Contents

국내 입법 동향

국외 입법 동향

인터넷 법제동향

•• 국내 입법 동향 ••

1. 입법동향

1 「방송법」 일부개정안 국회제출 (정부 발의, 2014. 11. 10)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유 및 주요내용

■ 「방송법」에서 규정하고 있는 기술기준 위반에 대한 시정명령과 그 내용이 중복되는 종합유선방송사업자 등에 대한 전송 · 선로설비의 개선명령에 관한 규정을 삭제하는 한편, 방송시장의 자율성을 제고하고 전송망사업자의 불필요한 부담을 경감하기 위하여 사업자 간에 이루어지는 전송 · 선로설비의 이용약관 신고제를 폐지하려는 것임.

※ 출처 : 국회 (http://www.assembly.go.kr)

2 「이동통신단말장치 유통구조 개선에 관한 법률」 일부개정안 국회제출 (심재철의원 대표발의, 2014. 11. 10)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

- 당초 이동통신단말장치의 공정하고 투명한 유통 질서를 확립하고 가계통신비 부담을 줄이기 위해 「이동통신단말장치 유통구조 개선에 관한 법률」의 제정이 이루어졌지만, 이러한 입법 취지와 달리 오히려 기업들의 경쟁력이 저하되고 국민들의 부담이 가중되는 결과가 나타났음.

주요내용

- 이에 당초의 입법 취지를 살리기 위하여 지원금 상한제를 폐지하고, 이동통신단말장치 제조업자 및 이동통신사업자가 지원금에 관한 공시를 변경하려는 경우 공시 7일 전까지 방송통신위원회에 신고하도록 하려는 것임(안 제4조, 제22조제4항제1호의2 신설 등).

※ 출처 : 국회 (http://www.assembly.go.kr)

3 「이동통신단말장치 유통구조 개선에 관한 법률」 일부개정안 국회제출 (한명숙의원 대표발의, 2014. 11. 7)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

- 「이동통신단말장치 유통구조 개선에 관한 법률」은 당초의 입법취지와는 달리 시행 이후 이동통신 시장을 오히려 더욱 큰 혼란에 빠지게 하고 말았으며, 이로 인하여 소비자들이

불편을 감내하고 있음.

- 현행법은 이동통신단말장치 시장에 대하여 정부에 강한 규제 권한을 주고 있는데, 이러한 규제가 오히려 소비자의 후생을 악화시키고 있는 실정임. 특히 지원금에 상한을 두도록 하고 지원금에 대하여 각 시장주체들이 취할 수 있는 행위를 엄격하게 제한하는 규제 등은 이동통신사업자와 이동통신단말기 제조업자의 자유로운 경쟁을 저해하여 현행의 과점 체제를 옹호하는 결과를 낳았음.

- 이에 이동통신단말장치와 관련하여 소비자 보호 및 시장 질서의 유지를 위하여 필요한 규제는 제외하고, 일견 소비자 보호 규제인 것처럼 보이지만 실질적으로는 경쟁을 제한하는 규제들은 폐지하려는 것임.

주요내용

- 이동통신사업자, 대리점 또는 판매점이 지원금을 이용자의 가입 유형 및 요금제 등에 따라 차별 지급할 수 있도록 함(안 제3조 삭제).

- 이용자의 이동통신단말장치 구매에 대하여 이동통신사업자 · 대리점 및 판매점이 지급할 수 있는 지원금에 상한을 두도록 하는 지원금 상한제를 폐지함(안 제4조제1항 · 제2항 삭제 등).

- 이동통신단말장치 제조업자 및 이동통신사업자가 각각 이동통신사업자나 대리점 및 판매점에 장려금을 제공하거나 협정을 체결하면서 이용자에게 차별적인 지원금을 지급하지 못하도록 하는 협정 및 특약 관련 규제를 폐지함(안 제9조 삭제).

- 다른 벌칙과 중복적으로 규정되어 있는 이동통신단말장치 제조업자 · 이동통신사업자 · 대리점 및 판매점에 대한 긴급중지명령 제도를 폐지함(안 제11조 삭제).

- 이용자에게 지급하는 지원금을 이동통신단말장치 제조업자와 이동통신사업자가 분리하여 공시하도록 함(안 제12조제1항 단서 삭제 등).

※ 출처 : 국회 (http://www.assembly.go.kr)

4 「방송법」 일부개정안 국회제출 (정희수 의원 대표발의, 2014. 11. 7)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

- 현행법에서 인용하고 있는 법률 제명 중 법률의 전부개정으로 법률 제명이 변경되었는데도 변경되기 전의 제명을 그대로 명시하고 있거나, 기존에 폐지되었으나 폐지 법률에 대한 정보를 명확히 알 수 없게 규정하고 있는 경우가 있음.

- 법조문의 오류는 국민들로 하여금 해당 규정의 내용을 파악하는데 혼란을 줄 우려가 있는바, 오류 내용을 바로잡아 명확한 정보를 제공할 필요가 있음.

주요내용

- 이에 기존 법률 제명인 「정기간행물의등록등에관한법률」을 현재 시행 중인 「신문 등의 진흥에 관한 법률」로 개정하고, 폐지된 「사회보호법」에 대하여 종전의 법률임을 명확히 규정함으로써 국민들이 법을 올바르게 이해하는 데 도움을 주려는 것임(안 제8조제3항 및 제13조제3항 제6호).

※ 출처 : 국회 (http://www.assembly.go.kr)

5 「전기통신사업법」 일부개정안 국회제출 (정부 발의, 2014. 11. 4)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

■ 전기통신사업자의 부담 완화를 위하여 기간통신사업자 등이 시정명령을 이행하지 아니하는 경우에 부과하는 이행강제금 부과규정을 삭제하고, 다른 법률에서 규정하고 있는 사항과 중복되는 정보유용 금지에 관한 사항을 정비하며, 시외전화 사전선택제의 자율적인 운영을 강화하기 위하여 미래창조과학부장관이 정하여 고시하던 시외전화 사전선택제의 업무처리 방법 등에 관한 사항을 사전선택등록센터가 정하도록 하고, 전기통신사업에 대한 경쟁체제 도입으로 그 실효성이 없어진 전기통신설비 등의 통합운영 제도를 폐지하는 한편, 지방이양추진위원회에서 지방이양 사무로 결정된 자가전기통신설비 설치 신고 접수 등 미래창조과학부장관의 업무를 시 · 도지사에게 이양하려는 것임.

주요내용

■ 이행강제금 부과제도 폐지(현행 제13조 삭제)

– 현행 규정상 기간통신사업자 등이 시정명령을 이행하지 아니하는 경우에는 허가 취소, 과징금 부과 및 벌금 등이 가능하므로, 과도한 이중적인 제재수단인 이행강제금 부과제도를 폐지함.

■ 정보유용 금지에 관한 사항을 정비(안 제43조)

–「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제24조에서 규정하고 있는 이용자의 인적사항 등 개인정보 유용 금지에 관한 사항과 중복되는 내용을 정비함.

■ 시외전화 사전선택제 관련 고시의 위임근거 폐지(현행 제57조제4항 삭제)

– 시외전화 사전선택제의 자율적인 운영을 강화하기 위하여 미래창조과학부장관이 정하여

고시하던 시외전화 사전선택제의 시행 및 업무처리 방법 등에 관한 사항을 사전선택 등록 업무를 수행하는 전문기관인 사전선택등록센터가 자율적으로 정하도록 함.

■ 자가전기통신설비 관련 사무의 지방 이양(안 제64조, 제67조 및 제88조 등)

– 지방이양추진위원회에서 지방이양 사무로 결정된 자가전기통신설비 설치 신고 및 변경신고 접수, 자가전기통신설비 설치자에 대한 시정명령 및 과태료 부과 등에 관한 사항 등 미래창조과학부장관의 업무를 시 · 도지사에게 이양하되, 시 · 도지사는 미래창조과학부장관에게 자가전기통신설비의 설치 신고 현황 등을 보고하고 관련 자료를 갖추어 두도록 함.

■ 전기통신설비 등의 통합운영제도 폐지(현행 제70조 및 제71조 삭제)

– 미래창조과학부장관이 일정한 기준과 절차에 따라 선정한 기간통신사업자가 다른 기관의 전기통신설비 등을 통합운영할 수 있도록 한 규정은 현재 전기통신사업에 대한 경쟁체제가 도입되어 그 실효성이 없어졌으므로 폐지함.

※ 출처 : 국회 (http://www.assembly.go.kr)

6 「개인정보 보호법」 일부개정안 국회제출 (조원진 의원 대표발의, 2014. 11. 5)

소관 상임위원회 : 행정자치부

제안이유

■ 개인정보의 수집 · 유출 · 오용 · 남용으로부터 사생활의 비밀 등을 보호하기 위하여 2011년부터 현행법이 제정 · 시행되고 있음. 하지만 최근 카드사 개인정보 유출사고와 같은 대형 개인정보 유출이 빈발하는 등 아직까지는 민간사업자 등의 개인정보 보호에 대한 인식 수준이 낮고 개인정보의 안전성 확보를 위한 노력이 미진함.

■ 이에 대통령 소속 개인정보 보호위원회의 기능 강화, 개인정보 국외 제공 기준 마련, 수탁자 책임 강화 등 현행법의 운영상 미비사항을 보완하고, 징벌적 손해배상제 · 법정손해배상제를 도입하는 등 새로운 제도를 신설하여 개인정보 보호 강화를 위한 기업의 관심과 투자를 촉구하고 개인정보 유출사고 발생을 근본적으로 예방하려는 것임.

주요내용

■ 개인정보 보호위원회에 정책 · 제도 개선권고권 및 이행점검권, 자료제출요구권, 개인정보 분쟁조정위원 위촉권을 부여하는 등 개인정보 보호위원회의 기능을 강화함(안 제8조제4항 · 제5항, 제8조의2, 제11조제1항, 제40조제3항 · 제4항, 제63조제4항).

■ 자율규제를 촉진하기 위하여 안전행정부장관이 개인정보 보호 자율규제기구를 지정 · 운영할 수 있도록 함(안 제13조의2 및 제63조의2 신설).

■ 국외의 제3자가 안전행정부장관이 고시하는 인증을 받은 경우 또는 국외 제공 계약에 관한 지침을 준수하여 국외의 제3자와 계약을 체결하는 경우 등에 한하여 개인정보 국외 제공이 가능하도록 하여 글로벌 환경 하에서 개인정보 보호의 적정을 기함(안 제19조의2 신설).

■ 정보주체 이외로부터 개인정보를 수집한 경우 해당 개인정보의 수집 목적 및 출처 관리를 의무화하는 등 개인정보처리자의 책임성을 강화함(안 제20조의2 신설).

■ 개인정보 처리업무의 재위탁에 관한 법적 근거 및 한계를 명확히 함(안 제26조제6항 신설).

■ 개인정보 보호 인증기관의 지정 및 지정취소의 법적 근거를 명확히 함(안 제32조의2 신설).

■ 개인정보 영향평가의 대상을 확대하고 영향평가의 주요 결과를 공개하도록 함(안 제33조 및 제33조의2).

■ 필요한 최소한의 정보 외의 개인정보 수집에 대한 정보주체의 선택권을 보장하고, 열람 · 정정 · 삭제 요구권 행사의 편의성을 제고하는 등 정보주체의 권리를 강화함(안 제38조제4항, 제75조제2항제1호 및 제75조제3항제12호).

■ 징벌적 손해배상제 및 법정손해배상제를 도입하여 개인정보 유출 등에 따른 피해구제를 강화함(안 제39조제3항 · 제4항 및 제39조의2 신설).

■ 부정한 수단이나 방법으로 취득한 개인정보를 영리 또는 부정한 목적으로 제3자에게 제공한 자에게 10년 이하의 징역 또는 1억 원 이하의 벌금에 처하도록 하고, 개인정보 불법 유통 등으로 인한 범죄수익은 몰수 · 추징할 수 있도록 하는 등 제재수준을 강화함(안 제70조제2항 및 제74조의2 신설).

※ 출처 : 국회 (http://www.assembly.go.kr)

1. 입법 동향

1 미국 캘리포니아 주, 기존 개인정보보호의무 위반 관련법 확대 법안 입법추진 (2014. 9.30)

개요

■ 미국 캘리포니아주의 Jerry Brown 주지사는 기존의 개인정보보호의무 위반 관련법을 강화 및 확대시키는 새로운 법안(AB 1710)에 서명하였다(2014. 9. 30.).

배경 및 경과

■ 미국 내 다수의 주들은 개인정보에 대한 침해 건수가 늘어나면서 이를 효과적으로 다루기 위한 법안 추진에 노력을 하고 있으며 이들 중 캘리포니아 주가 선두를 달리고 있다.

■ 기존의 캘리포니아는 개인정보와 관련하여 보안절차를 이행할 의무를 특정 기업들에게 법적으로 요구하고 있었다.

– 기존법의 적용대상인 기업들은 캘리포니아 거주자의 개인정보를 소유(own)하고 있거나 이들 정보에 대해 허가(license)를 받은 기업들로 한정되어 있었고,

– 이는 어떠한 기업이 기업의 내부 고객 장부로서 개인정보를 보관하였거나, 혹은 그러한 정보와 관련 있는 자와의 거래에서 사용하기 위한 경우인 것을 의미한다.

■ 기존법으로 개인정보가 충분히 보호되지 않고 있는 현실을 감안하여 새로운 법안(AB 1710)이 출현하게 되었다.

주요 내용

■ 새로운 법안은 기존의 개인정보보호 위반 관련법과 비교할 때 변화한 점은 다음의 세 가지이다.

– **(보안절차의 이행 유지)** 캘리포니아 거주자의 개인정보를 보유하고(maintain) 있는 기업은 허락 없는 접근, 이용, 수정, 삭제 혹은 공개로부터 개인정보를 보호하기 위하여 그 개인정보의 성격에 적절한 합리적인 보안절차를 이행하고 유지하여야 한다.

※ 여기서 개인정보라 함은 개인의 이름 혹은 첫 번째 이니셜과 성, 개인의 사회보장번호, 의료정보, 금융계좌정보 혹은 운전면허증 번호 등의 정보를 포함함

※ 상기 요건은 보건의료 서비스 제공자, 보건의료 서비스 계획 혹은 의료정보의 기밀성에 관한 법(Confidentiality of Medical Information Act)에 의하여 규제되는 계약자에게는 적용되지 아니함

– **(개인정보침해방지 서비스 제공)** 개인 혹은 기업이 개인정보보호의 의무 위반을 한 경우, 적절한 신원도용방지 및 경감 서비스를 적어도 12개월 동안 피해자에게 무상으로 제공해야 한다.

※ 이 새로운 요건은 개인정보보호의 의무 위반이 사회보장번호, 운전면허증 번호 혹은 캘리포니아 사회보장번호에 대한 것을 포함하였을 경우에만 적용되는 것으로, 신용카드번호 혹은 그 외 기존의 캘리포니아 주법 내의 다른 개인정보 요소에 대해서는 적용되지 아니함

※ 그러나 1년간의 무상 신원도용방지 및 경감 서비스의 제공 요건이 모든 개인정보보호의무 위반자에게 발생하는 것인지, 이미 그러한 서비스를 제공하고 있는 자 혹은 기업에만 적용되는 것인지가 불분명함

– **(사회보장번호의 판매 등 금지)** 사회보장번호의 판매, 판매 제의, 혹은 판매 광고는 그러한 판매 등이 적법한 기업거래의 일부이거나 특별히 연방 혹은 주법에 따라 허가되거나 허용된 경우가 아닌 한 금지된다.

※ 기존법에 의해서도 사회보장번호에 대한 특별한 보호는 존재하였고, 개인의 사회보장번호를 대중에게 공개하는 행위 혹은 개인의 사회보장번호에 대한 보안을 저해할 수 있는 그밖의 행위는 금지되었음

평가

■ 법안에 사용된 다소간의 용어의 모호함에도 불구하고 동 법안은 캘리포니아 거주자의 개인정보를 보유하고 있는 모든 기업에 적용되기 때문에 캘리포니아 외의 지역에 소재한 기업에게도 영향을 미칠 것으로 예상된다.

– 연방 혹은 주법이 통과될 때까지 기업들은 현재 개인정보보호 의무 위반법과 관련한 많은 변화 및 수정을 예측하는 것이 바람직 할 것으로 보인다.

참고자료

http://www.lexology.com/library/detail.aspx?g=92a3ad2a-f113-4635-bbdf-1657533d26b7&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Other+states+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2014-10-24&utm_term=

http://www.workplaceprivacyreport.com/2014/10/articles/written-information-security-program/california-ab-1710-first-law-in-u-s-to-require-credit-monitoring-following-a-data-breach/

2 일본, 자유로운 모바일 이용환경 조성을 위한 「모바일 창생 플랜」 발표 (2014. 10. 30)

개요

■ 총무성은 모바일에 의한 일본의 창생과 국민부담의 경감을 목표로 “더욱 자유롭게”, “더욱 가깝게”, “더욱 빠르게”, “더욱 편리하게”모바일을 이용할 수 있는 환경을 실현하기 위한 “모바일 창생 플랜”을 종합하여 발표하였다 (2014.10.30.).

배경 및 목적

■ 현재 스마트폰 등 휴대전화는 국민생활에 필수불가결한 서비스가 될 정도로 보급되어 있고 앞으로 웨어러블 단말, M2M, IoT 등 경제사회활동 전체에 모바일이 폭 넓게 침투해 갈 것으로 전망되어 자유로운 모바일 이용환경의 조성이 요구된다.

■ 모바일 창생플랜은 모바일 이용환경 정비를 위하여 ① 단말기의 자유로운 선택 ② 저렴한 가격과 서비스 신뢰 ③ 모바일의 고속화 ④ 새로운 모바일 서비스의 창출에 대해 필요한 대응사항과 실시 시기를 밝히는 것을 목적으로 한다.

주요 내용

■ (단말기의 자유로운 선택) 단말기를 교체하지 않고 다른 사업자의 통신 서비스를 이용할 수 있도록 하고 서비스 경쟁을 통해 요금인하 및 이용자 선택의 폭을 넓히고자 한다.

– 단말기에 설정되어 있는 SIM Lock을 해제함으로써 해외여행 시 자신의 단말기에 해당 국가의 SIM 교체만으로 현지의 통신서비스의 이용이 가능하다.

※ 2015년 이후에 새롭게 판매되는 스마트폰과 태블릿 PC 등에 대해 원칙적으로 무료로 SIM Lock을 해제하는 내용에 관련 가이드라인 개정(안)을 실시하고자 함

※ "SIM Lock"은 휴대전화에 내장되어 있는 카드의 인식을 제한하는 기술의 하나로 통신사들은 이 기술을 이용하여 휴대폰이 특정한 sim카드만을 인식하게 함

– 2년간의 약정을 조건으로 기본요금을 할인하면서 자동갱신되는 "기간구속 · 자동갱신부계약"의 운영을 개선한다.

※ 계약해제료를 지불하지 않고 해제가능한 기간의 연장과 갱신월이 근접한 시점에 이용자에게 갱신에 관한 통지를 철저하고 신속하게 처리하도록 함

■ **(저렴한 가격과 서비스의 신뢰)** 월 1~2천 엔(1~2만 원)정도부터 이용가능한 MVNO 서비스를 통해 이용자가 저렴한 가격으로 안심하고 안전하게 이용할 수 있는 환경을 실현하고자 한다.

– 청소년에 대한 필터링의 제공과 본인확인방법에 관한 구체적인 대응을 촉진

– 청소년과 보호자 등의 스마트폰 활용능력향상을 위해 학교 및 지역 등에서 교육활동 실시

– 스마트폰용 어플리케이션의 프라이버시 보호에 대한 객관적인 기술검증 등을 수행하는 조직의 구축을 위한 실증 및 실험을 실시

※ MVNO(Mobile Vitual Network Operator)는 가상이동통신망사업자로 주파수를 보유하고 있는 이통통신망사업자(MNO: Mobile Network Operator)의 망을 통해 독자적인 이동통신서비스를 제공하는 사업자를 말함

■ (모바일의 고속화) 고속 · 대용량의 새로운 이동통신시스템의 도입으로 원활한 통신환경을 구현하고자 함

– 2016년까지 4G를 상용화하기 위해 올해 안에 3.5GHz(120MHz)할당을 실시

■ **(새로운 모바일 서비스의 창출)** M2M등 모바일통신을 활용한 다양한 서비스를 제공하고자

한다 (전기통신사업법 개정 예정).

– 시장지배적 사업자에 대한 규제를 일부 완화

– 이동통신 네트워크 언번들 (Unbundle)의 촉진

※ MVNO가 MNO의 네트워크를 이용해서 사업전개를 하는 때에 네트워크의 필요한 기능만을 선별하여 저렴하게 이용할 수 있도록 제도 정비

– 신속하게 MVNO에 의한 멀티 캐리어네트워크를 이용한 서비스 등의 실현

※ 멀티캐리어 네트워크는 여러개의 주파수중 속도가 더 빠른 쪽의 주파수에 접속해서 쓰는 기술을 의미함

기대 효과

■ 일본의 모바일 통신은 세계최고수준의 상황이지만, 앞으로 스마트폰의 보급과 트래픽 급증에 대한 대응이 과제가 되고 있으며 소비자의 모바일 통신비 부담을 완화하기 위한 MVNO의 보급 촉진이 기대되고 있다.

참고자료

http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000134.html

http://www.soumu.go.jp/main_content/000320320.pdf

3 호주,「국가안보법」(National Security Legislation Amendment Bill (No. 1) 2014) 개정안 통과 (2014. 10. 01)

개요

■ 호주 안보정보국(Australian Security Intelligence Organisation, ASIO)의 인터넷 감시에 대한 법적 권한을 확대하는 2014년 국가안보법 (National Security Legislation Amendment Bill (No. 1) 2014) 개정법안이 호주 양원에서 통과되었다(2014.10.01.).

– 이 법안은 호주안보정보국 직원이 한 개의 영장으로 호주인들의 인터넷을 감시하기 위해 접근할 수 있는 감시 대상 컴퓨터의 범위를 확대하는 등 법적 권한을 강화하는 내용 때문에 다수 의원들의 우려의 목소리를 고조시켰으나 최종적으로 통과되었다.

■ 이 법안은 국가안보기관들이 호주 안팎으로부터의 테러 위협, 특히 이슬람국가들(Islamic States, 이하 IS국가들)을 기반으로 하는 테러리스트 조직들의 초국경적인 테러 위협에 효율적이고 신속하게 대처할 수 있도록 하기 위한 막강한 테러방지법 개정안으로도 불리고 있으며, 호주의 테러방지법 패키지의 첫 번째 법으로도 알려졌다.

배경 및 경과

■ **(배경)** 호주 의회는 약 60명의 호주 국민들이 시리아와 이라크에서의 테러리스트 활동에 참여하는 것을 목적으로 테러리스트 단체들로부터 전투훈련을 받거나 함께 테러 관련 전투 활동에 참여하고 있으며, 총 150명에 이르는 호주 국민들이 국내 · 외에서 테러활동에 직접적으로 개입하거나 간접적으로는 활동을 위한 자금지원 기타 활동 촉진 및 원활화를 위한 도움을 주고 있다는 문제 상황을 밝혔다.

– 호주의 국내 안보에 가장 큰 위협이 되는 것은 해외에서 훈련을 받은 호주 국적 국민들이 귀국 후 급진적인 성향의 폭력적인 행위를 가해 자국내의 테러 위협이 견고해진다는 위험이 있다.

– 또한 정보통신 기술의 급격한 발전으로 테러리스트 단체 및 개인들은 자신들을 조직화하고, 테러의 위협을 미연에 방지하려는 정부 기관들의 탐지를 따돌리는데 새로운 기술을 사용하는 양상을 보이고 있다.

■ 뿐만 아니라 최근에 국제적으로 세간의 이목을 끌었던 스파이 활동 등 국가안보에 대한 위협에 맞서야 할 필요성이 대두되었으며, 호주의 정보기관들이 이에 효율적으로 대응하고 제대로 기능을 하기 위한 관련 권한을 부여하는 것이 중요해졌다.

■ **(경과)** 2013년 6월 24일 정보안보 양원합동위원회(Parliamentary Joint Committee on Intelligence and Security, PJCIS)는 “호주의 국가안보법제의 잠재적 개혁에 관한 보고서(Report on Potential Reforms of Australia’s National Security Legislation)”를 발표하여 상정하였으며, 동 보고서의 제4장은 관련 법제에 대한 실질적인 한계점들을 다수

지적하였다.

– 이에 따라 정부는 정보법제 개혁에 관해 양원합동위원회가 제시한 22건의 권고사항 중 21건을 정부가 받아들여 이 법안을 제정하였고, 1979년의 호주안보정보국법(Australian Security Intelligence Organization Act 1979)과 2001년 정보서비스법(Intelligence Services Act 2001)을 개정하는 것이다.

■ 국가안보법 개정법 법안은 2014년 7월 16일 상원에 우선 소개되어 9월 25일에 44표의 찬성표와 12표의 반대표로 가결되었다.

– 하원에는 9월 30일에 소개되어 10월 1일에 찬성으로 가결되어 최종 승인을 얻음으로써 양원을 통과하게 되었다.

목적

■ 이 법안은 호주 정보공동체(Australian Intelligence Community, AIC)의 활동을 규율하는 법적 제도를 진화해가는 안보환경에 적합하도록 현대화하고 개선하는 것이다. 이 법제도 중에서 특히 호주안보정보국법(Australian Security Intelligence Organization Act 1979, ASIO Act)과 2001년 정보서비스법(Intelligence Services Act 2001, IS Act)을 개정하는 것을 주요 목적으로 하고 있다.

– 이번 개정 법안은 호주의 정보기관이 테러 관련 조사를 실시함에 있어 컴퓨터 등 인터넷 디바이스에 접근하고 테러 및 간첩 활동에 연루된 호주 국민의 개인정보에 보다 수월하게 접근할 수 있도록 허용하는 내용을 골자로 다루고 있다.

주요 내용

■ 이 법안은 기존의 법에서 고의적인 무권한 통신 및 기밀관련 정보의 취급과 관련하여 규정하고 있는 비밀 유지 관련 범죄를 갱신하고 강화하기 위해 아래의 일곱 가지 주요 분야를 다루고 있다.

국가안보법개정법안의 주요 내용 개관

위치	핵심 내용
Schedule 1	– 호주안보정보국(ASIO)의 고용에 관한 법적 틀을 갱신하여 호주공공서비스(Australian Public Service, APS)의 기준에 보다 근접하도록 현대화함 – 고용 및 기타 관계를 설명하는 관련 용어를 간소화하고 단순화 하며 그 결과로서 영향을 받게 되는 여러 법에도 수정을 가함
Schedule 2	– ASIO의 영장 기반 정보수집 권한을 현대화하고 간소화함 ※ 컴퓨터 접근 영장, 감시 장치, 그리고 안보상 우려를 야기하는 식별된 개인에 대한 영장 등의 권한이 이에 포함됨
Schedule 3	– 적절한 안전장치(safeguard)와 관리와 함께 특수정보활동(special intelligence operations)으로 불리는 비밀정보활동을 수행하기 위한 ASIO의 역량을 강화함 – ASIO 직원 및 ASIO 관계자가 권한을 부여받은 비밀정보활동을 수행하는 중 발생하는 민 · 형사상 책임으로부터 제한적으로 보호함
Schedule 4	– ASIO가 민간부문과 협력하고 수사를 위해 법집행기관과의 정보공유활동을 위한 법적 틀을 명확화하고 개선함 ※ 이러한 정보공유는 신분 비공개 의무를 규정하는 호주안보정보국법(ASIO Act) 제92조의 위반을 법적으로 허용하는 것임
Schedule 5	– 정보서비스법(IS Act)을 개정하여 호주비밀정보서비스(Australian Secret Intelligence Service, ASIS)로 하여금 제한된 상황에서의 호주 국민들에 대한 정보의 생산과 관련하여 ASIO와 협력하는 새로운 기능을 임무로 부여하는 등 위 법과 관련된 기관들의 역량을 강화함 – 호주비밀정보서비스(ASIS)가 자신의 업무상 안보를 보호할 수 있도록 하는 장관의 승인에 대한 새로운 근거를 마련하고 특정 개인을 대상으로 무기 및 자기방어 기술의 사용을 훈련시킬 수 있도록 함 – 또한 정보서비스법의 기관들의 해외활동 관련 행위에 대한 면제를 확대하고 통제된 환경에서의 무기 또는 자기방어 기술의 예외적 사용을 허용하며 이에 대한 지원을 제공하기 위한 국방부의 국방화상및지리공간정보기구(Defence Imagery and Geospatial Organisation, DIGO)의 권한을 명확화 함
Schedule 6	– 두 개의 범죄 규정을 마련하고 기존의 범죄 규정을 갱신함으로써 기밀관련 정보의 보호를 향상함 ※ 기존에 정보서비스법과 호주안보정보국법에 규정되어있던 범죄에 대한 형량을 높인 것이 하나의 예임
Schedule 7	– 국방 기관들의 역할을 보다 잘 나타낼 수 있도록 명칭을 바꿈 ※ 국방화상및지리공간정보기구(DIGO)를 호주지리공간정보기구(Australian Geospatial Intelligence Organisation, AGO)로 개명하고 국방신호국(Defence Signals Directorate, DSD)을 호주신호국(Australian Signals Directorate, ASD)으로 개명함

평가

- 호주의 국가안보법제를 개혁하기 위한 기존 관련법의 개정은 정보당국이 자국의 국가안보에 대응을 잘 할 수 있도록 할 것이라는 찬성 입장과 정보 폭로에 대한 새로운 벌칙조항을 삽입하거나 특수 기밀작전의 공개 등 관련해 언론의 자유를 지나치게 침해한다는 반대 입장이 팽팽하게 맞서고 있다.

- **(찬성)** 법안을 찬성하는 입장에서는 위험한 시기에 호주 국민을 보호하기 위해 반드시 필요하다고 본다.

- **(반대)** Schedule 3에서 규정하는 특수정보활동(special intelligence operations) 중 발생하는 행위에 대한 민 · 형사상 면책 조항은 남용될 가능성이 있다는 우려가 법조계를 중심으로 제기되고 있으며, Schedule 2의 규정으로 인해 단 한 개의 영장만으로 폭넓은 범위의 컴퓨터와 네트워크 전부를 감시할 수 있는 권한이 주어진다는 점에 대해서도 지나치게 감시 대상이 넓다는 우려가 있다.

- **(정부)** 정부는 기존의 법을 개선함으로써 정보기관들이 호주의 국내 안보에 대한 현재와 미래의 위협에 대응할 수 있는 강력한 권한을 마련해주고 정보기관들의 완전성과 소속 직원들의 개인적인 안전도 보다 잘 보호할 수 있으며 정보기관들 간의 업무 협력을 강화 및 증진 할 수 있을 것으로 전망하고 있다. 또한 언론의 자유를 통제한다는 의견에 대해 이번 개정안은 언론의 자유를 억압하기 위한 것이 아니며 일반적인 정보기관의 활동이 아닌 비밀리에 진행되는 작전 등을 폭로하는 경우에 대한 처벌을 규정한 것이라고 반박하고 있다.

참고자료

http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=s969

http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fs969_ems_2dbf9bb1-59cd-44ed-8e6a-d106c5535c72%22

http://www.itnews.com.au/News/396365,parliament-passes-law-to-let-asio-tap-entire-internet.aspx

http://www.legislation.sa.gov.au/Web/Information/Understanding%20legislation/UnderstandingLegislation.aspx#bills

4 독일 연방 내무부, 형사소송기록의 전자화를 위한 법률안 입법예고 (2014.10.08.)

개요

■ 독일 연방법무부는 형사소송기록을 전자로 작성하게 하는 '형사소송기록의 전자화를 위한 법률'[1]을 입법예고 하였다(2014. 10. 8.). 이 법률안은 소송기록의 전자화와 수사기관 및 형사법원 사이의 형사소송기록의 전자적 교류에 관한 규정을 포괄적으로 두고 있다.

■ 이 법률은 11개의 관련 법률[2]을 개정하는 옴니버스 법률이다. 그 중에서 형사소송기록의 전자화에 관한 기본 조항들은 형사소송법에 규정되어 있고, 다른 법률들은 이 기본조항과 관련이 있거나 이와 달리 특별한 경우 관련 조항들을 제 · 개정하고 있다.

■ 따라서 이 법률이 발효되면 수사기록을 포함한 모든 소송기록은 원칙적으로 전자적으로 작성되어 제출되어야 한다. 다만 예외적으로 경과규정에 의하여 각 주는 2024년 1월 1일까지 형사소송기록의 전자화를 단계적으로 도입해야 한다.

※ 전자소송기록의 작성이란, 형사소송에서 여러 규정에 관련되는 '기록'의 형식을 변경하는 것으로 종이문서가 아닌 전자적으로 저장된 데이터를 개념화한 시스템을 말한다.

입법 배경 및 경과

■ 오늘날 대부분 영역에서 전자문서가 사용되고 있는 반면 형사소송기록은 여전히 종이형식으로 작성되고 있다. 기술 발전으로 인한 매체의 변화에 따라 형사절차에서 전자적 소송기록 방식을 도입하여 형사사법을 현대화할 필요가 있다.

■ 또한 형사소송법의 외부 영역에서 이용되고 있는 기술과 비교를 해 볼 경우 개정의 필요성이 더욱 시급하다. 종이형태의 소송기록의 우편 전송 및 열람의 경우에 경제적 비용과 시간이 낭비되며 특히 보관에도 어려움이 있기 때문이다.

1 Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen

2 형사소송법, 형사소송법시행법, 문서보관법, 형집행법, 형법, 질서위반법, 소송비용법, 가사소송비용법, 비송사건절차비용법, 사법행정비용법, 법원과 전자적 교류를 촉진하기 위한 법률.

■ 다만, 이러한 형사소송기록의 전자화를 위해서는 법적 토대가 요구된다.

– 이 법률안은 절차법의 관점에서 본 것이 아니므로 기술적 · 관리적 규정을 상세히 정하는 것을 의도적으로 배제하고 구체적인 내용은 법규명령(시행령이나 시행규칙)을 통하여 제정하기로 하였다.

– 형사소송법 규정들은 전자 기록 작성의 필요성의 관점에서 적합해야 한다. 즉 형사소추기관과 법원 사이의 전자문서의 전달은 매체의 혼란을 막기 위해서 기존의 접근 장애를 제거하여 새로이 규정하여야 한다.

■ 전자적 기록 작성으로 나타나는 자동적인 개인정보의 처리는 종이기반의 기록 작성과 비교하여 본질적으로 훨씬 간편하고 신속하게 데이터를 조사하고 필터링하거나 결합시킬 수 있다. 하지만 형사절차 관계자의 기본권(정보자기결정권)을 헌법에 합치하도록 형사절차 내부의 데이터보호규정들 뿐 아니라 절차법을 넘어서 특수한 영역에도 데이터보호규정이 적용되어야 한다.

주요 내용

■ **(새로 도입되는 규정)** 형사소송법에 새로 도입되는 규정들은 형사소송법 제1편 제4장의 소송기록 작성 및 절차상 고지와 관련한 제32조 내지 제32조g 그리고 제8편 제4장 전자기록에서 개인관련 데이터의 보호 및 전자기록으로부터 개인관련 데이터의 이용과 관련한 제496조 내지 제499조이다.

■ **(전자 기록 작성 및 통지)** 제32조 내지 제32조g는 형사절차에서 전자 기록 작성 및 통지에 관한 규정들이다. 이 규정들은 수사절차에서 형 집행절차에 이르는 전체 형사절차에 적용되는 것으로 형사소송법 제1편 (총칙 규정)에 독자적인 장으로 규정되어 있다.

– 전자기록 작성과 관련한 그밖의 규정들은 다른 장에서 규정하고 있는데 가령 증거조사에 있어서 전자문서의 취급에 관한 규정들의 경우 형사소송법 제244조 제5항, 제249조 제1항, 제256조 및 제325조 그리고 기록에 있어서 개인관련 데이터의 보호 등에 관한 규정 (형사소송법 제496조 이하) 등이 있다.

개정 규정

제32조 (전자소송기록 작성; 규칙제정권한)

① 소송기록은 전자적으로 작성된다.

② 연방정부와 주정부는 자신들의 영역을 위하여 법규명령을 통하여 전자적 기록 작성에 적용될 기술적 관리적 기본조건과 데이터보호, 데이터의 안전 그리고 장애 없는 접근에 준수되어야 할 요건들을 정한다. 연방정부와 주정부는 법규명령을 통한 수권을 연방 및 주의 관할 장관에 위임할 수 있다.

③ 연방정부는 연방상원의 동의를 얻어 법규명령을 통하여 연방 및 주의 관청 및 법원 사이에 전자소송기록의 전달을 위해서 적용되는 기준을 정한다.

1. 일부 주민에 대한 증오심을 선동하거나 그에 대한 폭력적 · 자의적 조치를 촉구하는 행위
2. 일부 주민을 모욕 또는 악의로 비방하거나 허위사실에 의하여 명예를 훼손함으로써 인간의 존엄을 침해하는 행위

– 제32조는 형사사건을 전자문서로 작성하도록 의무를 정한다. 이 규정은 기술과 관리에 요구되는 기본조건에 관한 법규명령을 제정할 권한을 부여하고 있다.

– 제32조 제1항은 형사절차에 관계있는 연방 및 각 주의 모든 관청 및 형사법원에게 형사기록을 전자적으로 작성할 의무를 부과하고 있다. 이 조항은 지금까지 종이형태로 작성되었던 기록을 전자 기록으로 대체하여 수사절차에서 형집행절차에 이르기까지의 전 형사절차에 적용된다.

개정 규정

제32조a (관청 및 법원과의 전자적 법적 거래, 법규명령 권한)

① 전자문서는 관청 또는 법원의 경우 다음 각 항의 기준에 따라서 제출되어야 한다.

② 연방정부는 연방상원의 동의를 얻어서 법규명령을 통해서 전달 및 처리에 적합한 기술적 기본요건들을 정한다.

③ 서면으로 작성, 서명 또는 기명해야 하는 문서는, 처리책임자의 인증된 전자서명이 있는 전자문서로 제공되거나 처리책임자에 의해서 서명되어 안전한 방법으로 제출되어야 한다.

④ 안전한 전달방법이란 다음 각 호의 하나에 해당하는 것을 말한다.

1. 발송자가 내용의 발송에서 데메일법(De-Mail-Gesetz)[3] 제4조 제1항[4] 제2문에 의하여 안전하게 신청되고 제5조 제5항[5]에 의해 안전한 신청이 증명된 경우의 데메일(De-Mail) 계정의 우편사서함서비스 및 발송서비스.

2. 연방변호사규정 제31조a에 의한 특정한 전자적 변호사사서함 또는 이에 상응한, 법률적 근거에서 설치된 전자 사서함 그리고 관청이나 법원의 전자 우편처(취급처) 사이의 전달방법.
3. 신원확인절차의 이행에 의해 설치된 관청이나 공법상 법인의 사서함 그리고 법원의 전자적 우편처 사이의 전달방법; 상세한 내용은 제2항 제2문의 법규명령에서 정한다.
4. 데이터의 진정성과 무결성 및 장애없는 접근이 보장되는, 연방상원의 동의를 얻은 연방정부의 법규명령을 통해서 규정된 그밖의 연방차원의 전달방법.

⑤ 전자문서는 수신자에게 관청 또는 법원의 특정된 시설에 저장되는 순간 도달된다. 발송자에게 자동적으로 도달 시간에 관한 증명이 전달되어야 한다.

⑥ 전자문서가 관청이나 법원을 통해서 처리를 하기에 적합하지 않는 경우에는, 이를 발송자에게 도달이 효과 없음을 언급하고 유효한 기술적인 기본요건을 지체 없이 통지해야 한다. 전자문서는, 발송자가 그것을 지체없이 관청이나 법원이 처리하기에 적합한 형식으로 추가하여 제출하고 먼저 제출한 문서와 내용적으로 일치하는 것이 신뢰할 만한 경우에는 이전의 제출의 시점에 도달한 것으로 본다.

– 제32조a는 법원이나 검찰에 다른 절차 관계인이 제출하는 전자문서의 도달에 관해서 규정하고 있다. 이 조항은 현행 형사소송법 제41조a[6]를 대신해서 들어왔고 민사소송법

3 데메일법(De-Mail-Gesetz)란 인터넷상에서 메일이나 문서를 법적 구속력이 있고 비밀이 보장되도록 전송할 수 있는 독일의 새로운 전자우편제도에 관한 법률로서 데메일서비스제공자 및 그가 제공하는 서비스를 규제하고 있다(2011.4.28 발효). 데메일법에 의한 '데메일서비스'란 '인터넷상에서 누구에게나 안전하고, 신뢰할 수 있고, 증명이 가능한 거래를 확보할 수 있도록 하는 전자통신 플랫폼에 관한 서비스'를 말한다(동법 제1조 제1항). 이 법률에 의한 데메일서비스를 제공하는 사업자는 데메일서비스가 안전하게 신청되어야 하고, 안전한 전자 우편을 위한 우편함서비스와 전송서비스를 이용하고 기록서비스를 이용할 수 있도록 해야 하며, 그 밖에 신분증명서비스와 문서보관서비스도 가능할 수 있도록 해야 한다. 데메일법에 대한 자세한 내용은, 박희영, 데메일법(De-Mail_Gesetz) 제정 : 독일의 새로운 전자우편서비스제도, 법제처 월간 법제, 2011.04, 46-63.

4 데메일법 제4조(데메일계정의 신청) 제1항 : 서비스제공자는 이용자의 데메일계정과 개별서비스를 안전하게 신청하도록 한다. 그렇게 하기 위해서 우선 서비스제공자는 이에 대한 적합한 절차를 진행한 이후에 이용자의 신청을 받게 된다. 그 절차의 적합성은 무권한 이용에 대해서 두 개의 서로 다른 보안수단을 통해서 보호되거나 절차와 관련하여 이용된 비밀의 준수와 유일성이 확보되는 경우에 있게 된다. 이용자는 자신의 데메일계정 신청 시 안전성이 유지되도록 서비스제공자에게 요청할 수 있다. 서비스제공자는 이용자가 데메일계정을 처음으로 이용하기 전에 안전한 신청의 가능성과 그 의미에 대하여 이용자에게 정보를 제공해야 한다.

5 데메일법 제5조 (전자우편함서비스 및 전송서비스) 서비스제공자는 이용자가 제4조에 의한 안전한 신청을 통신에서 증명하게 하여 증명에 거짓이 없음을 언제나 조사할 수 있도록 하여야 한다. 통신의 수신자에게 이것이 인식되도록 하기 위해서 송신자의 서비스제공자는 제4조에 의한 안전한 신청의 사용을 인증된 저자서명을 통하여 증명해야 한다.

6 형사소송법 제41조a(전자문서) ① 법원 또는 검사를 수신자로 하는 의사표명, 신청 또는 그 이유서 가운데 본 법률이 명시적으로 서면으로 작성하거나 서명을 요한다고 규정한 경우 서명법에 따른 특수한 전자서명을 구비하고 법원이나 검사가 처리하기에 적절한 때에는 전자문서의 형태로 제출할 수 있다. 본조 제2항에 따른 법규명령의 범위 내에서 특수한 전자서명 이외에도 전달된 전자문서의 진실성과 진정성을 보장하는 다른 확실한 절차도 허용될 수 있다. 전자문서는 법원과 검사의 수신 장치에 해당 문서가 기록되는 즉시 도달한 것으로 본다. 전달된 전자문서가 이를 처리하기에 적절하지 않은 경우에는 수신자에게 처리를 위해 적절한 기술적 조건과 함께 이를 즉시 통보해야 한다. 전자문서는 지체 없이 인쇄하여 기록문서로 만들어야 한다. ②연방정부와 주정부는 법규명령을 통해 법원과 검찰에 전자문서 제출이 가능하기 시작하는 시점 및 문서처리의 적절한 형태를 정한다. 주정부는 법규명령을 통해 주

제130조a[7]와 상응한 규정이다. 2002년 7월 1일부터 검찰과 법원은 전자적 방식으로 송달을 하거나 관계인에게 송달의무가 없는 문서를 전달하는 것을 허용해 왔기 때문에 법무부의 내부 통신은 이 규정에 의해서 포섭되지 않는다.

개정 규정

제32조b (전자적 양식, 법규명령 권한)

연방정부는 연방상원의 동의를 얻어서 법규명령을 통하여 전자적 양식을 도입할 수 있다. 이 양식에 포함된 정보의 전체 또는 일부는 구조적으로 기계가 읽을 수 있는 형식으로 전달될 수 있도록 규정할 수 있다. 양식은 법규명령에 규정될 인터넷 통신플랫폼에서 이용할 수 있도록 제공되어야 한다. 법규명령은 제32조a 제3항과 달리 양식이용자의 신원확인은 주민등록법 제18조 또는 외국인 체류법 제78조 제5항에 의한 전자적 신원증명의 이용을 통해서 행해지도록 한다. 연방정부는 법규명령을 통하여 권한을 관할 연방장관에게 위임할 수 있다.

– 제32조b는 법원의 절차 진행과정의 간편화와 표준화를 위하여 연방정부가 연방상원의 동의를 얻어서 법규명령을 통하여 법원의 절차를 위하여 전자적 양식을 도입하는 가능성을 규정하고 있다. 이 양식들은 누구나 무료로 법규명령에 규정될 통신플랫폼에서 이용할 수 있어야 한다. 구조적 데이터의 전달을 통해서 IT의 지원을 받은 서류(사건)의 처리는 미디어의 융합과는 상관없이 관청과 법원에 원활히 되어야 한다.

– 따라서 수많은 법원의 절차과정은 효율적으로 구축될 수 있다. 가령 고소장이나 고발장의 제출, 증인에 대한 보상 청구나 약식명령에 대한 이의제기의 제출은 웹의 양식으로 행해질 것이다.

사법행정부에 관련 권한을 위임할 수 있다. 전자형태의 허가는 특정 법원, 특정 검찰 또는 특정 절차에 국한될 수 있다.

7 민사소송법 제130조a (전자문서) ① 준비서면 및 첨부서, 당사자의 청구서 및 의사표명, 제3자의 정보, 진술, 감정 및 의사표명을 위해서 문서형식이 제출되는 한, 법원을 통하여 처리하기에 적합한 경우에는 전자문서로의 기록은 이 문서형식을 충족한다. 책임자는 이 문서에 서명법에 의해 인증된 전자서명을 갖추어야 한다. 전달된 문서가 법원이 처리하기에 적합하지 아니한 경우에는 이것은 발송자에게 유효한 기술적 조건에 관한 정보를 제공하여 지체 없이 통지하여야 한다. ② 연방정부 및 주정부는 자신들의 영역을 위하여 법규명령을 통하여 전자문서가 법원에 제출될 수있는 시점 및 문서 처리에 적합한 형식을 정한다. 주정부는 법규명령을 통하여 주 사법행정부에 수권을 위임할 수 있다. 전자적 형식의 허용은 개별 법원이나 절차로 제한될 수 있다. 이 규정은 2013.10.10. 법원과의 전자적 법적 거래를 촉진하기 위한 법률의 개정으로 도입되었다. ③ 전자문서는 수신자가 특정된 법원의 시설에 그것이 기록되는 즉시 도달된다.

개정 규정

제32조c (공공기관 및 법원의 전자문서)

① 공공기관 또는 법원의 문서가 전자문서로 작성된 경우에는 모든 처리책임자는 자신의 성명을 거기에 기재해야 한다. 서면으로 작성되거나 서명되거나 기명되어야 하는 문서는 그 외에 모든 처리책임자의 인증된 전자서명을 갖추어야 한다.

② 제1항의 전자문서는 그것이 처리책임에 의해서 또는 처리책임자의 원인으로 전자 기록으로 저장되는 즉시 기록으로 된다.

– 제32조c는 공공기관과 법원에 의해서 작성된 전자문서의 진정성과 무결성의 확보에 관한 요건을 규정하고 있다. 또한 이 규정은 그러한 문서가 기록으로 되는 시점을 규정하고 있다. 특히 이것은 판결 시에 중요한 의미를 가진다. 공공기관이나 법원의 문서를 전자적으로 작성할 법적 의무는 제32조b는 근거가 되지 못한다.

개정 규정

제32조d (전자문서의 제출 의무)

공소장, 공판절차 외에서의 약식명령의 청구서, 사소제기, 항소와 이의 정당성, 상고와 이의 근거 및 반대진술서가 검사, 변호인 또는 변호사를 통해서 제출되는 경우에는 전자 문서로 전달되어야 한다. 이것이 기술적인 이유로 일시적으로 가능하지 않는 경우에는 종이 형태의 전달이 가능하다. 일시적인 불가능이란 대체 제출이나 지체 없이 이에 대해서 신뢰할 수 없는 경우이다. 요청에 의해서 전자문서는 사후에 제출할 수 있다.

– 제32조d는 검사나 변호인 및 변호사에게 전자문서의 제출 의무를 도입할 것을 제안하고 있다. 물론 이것은 형사절차의 특수성 때문에 제1문에 열거한 절차 설명서로 제한되어야 한다. 이용의무는 그러한 서면에 의한 설명서를 위해서 존재해야 한다. 전자적 통신을 위해서 필요한 인프라에 하자가 있을 수 있는 특별한 긴급한 상황에서(예를 들어 공판기일에 제출되어야 하는 경우)는 배제된다.

– 제32조d는 이용의무를 처음부터 검사, 변호인, 변호사로 제한하고 있다. 피의자는 스스로 대리하지 않는 사소제기자 및 그밖의 절차 관계인과 같이 문서를 전자적으로 제출할 의무가 없다.

개정 규정

제32조e (기록 작성 목적으로 문서의 전달)

① 기록으로 될 형식에 맞지 않는 문서(초기문서)는 상응한 형식으로 전달될 수 있다. 증거방법으로써 보전된(확보된) 초기문서는 상응한 형식으로 전달될 수 있다.

② 전달의 경우 기술의 수준에 따라 확보되어야 한다. 전달된 문서는 초기문서와 형식상(화상) 및 내용상 일치하여야 한다.

③ 비전자적 초기문서의 전달의 경우 전자적 문서의 전달에 있어서 어떠한 절차들이 이용되었는지 기록되어야 한다. 전자적 초기문서의 전달의 경우 초기문서의 진정성 및 무결성의 심사가 어떠한 결과를 도출하였는지가 기록되어야 한다.

④ 증거방법으로 확보되지 않는 초기문서는 절차 진행 동안 전달 후 적어도 6개월 저장되거나 보관되어야 한다. 이것은 늦어도 시효가 만료되는 해의 말까지 보관될 수 있다. 절차가 종결된 경우 증거방법으로 확보되지 않은 초기문서는 늦어도 절차의 종결로 해당하는 해의 종료 시까지 저장되거나 보장될 수 있다.

⑤ 증거방법으로 확보되지 않는 초기문서는 확보된 증거수단과 같은 동일한 조건에서 열람될 수 있다. 기록을 열람할 권한이 있는 자는 증거물을 열람한 권한이 있다.

– 제32조e는 형사절차에서의 통신(고지)은 장래에도 오로지 전자적으로만 행해지지 않는다는 상황을 고려하고 있다. 종이 매체의 의미가 점차로 줄어든다는 것이 기대된다 하더라도, 전자문서로 이를 완전히 대체하는 것은 현재로서는 예상하기 어렵기 때문이다.

– 따라서 제1항 제1문은 기록이 작성되는 형식으로 존재하지 않는 문서의 전환의무를 규정하고 있다. 이것은 무엇보다 기록 작성을 위해서 적합한 포맷이 존재하지 않는 전자 문서 외에, 종이 형태의 접수를 포섭한다.

– 제2항 내지 제4항은 종이문서에서 전자문서로의 전환절차에서 준수되어야 할 기술적 관리적 요건 및 사건의 문서화를 위해서 필요한 정보를 규정하고 있다. 제4항은 변환에 의한 초기문서의 보관 또는 저장을 규정하고 있다. 제5항은 이 초기문서의 폐기권한을 두고 있다.

개정 규정

제32조f (기록열람의 허용 형식)

① 전자소송기록의 열람은 (인터넷) 호출에 대하여 기록이 제공될 수 있다. (오프라인) 청구에 대한 기록열람은 서비스 제공 공간(민원실 등)에서 전자적 재현을 통해서 허용된다. 기록의 출력은 청구인이 이에 대해 정당한 이익을 설명한 경우 청구에 의해서만 제공된다. 제3항의 결정에

대해서는 불복할 수 없다.

② 아직 종이형태로 존재하는 기록의 열람은 서비스제공 공간에서 열람할 기록을 제공함으로써 허용된다. 변호인 또는 변호사가 신청을 한 경우의 기록열람은 자신의 사무실에서 기록을 가져가도록 교부하거나 발송을 통해서 허용된다. 제1문 또는 제2문에 의한 열람이 특정된 형식의 열람과 모순되는 중요한 근거가 있는 경우, 기록 열람 등본의 교부를 통해서 허용된다. 제3문의 결정에 대해서는 불복할 수 없다.

③ 제3자가 기록열람과 관련하여 기록의 내용을 인지할 수 있는 것은 기술적 관리적 조치를 통해서 보장되어야 한다. 신청인의 성명은 기술적 조치를 통해서 호출된 기록과 전달된 전자적 문서에서 영구적으로 알 수 있어야 한다.

④ 청구인은 제1항 또는 제2항에 의해서 그에게 허용되어 있는 기록, 문서, 출력물 또는 등본의 전부 또는 일부를 공중에게 유포하거나 제3자에게 절차와 무관한 목적으로 전달하거나 접근하게 해서는 안 된다. 제1항 또는 제2항에 의해서 획득된 개인 관련 데이터를 신청인은 기록열람이 허용되는 목적으로 이용할 수 있다. 신청인은 목적 구속성에 대해서 통지받아야 한다.

– 제32조f는 변호인(제147조 제1항 내지 제3항), 피고인(제147조 제4항), 관계인(질서위반법 제49조 제1항), 사소제기자(형사소송법 제385조 제3항), 부대사소제기 및 피해자(형사소송법 제406조e), 질서위반금 관련 법인 또는 인적 단체(제444조 제2항 제2문), 사인 및 그밖의 기관(제475조 제2항), 형집행 중에 있는 자(형사소송법 제147조 제4항과 관련한 형집행법 제120조)의 소송기록 열람 및 사법기관 및 그밖의 공공기관(제474조 제1항)의 소송기록 열람을 규정하고 있다.

– 제32조f는 기록의 열람 형식만을 규정하고 있다. 규정의 적용은 오히려 앞서 언급한 규범들을 근거로 이미 열람의 허용 여부에 대한 공공기관이나 법원의 결정이 존재하는지가 요건이 된다. 제1항은 전자 기록의 열람 형식을 정하고 제2항은 종이 기록의 열람을 정하고 있다. 종이 기록의 열람에 대한 규정은 전자 기록 작성이 될지라도 필요하다.

– 형사소송법 제32조f 제3항은 보충적으로 특별히 데이터보호법상의 규정을 전자적 소송기록 작성을 위해서 포함하고 있다. 제32조 제2항 1문은 특별히 데이터보호를 위한 상세한 규정들을 포함하여야 하는 법규명령의 제정을 포함하고 있다.

– 제3항은 전자적 소송기록의 경우 제8편 제2장(데이터에 대한 규정)의 의미의 데이터와는 다르다. 제2장의 규정은 1999년 형사절차변경법(BGBl. 1 S. 1253)을 통하여 2000년 8월 2일에 도입된 데이터 규정이다.

※ 제2장의 데이터에 대한 규정으로는 형사절차의 목적을 위한 정보처리(제483조), 형사절차를 위한 정보의 이용(제484조), 기록의 정리(제485조), 공동데이터(제486조), 저장된 정보의 제공(제487조), 자동화된 정보전달(제488조), 저장된 정보의 전달, 삭제 및 차단(제489조), 자동화된 데이터에 대한 설비명령(제490조), 당사자에 대한 정보제공(제491조) 등이 있다.

– 이 규정은 특히 소송기록으로부터 개별적인 개인관련 데이터를 가진 등록부의 운영을 위한 데이터보호법상의 근거를 둘 필요성이 있었다. 데이터 규정들과 관련되는 이러한 보조 데이터들의 경우 소송 기록 자체로 보지않고 이와 상응한 소송기록에 적용되는 규정들과 구별되는 데이터의 처리 및 삭제에 관한 규정들을 포함하고 있다. 따라서 이 규정들은 전자적 소송기록에는 적용되지 않는다는 것을 명확히 했다.

개정 규정

제32조g (등본의 교부)

등본 및 공증된 등본은 종이형태로 또는 전자문서로 교부될 수 있다. 제32조c 제1항 제2문, 제32조e 제3항 제2문은 공증된 등본에 대해서도 준용한다.

– 제32조g는 등본 및 공증된 등본이 종이 형태로 출력되는 것 뿐만 아니라 전자문서로 제공될 수 있음을 규정하고 있다. 전자문서가 종이형태로 출력되는 경우, 전자문서의 진정성과 결함이 없다는 심사 결과가 출력물에 표시되어야 한다. 이는 전자서명법에 의한 공인된 전자서명을 통해서 확보되어야 하며 등본 및 공증된 등본의 제공은 이의 형식의 면에서 전자기록 작성의 경우 특수성을 보이지 않는다.

개정 규정

제496조 (전자적 소송기록에서 개인 관련 데이터의 이용)

① 형사절차적 목적인 경우 전자 소송기록에서 개인관련 데이터의 처리와 이용은 허용된다.

② 전자 소송기록을 작성하는 경우

1. 데이터 보호와 데이터 안전성을 위한 특별한 요구사항을 준수하기 위하여 필요한 조직적 관리적 조치를 취해야 하고,
2. 정당한 데이터 처리의 기본원칙을 준수하여야 한다. 특히 데이터가 항상 이용할 수 있도록 유지되어야 하고 데이터의 유실에 대한 조치를 취해야 한다.

③ 전자적 소송기록은 제2장에서 규정하고 있는 의미의 데이터가 아니다.

– 제496조는 전자적 소송기록의 작성에 있어서 데이터보호를 위한 특수한 영역의 조항들을 규정하고 있다. 개인관련 데이터의 수집, 처리 및 이용은 법률규정이 이를 허용하고 있거나 당사자가 동의한 경우에만 허용된다(연방데이터보호법 제4조 제1항). 따라서 제1항은 전자적 소송기록에 있어서 개인 데이터의 처리 및 이용에 대한 허락을 규정하고 있다. '처리'란 개인관련 데이터의 저장, 변경, 전달, 차단 및 삭제를 말하고, 이용은 처리에 문제가 되지 않는 한 개인 관련 데이터의 모든 사용을 말한다.

– 제1항의 허가는 개인관련 데이터의 수집은 포함되지 않는다. 개인 데이터의 수집에 대해서는 형사소송법은 수많은 일반적인 권한규정(제161조,[8] 제163조[9])과 특별한 권한규정(제94조 이하,[10] 제100조a 이하,[11] 제163조a 이하[12])이 있다. 제1항은 이들 권한에 영향을 주지 않는다.

– 전자적 소송기록에서 개인관련 데이터의 처리 및 이용을 위한 허가는 이것이 구체적이고 개별적인 형사절차의 목적에 필요한 경우에 한해서만 적용된다. 개별적인 형사절차의 목적을 넘어서는 일반적인 목적, 특히 절차를 초과하여 전자적 소송기록에서 정보의 사용을 위해서 이것은 허용되지 않는다.

– 소송기록이 진실되고 명확하며 완전하기 위한 원칙은 기본법 제20조 제3항에서 도출되는 법적안정성에 따라서 공공기관 또는 법원의 절차상 기록들에서 개인관련 데이터의 삭제는 (형사소송법 제101조 제8항[13]과 같은 특별한 법률 규정에 상관없이) 더 이상 기록이 필요하지 않는 경우에만 행해진다.

※ 다만, 보관해야 할 중요한 규정들은 문서보관법이 적용된다. 이 법률은 '소송기록보관 및 소송기록 저장법'으로 개정되어 소송기록에 있어서 정확하지 않은 데이터는 상응한 표시를 통해 수정되어야 한다. 이 경우 전자적 소송기록에서 정당한 데이터가 확보되어야 한다.

◆◆

8 형사소송법 제162조(수사; 비밀수사로 획득한 정보의 사용)

9 형사소송법 제163조(경찰의 임무)

10 형사소송법 제94조(증거대상의 보전), 제95조(제출 및 인도의무), 제96조(공문서의 예외), 제97조(압수금지대상), 제98조(압수명령), 제98조a(데이터 비교조사를 통한 수사), 제98조b(명령과 집행), 제97조c(데이터 비교조사), 제99조(우편물의 압수), 제100조(관할).

11 형사소송법 제100조a(통신감청), 제100조b(명령 및 이행), 제100조c(주거 감청), 제100조g(통신사실확인자료 조사), 제100조j(IMSI 캐처) 등.

12 형사소송법 제163조a(피의자신문), 제163조d(신원확인), 제163조d(데이터의 저장) 등.

13 형사소송법 제101조(통지; 개인관련 데이터의 삭제) ⑧ 처분을 통해 획득된 개인관련 데이터가 형사소추 및 처분에 대한 법원의 심사를 위해 더 이상 필요하지 않게 된 때에는 이를 즉시 삭제해야 한다. 삭제 사실은 문서로 기록한다. 삭제가 오로지 처분에 대한 법원의 심사로 인해 유예된 경우에 당해 데이터는 오로지 이 목적을 위해서만 당사자의 동의 없이 사용할 수 있다. 이에 준하여 데이터에의 접근을 차단한다.

– 제2항에 의한 조치들은 일반적으로 개인의 민감정보를 포함하고 있기 때문에 특별히 높은 보호가 요구된다. 또한 이들 데이터는 대부분 관련자의 동의 없이 수집에 대한 권한 규정을 토대로 수집되므로 연방데이터보호법 제3조 제9항에서 의미하는 '특별한 종류의 개인관련 데이터'로 다루어진다. 이러한 데이터는 인종적 민족적 기원, 정치적 성향, 종교적 또는 철학적 확신, 노조가입, 건강 또는 성생활 등에 관한 정보를 포함한다. 이를 공개하는 경우에 개별 피고인뿐만 아니라 증인, 범죄피해자 그리고 무관한 제3자도 관련되기 때문에 당사자의 정보자기결정권이 중대하게 침해된다.

– 이러한 조치들은 데이터보호를 위해 다른 규정(예를 들어 형사소송법 제68조 제5항)[14]에 포함된 특별 규정에 상응하도록 보장되어야 한다. 현재의 기술 수준에 맞추어 연방데이터보호법 제9조 제1문의 별지에 상응한 조치가 요구된다. 동법 제9조[15]는 데이터 처리에 있어서 기술적 관리적 조치를 취하고, 특히 이 조항의 부칙에서 정한 요건이 보장되도록 정한다. 부칙이 요구하고 있는 조치들은 출입통제, 접속통제, 접근통제, 전달통제, 입력통제, 위탁통제, 처분통제를 위한 조치 및 다양한 목적으로 수집된 데이터는 분리되어 처리될 수 있도록 보장하는 조치들이다.

– 또한 제2호에 의한 합법적인 데이터처리를 해야 한다. 특히 데이터의 분실을 주의해야하며 기술의 상태에 따라서 적응되어야 한다. 미러형 데이터보관(저장), 규칙적인 백업을 통해 안전하게 분리된 장소에서 부당한 접근으로부터 보호하여 보관한다.

14 형사소송법 제68조 (증인신문) ① 증인의 성명, 나이, 신분 또는 직업 및 주소를 묻는 것으로 신문이 시작된다. 증인이 공직에 있었던 경우에는 주소 대신 근무지를 진술할 수 있다. ② 증인이 자신의 주소를 진술함으로써 증인 자신이나 타인을 위험에 빠뜨릴 우려가 있는 경우, 증인이 주소 대신 직장소재지나 근무지 또는 소환장 송달이 가능한 다른 주소지를 진술하도록 허용할 수 있다. 제1문의 요건이 충족되면 재판장은 공판에서 증인이 자신의 주소를 진술하지 않는 것을 허용할 수 있다. ③ 증인이 자신의 신상이나 주소 또는 거소를 공개함으로 인하여 자신이나 타인의 생명, 신체 또는 자유가 위험에 처할 우려가 있는 경우, 증인이 자신의 신상을 진술하지 않거나 과거의 신상만을 진술하도록 허용할 수 있다. 그러나 증인은 공판에서 자신이 증언하는 사실을 어떠한 신분으로 알게 되었는지에 대한 질문에는 답하여야 한다. 증인의 신분확인을 보증하는 자료는 검사가 보관한다. 위험이 사라진 때에 비로소 당해 자료를 소송기록에 포함시킨다. ④ 제2항과 제3항의 요건이 존재한다고 볼 수 있는 충분한 근거가 있을 때에는 증인에게 당해 조항에 정해진 권한을 지적해주어야 한다. 증인의 거주지 또는 신상의 확인을 보장하는 문서는 검찰에 보관한다. ⑤ 제2항 내지 제4항은 증인신문이 종결된 이후에도 적용된다. 증인이 개인 신상정보를 제시하지 않는 것이 허용되는 한, 기록상의 정보나 기록에 대한 열람을 할 때 증인의 신상정보가 다른 사람에게 알려지지 않도록 해야 하지만, 제2항과 제3항에서 의미하는 위태화가 배제되는 경우에는 그렇지 아니하다.

15 연방데이터보호법 제9조 (기술적 관리적 조치) 스스로 또는 위탁에 의해서 개인관련 데이터를 수집, 처리 또는 이용하는 공공기관 및 비공공기관은 이 법률의 규정의 이행을 보장하기 위해서, 특히 이 법률의 부칙에 기술된 요건들을 보장하기 위해서 필요한 기술적 관리적 조치를 취해야 한다. 이들 조치에 드는 비용이 추구하려는 목적과 적정한 관계에 있는 경우에만 이러한 조치가 필요하다.

개정 규정

제497조 (위탁에 의한 데이터 처리)

① 다른 공공기관에 데이터의 처리를 위탁할 수 있다.

1. 공공기관이 출입, 접근, 접속을 사실상 절대적으로 통제하는 시설에 있는 데이터가 처리되는 경우
2. 데이터처리를 위탁받은 비공공기관을 통하여 원격으로 데이터에의 접근과 수탁자 또는 무권한 제3자에게 데이터의 전달이 불가능한 경우

② 다른 기관이 데이터처리시설 또는 자동화 절차를 심사하고, 대기하거나 그밖의 보조활동을 하는 경우에 제1항이 준용된다.

– 형사절차에서의 데이터의 특별 보호 필요성은 위탁에 의한 데이터 처리가 제497조에서 정한 특별한 영역에 적용되도록 규정되어야 하고 이 규정은 제32조 제2항에 의한 법규명령으로 도입될 규정이나 연방데이터보호법의 일반적인 규정들(특히 제11조)[16]과 적용가능한 각 주의 데이터보호법의 규정들 보다 우선하여 적용된다. 이 규정은 소송기록을 작성할 기관이 아닌 다른 데이터 처리자에게 전자적 소송기록을 위탁할 가능성을 규정하고 있다(위탁데이터 처리).

16 연방데이터보호법 제11조(위탁에 의한 개인관련 데이터의 수집, 처리 또는 이용) ① 개인관련 데이터가 다른 기관에 의해서 위탁으로 수집, 처리 또는 이용되는 경우 위탁자는 이 법률의 규정 및 데이터보호에 관한 다른 규정들의 준수에 대하여 책임을 진다. 제6조(정보주체의 권리), 제7조(손해배상청구), 제8조(공공기관을 통한 자동화 데이터 처리에 있어서 손해배상청구)에 언급된 권리들은 위탁자에 대해서 주장될 수 있다. ② 수탁자는 그가 행한 기술적 관리적 조치의 적성을 특별히 고려하여 주의 깊게 선정되어야 한다. 청구는 문서로 제출되고, 특히 구체적으로 다음이 확인되어야 한다. 1. 위탁의 대상 및 기간. 2. 범위, 예정한 데이터의 수집, 처리 또는 이용의 종류와 목적, 데이터의 종류 및 데이터 주체의 범위. 3. 제9조에 의해서 행해질 기술적 관리적 조치. 4. 데이터의 정정, 삭제, 차단. 5. 제4항에 이한 수탁자의 현존 의무, 특히 그에 의해서 행해지는 통제. 6. 하도급 관계의 근거를 위한 권한. 7. 위탁자의 통제 및 이에 상응한 수탁자의 수인의무 및 협력의무. 8. 수탁자 또는 그에게 고용된 자의 개인관련 데이터 보호 규정 및 위탁으로 정해진 사항의 위반에 대한 통지. 9. 위탁자아가 수탁자에 대하여 유보할 지시권한의 범위. 10. 위탁 종료 후 위탁한 데이터저장매체의 반환 및 수탁자에게 저장되어 있는 데이터의 삭제. 수탁자는 공공기관의 경우 전문감독관청을 통해서도 승낙될 수 있다. 위탁자는 데이터처리를 시작하기 전에 그리고 정기적으로 수탁자가 행하는 기술적 관리적 조치의 준수를 확인시켜야 한다. 그 결과는 문서로 기록되어야 한다. ③ 수탁자는 위탁자의 지시와 관련하여서만 데이터를 수집, 처리 또는 이용해야 한다. 수탁자는 위탁자의 지시가 이 법률 또는 데이터보호의 다른 규정에 위반한다고 생각한다면 지체없이 이에 대해서 위탁자에게 알려야 한다. ④ 제5조, 제9조, 제43조 제1항 제2호, 제10호, 제11호, 제2항 제1호 내지 제3호, 제3항, 제44조 외에데이터보호 통제 또는 감독에 관한 규정만이 수탁자에게 적용되고, 1. a) 공공기관, b) 공공기관이 다수의 지분을 가지고 있거나 다수의 결정권을 보유하고 있고 위탁자가 공공기관인 비공공기관에게는 제18조, 제24조 내지 제26조 또는 각 주의 데이터보호법의 상응한 규정들이 적용된다. 2. 그밖의 비공공기관이 서비스업체로서 위탁에 의해서 개인관련 데이터를 영리적으로 수집, 처리 또는 이용하는 경우에는 제4조f, 제4조g 제38조가 적용된다. ⑤⑥ 자동화 절차 또는 데이터처리시설의 심사 또는 점검이 다른 기관에 의해서 위탁으로 처리되는 경우 그리고 개인 관련 데이터에의 접근이 배제될 수 없는 경우에는 제1조 내지 제4조를 준용한다.

– 제1항은 위탁데이터처리에 가능한 수탁자를 규정하고 있다. 공공기관에 의한 위탁데이터 처리 외에도 기본적으로 비공공기관을 통해서도 허용되어야 한다.

– 비공공기관을 통한 위탁에 의한 데이터처리는 두 가지 요건을 동시에 충족되는 경우에만 허용될 수 있다.

※ 데이터는 제1호에 의해서 공공기관이 출입, 접근, 접속을 사실상 절대적으로 통제하는 시설에서 처리되어야 한다. 공공기관은 데이터처리 시설에 대해서 오로지 계약상 근거에서 기인하는 처분권이 아니라 완전한 처분권을 가져야 하며 출입, 접근, 접속을 조종하고, 금지하고, 허용할 수 있어야 한다. 이 공공기관의 처분권한은 다른 사설기관과 나누어서는 안 된다. 데이터의 저장 및 처리 시설은 물리적으로 완전히 공공기관의 영역 내에 있어야 한다. 다만 모든 데이터처리가 사인의 기업의 전산실에서 이루어져 공공기관에 의해서 전혀 관여할 수 없는 클라우드에서 일어나는 것은 배제한다.

※ 또한 제2호에 의해서 데이터처리를 위탁받은 비공공기관을 통한 원거리 데이터의 접근과 그로부터의 전달은 배제된다. 데이터에 대한 원격관리나 그밖의 원격접근은 허용되지 않으므로 사기업은 제1호에 의한 데이터처리 장소에서만 활동할 수 있다. 하지만 데이터처리를 위탁받은 비공공기관이 데이터를 권한 없는 제3자 또는 자신의 영업소 및 데이터처리장소에 없는 자신의 동료에게 전달하는 것은 가능하다. 따라서 인터넷에 대한 접근은 필요한 경우 허용될 수 있고 그렇지 않으면 기술적 조치를 통하여 차단되어야 한다.

– 제2항은 연방데이터보호법 제11조 제5항과 일치한다. 제2항은 위탁데이터 처리의 영역에서 수탁자를 포함한다. 데이터의 처리는 위탁받지 않았지만, 점검서비스, 관리서비스 또는 그밖의 보조 및 지원서비스(예를 들어 하드웨어부품의 점검 및 교체, 소프트웨어의 업데이트 조정)를 통해서 데이터에 접근이 가능할 수 있다. 접근의 범위와 상관없이 그 접근이 배제될 수 없는 경우 가능하고 사실상의 접근이나 기존의 가능성은 필요하지 않다. 이 경우 법적인 보장과 관련한 서비스가 제공되는지는 중요하지 않다.

개정 규정

제498조 (전자 기록으로부터 개인관련 데이터의 이용)

① 법규정이 형사절차에서 개인관련 데이터의 이용을 허용하거나 명령한 경우에는 전자적 소송기록으로부터 개인관련 데이터의 처리와 이용도 허용된다.

② 개별적이고 사전에 개인화되어 있는 기록과 함께 행해지는 한 제98조c에 의한 개인 관련 데이터와 전자 기록의 기계적 비교는 허용되지 않는다.

– 제1항은 전자적 소송기록으로부터 개인관련 데이터의 목적을 변경 가능하게 한다. 하지만 법률규정이 개인관련 데이터의 수집, 처리 및 이용을 형사절차에서 허용하거나 명령한 경우에 한정한다. 특히 전자적 소송기록으로부터 특정한 개인관련 데이터를 추론하는 것이

가능하고 이를 법원사무보조의 기록정리업무의 목적(제485조 제1문)[17]으로 사용할 수 있다. 상응한 법률규정이 있는 경우(예를 들어 제474조)[18] 소송기록이나 특정한 기록의 내용을 다른 기관에 전달하는 것도 허용된다.

– 제2항은 개인관련 데이터를 전자적 소송기록과 일괄적이고 기술적으로만 비교하는 것(형사소송법 제98조c)[19]은 허용되지 않는다. 따라서 전자적 소송기록과 동반해서 나타나는 특별한 사실상의 위험에 대처해야 한다. 종이 기반의 소송기록의 작성의 경우와는 달리 여러 형사 절차 또는 전체 형사 절차의 소송기록을 하나의 데이터로 연결하거나 서로 결합해서 수색(조사)하는 것이 간단하게 가능해진다.

– 관할구역별로 각 주와 연방에서 중앙에 집중시켜서 모든 소송기록을 저장하는 경우 형사절차의 목적을 위해서 언제나 체계적으로 복잡한 전체데이터베이스에 저장된 개인관련 데이터에 관하여 검색조회를 실행할 수 있고 이 경우 피고인뿐만 아니라 그밖의 모든 절차관계인이나 무관한 사람까지도 조회할 수 있다.

개정 규정

제499조 (복제의 삭제)

전자 기록 또는 전자 문서의 복제본(사본)은 더 이상 필요 없는 경우에는 지체 없이 삭제되어야 한다.

---

17 형사소송법 제485조 (기록의 정리) 법원, 집행기관을 포함한 형사소추기관, 보호관찰관, 행장감독을 담당하는 감독청 내지 법원의 사무보조는 기록정리업무의 목적을 위해서 필요한 경우에 한해 정보들 가운데 개인관련 정보를 저장, 변경 및 이용할 수 있다. 제484조에 기재된 목적에 따른 이용도 그 규정에 따라 저장이 허용된 경우라면 가능하다. 제483조 제3항을 준용한다.

18 형사소송법 제474조(사법기관 및 여타 공공기관을 위한 정보제공과 기록열람) ① 법원과 검찰 그리고 기타 사법기관은 사법절차의 목적으로 필요한 경우에는 기록을 열람할 수 있다. ② 또한 다음과 같은 경우에는 공공기관에게 소송기록에 관한 정보를 제공할 수 있다. 1. 정보의 제공이 범죄행위와 관련된 권리관계들을 확정 또는 관철 하거나 보장하는 데 필요한 경우. 2. 이 밖에 형사절차로부터 개인관련 정보를 기관에게 직권으로 전달할 수 있도록 허용하는 특별한 규정이 있는 경우 또는 정보의 전달 이후 추가적인 개인관련 정보의 전달이 그 기관의 과제를 달성하기 위하여 필요한 경우. 3. 보안처분의 준비를 위하여 정보가 필요한 경우로서, 해당 조치 이후에 특별한 규정에 따라 직권으로 당해 기관에게 형사절차와 관련된 정보를 전달하는 것이 허용되는 경우. 국가정보기관에 대한 정보제공은 연방헌법보호법 제18조, 군사비밀기관법 제10조, 연방정보기관법 제8조 및 해당되는 각 주의 법률규정에 따른다. ③ 제2항의 요건 하에서 정보제공에 과도한 비용이 소요될 우려가 있거나, 기록을 열람하고자 하는 기관이 정보를 제공받는 것으로 그 과제를 수행하기에 충분하지 아니할 것이라는 이유를 제시하는 때에는 기록의 열람을 허용할 수 있다. ④ 제1항과 제3항의 경우에는 사법기관이 보관하고 있는 증거물도 열람할 수 있다. ⑤ 제1항과 제3항의 경우 열람을 위해 기록을 송부할 수 있다. ⑥ 의회 위원회에 기록열람권을 허용하고 있는 주법률의 규정에는 영향을 미치지 않는다.

19 형사소송법 제98조c(데이터 비교조사) 범죄를 수사할 목적에서 또는 형사절차를 위해 추적하고 있는 자의 체류지를 확인할 목적에서 형사절차로부터 획득된 신상 관련 데이터를 형사소추, 형집행 또는 위험예방을 위하여 획득된 데이터와 기계적으로 비교조사 할 수 있다. 단 연방의 특별법이나 이에 상응하는 주법이 그러한 데이터사용을 금지하고 있을 때에는 비교조사를 할 수 없다.

– 제499조는 소송기록의 작성을 위한 그밖의 데이터보호규정을 포함하고 있다. 이 규정은 전자적 소송기록의 복제 또는 전자적 문서의 복제가 더 이상 필요하지 않는 한 지체없이 이를 삭제하도록 규정하고 있다. 이것은 특히 전자적 소송기록의 경우 종이기록 작성의 경우와는 달리, 기술적인 문제로 기록의 복제가 남아있는 경우가 있다. 기술적 전환의 개별성에 의존하여 여기서 소송기록의 복제는 전달 후 전달하는 기관에 남아있을 수 있다. 그러한 복제본은 전달이 완료되면 이어서 지체없이 삭제되어야 한다.

참고자료

연방법무부 법률안 :

http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RefE_ElektronAkteStrafsachen.pdf?__blob=publicationFile

2. 판례 및 이슈

1 유럽사법재판소, 상업적 공개 무선랜 운영자의 안전의무와 인터넷 접속중개자에 대한 면책의 적용범위를 우선 판단해야 한다고 판결 (2014.10.09.)

개요

■ 독일 뮌헨 지방법원은 2014년 10월 9일 공개 무선랜(WLAN)의 운영과 관련하여 독일의 텔레미디어법(TMG, 전자적 정보통신서비스법) 및 EU전자상거래지침의 면책규정의 적용 영역과 그 범위에 대한 9가지의 법적 문제를 유럽사법재판소에 판단해 줄 것을 요청하였다. 인터넷서비스제공자의 책임면제를 정하고 있는 EU 전자상거래지침의 관련 규정을 국내법으로 이행한 독일의 텔레미디어법 관련 규정이 이 지침의 관련규정의 해석을 전제로 하고 있기 때문이다.

■ 뮌헨 지방법원은 2014년 9월 18일 이와 관련하여 해당 절차를 중단하고 EU기능조약(AEUV) 제267조에 의해서 유럽사법재판소에 우선 판단을 요청하기로 결정한바 있다.[20]

– 현재 독일 법원은 상업적 무선랜 운영자에게 안전의무를 부과하려는 경향이 있고 인터넷접속중개자의 면책을 규정하고 있는 텔레미디어법(TMG) 제8조를 적용하지 않으려고 하고 있다. 따라서 유럽사법재판소는 지방법원의 우선 판단 요청으로 독일 법원의 이러한 경향이 모니터링 의무를 금지한 EU상거래지침 제15조[21]의 배경에서 과연 정당한지를 밝혀야 한다.

20 LG München, Beschluss vom 18.09.2014, 7 O 14719/12.

21 EU 전자상거래지침 제15조 (모니터 의무 없음) 1. 회원국은 서비스제공자가 제12조 내지 제14조까지의 서비스를 제공하는 경우 서비스제공자에게 송신하거나 저장하는 정보를 모니터할 일반 의무를 과해서는 안 되며, 불법한 활동을 나타내는 사실 · 상황을 적극적으로 탐색할 일반 의무를 과해서는 안된다. 2. 회원국은 정보사회서비스제공자로 하여금 그들의 서비스를 수신하는 자에 의한 불법한 활동이 행해지거나 불법한 정보제공 혐의가 있는 경우 즉각적으로 소관 관청에 알리도록 하는 의무를 만들 수 있고 소관 관청의 요구에 서비스제공자가 저장계약을 갖고 있는 수신자를 인식할 수 있는 정보를 보고할 의무를 만들 수 있다.

우선 판단 요청의 배경

■ **(원고)** 원고는 조명기술과 음향기술을 판매하거나 대여하는 중소기업을 운영하고 있다. 독일 해적당의 당원이며 과거에는 본 소송의 대상인 인터넷 접속의 가입자로 무선랜(WLAN)을 운영하였다. 2010년 9월 4일 이 인터넷 접속을 통하여 소송대상인 그룹의 앨범이 인터넷 파일공유사이트 이용자들에게 무제한 다운로드 되도록 제공되었다.

■ **(피고)** 피고는 이 앨범의 제작자로 2010년 10월 29일 서면으로 원고에게 이 저작권침해 내용에 대해 경고 하였으나 변화가 없자 원고를 저작권 침해에 대한 방해자로서 금지청구를 하였다.

■ 이에 대하여 원고는 자신이 직접 권리를 침해하지 않았고 또한 자신의 공개 무선랜 이용자들이 행한 권리침해에 대해 방해자로서 책임이 없다는 확인의 소를 뮌헨지방법원에 제기하였다.

– 원고는 소송대상인 무선랜을 공개 무선랜으로 운영하였고, 이 무선랜에 임의의 이용자가 접속하였다고 진술하고 있다. 또한 공개 무선랜에 접속하는 경우 통제는 기술적으로 불가능하고 기대할 수도 없기 때문에 통제할 수 없었다고 진술했다.

– 원고는 또한 저작권 침해를 본인이 행하지 않았으나 제3자가 그 무선랜을 통하여 권리침해를 행하였을 가능성은 있다고 한다. 누가 언제 어떠한 목적으로 자신의 무선랜을 이용하였는지를 알 수 없다.

※ 무선랜을 대부분 기간동안 ○○○라는 네트워크 이름으로 운영하였는데 이러한 이름으로 공개무선랜을 운영하는 것은 자신의 영업소에 인접한 기업들, 통행인 그리고 이웃의 고객들이 자신의 기업을 인지할 수 있고 자신의 영업소나 홈페이지 'www.xxx.de'의 방문을 유인하기 위해서라고 한다.

– 또한 원고는 피고가 주장하고 있는 저작권 침해 이후에 무선랜의 이름을 'Freiheitstaatangst.de'라는 이름으로 변경하였고 이는 데이터보호를 지지하고 한계없는 국가의 감시에 반대하는 시위를 알리기 위해서라고 한다.

■ 피고는 2014년 1월 16일 원고에 대하여 소송을 제기하면서, 원고의 청구는 기각하여 유책으로 판결되고 소송비용을 지불해야 하고, 판결은 가집행될 수 있어야 한다고 주장하였다.

– 피고는 소송대상인 인터넷접속은 원고의 영업적 접속이 아닌 사설 인터넷 접속이고 피고는 원고가 소송대상인 권리침해를 스스로 범하지 않았다는 것을 몰랐다고 주장한다. 그리고 접속 가입자인 원고가 사실상 추정을 근거로 권리침해의 행위자이며 제3자가 저작권침해를

범하였다고 하는 것은 상당한 추측에 근거하여 납득할 수 없다고 주장한다. 또한 피고는 원고가 '공개 무선랜'을 운영하면서 접근보호나 패스워드보호를 하지 않았음에 책임이 있다고 한다.

■ 원고는 피고의 청구를 철회할 것을 주장하였다. 만일 법원이 텔레미디어법 제8조의 적용을 고려하지 않는다면, EU기능조약 제267조에 의해서 유럽사법재판소에 다음의 문제를 선결판단의 문제로 요청해야 한다고 주장하였다.

– "공개 또는 익명으로 접근할 수 있는 인터넷 접속 서비스 제공자가, 자신에 게 제기된 법원 또는 관청의 결정과 특정한 권리침해에 대한 구체적인 근거와는 상관없이, 공개 인터넷접속 서비스의 가입자의 장래의 권리침해를 예방하기 위해서 일반적이고 영구적인 조치를 취하도록 의무를 부과하는 것을 전자상거래지침 또는 유럽기본권헌장이 회원국에게 금지하고 있는 것으로 해석되어야 하는가?"에 대한 판단을 요청하였다.

지방법원의 우선 판단 요청 내용

■ 지방법원은 지금까지 수행된 증거조사를 근거로 소송대상인 인터넷접속은 원고의 기업에 속하고, 2010년 9월 xxx에서 운영하였다는 점을 인정한다. 또한 법원은 무선랜을 통해서 도달할 수 있는 이 인터넷접속은 침해 시에 'Freiheitstattangst.de'로 표시되었고 패스워드를 통해서 보호되지 않았다는 점도 거의 인정한다.

■ 재판부는 원고가 적정하고 허용되는 기술적인 보호조치를 하지 않고 자신의 무선랜을 운영하였기 때문에 원고의 책임과 부작위 의무를 고려할 것에 주목했다. 재판부의 견해에 의하면 원고는 기본적으로 가능한 기술적인 보호조치를 취할 의무가 있다고 본다.

– 이 점에서 재판부는 이전에 유사한 사건에 관한 연방대법원의 판례(BGH, Urteil vom 12.05.2010 – I ZR 121108, Sommer unseres Lebens)를 적용한다. 이 판례에 따르면 자신의 무선랜 접속이 적정한 보호조치를 통해서 외부의 제3자의 권리침해로부터 충분히 보호되고 있는지를 점검하는 것은 무선랜을 운영하는 사인에게도 가능하다고 한다. 이러한 기대가능성은 외부의 권한 없는 침입으로부터 자신의 데이터를 보호하는 것이 일반적으로 접속가입자의 독자적인 이익에서 나오므로 무권한 제3자의 저작권침해를 방지하기 위해 행해지는 무선랜 접속에 대한 보호조치들은 접속보유자의 이익에도 기여한다고 한다(vgl. BGH, Urteil vom 12.05.2010 – I ZR 121/08).

■ 재판부는 연방대법원의 판단이 원고와 같은 영업운영자들은 일반인보다 더 높은 점검의무 및 주의의무를 부담해야하기 때문에 더욱 더 강력하게 책임이 있어야 한다고 판단한다. 다만 원고가 EU 전자상거래지침(2000/31/EC) 제12조[22] 제1항 전단의 규정을 독일법으로 이행한 인터넷접속중개자의 면책을 규정하고 있는 텔레미디어법 제8조[23] 제1항 제1문을 근거로 하고 있는 경우에는 기본적으로 원고의 책임은 없다.

– 본 사안에서 공개 무선랜을 운영하고 제3자의 무선랜 접속의 남용을 방지하기 위해서 원고가 구체적으로 어떠한 기술적 보호조치를 해야하는지에 대해 당사자들 사이에서 다툼이 있다. 그러나 재판부는 본 사안에서 피고의 주장은 텔레미디어법 제8조 제1항 제1문 및 제12조 제1항이 원고의 책임을 일반적으로 배제하는지에 초점을 맞췄다.

■ 본 재판부는 독일의 텔레미디어법 제8조 제1항 제1문으로 이행된 지침 제12조 제1항은 다음의 이유로 적용할 수 없다고 본다. 해당 저작권자 및 저작인접권자에 대한 금지청구나 손해배상청구 및 경고비용보전 및 소송비용의 보전(그리고 그밖의 저작권법상의 청구권)에 대해서 책임을 지지 않는다.

– 이유는 다음과 같다. 이 사안은 기업운영자가 직원에게 안전조치가 되어 있지 않은 무선랜의 인터넷 접속을 사용하도록 하였고 제3자가 이를 통하여 인터넷에 무제한 접근하도록 하여 보호받아야 하는 저작물이 공중에게 접근될 수 있도록 한 상태에서 기업운영자가 아닌 알 수 없는 제3자가 침해한 경우이다. 이때 기업운영자는 서비스제공자가 그 송신을 시작하지 아니한 경우(전자상거래지침 제12조 제1항 후단 a) 내지 c)의 요건들을 충족하지 않음) 또는 그 송신의 수신자를 선택하지 아니한 경우, 그 송신에 담겨 있는 정보를 선택도 수정도 하지 아니한 경우에는 제3자에 의해서 전달되는 정보에 대해서 책임을 지지 않는다.

22 EU 전자상거래지침 제12조 (단순 도관) 1. 서비스수신자가 제공하는 정보를 통신네트워크상에 송신하거나 통신네트워크에 접근을 제공하는 정보사회서비스를 제공하는 경우, 회원국은 다음 조건 하에서 서비스제공자는 송신된 정보에 대해 책임이 없도록 보장한다. (a) 서비스제공자가 그 송신을 시작하지 않은 경우. (b) 서비스제공자가 그 송신의 수신자를 선택하지 않은 경우. (c) 서비스제공자가 그 송신에 담겨 있는 정보를 선택도 수정도 하지 않은 경우. 2. 제1항에 언급된 송신 및 접근제공 행위는, 송신된 정보저장이 통신네트워크에서 송신을 하기 위한 유일한 목적으로 발생한 것이고 그 정보가 송신에 합리적으로 필요한 기간 이상 저장되지 않은 경우라면, 송신된 정보의 자동적 · 매개적이고 순간적인 저장을 포함한다. (3) 이 조는, 회원국의 법적 체계를 준수하여 서비스제공자에게 침해의 제거나 방지를 요구할 법원이나 관청의 가능성에 영향을 미치지 않는다.

23 텔레미디어법 제8조 (정보의 중개) (1) 서비스제공자는 자신이 통신망에서 전달되거나 이용을 위해 접속을 중개하는 타인의 정보에 대하여 다음 각 호에 모두 해당하는 경우에는 책임을 지지 않는다. 1. 서비스제공자가 중개를 야기하지 않는 경우. 2. 서비스제공자가 전달되는 정보의 수신자를 선택하지 않는 경우. 3. 서비스제공자가 전달되는 정보를 선택하지 않거나 변경하지 않는 경우. 서비스제공자가 위법한 행위를 하기 위해서 의도적으로 자신의 서비스 이용자와 협력하는 경우에는 제1문은 적용되지 않는다. (2) 오로지 통신망에서 전달을 이행하기 위해서 발생하고 이 정보가 전달되는 동안 통상적으로 필요한 정도로 더 이상 저장되지 않는 한, 제1항의 정보의 전달과 정보에의 접근의 중개는 이러한 정보가 일시적으로 자동으로 중간 저장되는 경우를 포함한다.

– 지침 제12조 제1항 전단의 이러한 해석의 결과는 다음과 같은 견해이다. 본 법원의 견해에 따르면 보호조치가 되지 않은 공개 무선랜의 접근을 제공하는 것은 지침 98/34/EC 제1조 제2호와 관련하여 지침 2000/31/EC[24] 제2조 (a)에서 의미하는 정보사회서비스에 해당한다. 즉 전자적 수단과 서비스 수신자의 개별적 요청에 의해서 '일반적으로 유상으로'제공되는 모든 서비스인 정보사회서비스를 말한다. 일반적으로 유상으로 제공되는(예를 들어 전기통신사업자의 유료 HOT-Spot 서비스 제공) 인터넷접속의 승낙은 정보사회서비스로 보는 것도 같은 맥락이다.

■ **(정보사회 서비스에 포함되는지 여부)** 재판부는 소송대상인 보호조치가 되지 않은 공개 무선랜의 접근을 제공하는 것이 과연 정보사회서비스에 해당하는지 그리고 어떠한 요건 하에서 해당하는지의 사실 인정이 필요하여 '일반적으로 유상으로'란 개념의 해석을 첫 번째 물음으로 유럽사법재판소에 요청한다.

Q EU 전자상거래 지침 제12조 제1항은 지침 제2조 (a)와 지침 98/48/EC에 의해서 수정된 지침 98/34/EC 제1조 제2호와 관련하여, '일반적으로 유상으로'라는 문언은 서비스제공자의 자격의 근거가 되는 구체적 관련있는 자가, 이 서비스를 '일반적으로 유상으로'제공하는 자인지 또는 이 서비스 및 유사 서비스를 유상으로 제공하는 시장의 제공자인지 또는 이 서비스 및 유사 서비스의 다수가 유상으로 제공되는 것인지를 국내법원이 확인하여야 하는 것을 의미하는 것인지에 대한 판단을 요청한다.

A 공개 무선랜을 선택하는 자는 누구나 정보사회서비스를 이용하므로 전자상거래 제2조 d)에서 의미하는 서비스 수신자(즉 이용자)[25]로 해석될 수 있다. 즉, 보안조치가 되지 않은 무선랜이 운영되고 이용자는 이 무선망을 선택함으로써 지침 제12조 제1항 전단에서 의미하는 이용자에게 통신망에의 접근을 중개하게 된다.
이때 접근 중개의 기술적인 과정만 문제되므로 이용자와 서비스제공자 사이의 계약관계가 존재하는지,[26] 타인의 정보에 직접 또는 간접 접근이 이루어졌는지 그리고 이것이 의도적으로 또는 무의식적으로

24 이 지침은 1998년 7월 20일 지침 98/48/EC에 의해서 개정되었다. 특히 제1조 제2호 서비스의 개념이 변경되었다. 서비스란 원거리에서, 전자적 수단을 통해서 그리고 서비스 수신자의 개별적 요청에 의해서 일반적으로 유상으로 제공되는 모든 서비스인 정보사회서비스를 말한다. '원거리에서'(at a distance)란 서비스가 동시에 현존하는 당사자들 없이 제공되는 서비스를 말한다. '전자적 수단으로'(by electronic means)란 서비스가 데이터의 처리(디지털 압축을 포함하여)와 저장을 위해 전자적 설비에 의해서 원격으로 송수신되거나, 유선, 방송, 광학적 수단 또는 그밖의 전자기적 수단에 의해서 전적으로 전달, 중개, 수신되는 서비스를 말한다. '수신자의 개별적 요청에 의해서'(at the individual request of a recipient of services)란 개별적인 요청으로 데이터의 전송을 통해서 제공되는 서비스를 말한다.

25 EU 전자상거래지침 제2조 (d) '서비스 수신자': 직업상 또는 기타의 목적으로 정보사회서비스를 이용하는 모든 자연인 또는 법인, 특히 정보의 검색 또는 접근제공 목적으로 정보사회서비스를 이용하는 모든 자연인 또는 법인.

26 EuGH, Urteil vom 27.3.2014, Rs. C-314/12-UPC Telekabel Wien GmbH.

발생하였는지[27]는 중요하지 않다.
그러나 만일 제공자가 자신의 서비스를 중립적으로 제공하는 것이 아니라 그가 처리하는 데이터를 인식하고 통제하는 적극적인 역할을 하는 경우에는 연방대법원의 판례와 일치하게 제공자는 더 이상 중개자가 아닐 수 있다.[28]
따라서 자신의 가족 구성원이나 손님들에게 자신의 인터넷 접속의 이용을 허용하는 사설 인터넷 접속보유자도 인터넷과 통신망에의 접근을 중개하는 것으로 본 과거 판례처럼,[29] 재판부는 원고도 본 사안에서 통신망의 접속을 중개한다고 판단한다.

■ **(통신망 접속의 중개를 위해 필요한 개념의 해석)** 본 재판부는 통신망에의 접속의 중개를 위해서 필요한 사실 확정을 하기 위하여 사법재판소에 '통신망의 접속을 중개하는'의 개념을 해석하는 것을 두 번째의 질문으로 요청한다. 특히 접속 중개의 기술적인 과정이 충분하지 않을 경우 다른 요건이 추가적으로 더 요구되는지를 판단해야한다.

Q 전자상거래 지침 제12조 제1항은, '통신네트워크의 접속을 중개'란, 지침에 합치적인 중개를 위해서는 인터넷과 같은 통신네트워크의 접속이 중개됨으로써 그 결과가 발생하면 충분한 것으로 해석되어야 하는가?

A 공개 무선랜 제공자는 정보사회서비스(공개적이고 보호조치가 되지 않는 무선랜 접속의 제공)를 제공하기 때문에 공개 무선랜을 제공하는 사람은, 지침 제2조 (b)에서 의미하는 서비스제공자에 해당한다.

■ **(서비스'제공'의 의미)** 지침 제2조 (b)의 '제공'이라는 문언이 사실상 (혹은 암묵적인) 서비스 제공으로 충분한 지 아니면 그밖의 요건이 더 필요한지 판단이 필요하다.

27 Holznagel/Ricke, in: Spindler/Schuster/Hoffmann, TMG § 2Rn.2ff.

28 EuGH, Urteil vom 12.7.2011, Rs. C-324/09, Rn. 113-L'Oreal/eBay.

29 Mantz, MMR 2006, 764, 765; Gietl, MMR 2006, 630, 631; Stang/Hahner, GRUR-RR 2008, 273, 275; Borges, NJW 2014,2305,2310 mit weiterem Verweis auf jurisPK-Internetrecht, Roggenkamp/Stadler, Stand 1.2.2014, Kap. 10 Rn. 139; Hügel, Haftung von Inhabern privater Internetanschlüsse für fremde Urheberrechtsverletzungen, 1. Auflage, 2014, S. 126.

Q 전자상거래지침 제12조 제1항 및 제2조 b)와 관련하여, 지침 제2조 b)에서 말하는 '제공'은 정보사회서비스가 사실적으로 이용되는 경우인지, 구체적으로 공개 무선랜이 제공되는 경우에 충분한가?

A 본 재판부는 원고는 이미 지침 제12조 제1항을 국내법으로 이행한 텔레미디어법 제8조 제1항 제1문으로 부작위청구, 손해배상청구, 경고비용의 보전 (및 그밖의 저작권법상의 청구) 및 소송비용의 보전에 대해서 피고에게 책임이 없다는 점에서 출발한다. 왜냐하면 원고는 제3자에 의해서 중개되는 정보에 대해서 책임이 없기 때문에 이를 근거로 피고의 청구를 기각할 수도 있기 때문이다.
이러한 의미에서 함부르크 구법원도 호텔이나 민박집 무선랜 접속을 통한 손님의 권리침해에 대해서 호텔 운영자의 책임이나[30] 민박임대업자의 책임을[31] 부정하였다. 왜냐하면 텔레미디어법 제8조 제1항 제1문 전단의 요건을 충족을 통해서 이들의 책임이 배제되기 때문이다.

■ **(전달된 정보에 대한 책임 여부)** 지침 제12조 제1항에 의한 '전달된 정보에 대하여 책임을 지지 않는다'의 개념의 해석을 사법재판소에 요청한다. 왜냐하면 법원은, '책임을 지지 않는다'는 의미는 지침 제12조 제1항과 관련하여 책임이 배제되는 것으로 인정하여야 하기 때문이다.

Q 지침 제12조 제1항 1문은, '중개된 정보에 대해서 책임을 지지 않는다'는 의미는 저작권 침해를 이유로 한 접속중개자에 대한 금지청구, 손해배상청구, 경고비용보전청구 그리고 소송비용의 청구가 기본적으로 인정된 저작권침해와 관련해서 배제되는 것으로 해석되어야 하는가?

A 본 재판부는 지침 부작위의무의 관점에서 지침 제12조 제1항 이 우선하기 때문에 제12조 제3항의 규정[32]도 법적 근거로서 피고가 제기한 원고에 대한 부작위의무를 진술할 가능성을 열어주지 않는다는 점에서 출발한다.

■ **(규범적 해석)** 지침 제12조 제1항 전단과 제12조 제3항의 규범적 긴장관계의 해석을 요청한다.

30 AG Hamburg Urteil vom 10.06.2014, 25b C 431/13.

31 AG Hamburg Urteil vom 24.06.2014, 25b C 924/13.

32 EU전자상거래지침 제12조 (3) 이 조는, 회원국의 법적 체계를 준수하여 서비스제공자에게 침해의 제거나 방지를 요구할 법원이나 관청의 가능성에 영향을 미치지 않는다.

Q 지침 제12조 제3항과 관련하여 제12조 제1항 전단은, 접속제공자가 인터넷접속을 통하여 저작권으로 보호되는 특정 저작물을 인터넷 파일교환사이트에 제공하여 제3자에게 제공하는것을 못하도록 하는 명령을 회원국이 국내 법원에게 허용해서는 안 되는 것으로 해석되어야 하는가?

A 지침 제14조[33] 제1항 b)의 적용에 있어서 서비스제공자가 구체적인 권리침해를 인식하는 즉시 통상적인 보호조치를 취함으로써 장래의 동일한 권리침해를 방지하기 위해 조치를 취하지 않는 경우에 서비스제공자의 책임이 존재하는 것으로 지침 제12조 제1항이 해석될 수 있는지의 문제가 제기된다. 저작권자는 제3자가 공개 무선랜을 통하여 저작권을 침해하는 파일 공유를 운영한 경우, 자신의 권리침해에 대해서 법원에 소를 제기하여 승소할 수 없고 이에 해당하는 부작위의무도 성취하지 못할 수 있다. 하지만 저작권자들은 공개 무선랜 시스템 운영자에게 권리침해를 통지하고 무선랜 운영자의 인터넷접속이 장래의 권리남용에 이용되는 것을 방지하기 위해서 통상적인 보호조치를 설치하게 할 의무를 부담시키는 방식은 가능하다. 서비스 제공자들이 이러한 조치들을 취하지 않아서 공개 무선랜 접속을 통한 권리침해가 더 발생하게 될 때 비로소 법원에 이행을 청구할 수 있는 부작위청구가 존재하게 될 것이다.[34]

■ **(금지청구에 적용 여부)** 재판부는 지침 제12조 제1항 및 제14조 제1항 b)의 규범적인 관계의 해석을 위하여 여섯 번째 물음을 재판소에 요청한다.

Q 지침 제12조 제1항 전단은 본안절차의 상황에서 지침 제14조 제1항 b)의 규정은 금지청구에도 상응하게 적용되어야 하는 것으로 해석되어야 하는가?

A 본 재판부가 지침 제12조 제1항을 근거로 원고의 책임을 모두 부정할 경우 저작권으로 보호되는 내용의 (불법) 파일공유는 판결되어야 할 사례와 같은 경우에 실제로 소추될 수 없다. 왜냐하면 접속 보유자는 접속중개자로서 책임을 지지 않고, 직접 행위자는 신원이 파악될 수 없기 때문에 조사될 수 없어 체포될 수도 없기 때문에 보호조치가 되지 않기 때문이다. 원고는 자신의 무선랜 네트워크 이용자들에게 완전히 익명으로 활동하는 것을 가능하게 하였기 때문에[35] 접속중개자의 이러한 책임면제는 접속중개자가 자신의 이용자에게 접근을 선택하는 서비스에서 권리침해가 행해지는 것을 인식한 경우에도 적용된다.[36]

33 EU 전자상거래지침 제14조 (호스팅) 1. 서비스수신자가 제공하는 정보를 저장하는 것으로 구성되는 정보사회서비스를 제공하는 경우, 회원국은 다음 조건 하에서 서비스제공자가 서비스수신자의 요구로 저장된 정보에 대해 책임이 없도록 보장한다. (a) 서비스제공자가 불법한 활동 · 정보에 대한 실제 인식이 없고 손해배상과 관련하여 불법한 활동 · 정보가 분명한 사실이나 상황을 의식하지 못한 경우. (b) 서비스제공자가 그러한 인식 · 의식을 한 시점에 지체 없이 해당 정보를 제거하거나 정보에 대한 접근을 차단한 경우. 2. 이 조는 회원국의 법체계에 따라 서비스제공자에게 침해를 종료시키거나 막도록 요구하는 법원 또는 행정청의 가능성에 영향을 미치지 아니한다.

34 Hügel. Haftung von Inhabern privater Internetanschlüsse für fremde Urheberrechtsverletzungen, 1. Auflage, 2014, S. 127 ff.

35 vgl. OLG Hamburg ZUM-RD 2013, 536, 542 – Haftung eines Sharehosters als Störer.

36 BeckOK UrhG, Reber § 97 Rn. 80; Noltel/Nimmers, GRUR 2014,16,17.

■ **(정보제공자의 요건)** 서비스제공자가 정보사회서비스를 제공하는 모든 자연인 또는 법인이라는 점에서 서비스제공자에 대한 요구사항이 국한되는 취지에서 지침 제2조 b)와 관련하여 제12조 제1항 전단의 해석을 일곱 번째 물음으로 사법재판소에 요청한다.

Q 서비스제공자에 대한 요구조건은 서비스제공자가 정보사회서비스를 제공하는 모든 자연인 또는 법인이라는 점으로 제한하는 것으로 해석하여야 하는가?

A 사법재판소가 일곱 번째 질문을 부정하는 경우에는 본 재판부는 당법원이 판결할 사실을 인정하기 위해서 이 규범의 해석과 추가적인 기준의 언급을 요청한다.

어떠한 추가적인 요구사항이 지침 제2조 b)의 해석과 관련하여 서비스제공자에게 있게 되는지 판단이 요구된다. 본 재판부가 판결해야 될 사안에서 그 적용이 의미를 가지게 될 지침 제12조 제1항 전단의 해석을 위해서 사법재판소가 원고의 저작권법상의 책임을 부정할 수 있는 것으로 결론을 내려야 하는 경우에는 본 재판부는 이러한 해석이 지침 2001/29/EC, 지침 2004/48/EC의 내용과 적용될 기본권의 보호에서 나오는 요건들의 관점에서 서로 관련되어 해석되어 어느 정도 일치할 수 있는지의 문제를 추가로 제기한다. 경우에 따라서 본 재판부는 지침 제15조 제1항[37]에 열거된 금지의 범위에 의한 접속의 문제를 제기한다. 서비스제공자에게 그가 전달하거나 저장하는 정보를 감시하거나 적극적으로 위법한 행위를 암시하는 상황을 조사할 일반적인 의무를 부과할 수 없도록 하고 있다. 그러한 점에서 2014년 3월 27일자 사법재판소의 판결(C-314/12)을 어떻게 이해하여야 하는지 본 재판부는 확신할 수 없다.

평가 및 전망

■ 뮌헨 지방법원은 연방대법원의 판결과 같이 공개 무선랜 운영자에게 방해자로서의 부작위책임이 존재하고 무선랜 운영에 있어서 이에 상응한 보안조치를 해야 할 의무가 있는 것으로 보고 있다. 마찬가지로 텔레미디어법 제8조 및 EU전자상거래지침 제12조 제1항의 책임면제도 적용될 수 있다는 해석도 가능하다고 보고 있다. 따라서 지방법원은 본안절차를

37 제15조 (모니터 의무 없음) 1. 회원국은 서비스제공자가 제12조 내지 제14조까지의 서비스를 제공하는 경우 서비스제공자에게 송신하거나 저장하는 정보를 모니터할 일반 의무를 과해서는 안 되며, 불법한 활동을 나타내는 사실 · 상황을 적극적으로 탐색할 일반 의무를 과해서는 안 된다. 2. 회원국은 정보사회서비스제공자로 하여금 그들의 서비스를 수신하는 자에 의한 불법한 활동이 행해지거나 불법한 정보제공 혐의가 있는 경우 즉각적으로 소관 관청에 알리도록 하는 의무를 만들 수 있고 소관 관청의 요구에 서비스제공자가 저장계약을 갖고 있는 수신자를 인식할 수 있는 정보를 보고할 의무를 만들 수 있다.

중단하고 전자상거래지침의 다양한 해석 가능성의 문제를 우선 판단해 줄 것을 유럽사법재판소에 요청한 것이다.

■ 최근 함부르크 구법원은 텔레미디어법 제8조의 면책이 무선랜 운영자에게도 기본적으로 적용될 수 있는 판결이 내린 바 있다.[38] 뮌헨 지방법원의 우선 판단 요청에 대하여 무선랜의 운영과 관련한 법적인 문제에 대해서 중요한 의미를 가지지만 유럽사법재판소의 판결이 나오기까지 적어도 1년이 넘게 걸리므로 그 때까지는 여전히 법적 불안전이 지속될 것이라는 우려가 있다.

■ 무상 서비스에 대해서 전자상거래의 적용은 문제가 많다고 보는 견해도 있다. 또 한편 전자상거래 지침이 금지청구의 경우에도 적용되는지에 판단 요청은 상당한 의미가 있는 것으로 보는 견해도 있다. 이러한 견해는 연방대법원의 견해와 모순되기 때문이다. 이번 결정은 공개 무선랜의 책임을 중대하게 제한할 수도 있을 것이지만 적어도 거래안전의무를 명확히 한다는 점에서는 의의가 있을 것이라는 평가를 받고 있어 유럽사법재판소가 어떤 결정을 내릴지 주목된다.

참고자료

지방법원의 우선 판단 요청 결정 전문 :

http://www.damm-legal.de/lg-muenchen-i-grundsatzfrage-der-haftungsbefreiung-bei-betrieb-eines-offenen-wlan-durch-gewerbetreibenden-wird-dem-eugh-zur-entscheidung-vorgelegt

http://www.cr-online.de/38218.htm

http://www.golem.de/news/offenes-wlan-eu-gerichtshof-soll-ueber-wlan-haftung-entscheiden-1410-109731.html

https://www.wbs-law.de/abmahnung-filesharing/offenes-wlan-und-filesharing-abmahnung-gericht-schaltet-eugh-ein-56618/

38 AG Hamburg Urt. v. 10.6.2014 – Az. 25b C 431/13, CR 2014, 536 m. Anm. Mantz sowie Urt. v. 24.6.2014 – Az. 25b C 924/13, ITRB 2014, 205 (Rössel) sowie zu beidem Hrube, CR 2014, R85).

2 미국 FDA,의료장비제조자의 사이버보안의무를 강화하는 가이드라인 발간 (2014.10. 2)

개요

■ 미국 식품의약청(the Food and Drug Administration, FDA)은 의료장비 제조업자들이 인터넷, 네트워크 혹은 휴대용 미디어에 연결할 수 있는 의료장비를 구상할 경우 사이버보안 통제 메커니즘을 개발할 것을 권고하는 가이드라인을 발간하였다(2014.10. 2).

■ 이 가이드라인의 정식명칭은 “의료장비에서의 사이버보안 관리를 위한 시판 신청서의 내용”(Content of Premarket Submissions for Management of Cybersecurity in Medical Devices)이며 의료장비 시판시에 사용하는 신청서에 포함되어야 할 보안 관련 사항을 권고하고 있다.

배경

■ 현재 상호 연결되어 있는 의료장비들은 환자에 대한 간호 및 의료보건에 있어서 효율성을 증진시킬 수 있는 장점이 있으나 보안과 관련해 취약하다는 단점이 있다.

– FDA는 이 때문에 네트워크를 통한 각종 의료장비의 악성코드(malware)감염, 보안되지 아니한 비밀번호의 유통, 시기에 맞지 않는 소프트웨어 업데이트 및 패치, 규격 소프트웨어 제품에서의 보안 취약성 등이 우선적으로 해결되어야 할 주요사항이라고 판단하여 이번 가이드라인을 발간하였다.

의료장비 보안현황

■ **(보안패치 설계미비)** 윈도우나 리눅스와 같은 운영체제에서 새로운 보안 취약성이 발견되고 이러한 취약성으로부터 보안을 유지하기 위해 지속적인 패치가 필요함에도 불구하고 이들 운영체제를 사용하고 있는 대부분의 의료장비들은 패치를 넣을 수 있도록 설계가 되어있지 않거나 거의 넣을 수 없도록 설계가 되어 있고,

– 의료장비 제조자들은 이미 제조된 장비들의 보안 시스템을 갱신할 방법이 거의 없는 상황이다.

■ **(해킹시 중대피해 우려)** 의료장비가 해킹되는 경우 환자에 대한 의료서비스 제공과 관련하여 심각한 위험이 발생할 수 있다.

– IP로 작동 가능한 많은 의료장비들은 환자들의 투약에 관련이 되어있고 이들 장비가 해킹 등으로 오작동 되는 경우 치명적인 무기가 되는 위험이 있으며,

– 환자의 병상에 설치되어 있는 모니터링 시스템 역시 해킹되는 경우 입원환자 전체의 목숨이 위험에 놓이게 된다.

■ 아직까지 의료 장비의 보안 취약성으로 인한 인명피해 사건은 보고되지 않았으나 이는 시간 문제일 뿐이라는 것이 FDA 및 전문가들의 의견이다.

주요내용

■ **(목적)** 의도적 혹은 비의도적 사이버보안에 대한 위험으로부터 의료장비의 기능성 및 안전성을 보장하기 위한 것이다.

■ 시판 신청서에 포함되어야 할 내용

① 해당 의료장비의 제조자가 고려한 사이버보안과 관련한 위험 목록
② 동 의료장비에 포함된 사이버보안 통제 메커니즘의 목록
③ 사이버보안 통제 메커니즘이 위험에 대응할 수 있는지에 대한 설명
④ 소프트웨어 업데이트 및 패치의 입증 계획 등에 대한 내용을 포함

– 이에 따라 의료장비 제조자는 해당 의료장비의 의도된 사용 및 의도된 환경에 근거한 위험을 식별해내고 이에 맞는 사이버보안 통제 메커니즘을 개발해야 한다.

– 또한 의료장비 제조자 및 보건의료 시설은 기존의 의료장비 및 네트워크가 가지는 사이버보안 관련 취약성을 테스트하고 소프트웨어 업데이트 및 패치가 필요한 경우 이를 제공하여야 한다.

■ **(접근 통제)** 또한 FDA는 보안 통제 메커니즘을 고려함에 있어 보안 조치와 해당 장비의 가용성 간 균형을 맞춰야 하는 필요성 때문에 사용자마다 접근할 수 있는 수준을 달리 설정하는 허가절차를 사용할 것을 제안한다.

– 보안 통제 메커니즘 설계시 응급실 의료진이 사전 허가 없이 환자의 장비에 긴급하게 접근해야할 필요가 있는 경우와 같이 허가받지 않은 사용자가 의료장비에 접근할 필요성이 있는 보건의료 부문의 특수한 상황이 반드시 고려되어야 한다.

가이드라인의 효력

■ 이 가이드라인은 구속력 없는 권고사항을 담고 있는 문서이나 FDA는 동 문서를 의료장비의 상업적 유통의 투명성을 위해 사용할 것임을 분명히 하였다.

– 의료장비 내의 사이버보안 조치에 대해 충분히 설명하지 못하는 의료장비 업체들은 FDA로부터의 시판 신청서 승인이 지연되거나 혹은 거절될 수 있다.

평가

■ 의료장비 제조자들 및 보건의료 시설에 대하여 사이버보안이 보건의료 서비스의 제공에 있어 불가분의 일체를 이루고 있다는 점을 인식시켜야 할 필요성을 강조하고 있는 것이다.

– 비록 동 가이드라인에서 특정 의료장비나 보건의료 시설을 대상으로 하고 있거나 사이버보안 침해로 인한 환자의 피해에 대해 언급하고 있지는 않지만 의료장비 제조자들 및 보건의료 시설이 환자들을 사이버보안 관련 위험으로부터 보호하기 위한 적극적인 조치를 취할 필요성을 보여주고 있다.

참고자료

http://www.harrisbeach.com/media-news/10170

http://www.kslaw.com/imageserver/KSPublic/library/publication/ca102414.pdf

http://www.forbes.com/sites/groupthink/2014/10/03/fda-guidance-on-medical-device-cybersecurity-too-little-too-late/

http://www.usatoday.com/story/tech/2014/10/01/fda-medical-devices-cybersecurity/16543731/

3 독일, 바이에른 州(주) 개인정보보호감독청, 자동차 블랙박스 영상을 인터넷에 올리는 경우 최고 300,000 유로 과태료 부과 예정 (2014.10.09)

개요

■ 독일 바이에른 주 개인정보보호감독청(BayLDA)[39]은 2014년 10월 9일 교통사고 시 증거를 수집하여 경찰서나 보험회사에 제출하거나 인터넷 등에 올릴 목적으로 자동차 블랙박스로 영상을 촬영하는 경우 연방데이터보호법(BDSG)이 정한 최고 300,000유료(원화 720,000,000원)의 과태료를 부과하겠다고 발표하였다.

배경

■ 개인정보보호감독청은 2013년 8월 13일 차량에 블랙박스(On-Board-Kamera (Dashcam)를 설치하여 운전 중에 공공장소를 촬영하는 것을 금지하고 촬영된 영상을 삭제하도록 결정한바 있다.

– 변호사인 이 운전자는 교통법규위반자를 촬영하여 경찰서에 신고할 목적으로 자기 차에 블랙박스를 달았고 교통법규위반자를 신고하면서 22장의 사진을 경찰서에 제출하였는데, 그 중 5장이 블랙박스로 촬영된 것이었다. 경찰은 이 사진이 개인정보를 침해할 수 있기 때문에 개인정보보호감독청으로 전달하였다. 사진을 전달 받은 개인정보보호감독청은 그 운전자에게 블랙박스의 설치 목적 등 질문을 하면서 촬영된 영상을 삭제하도록 명령하였으나 운전자는 개인정보보호감독청의 처분을 취소해 달라는 행정소송을 안스바흐(Ansbach) 행정법원에 제기하였다.

안스바흐 행정법원의 판결

■ 안스바흐(Ansbach) 행정법원은 독일 헌법(기본법)에는 개인의 인격권 보호가 규정되어 있고, 이 인격권 안에는 개인의 정보자기결정권이라는 기본권이 포함되어 있다고 하면서, 개인에 관한 정보의 수집이나 처리는 당사자의 허락이 있거나 법률에 규정되어 있는 경우에만 가능하다고 하였다. 따라서 블랙박스 촬영은 피촬영자(블랙박스의 경우 상대방

39 바이에른 주 개인정보보호감독청(Bayerische Landesamt für Datenschutzaufsicht) 바이에른 주의 민간부문에서의 개인정보보호법의 준수여부를 감시하는 기관으로써 민간 기업체, 사설병원, 단체, 인터넷, 개인 등을 그 대상으로 하고 있다.

차량 운전자나 인도에 걸어 다니는 사람)의 허락을 받지 않은 것이고, 연방데이터보호법(BDSG)에는 원칙적으로 도로와 같은 공공장소에서 개인정보를 수집하지 못하도록 규정하고 있고(블랙박스의 경우 촬영), 공공장소에서 촬영되는 경우는 법률에 그 예외사유를 규정하고 있는데, 블랙박스 촬영은 여기에 해당되지 않는다고 하였다.

- 따라서 운전자가 운전 중에 거리상황을 지속적으로 촬영하는 목적이 필요시 제3자(예를 들어 경찰서나 보험회사 등)에 제출할 목적으로 또는 유튜브나 페이스북 등 인터넷 플랫폼에 공개하기 위한 것일 경우 데이터보호법상 허용되지 않는다고 판단하였다.

– 비밀리에 촬영되는 사람의 정보보호 이익은 사고 시 비디오 증명을 위한 운전자의 이익보다 더 높이 평가될 수 있기 때문이라고 하였다. 하지만 처음부터 블랙박스 촬영이 사적이고 개인적인 영역을 벗어나지 않는 경우에 한해서는 연방데이터보호법이 적용되지 않으므로 가능하다고 하였다.[40]

– 한편 안스바흐 행정법원은 개인정보보호감독청의 처분에 대해서는 처분의 대상이 된 카메라가 특정되지 않는 등 형식적 요건을 갖추지 않아서 위법하다고 판단하였다.

개인정보보호감독청의 항소 포기 및 블랙박스 촬영에 대한 경고

- 개인정보보호감독청은 2014년 10월 9일 항소를 포기하고 블랙박스 촬영에 대해 강력히 경고하였다. 앞으로 운전자가 블랙박스를 이용하여 촬영한 사진을 경찰서나 보험회사 또는 이에 유사한 곳에 제출하거나 인터넷에 올리는 것이 밝혀질 경우 연방데이터보호법이 규정한 최고액(300,000 유로)까지 질서위반금(과태료)을 부과하겠다고 하였다.

유사한 다른 판결

- 뮌헨 구 법원 판결[41]에서 운전자가 접촉사고와 관련한 민사 사건에서 블랙박스로 촬영된 사진을 증거로 제출했지만, 법원은 이를 증거로 받아들이지 않았다. 이 사안에서도 운전자의 블랙박스 설치 및 촬영이 교통 사고 시 증거제출을 위함이였지만 법원은 이를 증거로 받아들이지 않고, 이러한 촬영은 연방데이터보호법상 허락을 받지 않거나 법률이 허용하지 않는

40 VG Ansbach, Urteil vom 12.08.2014, 4 K 13.01634. 이 판결은 차량용 블랙박스 영상촬영에 대한 독일 최초의 판결로서 의미를 가진다.

41 AG München, Urteil vom 13.08.2014, 345 C 5551/14.

개인정보의 수집에 해당하며, 나아가서 '미술 및 사진 저작물의 저작권에 관한 법률'제22조의 초상권 침해에 해당한다고 보았다. 또한 증거 제출을 위한 블랙박스 촬영은 피촬영자의 인격권 침해보다 더 우월하지 않다고 보았다.

- 또 다른 뮌헨 구 법원 판결[42]에서 자전거 운전자가 개인 소장 목적으로 캠을 이용하여 주행 중 촬영하다가 앞 차가 차선을 바꾸면서 급정거하는 바람에 넘어져서 다친 사고에서 법원은 자전거 운전자가 촬영한 영상을 증거로 인정했다. 촬영 당시 그 목적이 증거제출이 아니었기 때문이다. 그런데 그 영상이 오히려 자전거 운전자에게 불리하게 작용되어 아무런 보상을 받지 못했다. 촬영된 영상을 통해서 밝혀진 사실은 앞 차는 교통법규를 준수하여 급정거를 하였으나, 자전거 운전자는 주행거리를 확보하지 않아서 급정거한 차량에 부딪혀 넘어졌기 때문이다.

평가 및 전망

- 현재 독일 각 주의 개인정보보호감독관들은 자동차 블랙박스의 촬영을 일반적으로 허용해서는 안 된다는 견해를 가지고 있다. 하지만 법원의 견해는 이와는 달리 순전히 사적인 목적의 블랙박스의 촬영은 허용하지만, 오로지 교통사고 시 증거 확보를 위한 목적으로 블랙박스로 촬영하는 것은 허용되지 않는다고 보고 있다. 기본적으로 블랙박스 촬영은 비디오 감시로 보고 있기 때문이다. 따라서 이를 허용할 경우 비디오 감시를 통제할 수 없게 되어 이로 인하여 시민의 인격권 침해를 제대로 보호할 수 없을 것이라고 한다.

- 법원의 판결과 개인정보보호감독청의 경고에 대한 국민들의 법감정은 상당히 부정적이다. 블랙박스의 촬영 목적을 입증하기란 쉽지 않기 때문에 결국 이 문제의 해결은 입법자의 손에 달려 있다. 현재 벨기에, 룩셈부르크, 오스트리아에서는 블랙박스 촬영을 일반적으로 금지하고 있고 독일 입법자가 이 문제를 어떻게 해결할 지 기대된다.

참고자료

https://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2014/pm013.html

http://www.gesetze-bayern.de/jportal/portal/page/bsbayprod.psml?doc.id=JURE140015287&st=ent&showdoccase=1&paramfromHL=true

http://www.justiz.bayern.de/gericht/ag/m/presse/archiv/2014/04469/

http://www.justiz.bayern.de/gericht/ag/m/presse/archiv/2013/04014/

42 AG München, Urteil vom 06.06.2013, 343 C 4445/13.

4 홍콩 개인정보보호위원회, 은행부문 개인정보보호의무 준수 가이드라인 발표 (2014.10. 6.)

개요

■ 홍콩 개인정보보호위원회(the Office of the Privacy Commissioner for Personal Data, PCPD)는 은행부문을 대상으로 개인정보보호 의무에 대한 가이드라인을 발표하였다(2014. 10. 6.).

배경 및 경과

■ 금융업무를 담당하는 은행 및 그밖의 금융기관은 고객의 성명, 연락처 상세내용, 신분증명 번호, 고용 상세내역, 금융 및 신용정보 등 업무에서 엄청난 양의 고객정보를 수집, 보유, 처리 및 사용하고 있다. 이때 홍콩 내 은행 및 그밖의 금융기관은 개인정보법령 제486장(Personal Data (Privacy) Ordinance Chapter 486)을 준수하도록 되어있다.

■ 상기 은행부문 업무의 특성상 개인정보를 다룸에 있어 세심한 주의가 필요함에도 불구하고, 개인정보보호위원회에 접수된 민원제기가 가장 많았던 사적부문 중 은행부문이 3위를 기록하는 등 문제점이 발생하고 있다.

※ 2012년부터 2013년간 개인정보보호위원회에 접수된 민원건수는 198건으로 전년 동기 212건에서 줄어든바 있으나, 2013년에서 2014년에는 그 건수가 373건으로 증가하면서 역행하는 양상을 나타내었다.

■ 이에 개인정보보호위원회는 급증하는 민원에 대응하고, 은행부문 기업들의 법령 준수를 촉진시킬 목적으로 동 가이드라인을 발표하였다.

– Allan Chiang 개인정보보호위원회 위원은 “은행부문이 보유하고 있는 방대한 양의 고객 데이터베이스 및 개인금융정보의 민감성을 고려하였을 때, 고객의 개인정보를 다룰때 은행부문에서의 홍콩 개인정보보호법에 대한 준수를 고취시키고 강화시키기 위한 지침을 발표하는 것이 적절하다고 생각한다”고 언급하였다.

가이드라인의 의무사항

■ **(개인정보 수집 목적과 방법)** 개인정보의 수집 목적과 방법은 적법하여야 하고 정보사용자의 기능 혹은 행위에 직접적인 관련성을 가져야 하며 필요한 범위를 벗어나지 않아야 한다.

■ **(개인정보보유의 정확성 및 기간)** 개인정보는 정확하여야 하며 필요한 기간 이상으로 보관되어서는 안된다. 홍콩역내 및 역외로 정보처리자에게 개인정보를 전송하는 경우에도 이는 동일하게 적용된다. 법률에 근거하였거나 혹은 대중의 이익을 위한 예외적인 경우를 제외하고 목적 달성에 더 이상 필요치 않게 된 개인정보는 모든 실행 가능한 수단을 통하여 삭제되어야 한다.

■ **(개인정보의 사용)** 개인정보의 사용은 정보의 주체로부터 사전에 규정된 동의(prior prescribed consent)를 획득하지 아니하는 한 새로운 목적(new purpose)을 위하여 사용될 수 없다. 이때 사전에 규정된 동의란 서면으로 철회되지 아니한 자발적으로 주어진 명시적인 동의를 의미한다(개인정보보호법령 제2조제3항).

■ **(개인정보에 대한 보안)** 정보사용자는 개인정보의 허가받지 않은 혹은 우발적인 접근, 처리, 삭제, 분식 혹은 사용으로부터 개인정보를 보호하기 위하여 실행 가능한 모든 수단을 취하여야 한다. 정보사용자가 홍콩 역내 혹은 역외지역으로 자신을 대신하여 정보를 처리해 줄 정보처리자에게 개인정보를 전송하고자 할 때 해당 정보사용자는 자신이 전송하는 정보의 보호를 보장하기 위하여 계약적 혹은 그밖의 수단을 채택하여야 한다.

■ **(개인정보처리방침에 대한 정보 공개)** 정보사용자는 자사의 개인정보처리방침 및 관행을 투명하게 공개하여야 할 의무를 지닌다.

■ **(개인정보에 대한 접근)** 정보의 주체는 정보사용자가 보유하고 있는 자신의 개인정보에 대한 접근권 및 정정권을 갖는다. 개인정보보호법령 제19조 및 제23조에 따르면 정보사용자는 정보의 주체가 자신의 개인정보에 대한 접근 혹은 정정을 요청하는 경우 그러한 요청이 있은 지 40일 내에 이에 따라야 한다.

※ 이번 가이드라인은 관련 사건들에 대한 행정심판위원회(Administrative Appeals Board)의 결정, 개인정보보호담당위원회가 다룬 과거 민원에 대한 결정 및 홍콩 은행연합회의 개인정보법령작업반의 의견 등을 엮고 있다. 가이드라인에 따르면 개인정보보호법령이 개인정보보호와 관련하여 다루고 있는 원칙은 위에 총 6가지(개인정보보호법령 별표1)이다.

은행부문 가이드라인의 주요 내용

■ **(충분한 설명)** 은행부문 기업들은 개인정보수집설명서에 다음의 네 가지 정보를 포함하여야 한다.

i) 고객의 개인정보가 어떠한 목적을 위하여 수집되고 사용되는지에 대하여 명확한 문구를 통해 설명하여야 한다.
ii) 고객의 개인정보가 전송될 가능성이 있는 제3자에 대한 명시적인 언급이 있어야 한다.
iii) 정황상 분명한 경우를 제외하고, 은행부문 기업들은 자사의 고객들에게 자신의 고객 개인정보의 제공이 자발적인지 혹은 의무적인지의 여부에 대해 명확하게 설명하여야 한다.
iv) 관련 기업들은 자사의 고객들에게 자신의 개인정보, 성명, 직업명 등에 대한 접근권 및 정정권이 있음을 알리고 그러한 접근 혹은 정정에 대한 요청을 처리하는 자의 주소에 대한 정보를 제공하여야 한다.

■ **(고유 번호 수집 금지)** 은행들은 자사에 계좌를 개설하지 아니한 자에 대하여 자사의 서비스 제공에 직접적으로 연관되지 아니한 이상 개인정보를 수집할 수 없다. 홍콩신분증 번호 혹은 그밖의 신분증번호의 수집은 신분증번호 및 그밖의 개인식별자에 관한 행동강령(Code of Practice on the Identity Card Number and other Personal Identifier)에 의하여 규율되고 있는바, 동 행동강령 제2.3문단에서 허용된 경우를 제외하고 정보사용자는 홍콩신분증 번호 및 그밖의 신분증번호를 수집할 수 없다.

■ **(고객정보의 최신성 유지 등)** 업무상 고객의 주소로 고객의 개인정보가 포함된 문서를 우편발송하게 되는 경우가 많은 사실을 감안하여 은행은 고객의 개인정보를 항상 갱신된 상태로 유지하여 해당 고객의 개인정보가 의도치 않은 제3자에게 수령되지 아니하도록 보장하여야 한다.

■ **(개인정보의 파기)** 은행들은 개인정보수집의 목적이 완수된 경우 해당 개인정보의 삭제를 보장하는 자사의 개인정보처리방침 및 관행을 수립하고 이를 이행하여야 한다.

■ **(계열사간 고객정보 공유의 고지 및 동의 등)** 금융, 증권 및 보험 등에 관련된 많은 계열사를 가지고 있는 은행부문 기업들이 고객에 대하여 어떠한 서비스를 제공하고자 할 때 상호 고객의 개인정보를 공유할 수 있다는 사실을 고려하여 은행은 사전에 고객으로부터 해당 고객의 정보가 동일 은행 그룹내 공유가 될 수 있다는 사실에 대하여 상세히 고지하여야 하며 이러한 사용에 대하여 사전 동의를 획득하여야 한다. 또한 개인정보를 동일 그룹 내 공유하는 경우 정보사용의 목적을 변경하거나 불필요하게 정보를 공유하여서는 아니 된다. 은행은 공유된 정보의 소재에 대하여 지속적인 모니터링을 해야 하며 개인정보가 사용된 이후 이의 적절한 처분을 보장하고그룹내 고객정보 공유에 대한 정책을 수립하여야 한다.

■ **(고객정보 역외지역 전송제한)** 고객개인정보의 홍콩 외 지역으로의 전송은 개인정보보호법령 제33조에 의해 규정되어 있으나 동 조항은 아직 발표되지 않았다. 고객개인정보를 홍콩 역외지역으로 전송하기 위해서는 아래의 요건을 만족하여야 한다.

i) 고객정보 수집시 전송에 대해 고객에게 알릴 것
ii) 정보사용의 목적 변경 금지 및 부정확한 정보의 전송 금지
iii) 인터넷 등을 통하여 제3자에게 개인정보의 역외전송을 하는 경우 데이터암호화 등을 통한 정보보안에 요구되는 조치를 반드시 취해야 함
iv) 개인정보 사용 이후 정보의 적절한 처분을 보장할 것

■ **(기관 간 정보공개 제한)** 법집행기관 및 금융규제기관에 대한 정보공개가 정보수집의 원목적과 직접적으로 관련되지 않은 경우, 동 기관들에 대한 정보공개는 개인정보보호법령 제8장에 예외부분에 해당되는 경우나 해당 개인으로부터 사전에 규정된 동의를 받은 경우에만 가능하다.

■ **(채무수급시 고객정보 이용 고지)** 은행은 고객에게 채무 수금을 위하여 고객의 개인정보를 사용할 가능성이 있음을 알리고, 고객의 채무상태에 대한 정보를 발송하는 경우 발송편지는 편지봉투에 동봉하여 수신자 본인만 열어볼 수 있음을 알리는 문구를 삽입하여야 한다. 채무수금을 위하여 수금전문업체에 이를 의뢰하는 경우, 은행은 여전히 정보사용자로서의 개인정보보호법령상의 의무를 준수하여야 하며 수금전문업체에 대하여 업무에 필요한 정도 이외의 정보는 제공하여서는 아니 된다.

■ **(현장 외 마케팅 광고 중 고객 개인정보의 보호)** 현장 외에서 마케팅 광고 중 수집된 개인정보를 보호하기 위하여 다음의 7가지를 보장하여야 한다.

i) 정보 수집중, 혹은 수집 이후 관련 없는 자가 정보를 열람하거나 접근하지 아니할 것
ii) 수집된 신청서는 적절히 기록할 것
iii) 신청서는 지정된 직원의 관리 하에 잠금장치가 설치된 컨테이너 내에 안전하게 보관되어야 함
iv) 휴대용 저장소에 보관된 개인정보는 암호화하여 충분한 보안을 제공할 것
v) 신청서가 보관되거나 처리될 은행 지점으로의 신청서 전달이 안전하게 이루어질 수 있도록 특정한 예방 조치를 이행할 것
vi) 직원들이 신청서를 자택으로 가져가는 행위를 금지할 것
vii) 신청서의 보안을 감독하기 위한 직원을 지정할 것

■ **(개인정보 수집 설명서 제공)** 고객이 인터넷 뱅킹 시스템에 접속하는 경우 은행은 고객의 개인정보를 수집하기 전에 개인정보수집설명서를 제공하여야 하며, 온라인 문서를 작성하여야 하는 경우 이는 서면의 것과 같아야 한다. 또한 쿠키가 사용되는 경우, 그러한 쿠키 내에 어떠한 정보가 저장이 되는지에 대해서 명확한 설명을 제공하여야 한다.

■ **(개인정보 보유 확인 요청권)** 각 개인은 정보사용자에 대하여 그 정보사용자가 자신의 개인정보를 보유하고 있는지, 보유하고 있는 정보의 사본을 제공해줄 수 있는지 대해서 확인을 요청할 수 있다. 이러한 요청은 해당 개인정보의 주체 혹은 관련 있는 자(relevant person)에 의해서 이루어질 수 있다. 여기서 관련 있는 자란 해당 개인정보 주체로부터 그를 대신하여 정보접근에 대한 요청을 할 수 있도록 서면으로 허가받은 자를 의미하고, 이러한 요청을 받은 정보사용자는 해당 요청을 처리하는데 드는 비용을 과다하게 청구하여서는 아니 된다.

평가

■ 동 가이드라인은 실무자들이 공통적으로 직면하는 실제상황을 다루고 있다는 점에서 은행업계에 매우 유용할 것으로 판단되고 있다.

– Chiang 위원은 “우리는 모든 은행 및 그밖의 금융기관들이 이 가이드라인을 유용하게 사용할 수 있도록 장려하고 있다. 은행 및 금융서비스에서의 정보보호에 관한 전문가 워크숍의 내용을 동 가이드라인을 고려하도록 갱신할 예정이며 은행업무 관련 실무가들이 이에 적극적으로 참여할 것이다. 개인정보보호에 적극적인 은행부문 기업들은 이전보다 높아진 고객들의 신뢰와 충성도를 경험하게 될 것이며 이로써 고객, 기업 그리고 은행산업 전체가 서로 상생하는 환경이 조성될 것으로 전망된다”고 평가한바 있다.

참고자료

http://www.pcpd.org.hk/english/infocentre/press_20141006.htm

http://www.pcpd.org.hk/english/publications/files/GN_banking_e.pdf

http://www.lexology.com/library/detail.aspx?g=c1770f49-cac4-4715-9d8c-837866b5e89a

http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2880

http://www.out-law.com/en/articles/2014/october/hong-kong-watchdog-issues-new-data-protection-guidelines-for-banks-amidst-rising-number-of-complaints/

참고 웹사이트

1 국내 웹사이트

[1] 국회 (http://www.assembly.go.kr)

2 국외 웹사이트

[1] http://www.lexology.com/library/detail.aspx?g=92a3ad2a-f113-4635-bbdf-1657533d26b7&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Other+states+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2014-10-24&utm_term=

[2] http://www.workplaceprivacyreport.com/2014/10/articles/written-information-security-program/california-ab-1710-first-law-in-u-s-to-require-credit-monitoring-following-a-data-breach/

[3] http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000134.html

[4] http://www.soumu.go.jp/main_content/000320320.pdf

[5] http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s969

[6] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fs969_ems_2dbf9bb1-59cd-44ed-8e6a-d106c5535c72%22

[7] http://www.itnews.com.au/News/396365,parliament-passes-law-to-let-asio-tap-entire-internet.aspx

[8] http://www.legislation.sa.gov.au/Web/Information/Understanding%20legislation/UnderstandingLegislation.aspx#bills

[9] http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RefE_ElektronAkteStrafsachen.pdf?__blob=publicationFile

[10] http://www.damm-legal.de/lg-muenchen-i-grundsatzfrage-der-haftungsbefreiung-bei-betrieb-eines-offenen-wlan-durch-gewerbetreibenden-wird-dem-eugh-zur-entscheidung-vorgelegt

[11] http://www.cr-online.de/38218.htm

[12] http://www.golem.de/news/offenes-wlan-eu-gerichtshof-soll-ueber-wlan-haftung-entscheiden-1410-109731.html

[13] https://www.wbs-law.de/abmahnung-filesharing/offenes-wlan-und-filesharing-abmahnung-gericht-schaltet-eugh-ein-56618/

[14] http://curia.europa.eu/juris/celex.jsf?celex=62013CO0348&lang1=en&type=TXT&ancre=

[15] http://www.telemedicus.info/article/2575-EuGH-Vorlage-Verletzt-Framing-das-Urheberrecht.html?pk_campaign=feed

[16] http://www.harrisbeach.com/media-news/10170

[17] http://www.kslaw.com/imageserver/KSPublic/library/publication/ca102414.pdf

[18] http://www.forbes.com/sites/groupthink/2014/10/03/fda-guidance-on-medical-device-cybersecurity-too-little-too-late/

[19] http://www.usatoday.com/story/tech/2014/10/01/fda-medical-devices-cybersecurity/16543731/

[20] https://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2014/pm013.html

[21] http://www.gesetze-bayern.de/jportal/portal/page/bsbayprod.psml?doc.id=JURE140015287&st=ent&showdoccase=1&paramfromHL=true

[22] http://www.justiz.bayern.de/gericht/ag/m/presse/archiv/2014/04469/

[23] http://www.justiz.bayern.de/gericht/ag/m/presse/archiv/2013/04014/

[24] http://www.pcpd.org.hk/english/infocentre/press_20141006.htm

[25] http://www.pcpd.org.hk/english/publications/files/GN_banking_e.pdf

[26] http://www.lexology.com/library/detail.aspx?g=c1770f49-cac4-4715-9d8c-837866b5e89a

[27] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2880

[28] http://www.out-law.com/en/articles/2014/october/hong-kong-watchdog-issues-new-data-protection-guidelines-for-banks-amidst-rising-number-of-complaints/

[29] https://privacyassociation.org/news/a/belgiums-new-government-sets-privacy-high-on-the-agenda-appointing-minister-of-privacy/

[30] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2899

[31] http://www.technologyslegaledge.com/2014/10/16/belgium-belgian-governments-new-focus-on-privacy-and-technology-laws/