넷과 검색 엔진

417. 인터넷 사이트는 무엇보다 정보의 저장과 전달 능력 측면에서 인쇄매체와 뚜렷이 구별되는 정보·소통 수단이다(*Węgrzynowski and Smolczewski v. Poland*, 2013, § 58; *M.L. and W.W. v. Germany*, 2018, § 91; *Hurbain v. Belgium* [GC], 2023, § 236). 접근성이 뛰어나고 방대한 양의 정보를 저장·전달할 수 있는 특성을 고려할 때, 인터넷은 대중의 뉴스

접근을 확대하고 일반적인 정보의 전파를 촉진하는 중요한 역할을 한다(*Times Newspapers Ltd v. the United Kingdom (nos. 1 및 2),* 2009, § 27).

418. 인터넷상의 콘텐츠와 의사소통이 인권과 자유 및 특히 사생활 존중권의 행사와 향유에 미치는 위험은, 무엇보다 검색엔진의 중요한 역할을 고려할 때, 언론이 제기하는 위험보다 확실히 더 크다(*Hurbain v. Belgium* [GC], 2023, § 236; *M.L. and W.W. v. Germany*, 2018, § 91 및 이 조항에서 관련 판례 다수 참고).

419. 언론사가 보유한 정보(개인데이터 포함)는 인터넷 이용자들이 검색엔진으로 손쉽게 찾아낼 수 있다. 이러한 정보 전파의 증폭 효과와 정보 공개 활동의 성격 때문에, 검색엔진이 정보의 대상이 되는 개인에게 부담하는 의무는 최초로 그 정보를 게시한 주체의 의무와는 달라질 수 있다(*Hurbain v. Belgium* [GC], 2023, § 207; *M.L. and W.W. v. Germany*, 2018, § 97). 검색엔진 운영자의 활동과 의무는 뉴스 발행자의 활동과 의무와 구별되므로, 이 맥락에서 자신의 개인데이터를 보호하려는 정보주체는 검색엔진에 대한 권리를 행사하기 위해 최초로 정보를 게시했던 뉴스 웹사이트에도 별도로 연락할 의무는 없는데, 이는 두 가지가 서로 다른 형태의 처리 행위로서 각각 정당성의 근거가 다르고 개인의 권리와 이익에 미치는 영향도 다르기 때문이다. 마찬가지로, 미리 검색 엔진에 삭제 요청을 해야만 뉴스 웹사이트 발행자를 상대로 한 소송을 제기할 수 있는 것도 아니다(*Hurbain v. Belgium* [GC], 2023, § 208). 또한, "잊힐 권리"에 관한 더 자세한 내용은 본 해설서 **오류! 참조 원본을 찾을 수 없습니다.~오류! 참조 원본을 찾을 수 없습니다.** 참조.

420. 재판소의 견해에 따르면, 온라인 기사 보관소는 뉴스와 정보를 보존하고 가용하게 한다(*Times Newspapers Ltd v. the United Kingdom (nos. 1 및 2),* 2009, § 45). 이러한 보관소는 특히 대중이 손쉽게 접근할 수 있고 일반적으로 무료라는 점에서, 교육과 역사 연구를 위한 중요한 자료원이 된다(*Hurbain v. Belgium* [GC], § 180). 과거 사건에 관한 뉴스 보관소가 문제 되는 경우에는, 현안 보도와 달리 상충하는 권리들 사이에서 균형을 맞추기 위해 국가에 더 큰 재량을 부여한다(*Times Newspapers Ltd v. the United Kingdom (nos. 1 및 2),* § 45). 언론은 책임 있는 저널리즘 원칙에 따라, 휘발성 정보가 아니라 역사적 정보의 정확성을 보장해야 할 의무가 있으며, 긴급히 보도할 필요가 없는 상황에서는 그 의무가 더욱 무겁다(*ibid.*, § 45).

421. *Hurbain v. Belgium* [GC], 2023 사건 §§ 180-185 에서 재판소는, 언론이 그 사명을 다할 수 있도록 보관소는 일반적으로 진본성·신뢰성·완전성을 유지해야 한다는 공감대가 유럽 내에 형성되고 있다고 하였다. 따라서 언론 보관소의 무결성은, 특히 그 적법성이 한 번도 문제 된 적이 없는 경우, 보관된 기사 전체 또는 일부의 삭제나 변경 요청을 심사할 때 지침이

되는 원칙이 되어야 한다. 이러한 요청은 국가 당국이 특별히 주의하여 철저하게 심사하여야 한다.

C. 데이터 이전과 데이터 흐름

422. 개인데이터의 대량 유통과 관련된 *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC] 2017 사건에서는 120 만 명의 개인 과세 데이터가 한 잡지에 게재된 후 문자메시지 서비스를 통해 유포되었다. 재판소의 견해에 따르면, 언론 목적을 위해 방대한 과세 데이터에 대한 접근을 허용하고 그 수집을 가능하게 하는 데 공익이 존재한다고 해서, 아무런 분석도 하지 않고 가공되지 않은 원자료를 대량으로 그대로 유포하는 데에도 공익이 존재한다고 보아야 하는 것은 아니었다. 데이터를 언론 목적으로 처리하는 것과 언론인만 특권적으로 접근할 수 있었던 원자료를 그대로 유포하는 것은 서로 구별해야 했다(*ibid.*, § 175). 그러한 맥락에서, 과세 관련 개인데이터의 대량 공개를 국내 규정 및 EU 데이터 보호 규정과 양립할 수 없는 절차에 따라 금지하는 것은 그 자체로 제재가 되는 것은 아니며, 설령 공개되는 정보의 양이 제한되어 실무적으로 일부 청구인 회사들의 사업 활동 수익성이 떨어지게 되었더라도 마찬가지이다(*ibid.*, § 197).

423. *Big Brother Watch and Others v. the United Kingdom* [GC], 2021 사건에서는, 외국 정보기관, 특히 미국 국가안보국(“NSA”)이 가로챈 데이터를 공유하는 것이 협약 제 8 조와 양립 가능한지가 문제 되었다. 재판소는 데이터 교환은 명확하고 상세한 규칙으로 규율해야 하고, 그 규칙은 당국이 언제 어떤 조건에서 그러한 요청을 할 권한이 생기는지 시민이 충분히 알 수 있도록 하고, 또한 이 권한이 국내법이나 협약상 국가의 의무를 우회하는 데 사용되지 않도록 하는 효과적인 보호조치를 제공해야 한다고 밝혔다. 가로챈 자료를 받은 국가는 그 자료의 검토·이용·보관, 재전송, 삭제 및 폐기에 관한 적절한 보호조치를 마련해야 한다. 이러한 보호조치는 체약국이 외국 정보기관으로부터 요청에 따라 가로챈 자료를 제공받는 경우에도 동일하게 적용된다. 만약 국가가 외국 정보기관으로부터 받은 자료가 실제 가로채기의 산물인지 항상 알 수 없는 상황이라면, 재판소는 가로채기의 산물일 수 있는 외국 정보기관의 모든 자료에 동일한 기준을 적용해야 한다고 보았다. 끝으로, 정보기관이 비체약국에 감청이나 가로챈 자료 제공을 요청할 수 있도록 허용하는 제도는 무엇이든 독립적인 감독을 받아야 하며, 아울러 독립적인 사후 심사의 가능성도 보장되어야 한다(*ibid.*, §§ 498-499).

인용 판례 목록

이 해설서에 인용된 판례는 유럽인권재판소가 내린 판결 또는 결정과 유럽인권위원회("위원회")의 결정 또는 보고서를 의미합니다.

특별한 표시가 없는 한, 모든 인용문은 소재판부(Chamber)가 선고한 본안판결(judgment on the merits)에 대한 것입니다. 약칭 "(dec.)"은 재판소의 결정에서 인용하는 것을 의미하고, "[GC]"는 해당 사건이 대재판부(Grand Chamber)에서 심리된 것임을 나타냅니다.

협약 제 44 조의 의미에 따라 최종이 아닌 소재판부 판결은 아래 목록에서 별표(*)로 표시되어 있습니다. 협약 제 44 조제 2 항의 규정에 따르면 "소재판부 판결은 (a) 당사자들이 대재판부에 회부 요청을 하지 않겠다고 선언한 경우, (b) 대재판부로 회부를 요청하지 않은 상태에서 판결일로부터 3 개월이 경과한 후 또는 (c) 대재판부 패널이 제 43 조에 따른 회부 요청을 거절하는 경우 확정"됩니다. 대재판부 패널이 회부 요청을 승인하면, 소재판부 판결은 확정되지 않으며 법적 효력이 없고, 이어지는 대재판부 판결이 최종 판결이 됩니다.

이 해설서의 전자판에 인용된 사건의 하이퍼링크는 재판수 판례(대재판부, 소재판부 및 위원회 판결과 결정, 언급된 사건, 권고적 의견 및 판례정보노트(Case-Law Information Note)의 결정요지(legal summaries), 위원회 판례(결정 및 보고서), 각료위원회 결의에 접속할 수 있는 HUDOC 데이터베이스(http://hudoc.echr.coe.int)로 연결합니다.

재판소는 공식 언어인 영어와 프랑스어 또는 둘 중 하나로 판결과 결정을 내립니다. HUDOC 는 다수의 주요 판례를 30 가지 이상의 비공식 언어로 번역한 번역본 및 제 3 자가 작성한 100 여 개 온라인 판례집으로 연결되는 링크도 제공합니다. 인용된 사건에 대한 언어별 번역본은 모두 해당 사건의 하이퍼링크를 클릭하면 연결되는 HUDOC 데이터베이스에서 '번역본(Language versions)' 탭을 통해 이용할 수 있습니다.

—A—

A.B. v. the Netherlands, no. 37328/97, 29 January 2002
A.P., Garçon and Nicot v. France, nos. 79885/12 and 2 others, ECHR 2017
A.P. v. Armenia, no. 58737/14, 18 June 2024
Adomaitis v. Lithuania, no. 14833/18, 18 January 2022
Akgün v. Turkey, no. 19699/18, 20 July 2021
Allan v. the United Kingdom, no. 48539/99, ECHR 2002-IX
Alexandridis v. Greece, no. 19516/06, 21 February 2008
Alkaya v. Turkey, no. 42811/06, 9 October 2012

Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece, no. 72562/10, 22 February 2018
Amann v. Switzerland [GC], no. 27798/95, ECHR 2000-II
Anchev v. Bulgaria (dec.), nos. 38334/08 and 68242/16, 5 December 2017
André and Others v. France, no. 18603/03, 24 July 2008
Antoneta Tudor v. Romania, no. 23445/04, 24 September 2013
Antović and Mirković v. Montenegro, no. 70838/13, 28 November 2017
Apostu v. Romania, no. 22765/12, 3 February 2015
A.R. v. the United Kingdom, no. 6033/19, 1 July 2025
Armonienė v. Lithuania, no. 36919/02, 25 November 2008
Association « 21 December 1989 » and Others v. Romania, nos. 33810/07 and 18817/08, 24 May 2011
Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, 28 June 2007
Avilkina and Others v. Russia, no. 1585/09, 6 June 2013
Axel Springer AG v. Germany [GC], no. 39954/08, 7 February 2012
Axel Springer SE and RTL Television GmbH v. Germany, no. 51405/12, 21 September 2017
Aycaguer v. France, no. 8806/12, 22 June 2017

—B—

B.B. v. France, no. 5335/06, 17 December 2009
Batiashvili v. Georgia, no. 8284/07, 10 October 2019
Bărbulescu v. Romania [GC], no. 61496/08, 5 September 2017 (extracts)
Bédat v. Switzerland [GC], no. 56925/08, ECHR 2016
Beghal v. the United Kingdom, no. 4755/16, 28 February 2019
Benedik v. Slovenia, no. 62357/14, 24 April 2018
Ben Faiza v. France, no. 31446/12, 8 February 2018
Bernh Larsen Holding AS and Others v. Norway, no. 24117/08, 14 March 2013
Biancardi v. Italy, no. 77419/16, 25 November 2021
Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, 25 May 2021
Biriuk v. Lithuania, no. 23373/03, 25 November 2008
Bogomolova v. Russia, no. 13812/09, 20 June 2017
Boljević v. Serbia, no. 47443/14, 16 June 2020
Brunet v. France, no. 21010/10, 18 September 2014
Breyer v. Germany, no. 50001/12, 30 January 2020
Buck v. Germany, no. 41604/98, ECHR 2005-IV
Buturugă v. Romania, no. 56867/15, 11 February 2020
Bykov v. Russia [GC], no. 4378/02, 10 March 2009

—C—

C.C. v. Spain, no. 1425/06, 6 October 2009
Cakicisoy and Others v. Cyprus (dec.), no. 6523/12, 23 September 2014
Canonne v. France (dec.), no. 22037/13, 2 June 2015
Caruana v. Malta (dec.), no. 41079/16, 15 May 2018
Casarini v. Italy (dec.), no. 25578/11, 5 November 2024
Catt v. the United Kingdom, no. 43514/15, 24 January 2019
Cherrier v. France, no. 18843/20, 30 January 2024
Cemalettin Canlı v. Turkey, no. 22427/04, 18 November 2008
Centre for Democracy and the Rule of Law v. Ukraine v. Ukraine, no. 10090/16, 26 March 2020

Centrum för rättvisa v. Sweden [GC], no. 35252/08, 25 May 2021
Cevat Özel v. Turkey, no. 19602/06, 7 June 2016
Christine Goodwin v. the United Kingdom [GC], no. 28957/95, ECHR 2002-VI
Ciubotaru v. Moldova, no. 27138/04, 27 April 2010
Coban v. Spain (dec.), no. 17060/02, 25 September 2006
Copland v. the United Kingdom, no. 62617/00, ECHR 2007-I
Cossey v. the United Kingdom, 27 September 1990, Series A no. 184
Craxi v. Italy (no. 2), no. 25337/94, 17 July 2003

—D—

D.H. and Others v. North Macedonia, no. 44033/17, 18 July 2023
D.L. v. Bulgaria, no. 7472/14, 19 May 2006
Dalea v. France (dec.), no. 964/07, 2 February 2010
DELTA PEKÁRNY a.s. v. Czech Republic, no. 97/11, 2 October 2014
Demirtepe v. France, no. 34821/97, ECHR 1999-IX (extracts)
Denysyuk and Others v. Ukraine, nos. 22790/12 and 3 others, 13 February 2025
Deveci v. Türkiye (dec.), no. 42785/11, 28 June 2022
Dimitras and Others v. Greece, nos. 42837/06 and 4 others, 3 June 2010
Dimitrov-Kazakov v. Bulgaria, no. 11379/03, 10 February 2011
Doerga v. the Netherlands, no. 50210/99, 27 April 2004
Dragan Petrović v. Serbia, no. 75229/10, 14 April 2020
Dragojević v. Croatia, no. 68955/11, 15 January 2015
Drakšas v. Lithuania, no. 36662/04, 31 July 2012
Drelon v. France, nos. 3153/16 and 27758/18, 8 September 2022
Dudgeon v. the United Kingdom, 22 October 1981, Series A no. 45
Dumitru Popescu v. Romania (no. 2), no. 71525/01, 26 April 2007
Dupuis and Others v. France, no. 1914/02, 7 June 2007

—E—

Editions Plon v. France, no. 58148/00, ECHR 2004-IV
Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, ECHR 2011 (extracts)
Egeland and Hanseid v. Norway, no. 34438/04, 16 April 2009
Ekimdzhiev and Others v. Bulgaria, no. 70078/12, 11 January 2022
Elberte v. Latvia, no. 61243/08, ECHR 2015
Erdem v. Germany, no. 38321/97, ECHR 2001-VII (extracts)
Ernst and Others v. Belgium, no. 33400/96, 15 July 2003
Eternit v. France (dec.), no. 20041/10, 27 March 2012

—F—

Financial Times Ltd and Others v. the United Kingdom, no. 821/03, 15 December 2009
Florindo de Almeida Vasconcelos Gramaxo v. Portugal, no. 26968/16, 13 December 2022
Foxley v. the United Kingdom, no. 33274/96, 20 June 2000
Frâncu v. Romania, no. 69356/13, 13 October 2020
Friedl v. Austria, no. 15225/89, Commission report, 19 May 1994

—G—

G.S.B. v. Switzerland, no. 28601/11, 22 December 2015
Gafiuc v. Romania, no. 59174/13, 13 October 2020
Gardel v. France, no. 16428/05, ECHR 2009
Garnaga v. Ukraine, no. 20390/07, 16 May 2013
Gaskin v. the United Kingdom, 7 July 1989, Series A no. 160
Gaughran v. the United Kingdom, no. 45245/15, 13 February 2020
Gauvin-Fournis and Silliau v. France, nos. 21424/16 and 45728/17, 7 September 2023
Gawlik v. Liechtenstein, no. 23922/19, 16 February 2021
Giesbert and Others v. France, nos. 68974/11 and 2 others, 1er June 2017
Gillan and Quinton v. the United Kingdom, no. 4158/05, ECHR 2010 (extracts)
Gîrleanu v. Romania, no. 50376/09, 26 June 2018
Glukhin v. Russia, no. 11519/20, 4 July 2023
Godelli v. Italy, no. 33783/09, 25 September 2012
Gorlov and Others v. Russia, nos. 27057/06 and 2 others, 2 July 2019
Görmüş and Others v. Turkey, no. 49085/07, 19 January 2016
Grande Oriente d'Italia v. Italy, no. 29550/17, 19 December 2024
Grant v. the United Kingdom, no. 32570/03, ECHR 2006-VII
Greuter v. the Netherlands (dec.), no. 40045/98, 19 March 2002
Guerra and Others v. Italy, no. 14967/89, *Reports of Judgments and Decisions* 1998-I
Guillot v. France, 24 October 1996, *Reports of Judgments and Decisions* 1996-V
Guiorgui Nikolaïchvili v. Georgia, no. 37048/04, 13 January 2009
Güzel Erdagöz v. Turkey, no. 37483/02, 21 October 2008

—H—

Haldimann and Others v. Switzerland, no. 21830/09, ECHR 2015
Halford v. the United Kingdom, 25 June 1997, *Reports of Judgments and Decisions* 1997-III
Hämäläinen v. Finland [GC], no. 37359/09, ECHR 2014
Haralambie v. Romania, no. 21737/03, 27 October 2009
Hájovský v. Slovakia, no. 7796/16, 1 July 2021
Haščák v. Slovakia, nos. 58359/12 and 2 others, 23 June 2022
Hassine v. Romania, no. 36328/13, 9 March 2021
Heglas v. Czech Republic, no. 5935/02, 1 March 2007
Henry Kismoun v. France, no. 32265/10, 5 December 2013
Hurbain v. Belgium [GC], no. 57292/16, 4 July 2023
Huvig v. France, 24 April 1990, Series A no. 176-B

—I—

I. v. Finland, no. 20511/03, 17 July 2008
I. v. the United Kingdom [GC], no. 25680/94, 11 July 2006
Iordachi and Others v. the Republic of Moldova, no. 25198/02, 10 February 2009
İrfan Güzel v. Turkey, no. 35285/08, 7 February 2017
Ivashchenko v. Russia, no. 61064/10, 13 February 2018

—J—

J.L. v. Italy, no. 5671/16, 27 May 2021
J.P.D. v. France (dec.), no. 55432/10, 16 September 2016
J.S. v. the United Kingdom (dec.), 445/10, 3 March2015
Jäggi v. Switzerland, no. 58757/00, ECHR 2006-X
Jarnea v. Romania, no. 41838/05, 19 July 2011
Jecker v. Switzerland, no. 35449/14, 6 October 2020
Jehovah's Witnesses v. Finland, no. 31172/19, 9 May 2023
Joanna Szulc v. Poland, no. 43932/08, § 13 November 2012

—K—

K.H. and Others v. Slovakia, no. 32881/04, ECHR 2009 (extracts)
K.S. and M.S. v. Germany, no. 33696/11, 6 October 2016
K.U. v. Finland, no. 2872/02, ECHR 2008
Kaczmarek v. Poland, no. 16974/14, 22 February 2024
Kahn v. Germany, no. 16313/10, 17 March 2016
Karabeyoğlu v. Turkey, no. 30083/10, 7 June 2016
Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010
Khadija Ismayilova v. Azerbaijan, nos. 65286/13 and 57270/14, 10 January 2019
Khan v. the United Kingdom, no. 35394/97, ECHR 2000-V
Khoujine and Others v. Russia, no. 13470/02, 23 October 2008
Khelili v. Switzerland, no. 16188/07, 18 October 2011
Kinnunen v. Finland, no. 18291/91, Commission decision, 13 October 1993
Kinnunen v. Finland, no. 24950/94, Commission decision, 15 May 1996
Kırdök and Others v. Turkey, no. 14704/12, 3 December 2019
Kiyutin v. Russia, no. 2700/10, ECHR 2011
Klass and Others v. Germany, 6 September 1978, Series A no. 28
Khmel v. Russia, no. 20383/04, 12 December 2013
Konovalova v. Russia, no. 37873/04, 9 October 2014
Köpke v. Germany (dec.), no. 420/07, 5 October 2010
Kotilainen and Others v. Finland, no. 62439/12, 17 September 2020
Krone Verlag GmbH & Co. KG v. Austria, no. 34315/96, 26 February 2002
Kruglov and Others v. Russia, nos. 11264/04 and 15 others, 4 February 2020
Kruslin v. France, 24 April 1990, Series A no. 176-A
Kurier Zeitungsverlag und Druckerei GmbH v. Austria, no. 3401/07, 17 January 2012
Kvasnica v. Slovakia, no. 72094/01, 9 June 2009

—L—

L.B. v. Hungary [GC], no. 36345/16, 9 March 2023
L.F. v. France (dec.), nos. 3866/20 and 9292/20, 13 February 2024
L.H. v. Latvia, no. 52019/07, 29 April 2014
L.L. v. France, no. 7508/02, ECHR 2006-XI
Labita v. Italy [GC], no. 26772/95, ECHR 2000-IV
Lambert v. France, no. 23618/94, *Reports of Judgments and Decisions* 1998-V
Lavents v. Latvia, no. 58442/00, 28 November 2002
Le Marrec v. France (dec.), no. 52319/22, 5 November 2024
Leander v. Sweden, 26 March 1987, Series A no. 116

Libert v. France, no. 588/13, 22 February 2018
Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008
Liblik and Others v. Estonia, no. 173/15 and 5 others, 28 May 2019
Liebscher v. Austria, no. 5434/17, 6 April 2021
López Ribalda and Others v. Spain [GC], nos. 1874/13 and 8567/13, 17 October 2019
Lüdi v. Switzerland, no. 12433/86, Series A no. 238
Lupker and Others v. the Netherlands, 18395/91, Commission decision, 7 December 1992

—M—

M.B. v. France, no. 22115/06, 17 December 2009
M.C. v. the United Kingdom, no. 51220/13, 30 March 2021
M.D. and Others v. Spain, no. 36584/17, 28 June 2022
M.G. v. the United Kingdom, no. 39393/98, 24 September 2002
M.K. v. France, no. 19522/09, 18 April 2013
M.L. and W.W. v. Germany, nos. 60798/10 and 65599/10, 28 June 2018
M.M. v. the United Kingdom, no. 24029/07, 13 November 2012
M.N. and Others v. San Marino, no. 28005/12, 7 July 2015
M.P. v. Portugal, no. 27516/14, 7 September 2021
M.S. v. Sweden, 27 août 1997, *Reports of Judgments and Decisions* 1997-IV
MGN Limited v. the United Kingdom, no. 39401/04, 18 January 2011
Magyar Helsinki Bizottság v. Hungary [GC], no. 18030/11, ECHR 2016
Malanicheva v. Russia (dec.), no. 50405/06, 31 May 2016
Malone v. the United Kingdom, 2 August 1984, Series A no. 82
Marchiani v. France (dec.), no. 30392/03, 27 May 2008
Margari v. Greece, no. 36705/16, 20 June 2023
Matheron v. France, no. 57752/00, 29 March 2005
McGinley and Egan v. the United Kingdom, 9 June 1998, *Reports of Judgments and Decisions* 1998-III
McVeigh, O'Neill and Evans v. the United Kingdom, nos. 8022/77 and two others, Commission report, 18 March 1981
Mediengruppe Österreich GmbH v. Austria, no. 37718/18, 26 April 2022
Mehmedovic v. Switzerland (dec.), no. 17331/11, 11 December 2018
Mentzen v. Latvia (dec.), no. 71074/01, ECHR 2004-XII
Messina v. Italy (no. 2), no. 25498/94, ECHR 2000-X
Michaud v. France, no. 12323/11, ECHR 2012
Mik and Jovanović v. Serbia (dec.), nos. 9291/14 and 63798/14, 23 March 2021
Mikulić v. Croatia, no. 53176/99, ECHR 2002-I
Mifsud v. Malta, no. 62257/15, 29 January 2019
Mitov and Others v. Bulgaria (dec.), no. 80857/17, 28 February 2023
Mityanin and Leonov v. Russia, nos. 11436/06 and 22912/06, 7 May 2018
Mockutė v. Lithuania, no. 66490/09, 27 February 2018
Modestou v. Greece, no. 51693/13, 16 March 2017
Moldovan v. Ukraine, no. 62020/14, 14 March 2024
Montera v. Italy (dec.), no. 64713/01, 9 July 2002
Moskalev v. Russia, no. 44045/05, 7 November 2017
Mosley v. the United Kingdom, no. 48009/08, 10 May 2011
Murray v. the United Kingdom [GC], 28 October 1994, Series A no. 300-A
Murtazaliyeva v. Russia [GC], no. 36658/05, 18 December 2018
Mustafa Sezgin Tanrıkulu v. Turkey, no. 27473/06, 18 July 2017

—N—

N.F. and Others v. Russia, no. 3537/15 and 8 others, 12 September 2023
N. Š. v. Croatia, no. 36908/13, 10 September 2020
Nada v. Switzerland [GC], no. 10593/08, ECHR 2012
Nagla v. Latvia, no. 73469/10, 16 July 2013
National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France, nos. 48151/11 and 77769/13, 18 January 2018
Negru v. the Republic of Moldova, no. 7336/11, 27 June 2023
News Verlags GmbH & Co.KG v. Austria, no. 31457/96, ECHR 2000-I
Niedbała v. Poland, no. 27915/95, 4 July 2000
Nuh Uzun and Others v. Turkey, nos. 49341/18 et seq., 29 March 2022

—O—

Odièvre v. France [GC], no. 42326/98, ECHR 2003-III
Oleynik v. Russia, no. 23559/07, 21 June 2016

—P—

P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001-IX
P.N. v. Germany, no. 74440/17, 11 June 2020
P.T. v. the Republic of Moldova, no. 1122/12, 26 May 2020
P. and B. v. the United Kingdom, no. 36337/97 and 35974/97, ECHR 2001-III
P. and S. v. Poland, no. 57375/08, 30 October 2012
Panteleyenko v. Ukraine, no. 11901/02, 29 June 2006
Peck v. the United Kingdom, no. 44647/98, ECHR 2003-I
Peers v. Greece, no. 28524/95, ECHR 2001-III
Pendov v. Bulgaria, no. 44229/11, 26 March 2020
Peruzzo and Martens v. Germany (dec.), nos. 7841/08 and 57900/12, 4 June 2013
Perry v. the United Kingdom, no. 63737/00, ECHR 2003-IX (extracts)
Petrova v. Latvia, no. 4605/05, 24 June 2014
Pietrzak and Bychawska-Siniarska and Others v. Poland, nos. 72038/17 and 25237/18, 28 May 2024
Pinto Coelho v. Portugal (no. 2), no. 48718/11, 22 March 2016
Podchasov v. Russia, no. 33696/19, 13 February 2024
Polanco Torres and Movilla Polanco v. Spain, 34147/06, 21 September 2010
Prado Bugallo v. Spain, no. 58496/00, 18 February 2003
Pruteanu v. Romania, no. 30181/05, 3 February 2015

—R—

R.E. v. the United Kingdom, no. 62498/11, 27 October 2015
Radio Twist, a.s. v. Slovakia, no. 62202/00, ECHR 2006-XV
Radu v. the Republic of Moldova, no. 50073/07, 15 April 2014
Ramadan v. France (dec.), no. 23443/23, 9 January 2024
Rees v. the United Kingdom, no. 9532/81, Series A no. 106
Reklos and Davourlis v. Greece, no. 1234/05, 15 January 2009
Reznik v. Ukraine, no. 31175/14, 23 January 2025
Ricci v. Italy, no. 30210/06, 8 October 2013

Robathin v. Austria, no. 30457/06, 3 July 2012
Roche v. the United Kingdom [GC], no. 32555/96, ECHR 2005-X
Roemen and Schmit v. Luxembourg, no. 26419/10, ECHR 2003-IV
Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015
Rook v. Germany, no. 1586/15, 25 July 2019
Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V

—S—

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008
S.V. v. Italy, no. 55216/08, 11 October 2018
Sanoma Uitgevers B.V. v. the Netherlands [GC], no. 38224/03, 14 September 2010
Samoylova v. Russia, no. 49108/11, 14 December 2021
Šantare and Labazņikovs v. Latvia, no. 34148/07, 31 March 2016
Sârbu v. Romania, no. 34467/15, 28 March 2023
Särgava v. Estonia, no. 698/19, 16 November 2021
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, ECHR 2017 (extracts)
Schmidt v. Germany (dec.), no. 32352/02, 5 January 2006
Sciacca v. Italy, no. 50774/99, ECHR 2005-I
Sedletska v. Ukraine, no. 42634/18, 1 April 2021
Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, ECHR 2006-VII
Selishcheva and Others v. Russia, nos. 39056/22 and 9 others, 27 May 2025
Sérvulo & Associados - Sociedade de Advogados, RL, and Others v. Portugal, no. 27013/10, 3 September 2015
Sheffield and Horsham v. the United Kingdom, 30 July 1998, *Reports of Judgments and Decisions* 1998-V
Sher and Others v. the United Kingdom, no. 5201/11, ECHR 2015 (extracts)
Shimovolos v. Russia, no. 30194/09, 21 June 2011
Silver and Others v. the United Kingdom, 25 March 1983, Series A no. 61
Sinan Işık v. Turkey, no. 21924/05, ECHR 2010
Smirnov v. Russia, no. 71362/01, 7 June 2007
Smith and Grady v. the United Kingdom, no. 33985/96 and 33986/96, *Reports of Judgments and Decisions* 1999-VI
Société de Conception de Presse and d'Édition v. France, no. 4683/11, 25 February 2016
Söderman v. Sweden [GC], no. 5786/08, ECHR 2013
Sommer v. Germany, no. 73607/13, 27 April 2017
Sõro v. Estonia, no. 22588/08, 3 September 2015
Standard Verlagsgesellschaft mbH v. Austria (no. 3), no. 39378/15, 7 December 2021
Stolkosa v. Poland (dec.), no. 68562/14, 14 September 2021
Succession Kresten Filtenborg Mortensen v. Denmark (dec.), no. 1338/03, ECHR 2006-V
Suprunenko v. Russia (déc), no. 8630/11, 19 June 2018
Surikov v. Ukraine, no. 42788/06, 26 January 2017
Sytnyk v. Ukraine, no. 16497/20, 24 April 2025
Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016
Szuluk v. the United Kingdom, no. 36936/05, ECHR 2009

—T—

Taylor-Sabori v. the United Kingdom, no. 47114/99, 22 October 2002

Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, no. 39315/06, 22 November 2012
Tena Arregui v. Spain, no. 42541/18, 11 January 2024
Thoma v. Luxembourg, no. 38432/97, ECHR 2001-III
Tillack v. Belgium, 20477/05, 27 November 2007
Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), nos. 3002/03 and 23676/03, ECHR 2009
Toma v. Romania, no. 42716/02, 24 February 2009
Tonchev v. Bulgaria, no. 40519/15, 16 April 2024
Tønsbergs Blad A.S. and Haukom v. Norway, no. 510/04, 1er March 2007
Trabajo Rueda v. Spain, no. 32600/12, 30 May 2017
Trajkovski and Chipovski v. North Macedonia, nos. 53205/13 and 63320/13, 13 February 2020

—U—

Ungváry and Irodalom Kft. v. Hungary, no. 64520/10, 3 December 2013
Uzun v. Germany, no. 35623/05, ECHR 2010 (extracts)

—V—

Valašinas v. Lithuania, no. 44558/98, ECHR 2001-VIII
Valenzuela Contreras v. Spain, no. 2767/95, *Reports of Judgments and Decisions* 1998-V
Van der Velden v. the Netherlands (dec.), no. 29514/05, ECHR 2006-XV
Van Vondel v. the Netherlands, no. 38258/03, 25 October 2007
Vasil Vasilev v. Bulgaria, no. 7610/15, 16 November 2021
Vasylchuk v. Ukraine, no. 24402/07, 13 June 2013
Verlagsgruppe Droemer Knaur GmbH & Co. KG v. Germany, 35030/13, 19 October 2017
Vetter v. France, no. 59842/00, 31 May 2005
Vicent Del Campo v. Spain, no. 25527/13, 6 November 2018
Vinci Construction and GTM Génie Civil and Services v. France, nos. 63629/10 and 60567/10, 2 April 2015
Visy v. Slovakia, no. 70288/13, 16 October 2018
Volodina v Russia (no. 2), no. 40419/19, 14 September 2021
Von Hannover v. Germany, no. 59320/00, ECHR 2004-VI
Von Hannover v. Germany (no. 2) [GC], nos. 40660/08 and 60641/08, ECHR 2012
Vučina v. Croatia (dec.), no. 58955/13, 24 September 2019
Vukota-Bojić v. Switzerland, no. 61838/10, 18 October 2016

—W—

W. v. the Netherlands (dec.), no. 20689/08, 20 January 2009
Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI
Węgrzynowski and Smolczewski v. Poland, no. 33846/07, 16 July 2013
Wieser and Bicos Beteiligungen GmbH v. Austria, no. 74336/01, ECHR 2007-IV
Willems v. the Netherlands (dec.), no. 57294/16, 9 November 2021
Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no. 2) (dec.), no. 62746/00, ECHR 2002-X
Wisse v. France, no. 71611/01, 20 December 2005

—X—

X and Others v. Russia, nos. 78042/16 and 66158/14, 14 January 2020

—Y—

Y. v. Turkey (dec.), no. 648/10, 17 February 2015
Y.B. and Others v. Turkey, nos. 48173/99 and 48319/99, 28 October2004
Y.G. v. Russia, no. 8647/12, 30 August 2022
Y.Y. v. Russia, no. 40378/06, 23 February 2016
Yonchev v. Bulgaria, no. 12504/09, 7 December 2017
Youth Initiative for Human Rights v. Serbia, no. 48135/06, 25 June 2013
Yvonne Chave née Jullien v. France, no. 14461/88, Commission decision of 9 July 1991

—Z—

Z v. Finland, 25 February 1997, *Reports of Judgments and Decisions* 1997-I
Zoltán Varga v. Slovakia, nos. 58361/12 and 2 others, 20 July 2021