방통융합정책연구 KCC-2017-21

정보통신서비스 분야의 민감정보 유형과 보호방안 연구

(A Study on Types of Sensitive Personal Information and Protective Measures in the Field of Information and Communication Services)

김민호/김현경/김선아

2017. 11

연구기관 : (사)개인정보보호법학회

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

이 보고서는 2017년도 방송통신위원회 방송통신발전기금 방송통신 융합 정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『**정보통신서비스 분야의 민감정보 유형과 보호방안 연구**』의 연구결과보고서로 제출합니다.

2017년 11월

연구기관 : 개인정보보호법학회

총괄책임자 : 김민호 교수(성균관대학교)

참여연구원 : 김현경 교수(서울과학기술대학교)

김선아 초빙교수(숭실대학교)

목 차

표 목 차

요 약 문

1. 제 목

정보통신서비스 분야의 민감정보 유형과 보호방안 연구

2. 연구 목적 및 필요성

민감정보는 통상의 개인정보와는 달리 그 침해 시 프라이버시 침해요소가 심각한 정보로 세계 각국에서도 이에 대하여 특별히 규율하고 있다. 국내에서도 「개인정보 보호법」이나 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 “정보통신망법”이라 한다)을 통해 민감정보에 대하여 원칙적으로 수집을 금하되, 예외적으로 정보주체의 동의나, 법령상 규정에 의해서만 수집하도록 허용하고 있다. 다만 “민감정보”에 해당되는지에 대한 판단기준의 미흡, 달리 취급하는 정도의 불명확함 등으로 인해 규율에 혼선이 야기될 우려가 있다. 특히 민원발급기, 스마트폰 등에서 이용이 확산되고 있는 생체정보도 일반법인 개인정보보호법이 적용되지만, 법적용에 한계가 있다는 지적을 받고 있으며, 지문, 홍채 등의 생체정보 뿐만 아니라 웨어러블 기기가 측정하는 다양한 생체 정보가 활용될 전망이라고 하면서, 이러한 생체정보에 대한 규율 필요성 이 제기되고 있다. 뿐만 아니라 “개인영상정보”는 특히나 다양한 이동형 영상정보처리기기의 발달로 그 침해가능성이 증대되고 있다. 특히 얼굴인식 기술이 페이스북, 구글 글라스의 사례처럼 널리 활용되고 있어 정보매개자를 통한 개인영상정보의 처리도 문제된다. 따라서 정보통신서비스 제공 과정에서 수집·이용되는 민감정보의 유형을 분류하고 특성에 부합하는 개선방안을 마련할 필요가 있다.

따라서 이 연구는 민감정보와 관련된 「정보통신방법」 의 개정방안을 마련하는 것을 주된 목표로 한다. 특히 민감정보 중에서도 ‘생체정보’와 ‘개인영상정보’에 대한 부분을 별도로 검토하고 개정방안을 도출하였다.

3. 연구의 구성 및 범위

이 연구는 민감정보와 관련된 「정보통신방법」 개정(안)을 마련하는 것을 주된 연구의 범위로 정하였는바, 이에 관련한 연구의 범위를 다음과 같이 제한하였다.

첫째, 현행 개인정보 보호법제상 “민감정보”의 개념 정의 및 규율 현황을 분석 한 후, 정보통신서비스 제공과정에서 수집·이용되는 민감정보의 활용사례를 분석하였다.

둘째, 특히 최근 가장 쟁점화 되고 있는 “생체정보”와 “개인영상정보”의 현행법상 규율 현황 및 한계를 분석하고 「정보통신망법」 개선방안을 제안하였다.

셋째 민감정보와 관련하여 EU, 일본, 독일 등 국외 법제 현황을 조사·분석하였다.

넷째, 민감정보에 대한 현행 정보통신망법의 한계점과 개선방안 도출하였다.

다섯째, 위 연구결과를 반영한 「정보통신망법」 개정안을 제안하였고 입법설명자료로서 입법의 필요성, 주요내용, 쟁점사항, 참조입법례를 부가하였다.

4. 연구 내용 및 결과

연구의 결과를 요약하면 다음과 같다.

첫째, 현재 「정보통신망법」은 민감정보 해당성의 융통성을 발휘하기 위하여 ‘예시적 방식’으로 규정하고 있다. 그러나 민감정보 해당성 여부가 개개인의 주관적 성향에 따라 달라진다면 법적 안정성이나 명확성 측면에서 바람직하지 않으므로, 한정적 열거방식이 타당하다. 「개인정보 보호법」도 이러한 점을 반영하여 대통령령 위임을 통해 한정적 열거방식을 채택하고 있으며, GDPR의 경우도 열거방식을 채택하고 있다. 불가피하게 융통성을 두고자 한다면 현행 「개인정보 보호법」과 같이 기준을 정하여 대통령령에 위임하는 방안도 검토될 수 있으나 기본취지는 한정적 열거방식을 취하는 것이 바람직하다. 또한 「정보통신망법」은 민감정보 수집의 정당화 근거를 “법률”로 제한하고 있으나, 「개인정보 보호법」은 대통령령을 포함한 “법령”으로 그 범위를 넓히고 있다. 「정보통신망법」에서 특별히 더 수집, 이용의 근거를 더 강화해야할 실익이 없는 한 이는 기본법 수

준에 부합하는 것이 타당하다.

둘째, ‘개인을 고유하게 하는 목적의 생체정보(biometric data for the purpose of uniquely identifying a natural person)’를 ‘민감정보’에 포함시키는 것이 타당하다. 현행 「개인정보 보호법」 및 「정보통신망법」상 ‘생체정보’는 ‘민감정보’에 해당되지 않으므로 일반 개인정보로 취급된다. 한편 단순히 서비스제공과정에서 처리되는 모든 생체정보를 민감정보를 규율한다면, 전혀 프라이버시침해적 요소나 권리와 자유침해의 리스크가 없음에도 불구하고 과도한 규율이 된다. GDPR 역시 민감정보로서 ‘생체정보’에 대하여는 ‘개인을 식별하기 위한 목적으로 사용되는 경우’로만 한정하는 것은 결국 ‘인증’ 이나 본인확인을 목적으로 생체정보를 활용하는 경우를 의미한다고 보여 진다. 따라서 본인을 인증 또는 확인하기 위한 수단으로 사용되지 않는 한 생체정보는 민감정보로 규율하지 않는 것이 바람직하다. 민감정보에 해당되는 생체정보를 ‘특정인을 인증 또는 확인하기 위해 기술적으로 처리된 생체정보’ 제한하여 규정하는 것이 바람직하다.

한편 관리, 보관, 파기 등에 있어서 생체정보에 대한 특칙은 불필요하다. 다만 GDPR과의 관계에서 대규모 민감정보의 처리에 대하여 개인정보 영향평가의 실시를 규정하고 있는바 국내법에의 도입에 대하여는 좀 더 고민이 필요하다. 그밖에 파기의 기술적 기준, 기술적·관리적 조치에 대한 특별한 사항은 고시나 지침을 통해 구체화하는 것이 바람직하다.

세째, 정보통신서비스 제공자의 개인영상정보 처리와 이에 대한 법률적 취급은 정보통신서비스 제공자가 개인영상정보 처리에 개입하는 방식에 따라서 차별적으로 접근할 필요가 있다. 정보통신서비스 제공자가 직접 개인영상정보를 촬영하는 경우에는 영상정보처리기기의 설치 · 운영 등에 관한 사항을 규율하는 「개인영상정보 보호법(안)」의 적용대상으로 하는 것이 가능할 것이다. 그러나 정보통신서비스 이용자가 개인영상정보를 촬영하여 정보통신서비스 제공자의 서비스를 통해 유통하는 매개유형의 경우에는 정보통신서비스 제공자가 영상정보처리기기의 설치 · 운영하는 것이 아니므로 「개인영상정보 보호법(안)」의 적용대상으로 적절하다고 보기 어렵다.

이용자가 촬영한 개인영상정보를 정보통신서비스 제공자가 매개하는 서비스만 제공할 경우 정보통신서비스 제공자는 일일이 개인영상정보를 개별적으로 모니터링 할 수 없다. 따라서 타인에 의해 해당 정보의 매개를 통하여 수익을 창출하는 정보통신서비스 제공자는 개인영상정보를 처리하는 이용자로 하여금 준수해야 하는 일정한 지침을 마련하여 사

전에 개인영상정보 침해 위험에 대비하도록 하는 방안을 「정보통신망법」의 개정을 통해 도입할 필요가 있다. 또한 정보통신서비스의 전파성, 신속성 등에 비추어 볼 때 영상정보주체의 원치 않는 개인영상정보의 유출에 대한 신속한 권리구제 방안을 마련하는 것이 타당하다.

5. 정책적 활용 내용

본 연구는 방송통신위원회 등 정부부처의 정책 입안을 위한 이론적 기틀과 민감정보의 보호를 위한 정책수립근거를 제공할 것이다. 따라서 도출된 정책의 개선방향은 정책결정에 반영될 수 있다. 뿐만 아니라 향후 「개인영상정보 보호법」안의 제정으로 발생하는 현실적 문제점을 미리 예상함으로써 개인영상정보 보호 및 이를 활용하는 서비스 간의 균형적 규제방안을 마련하는데 참고할 수 있다.

6. 기대효과

기대효과는 크게 정책활용 가능성, 경제·사회적 기여도, 연구결과 활용방안, 관련분야 예상파급효과로 나누어 설명할 수 있다.

정책활용과 관련하여서는 방송통신위원회 등 정부부처의 정책 입안에 도움이 될 수 있다. 또한 현행 관련법의 문제점에 근거하여 민감정보 제도의 문제점에 대한 해결 방안을 제시하였으므로 이용자와 정보동신서비스제공자간의 분쟁과 혼선을 예방하는데 기여할 수 있다.

한편 연구결과는 향후 방송통신위원회, 대법원, 헌법재판소 등에서 정책 형성 및 결정을 하는데 있어 기초가 되는 참고자료로 활용되며 연구의 결론을 도출하기 위해 사용된 연구방법을 활용한 각종 조사자료 등은 향후 개별 연구자들의 논문 등을 통하여 국내·외의 연구자들에게 제공될 수 있다.

그리고 현재 생체정보와 개인영상정보를 이용하여 서비스를 제공하는 '정보통신서비스 제공자'가 법 적용의 혼선을 최소화하며 비즈니스를 영위하는데 참고할만한 가이드로

활용하리라 생각되다. 또한 민감정보에 대한 규율 개선방안 뿐만아니라 개인영상정보 및 생체정보와 관련된 미래지향적 정비방안을 제시함으로써 법제 정비에 대한 국민적 공감대 형성에도 기여할 수 있다.

제1장 서 론

제1절 연구의 필요성

민감정보는 통상의 개인정보와는 달리 그 침해 시 프라이버시 침해요소가 심각한 정보로 세계 각국에서도 이에 대하여 특별히 규율하고 있다. EU의 '일반정보보호규정'(General Data Protection Regulation, 이하 "GDPR"이라 한다) 역시 유전자정보, 개인을 특정하기 위한 목적으로 생체정보, 및 건강, 성생활, 성적 취향에 관한 정보를 처리하는 것은 원칙적으로 금지되고, 정보주체가 명시적인 동의(explicit consent)를 하는 경우 등에는 예외적으로 허용된다고 규율하고 있다. 일본 역시 사회적 차별의 원인이 될 우려가 있는 인종, 신념, 사회적 신분 및 범죄 기록 · 전력 등에 관한 정보를 민감 정보로 결정하고 개인정보에 이 정보가 포함된 경우에는 원칙적으로 취급을 금지하는 등 신중히 취급하고 있다.

국내에서도 「개인정보 보호법」이나 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 "정보통신망법"이라 한다)을 통해 민감정보에 대하여 원칙적으로 수집을 금하되, 예외적으로 정보주체의 동의나, 법령상 규정에 의해서만 수집하도록 허용하고 있다. 다만 "민감정보"에 해당되는지에 대한 판단기준의 미흡, 달리 취급하는 정도의 불명확함 등으로 인해 규율에 혼선이 야기될 우려가 있다. 특히 민원발급기, 스마트폰 등에서 이용이 확산되고 있는 생체정보도 일반법인 개인정보보호법이 적용되지만, 법적용에 한계가 있다는 지적을 받고 있으며,지문, 홍체 등의 생체정보 뿐만 아니라 웨어러블 기기가 측정하는 다양한 생체 정보가 활용될 전망이라고 하면서, 이러한 생체정보에 대한 규율 필요성 이 제기되고 있다.

민감정보 중 "개인영상정보"는 특히나 다양한 이동형 영상정보처리기기의 발달로 그 침해가능성이 증대되고 있다. 현재, 전국적으로 400만대 이상의

CCTV가 설치・운영 중이며, 인권위원회에 따르면 수도권 시민의 하루 평균 CCTV 노출 건수가 평균 83차례에 이르고 있어, 사생활 침해에 대한 우려가 높아지고 있다. 450만대가 설치된 것으로 추정되는 자동차 블랙박스는 설치・운영에 대한 별도의 규제가 없으며 촬영된 영상에 개인영상정보가 포함되었을 경우에만 개인정보보호법이 적용된다. 특히 얼굴인식 기술이 페이스북, 구글 글라스의 사례처럼 널리 활용되고 있어 정보매개자를 통한 개인영상정보의 처리도 문제된다.

따라서 정보통신서비스 제공 과정에서 수집·이용되는 민감정보의 유형을 분류하고 특성에 부합하는 개선방안을 마련할 필요가 있다. 현행「개인정보 보호법」제23조와 「정보통신망법」은 제23조에서 각각 민감정보에 대하여 규율하고 있으나, 「개인정보 보호법」이 민감정보의 판단기준을 "사생활 침해 우려"만 규정하고 있는 반면, 「정보통신망법」은 민감정보의 판단여부를 "사생활 침해" 뿐만 아니라 "개인의 권리·이익 침해"까지 포함하고 있으므로 「정보통신망법」민감정보의 범위가 더 넓어 질 수 있다. 또한 「개인정보 보호법」은 사생활을 현저히 침해할 우려여부에 대한 해석의 여지가 크기 때문에 민감정보로 특별히 보호할 필요가 있다고 사회적 합의가 이루어진 정보를 상황에 맞게 규정할 수 있도록 대통령령에 위임하여 현재 6가지 종류의 정보를 민감정보로 열거하고 있다. 그러나 「정보통신망법」은 "기타 ~~등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보"라고 규정함으로서 앞에 제시된 정보는 예시적 사항이며 추가적 민감정보가 법률상 포섭될 수 있도록 규정하고 있으므로 민감정보 해당성에 대한 추가적 판단이 더 절실히 필요하다.

한편 최근 다양한 분야에서 드론(Drone)기기·웨어러블(Wearable)기기·차량용블랙박스등 '이동형 영상처리기기'의 이용이 점차 확산되면서 국가기관을 비롯해 私人에 의해 개인의 영상정보가 언제어디서나 손쉽게 촬영될 수 있어 「헌법」이 개인에게 보장하고 있는 인간으로서의 존엄과 가치·사생활 비밀과 자유·행복추구권·인격권·개인정보자기정보결정권 등과 같은 개인의 기본적인 인권이 침해될 위험성이 증대된다. 특히 개인정보 중에서도 개인영상정보는

개인의 얼굴·신체부위는 물론 레저활동·업무활동 등과 같은 개인일상생활의 전체과정을 포함하고 있어, 그 처리과정에서 개인의 사적으로 내밀한 영역까지 침해 가능하다. 그러나 현행 개인영상보호법체계는 CCTV 등과 같은 고정형 영상정보처리기기에 주로 초점이 맞추어져 있을 뿐 수많은 분야에서 그 활용도가 증대된 이동형 영상정보처리장치에 의한 개인영상정보의 무분별한 수집·저장·유출·오남용 등의 침해위험성에 대비한 법제도적 대응이 충분하게 이루어지지 않고 있다. "개인영상정보"의 현행법상 규율 현황 및 한계를 분석하고 「정보통신망법」 개선방안이 제안될 필요가 있다.

제2절 연구의 범위 및 방법

1. 연구의 범위

이 연구는 민감정보와 관련된「정보통신방법」 개정(안)을 마련하는 것을 주된 연구의 범위로 정하였는바, 이에 관련한 연구의 범위를 다음과 같이 제한하였다.

첫째, 현행 개인정보 보호법제상 "민감정보"의 개념 정의 및 규율 현황을 분석 한 후, 정보통신서비스 제공과정에서 수집·이용되는 민감정보의 활용사례를 분석하였다.

둘째, 특히 최근 가장 쟁점화 되고 있는 "생체정보"와 "개인영상정보"의 현행법상 규율 현황 및 한계를 분석하고 「정보통신망법」 개선방안을 제안하였다.

셋째 민감정보와 관련하여 EU, 일본, 독일 등 국외 법제 현황을 조사·분석하였다.

넷째, 민감정보에 대한 현행 정보통신망법의 한계점과 개선방안 도출하였다.

다섯째, 위 연구결과를 반영한 「정보통신망법」 개정안을 제안하였고 입법설명자료로서 입법의 필요성, 주요내용, 쟁점사항, 참조입법례를 부가하였다.

2. 연구의 방법

이 연구를 수행하기 위해 다음과 같은 연구방법을 진행하였다.

첫째, 정보통신망법 상 민감정보 개선방안 제시를 위한 국내법 현황 및 동향을 분석하였다. 개인정보의 일반법이라 할 수 있는 개인정보 보화법과 관련 법령을 분석하고 개인정보 보호제도에 있어서 민감정보가 가지는 의의, 개념을 분석하였다 .

둘째, 민감정보 규율 개정방안을 도출하기 위해 외국법 현황 및 동향을 분석하였다. EU, 독일, 일본 등 각국의 민감정보 규율현황을 조사, 분석하였다.

셋째, 정보통신서비스 제공과정에 있어서 현행 민감정보 규율의 문제점을 파악 하고 그 개선방안을 제시하였다. 특히 생체정보와 개인영상정보의 활용 현황을 분석하고 민감정보로서 규율하는 것에 대한 타당성, 필요성 등을 검토하였다.

넷째, 개선방안과 연관된 법령 개정방안을 제시하였다. 기존 제도의 문제점을 파악하여 그 개선방안으로서 법령 개정방안을 도출하였다.

다섯째, 외국 입법례 및 현행 국내법 검토 분석을 위해 법학 등을 전공한 학계 전문가와 연구 협력체계를 구축하고 세부 과제별로 방송통신위원회 및 전문가로 구성된 연구협력팀을 구성 운영하였다.

여섯째, 연구결과의 공유 및 추진일정 점검을 위한 연구보고회를 개최하였다. 수시 연구협력회의와 전문가 자문회의를 통하여 연구에 대한 객관성, 신뢰성을 확보하였고, 향후 연구수행방향에 대한 구체적인 의견을 수렴하여 반영하였다.

제2장 개인정보보호와 민감정보 규율현안

제1절 개인정보보제도와 민감정보

1. 민감정보의 개념과 의의

민감정보의 개념, 기준에 대하여 현행법상 명확히 규정하고 있지는 않다. 다만 앞서 언급하였듯이 「개인정보 보호법」이 민감정보의 판단기준을 "사생활 침해 우려"라고 규정하고 있는 반면, 「정보통신망법」은 "사생활 침해" 뿐만 아니라 "개인의 권리·이익 침해"까지 포함하고 있다. 후술하겠지만. GDPR의 경우 '특수한 유형의 개인정보'라는 표현 하에 이러한 개인정보를 더 구체적으로 보호해야 하는 이유로 '기본권과 자유 침해의 위험'을 제시하고 있다. 일본의 경우는 "배려를 요하는 개인정보"라고 표현하고 있으며 본인에 대한 부당한 차별, 편견 등 불이익이 생기지 않도록 그 취급에 특별히 배려를 요하는 것을 기준으로 규정하고 있다. 이처럼 민감정보는 통상적으로 다른 개인정보와 달리 취급하여야 할 필요성이 인정되는 경우를 의미하며, 이에 대하여는 반드시 '민감정보'라고 표현하는 것은 아니며, '특수한 범주(유형)의 개인정보'(GDPR), '배려를 요하는 개인정보'(일본)등으로 표현되기도 한다.

우리나라에서 1994년 제정되어 1995년 1월 8일 시행된 「공공기관의개인정보보호에관한법률(법률 제4734호)」에 의하면 특별히 민감정보라는 표현으로 규율하고 있지는 않다. 다만 동법은 "공공기관의 장은 사상·신조등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다"고 규정함으로서(공공기관의개인정보보호에관한법률 제4조 전문) 기본적 인권을 침해할 우려가 있는 개인정보의 수집을 원칙적으로 금지하였다.[1] 이러

1) 예외적으로 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 수집이 가능하도록 규정하였다(공공기관의개인정보보호에관한법률 제4조 후문).

한 부분이 후일 「개인정보 보호법」의 민감정보 규정의 전신이라고 할 수 있다. 따라서 「공공기관의개인정보보호에관한법률」은 '기본적 인권을 침해할 우려'를 민감정보의 기준으로 설정한 것으로 보인다.

2. 개인정보보호자기결정권과 민감정보

헌법재판소는 주민등록법 제17조의8 등 위헌확인 등 사건에서 "개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다."고 하여 기존의 자기결정권 결정들과는 달리 '개인정보'자기결정권의 근거를 헌법상 명시되지 아니한 기본권이라고 처음으로 설명하였다. 또한 공직자등의병역사항신고및공개에관한법률 제3조 등 위헌확인사건에서 "이 사건 법률조항에 의하여 그 공개가 강제되는 질병명은 내밀한 사적 영역에 근접하는 민감한 개인정보이다."고 하여 '민감한' 개인정보보호를 위한 도출근거로 헌법 제17조를 들고 있다. 최근 접견 녹음파일 송부 요청 취소사건에서 헌법재판소는 "개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리로서, 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장된다."[2]고 결정하여 '개인정보'자기결정권의 헌법상 근거조항으로 헌법 제10조와 헌법 제17조를 제시하였다.

이 이후로 헌법재판소는 개인정보자기결정권의 헌법상 도출근거로 일관되게 "인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유"를 언급하고 있다.[3] 이렇게 볼 때 개인정보의 보호의 헌법적 근거는 일반적 행동자유권에서 비롯된

2) 헌재 2012. 12. 27. 2010헌마153

3) 헌재 2015. 7. 30. 2014헌마340・672, 2015헌마99(병합) ; 헌재 2016. 3.31. 2015헌마688 ; 헌재 2016. 4. 28. 2012헌마630

자기결정권과 법 제17조의 사생활의 비밀과 자유라고 볼 수 있다. 그렇다면 일반 개인정보와 민감정보의 구별기준은 그 침해 시 일반적인 행동자유권과 사생활 비밀의 침해가능성이 현저히 높은 경우가 되어야 할 것이다.

서론에서 언급한 바와 같이 민감하다는 것은 "자극에 빠르게 반응을 보이거나 쉽게 영향을 받음"을 의미한다. 특정한 개인정보가 처리됨으로서 정보주체에게 어떤 빠르고 쉬운 영향을 미친다는 것은 법문의 의미로서는 너무나 주관적이고 추상적이다. 따라서 현행 민감정보의 규율취지가 일반적인 행동자유권이나 사생활 침해가능성이 더 높은 개인정보를 특별히 취급할 필요성으로 인한 것이라면, '민감정보'라는 표현은 타당하지 않다. 오히려 EU의 경우처럼 '특수한 유형(또는 범주)의 개인정보'로서 규율하는 것이 바람직하다.

또한 앞서 일반적인 개인정보와 구별 짓는 기준으로 제안된 '개인의 권리·이익 침해'나 '차별·편견으로 인한 부당한 불이익'은 결국 정보주체의 일반적인 행동 자유의 제약으로 귀결된다. 또한 개인정보자기결정권에 대한 헌법적 근거는 기본적으로 '사생활의 비밀과 자유의 보장'이다. 따라서 특수한 유형의 개인정보와 일반적인 개인정보를 구별 하는 기준은 '정보주체의 자유와 사생활을 현저히 침해할 우려'이다.

이렇게 규율할 경우 '주민등록번호'는 우리나라의 경우 오남용 혹은 유출 되었을 때 '정보주체의 자유와 사생활을 현저히 침해할 우려'가 인정된다. 따라서 '민감정보'와 별도로 규율하는 것 보다는 '특수한 유형의 개인정보'로 함께 규율함이 더 체계적이다.

3. 정보통신서비스와 민감정보 활용

「정보통신망법」은 정보통신서비스제공자의 민감정보 처리에 대한 규정을 두고 있다. '정보통신망법'은 정보통신서비스제공자를 "전기통신사업법 제2조제1항제1호의 규정에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자"로 규정하고 있다(제2조제3호). 즉 이 법에 의하면 ①전기통신사업자, ②정보제

공자 및 ③정보제공매개자의 세 가지 행위주체가 모두 포함된다. ①은 인터넷 접속사업자(ISP)를 의미하는 것이고 ③이 정보를 복제·전송할 수 있도록 서비스를 제공하는 자(정보제공의 매개자)라고 한다면, ②는 직접적으로 정보를 발신 제공하는 자(CP)를 말한다.

이러한 정보통신서비스제공자가 개인정보를 활용하는 유형은 개인정보를 직접 수집하여 이용하는 경우와, 타인에 의해 수집된 개인정보를 매개만 하는 경우로 나누어 볼 수 있다. 특히 최근 가장 자주 활용대상이 되고 있는 개인정보는 개인영상정보를 포함한 '생체정보'이다. 생체정보는 다음과 같은 특성을 지닌다. 우선 "지참성"이다. 항상 본인과 함께 존재한다. 별도로 보관할 필요가 없으며 다른 정보와 달리 도난이나 분실의 우려가 거의 없다. 이러한 편리성과 경제성으로 인해 고도의 부가가치를 창출할 바이오와 정보기술의 새로운 융합산업군으로 전망되기도 한다.[4] 다음으로 '불변성·영구성'이다. 주민등록번호나 비밀번호 등 각종의 개인정보는 변경이 가능하나, 개인생체정보는 변경할 수 없다. 따라서 일단 유출이 되고 나면 다른 생체정보로 대체하지 않는 이상 그 생체정보를 사용할 수가 없게 된다. 생체정보는 다른 개인정보와는 달리 살아있는 동안 그 사람과 결합되어 있기 때문에 이름이나 주소, 식별번호, 암호와 같이 변경할 수 없다는 특수성을 가진다.[5] 이러한 특성으로 인해 생체정보는 여타 개인정보에 비해 더 엄격하게 보호되어야 한다고 주장된다. 즉 생체인식기술은 개인이 가진 신체 특징은 태어나서 죽을 때까지 변하지 않는다는 점에 착안한 기술로, 생체정보는 다른 개인정보와는 달리 정보 그 자체가 개인을 나타낼 수 있으므로 다른 개인정보보다 그 보호를 강화할 필요가 있다고 한다.[6] 따라서 '개인영상정보'를 포함한 생체정보는 '정보주체의 자유와 사생활을 현저히 침해할 우려'가 강하다.

---

4) 조규범, "생체정보보호를 위한 입법론적 대응방안", 「국회도서관회보」, 제45권 제9호(통권352호), 50면.

5) 김일환, "정보사회에서 생체정보의 보호에 관한 헌법적 고찰", 인권과 정의 제344호, 2005.4., 23면 이하 참조.

6) 김일환, 전제논문, 359-360면

대체적으로 정보통신서비스제공자가 이러한 정보를 직접 수집하여 이용하는 경우는 본인 확인을 위한 인증의 경우가 대다수라고 할 수 있다. 이러한 본인 확인을 위한 인증의 경우, 성인인증, 결제서비스, 기기인증 등에서 활용된다. 대면중심의 오프라인에서는 본인인증이 특별히 문제될 것이 없다. 주로 주민등록증/운전면허증 소지와 대면인식이 함께 이루어지므로 본인인증을 위한 특별한 기술적 이슈가 존재하지 않는다. 그러나 비대면인 온라인 상에서는 필수적으로 본인확인 즉 인증이 중요한 기술적 제도적 이슈가 될 수밖에 없다. "온라인 인증"이라 함은 여러 사람이 공유하고 있는 컴퓨터 시스템이나 통신망의 경우 이를 이용하려는 사람이나 장치 및 응용프로그램의 신분(identification)을 확인하여 불법적인 사용자가 들어올 수 없도록 시스템 보안을 유지하는 방법을 의미한다. 특히 생체기반 인증은 사용자가 가지고 있는 고유한 지문이나 홍체, 정맥등과 같은 생체적 특징을 이용하여 인증하는 방식으로 이용자의 생체정보(지문인식, 얼굴인식, 전자펜서명인식등)를 이용하여 본인 확인을 하는 방식이다. 얼굴구조, 지문, 홍채, 정맥 등 생체적 특징을 이용한 방식과, 목소리, 타이핑리듬 등 행동적 특징을 이용한 방식이 있다. 분실, 변경의 위험이 없어 다른 인증수단 보다 보안성이 높다는 장점이 있으나, i)생체정보를 인식할 시스템이 필요하여 비용이 많이 소요되고, ii)생체정보 이용에 대한 거부감이 있을 수 있으며, iii)변경이 불가능하여 유출시 복구가 불가능하다는 단점이 있다.

타인에 의해 수집된 정보를 매개만 하는 경우는 온라인동영상서비스 및 SNS 서비스제공과정에서 이루어지는 개인영상정보의 경우가 대표적이다. 최근 다양한 분야에서 드론(Drone)기기·웨어러블(Wearable)기기·차량용블랙박스등 '이동형 영상처리기기'의 이용이 점차 확산되고 있다. 과거와 달리 폐쇄회로텔레비전(CCTV) 등의 '고정형 영상정보처리기기' 뿐만 아니라, 차량용(Black box)영상처리기기·무인항공기(Drone)영상처리기기·웨어러블(Wearable)영상처리기기 등과 같이 누구나 언제어디서든 촬영이 가능한 이동형 영상정보처리기기의 급격한 이용과 확산으로 인하여 개인의 사적인 정보가 침해될 위험성이 증폭되고 있다. 초기 드론·스마트글래스·차량용블랙박스 등 이동형 영상정보처리기기는 정찰용·방범용·방송용·군사용 등 특정목적을 위해 공공분야에서 주

로 사용되어 왔지만 최근 그 판매가격과 이용비용이 낮아지면서, 레저용·농업용·택배용 등 민간의 여러분야로도 그 이용이 점차 확대되고 있다. 특히, 개인영상정보는 개인일상생활의 전체과정을 포함하고 있어, 그 처리과정에서 개인의 사적으로 내밀한 영역까지 침해가 가능하다. 이동형 영상정보처리기기의 운영과정에서 무분별하게 수집될 수 있는 개인의 전신·얼굴·옷차림새·활동 등의 개인영상정보는 개인의 프라이버시와 민감하게 관련되며, 이동형 영상정보처리기기는 이동성·휴대성·융합성·은밀성·연계성·첨단성 등의 특징으로 말미암아 과거에 비해 개인영상정보가 침해될 위험성이 높다. 현행「개인정보 보호법」제25조는 고정형 영상정보처리기기에 관한 사항만 규율하고 스마트폰, 블랙박스, 드론 등 이동형 영상정보처리기기는 규율 범위에서 제외된다. 따라서 이동형 영상정보처리기기에 의한 개인영상정보의 수집, 처리에 대하여는 '개인정보 처리자'에 해당될 경우 '개인정보 보호법'의 일반규정이 적용되는 것인지 모호하며, 이동형 영상정보처리기기를 통해 개인정보를 처리하는 자들이 '개인정보 처리자'에 해당될 경우, 현재 일상적인 블랙박스 사용자 등 수많은 범법자가 발생하게 된다. 이러한 점을 규율하고자 앞서 언급하였듯이 '개인영상정보 보호법(안)'이 현재 입법추진중이다. 정보통신서비스 제공자가 처리하는 개인영상정보는 크게 3가지로 구분할 수 있다. 첫째, 정보통신서비스 제공자가 직접 수집·이용하는 개인영상정보이다(예 : 구글의 스트리트뷰 또는 카카오의 로드뷰 등을 통하여 수집된 개인영상정보). 둘째, 일반인이 수집하여 정보통신서비스 제공자를 통해 제공된 개인영상정보이다(예 : 보배드림의 블랙박스영상 또는 유튜브의 개인영상). 셋째, 정보통신서비스 제공자의 플랫폼을 이용하여 생성되는 개인영상정보이다 (예 : 아프리카TV 등의 인터넷개인방송). 일반 공중이 수집하는 개인영상정보는 대면 또는 통신수단을 통해서 제3자에게 제공될 우려가 없는 것은 아니지만, 그 확산성은 높지 않다고 할 것이나. 이에 반해 정보통신서비스 제공자가 처리하는 개인영상정보는 널리 전파될 위험이 매우 높고 영리목적으로 사용될 가능성이 높다.

그밖에 최근 디지털 헬스케어플랫폼 서비스 제공과정에서는 직접 수집과 매개가 동시에 이루어지는 양상을 보인다. 헬쓰케어 영역에서 생체정보는 개인

건강기기(Personal Health Device)를 통해 수집된다. 이러한 개인건강기기는 가정용 또는 휴대용기기에 센서를 내장하여 언제 어디서나 개인의 건강상태를 측정할 수 있는 웨어러블 디바이스 등을 말한다.[7] 최근 미국 식품의약국(Food and Drug Administration, FDA) 및 한국 식약처에서 의료기기로서의 규제를 받지 않아도 된다고 정의한 건강관리용 제품들, 일명 "웰니스"제품들도 이에 해당된다. "웰니스"제품의 경우에는 건강관리용으로서 맥박, 수면 장애 등을 점검하여 사용자에게 정보를 알려줄 수는 있으나 본 데이터는 질병 진단의 목적을 가질 수 없기 때문에 의료용으로 사용할 수 없다. 또한 의료기기로서 규제를 받으나 ICT의 기술을 활용하는 심전도 측정 제품, 유전자 분석 제품들 또한 이에 해당한다. 이렇게 수집된 정보들은 스마트기기에 내장된 카메라 센서 및 앱세서리(앱과 연결된 악세서리를 이용하여 개인의 건강상태를 측정·관리할 수 있는 어플리케이션)인 PHA(Personal Health Application)를 통해 전송된다. 주요 PHA 제품으로는 Nike Move(나이키), S-헬스(삼성전자), RunKeeper(피트니스키퍼) 등이 있다.[8]

두 번째로는 각 기기들로부터 측정된 결과가 집결되는 데이터 관리의 영역이다. 생체정보를 비롯한 개인건강정보들은 각각의 정보를 통합하여 저장·관리할 수 있는 데이터 플랫폼이 필요하며, 이를 '개인건강정보 플랫폼(PHI Platform)' 또는 '디지털헬스케어 플랫폼'이라 한다. 외부사업자들이 개발한 헬스케어 제품들로부터 수집된 생체정보 또는 개인건강정보들은 이러한 하나의 플랫폼에서 통합·관리함으로서 개인의 건강상태를 종합적으로 분석할 수 있다. 개인건강정보(PHI)를 효율적으로 관리할 수 있는 플랫폼을 중심으로, 개인의 건강정보를 수집하는 제품공급자(PHD, PHA)와 건강관리·의료서비스 제공자가 참여함으로써 디지털헬스케어 생태계의 구현이 가능하다.[9] 클라우드컴퓨

---

7) 주요 제품으로는 Fitbit Flex(핏비트), Fuel Band(나이키), Shine(미스핏), Gear Series (삼성전자) 등이 있다. 이진수, "디지털 헬스케어 플랫폼과 주요기업 동향", 보건산업브리프 vol 140, 한국보건산업진흥원, 2014. 9, 4면.

8) 이진수, 전게논문, 4면.

9) 이진수, 전게논문, 4~5면.

팅을 이용하여 개인용 의료 히스토리(PHR, EMR)를 모으는 형태와, SNS서비스로 구성되어 이용자들이 자발적으로 자신들의 의료 기록 및 정보를 공유하는 형태가 있다.[10] 개인건강정보 플랫폼 서비스의 특성상 다양한 공급자와 참여자(소비자)를 수용할 수 있는 사업자가 유의미한 개인건강정보 플랫폼 사업자로서 참여할 수 있어 애플, 구글과 같이 많은 이용자의 트래픽을 유도할 수 있는 플랫폼 사업자들이 이 영역에서 성과를 낼 수 있을 것으로 생각된다. 정보통신서비스제공자의 생체정보 활용과 관련된 부분이 바로 이 플랫폼 사업자 영역이라고 할 수 있다.

10) SNS를 통해 의료정보를 공유하는 대표적 케이스로 'PatientsLikeMe'가 있다. 'PatientsLikeMe'는 2004년 29살의 젊은 나이로 희귀 질환인 루게릭병에 걸린 형제를 위해 3명의 MIT출신 엔지니어가 모여서 만든 환자들의 SNS로 2011년까지 루게릭병, 파킨슨씨병 등 22가지 만성 질환에만 제한적으로 새로운 멤버들을 받아들이다가, 이후로는 완전히 공개하여 암이나 당뇨병등 여타 다른 질병에 대한 환자들의 가입도 허용하고 있다. 이렇게 환자들을 통해 쌓인 데이터를 바탕으로 기존의 의학계 연구를 정면으로 반박하는 논문을 Nature Biotechnology 에 출판하기도 하였으며 매우 희귀한 질병을 가진 환자들을 서로 이어줌으로써, 학계와 제약업계에서 아직 연구가 되지 않은 해당 질병을 파악하기 위한 방도로도 많이 이용되고 있다.

제2절 국외 민감정보 보호 제도 현황

1. EU : GDPR

민감정보를 규율하는 취지에 대하여는 전문을 통하여 밝히고 있다. 특별히 이러한 개인정보를 더 구체적으로 보호해야 하는 이유는 '기본권과 자유 침해의 리스크'이다. 또한 각국의 자의적 입법에 의한 허용을 금지하기 위해 GDPR에서 구체적으로 허용되는 경우를 열거하고 있다.[11)]

구체적으로 허용되는 경우를 정리하면 다음과 같다. i)기본권을 보호를 위한 사회보장제도의 실행을 위한 경우(고용법, 사회보장법, 의료보장법, 건강보험법 등), ii) 전염병, 건강안보, 공중보건 등(공중보건법, 전염병관리법 등) iii)공익적인 기록보존, 연구 목적, 통계목적을 위해 허용(기록물관리법, 통계법 등) iv)소송상 공격방어 수단, v)정보주체의 명백한 공개 등의 경우이다.

특히 민감정보 중 건강관련 정보의 처리가 가능한 '공중보건'의 범위에 대하여 각 국이 자의적으로 확장하지 못하도록 '공중 보건'은 유럽의회와 각료이사회의 규정(EC) No1338/2008에 정의에 따라 해석되어야 한다. 여기서 '공중보건'이란, 건강과 관련된 모든 요소로 질병 상황이나 장애 등의 건강상태, 이러한 건강상태에 영향을 미치는 결정적 요소, 의료보호서비스의 필요성, 의료보호서비스에 할당된 자원, 이에 대한 지출과 재정, 의료보호서비스 제공 및 보편적 이용, 그리고 사망 사유 등을 의미한다.[12)]

<민감정보 관련 GDPR 전문 내용>

(51) 개인정보의 특성 상, 기본권과 자유와 관련해 특히 민감한 개인정보는 기본권 및 자유 침해의 리스크를 야기할 수

11) GDPR 전문 (51)
12) GDPR 전문(54)

있기 때문에 구체적인 보호를 받아야 한다. 이러한 정보에는 인종 또는 민족출신을 드러나는 개인정보도 포함되어야 하며, 이 법에서의 '인종출신'이라는 단어의 사용이 유럽연합이 인종을 분리하려는 이론을 용인한다는 의미가 아니다. 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술적 수단을 통해 처리되는 경우에 한해서만 생체정보의 정의에 해당되기 때문에, 시스템적으로 민감처리로 분류되지 않는다. 이러한 개인정보는, 회원국의 법률이 공익 또는 정보처리자에게 부여된 공적 권한을 이행하기 위한 직무의 수행 또는 법적 의무의 준수를 위해 이 법의 규칙 적용을 변경하고자 개인정보에 대한 구체적인 조문을 규정할 수 있다는 사실을 고려하여 이 법에 따라 구체적인 상황에서 처리가 허용되는 경우가 아닌 이상, 처리되어서는 안된다. 이러한 처리에 대한 구체적인 요건과 함께, 이 법의 일반적인 원칙 및 기타 규정은 특히 합법적 처리를 위한 조건과 관련하여 적용되어야 한다. 특정 범주의 개인정보 등의 처리에 대한 일반적인 금지로부터의 일부 제외는 명백하게 제공되어야하는데, 특히 정보주체가 명백한 동의를 제공한 경우나 특별한 필요성이 있는 경우로, 특정 협회나 재단의 기본적 자유의 행사를 허용하는 목적으로 하는 합법적 활동과정에서 처리가 수행되는 경우 그러하다.

(52) 특정 범주의 개인정보처리의 금지로부터의 일부제외는 유럽연합 또는 회원국의 법률에 규정되고 적절한 안전장치에 적용받을 경우 허용될 수 있으며, 이는 개인정보와 기타 기본권을 보호하고, 공익에 부합하는 경우 고용법, 연금 등 사회보호법, 건강안보, 모니터링, 경계 목적을 위해, 전염병과 건강의 기타 심각한 위협을 예방 또는 통제하기 위함이다. 이러한 일부제외는 공중보건, 의료보장서비스 관리 등 건강 목적을 위해 허용될 수 있으며, 특히 건강보험시스템의 혜택과 서비스에 대한 청구권 처리에 사용되는 절차의 품질과 비용대비 효과를 보장하기 위해서, 또는 공익적인 기록보존 목적, 과학 및 역사연구 목적 또는 통계목적을 위해 허용될 수 있

다. 일부제외는 법원 절차로 또는 행정절차나 법원 외의 절차인지 여부와 상관없이, 청구권 입증, 행사 및 방어에 필요한 경우 이러한 개인정보의 처리를 허용할 수있어야 한다.

(53) 더 높은 수준의 보호를 받아야 하는 특정범주의 개인정보는 건강관련 목적에 한해 처리되어야하며, 개인과 사회 전체의 이익을 위해 해당 목적을 성취하는데 필요한 경우 그러하다. 특히, 품질관리, 경영정보, 의료 및 사회보장시스템에 대한 일반적인 국가 및 지역적 감시의 목적, 건강 또는 사회보장의 연속성과 회원국 간 건강보험과 건강안전성을 보장하고, 감시 감독 목적으로 또는 공익적인 기록보존 목적, 과학 및 역사연구 목적 또는 통계 목적을 위하여, 이러한 데이터의 관리 및 중앙국립건강당국에 의해 처리되는 경우에 그러하다. 따라서 이 법은 이러한 개인정보의 처리가 직무상 기밀이란 법적 의무에 적용받는 개인에 의해 특정한 건강관련 목적으로 처리되는 경우 등, 구체적인 필요성과 관련하여 건강에 대한 특정범주의 개인정보 처리를 위한 통일된 조건을 규정해야 한다. 유럽연합 또는 회원국의 법률은 개인의 개인정보와 기본권을 보호하기 위해 구체적이고 알맞은 조치를 규정해야 한다. 회원국은 제한 등, 유전자 정보, 생체정보 또는 건강관련 정보처리와 관련한 추가적 조건을 유지 또는 도입하도록 허용되어야 한다. 그러나 이러한 조건이 회원국 간의 해당 정보처리에 적용될 때, 유럽연합 내 개인정보의 자유로운 흐름을 방해해서는 안된다.

(54) 특정범주의 개인정보처리는 정보주체의 동의 없이 공중보건 분야에서 공익상의 이유로 필요할 수 있다. 이러한 처리는 개인의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 적용받아야 한다. 이러한 상황에서, '공중 보건'은 유럽의회와 각료이사회의 규정(EC) No1338/2008에 정의에 따라 해석되어야 한다. 즉, 건강과 관련된 모든 요소로 질병 상황이나 장애 등의 건강상태, 이러한 건강상태에 영향을 미치는 결정적 요소, 의료보호서비스의 필요성, 의료보호서비스에 할

당된 자원, 이에 대한 지출과 재정, 의료보호서비스 제공 및 보편적 이용, 그리고 사망 사유 등을 의미한다. 공익상의 이러한 건강관련 개인정보의 처리는 고용인 또는 보험사와 금융사 등 제 3자가 기타목적으로 개인정보를 처리하는 결과를 초래하지 않아야 한다.

유럽연합은 개인정보보호의 권리 신장과 디지털단일시장에서 개인정보의 자유로운 이동을 원활하게 하는 내용의 '일반개인정보보호규칙 (General Data Protection Regulation, 이하 GDPR)'을 채택하였다. GDPR은 2018년 5월 28일자로 발효하며, 기존 1995년 개인정보보호지침(Data Protection Directive 95/46/ec)을 대체하게 된다. GDPR은 유럽연합의 입법 형식 가운데 규칙(regulation)의 형식을 취하고 있으므로, 모든 회원국에서 직접적으로 적용된다.

GDPR은 우리나라처럼 "민감정보"라고 명백히 표현하고 있지 않으나 "특정범주의 개인정보 처리"에 대한 취급은 특별한 조건에 따르도록 하고 있다. "특정범주의 개인정보 처리"에 대해서는 제9조 제1항을 통해 정의하고 있다. 즉, 인종이나 민족, 정치적 견해, 종교나 철학적 신념, 노조 가입여부가 드러나는 개인정보의 처리와 유전자정보 또는 개인을 특정하게 식별할 수 있는 생체정보, 또는 건강정보, 성생활, 성적 성향에 관한 정보의 처리는 금지된다.

따라서 개인을 특정하게 식별할 수 있는 "생체정보"를 특정범주의 개인정보에 포함하고 있다. 한편 1995년 개인정보보호지침과 비교하여 GDPR은 이러한 민감정보의 범위를 상당하게 확대하였다. GDPR은 유전데이터, 자연인을 고유하게 식별하는 목적의 생체데이터, 자연인의 성적성향에 관한 데이터를 민감정보에 추가하였다.

또한 범죄경력 및 범죄행위에 관한 개인정보의 처리에 대하여는 제10조에서 별도로 정하고 있다. 이러한 개인정보는 제9조의 특정범주의 개인정보에 해당되지 않으며, 공공기관의 규제 하에서만, 또는 회원국 법률에 승인되는 경우에

만 처리 가능하므로 '특정범주의 개인정보' 보다 더 엄격하게 규율하고 있다고 볼 수 있다.

제10조 범죄유죄판결 및 범죄행위에 관한 개인정보의 처리

범죄경력 및 범죄 행위 또는 제6조 (1)항에 근거한 안보조치와 관련한 개인정보의 처리는 **공공기관의 규제 하에서만 수행될 수 있거나,** 해당 처리가 정보주체의 권리와 자유를 위한 적절한 안전조치를 규정하는 유럽연합 또는 회원국 **법률에 승인되는 경우** 수행될 수 있다. 종합 전과 기록은 공공 기관의 규제 하에서만 보관될 수 있다.

<표 2-1> 1995년 개인정보보호지침과 GDPR

1995년 개인정보보호지침	GDPR
Article 8 특별한 유형의 개인정보 처리(The processing of special categories of data)	Article 9 특별한 유형의 개인정보 처리 (Processing of special categories of personal data)
1. 회원국들은 인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 노조 가입을 드러내는 개인정보의 처리, 및 건강 또는 성생활에 관한 데이터의 처리를 금지해야 한다	인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 또는 노조가입을 드러내는 개인정보의 처리, 및 **유전데이터, 자연인을 고유하게 식별하는 목적의 생체데이터,** 건강에 관한 데이터 또는 자연인의 성생활 **또는 성적 성향에 관한 데이터**의 처리는 금지되어야 한다
1 . Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union	1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, **and the**

membership, and the processing of data concerning health or sex life.	**processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,** data concerning health or data concerning a natural person's sex life **or sexual orientation** shall be prohibited.

이러한 특정범주의 개인정보에 대하여는 처리금지가 원칙이며, ①정보주체의 명백한 공개 ② 고용, 사회 안보나 사회보장법 또는 단체협약에 따른 의무의 이행 ③ 동의무능력 정보주체의 중대한 이익의 보호 ④ 정치, 철학, 종교 목적을 지닌 비영리단체나 노동조합이 하는 처리 ⑤ 정보주체가 일반에게 공개한 것이 명백한 정보 ⑥ 법적 주장의 구성, 행사나 방어 ⑦ 중대한 공익을 위해 법률을 근거로 하는 처리 ⑧법률 또는 계약을 근거로, 예방 의학이나 직업 의학, 종업원의 업무능력 판정, 의료 진단, 보건·사회 복지·치료, 보건이나 사회복지 시스템의 관리 및 서비스 제공 ⑨공중보건 영역에서의 공익을 위해 필요한 경우 ⑩ 공익을 위한 저장, 과학적·역사적 연구 목적이나 통계 목적을 위해 필요한 경우에만 예외적으로 처리가 허용된다.

즉 제9조 제2항이 열거하고 있는 10가지의 예외 조항 중 하나에 명시적으로 해당하는 경우에만 이러한 정보를 취급할 수 있다. 제9조 제2항의 자세한 내용은 다음과 같다.

(a) 정보 주체가 단일 또는 복수의 특정 목적으로 특정범주의 개인정보를 처리하는데 명백한 동의를 제공한 경우. 단, 유럽연합 또는 회원국 법률에서 제1항에 규정된 금지조문을 정보주체가 철회할 수 없다고 명시하는 경우는 제외된다.
(b) 정보주체의 기본권 및 이익에 대해 적절한 안전장치를 제공하는 회원국 법률에 따른 단체협약이나 유럽연합 또는

회원국 법률이 허용하는 범위에서, 고용, 사회안보와 사회보호법 분야에서 정보처리자 또는 정보주체의 특정권리를 행사하고 이들의 의무를 수행하기 위한 목적으로 처리가 필요한 경우;

(c) 정보주체가 물리적 또는 법률적으로 동의를 제공할 수 없는 경우로 정보주체 또는 다른 사람의 생명과 관련된 이익을 보호하는 데 필요한 경우;

(d) 정치적, 철학적, 종교적 또는 노동조합의 목적을 지닌 재단, 조합, 비영리기관이 적절한 안정 조치를 갖추어 수행하는 합법적인 활동의 과정에서, 그리고 해당 처리가 그 목적에 맞게 관련 기관의 회원 또는 이전 회원 또는 관련 단체와 정기적으로 접촉하는 사람에 한하여 관련된다는 조건과, 정보주체의 동의 없이 이러한 개인정보를 기관 외부에 제공하지 않는다는 조건에 따른 합법적 활동의 과정에서 처리가 수행되는 경우;

(e) 정보주체가 명백히 공개한 개인정보를 처리하는 경우;

(f) 청구권의 입증이나 행사, 또는 방어를 목적으로, 또는 법원이 사법능력을 행사하는 때마다 처리가 필요한 경우

(g) 개인정보보호권의 본질을 존중하고 정보주체의 기본권 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하며, 추구하는 목적에 비례하는 유럽연합 또는 회원국 법률에 근거하여, 중요한 공익상의 이유로 처리가 필요한 경우,

(h) 유럽연합 법률이나 회원국 법률, 의료전문가와의 계약, 제3항에 규정된 조건 및 안전조치에 따라 예방의학이나 직업의학의 목적으로 또는 직원의 업무능력 평가나 의학적 진단, 의료나 사회복지 및 치료의 제공, 또는 의료나 사회복지 제도 및 서비스의 관리를 위해 처리가 필요한 경우;

(i) 직무상 기밀 등, 정보주체의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거하여, 회원국 간 중대한 건강위협으로부터 보호하거나 높은 수준의 의료 품질 및 안전성과 의약품이나 의학장비를 보장하기 위함 등, 공중보건 분야에서 공익상

의 이유로 처리가 필요한 경우;

(j) 추구하는 목적에 비례하고 개인정보보호권의 본질을 존중하며 정보주체의 기본권 및 이익을 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거한 제 89조(1)항에 따라, 공익상의 기록보관 목적이나 과학 및 역사 연구 목적, 또는 통계목적을 위해 처리가 필요한 경우.

이러한 특정 범주의 개인정보가 유럽연합 또는 회원국 법률이나 국가 관련 기관이 수립한 규정에 따른 직무상 비밀 의무를 적용 받는 전문가의 책임에 의해 또는 책임 하에 처리되는 경우, 또는 유럽연합 또는 회원국 법률이나 관련 국가기관에 수립한 규정에 따른 비밀의 의무에 적용 받는 또 다른 개인에 의해 이러한 개인정보가 처리되는 경우, 제2항의 (h)에 규정된 목적을 위해 처리될 수 있다.

또한 회원국은 유전자정보나 생체정보, 건강정보와 관련하여, 제한을 포함한 추가 조건을 유지 또는 도입할 수 있다(제9조제4항). 즉 유전자, 생체 및 건강정보에 대해서는 더 엄격한 제한 기준을 설정할 가능성을 열어 두고 있다.

〈표 2-2〉 국내법과 GDPR 민감정보 규정 비교

	개인정보 보호법	정보통신망법	GDPR
민감정보	① 사상·신념 ② 노동조합·정당의 가입·탈퇴 ③ 정치적 견해 ④ 건강, 성생활 등에 관한 정보 ⑤ 유전정보 ⑥ 범죄경력에 관한 정보	① 사상, 신념 **② 가족 및 친인척관계** ③ 학력(學歷)·병력(病歷) **④ 기타 사회활동 경력**	**① 인종적 또는 민족적 출신을 드러내는 정보** ② 정치적 의견을 드러내는 정보 ③ 종교적 또는 철학적 믿음을 드러내는 정보 ④ 노조가입을 드러내는 정보 **⑤ 유전데이터** **⑥자연인을 고유하게 식별하**

			는 목적의 생체데이터 ⑦ 건강에 관한 데이터 ⑧ 성생활에 관한 데이터 **⑨ 성적 성향에 관한 데이터** **⑩ 범죄유죄판결 및 범죄행위**에 관한 개인정보
	열거규정	예시규정	열거규정
처리가 허용되는 경우	①**별도의** 동의 ②**법령**의 규정	① 동의 ② **법률**의 규정	①명시적 동의 ②고용, 사회 안보나 사회보장법 또는 단체협약에 따른 의무의 이행 ③ 동의무능력 정보주체의 중대한 이익의 보호 ④ 정치, 철학, 종교 목적을 지닌 비영리단체나 노동조합이 하는 처리 ⑤ 정보주체가 일반에게 공개한 것이 명백한 정보 ⑥ 법적 주장의 구성, 행사나 방어 ⑦ 중대한 공익을 위해 법률을 근거로 하는 처리 ⑧법률 또는 계약을 근거로, 예방의학이나 직업 의학, 종업원의 업무능력 판정, 의료 진단, 보건·사회 복지·치료, 보건이나 사회복지 시스템의 관리 및 서비스 제공 ⑨공중보건 영역에서의 공익을 위해 필요한 경우 ⑩ 공익을 위한 저장, 과학적·역사적 연구 목적이나 통계 목적 **다만** '범죄경력 및 범죄행위'는 ① 공공기관의 규제 하에서만 또는 ② 법률의 규정에 의해서만 처리 가능

또한 민감정보에 대하여는 개인정보보호 영향평가를 수행하도록 규율하고 있다. 개인정보의 처리가 개인의 권리와 자유에 중대한 위험을 초래할 수 있는 경우, 정보처리자는 정보를 처리하기 전에 개인정보의 보호에 대한 예상되는

처리 작업에 대한 영향평가를 수행해야 하는데, 민감정보의 경우 특히 이를 하도록 요구하고 있다.

제35조 개인정보보호 영향평가

1. 처리의 성격과 범위, 상황, 목적을 참작하여, 특히 신기술을 사용하는 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 수 있는 경우, 정보처리자는 정보를 처리하기 전에 개인정보의 보호에 대한 예상되는 처리 작업에 대한 영향평가를 수행해야 한다. 한 번의 평가를 통해 유사한 중대한 위험을 초래하는 비슷한 일련의 처리 작업을 해결할 수 있다.

3. 제1항에 규정된 개인정보보호 영향평가는 특히 다음 각 호의 경우 요구되어야 한다.

(b) 또한 제9조 (1)항에 규정된 특정범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범죄경력 및 범죄행위에 관련된 개인정보에 대한 처리

2. 독일

독일은 세계 최초의 개인정보보호법으로 제정된 1970년 Hessen 주의 정보보호법과 1974년 Rheinland-Pfalz 주의 정보남용금지법에 이어 1977년에는 "연방정보보호법(BDSG : Bundesdatenschutzgesetz)"을 제정하였다. 연방데이터보호법은 데이터 처리에 있어서 개인에 관한 데이터의 남용 방지에 관한 포괄적인 법적 근거를 처음으로 마련하였고, 이를 기초로 각 주의 개인정보보호법이 제정되었다.[13)]

이 법은 연방헌법법원의 인구조사판결, 정보통신기술의 발달, 연방데이터보호법의 적용을 통하여 제기된 문제점으로 인해 개정의 필요성이 제기되어 1990년 12월에 개정되었고, 2003년 1월 14일 유럽연합의 개인정보보호지침을

13) 박병섭, "독일의 개인정보보호제도에 관한 연구", 민주주의법학연구회, 민주법학 25권, 단일호, pp.402-431, 2004년 2월; Prof. Rossnagel, "독일의 개인정보보호법," 개인정보 보호제도의 개선을 위한 한·독 국제 심포지엄, 2004년 11월

반영하기 위해 다시 개정되었다. 총6장 48개의 조로 이루어져있다.

민감정보와 관련하여서는 개념정의를 규정하고 있는 제3조에서 “특별한 종류의 개인관련 정보”란 인종 및 인종기원, 정치적인 신념, 종교적 또는 철학적인 확신, 노동조합에의 소속, 건강, 성생활 등에 대한 진술을 말한다(제3조제9항)[14]고 규정하고 있다. 특히 특별한 종류의 개인관련 정보가(제3조제9항) 수집, 가공, 이용되어지는 경우에, 이러한 정보에 대해서는 명시적으로 동의가 행하여져야 한다(제4a조).[15] 일반적인 개인정보와는 달리 명시적 동의를 요구하고 있다.

3. 일본

일본의 개인정보보호법(「개인정보의 보호에 관한 법률」)은 민간에 적용되는 일반법으로, 2003년에 제정되고 2015. 9. 9. 최종 개정되었다. 그 개정취지는 빅데이터/사물인터넷 등의 신사업 활성화에 개인정보의 ‘적정하고 효과적인 활용’의 가치를 인정하면서, 안전한 이용을 도모하고자 함이다. 즉 개인정보의 이용가치가 점차 높아지면서 개인정보보호법 제정 당시에는 예상하지 못했던 활용이 이루어지는 등 개인정보 및 프라이버시에 관한 사회적 상황이 현행법 제정 당시와는 다르게 크게 변화하고 있는 것을 반영한 것이다 .이러한 취지는 목적개정에서도 반영하고 있다. 제1조에서 “이 법률은 … 의무 등을 규정함으로써 [개인정보의 적정하고 효과적인 활용이 새로운 산업의 창출 및 활력 있는

---

14) §3 Weitere Begriffsbestimmungen

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

15) §4a Einwilligung

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

경제사회와 풍요로운 국민생활의 실현에 이바지하는 것이라는 점 외에] 개인정보의有用性을 고려하면서 개인의 권리이익을 보호하는 것을 목적으로 한다"고 밝히고 있다.

민감정보에 대하여 개정 전에는 일반 개인정보와 민감정보의 구분이 없이 일반개인정보와 동일하게 수집·이용·제3자 제공의 규제를 받았다. 그러나 개정법에서는 "배려를 요하는 개인정보(要配慮個人情報)"로서 별도로 규율하고 있다. 즉 "배려를 요하는 개인정보"라 함은 본인의 인종, 신조, 사회적 신분, 병력(病歷), 범죄의 경력, 범죄로 인해 피해를 입은 사실 및 그밖에 본인에 대한 부당한 차별, 편견 및 그 밖의 불이익이 생기지 않도록 그 취급에 특별히 배려를 요하는 것으로서 政令으로 정하는記述 등이 포함되는 개인정보를 말한다(제2조제3항)"고 규정하고 있다. 즉 '민감정보'라고 표현하고 있지 않으며, 본인에 대한 부당한 차별, 편견 및 그 밖의 불이익이 생기지 않도록 그 취급에 특별히 배려를 요하는 것, 즉 "배려를 요하는 개인정보"로 표현하고 있다.

개인정보취급사업자[16]는 이러한 "배려를 요하는 개인정보"를 '① 사전에 정보주체의 동의를 얻은 경우, ②법령에 의거한 경우, ③ 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때, ④ 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때, ⑤ 국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 法令이 정하는 사무를 수행하는 것에 대하

16) "개인정보취급사업자"는 개인정보데이터베이스 등을 사업용으로 이용하는 자를 말하며, i) 국가기관 ii) 지방자치단체 iii) 독립행정법인 등, iv) 지방독립행정법인 등은 제외한다(일본 개인정보 보호법 제2조제5항).
또한 "개인정보데이터베이스 등"이라 함은 개인정보를 포함하는 정보의 집합물로서 다음에 열거된 것(이용방법으로 보아 개인의 권리이익을 해할 우려가 적은 것으로서 政令으로 정하는 것을 제외한다)을 말한다(동법 제2조제4항).
1. 특정의 개인정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것
2. 전호의 것 이외에, 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로서 정령으로 정하는 것

여 협력할 필요가 있는 경우로서, 본인의 동의를 얻게 되면 당해 사무의 수행에 지장을 초래할 우려가 있는 때, ⑥ 당해 요배려개인정보가 본인, 국가기관, 지방자치단체, 제76조 제1항 각 호에 열거된 자 및 그밖에 개인정보보호위원회 규칙으로 정하는 자에 의해 공개되고 있는 경우, ⑦그밖에 전 각 호에 열거된 경우에 준하는 것으로서 政令으로 정하는 경우'에만 취득할 수 있다(법 제17조 제2항).

다만 일본 개인정보보호법은 제23조 제2항에서 '개인정보취급사업자는 제3자에게 제공되는 개인데이터에 대하여 본인의 요청이 있는 때에는 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지하는 것을 조건으로 일정한 사항을 개안정보보호위원회규칙에서 정하는 바에 따라 미리 본인에게 통지하거나 또는 본인이 용이하게 알 수 있는 상태에 두고 있으면서 개인정보보호위원회에 신고한 때에는 정보주체의 사전 동의 없이 개인정보를 제3자에게 제공할 수 있다'고 규정하고 있다. 일명 개인정보 제공에 있어서 opt-out 방식을 부분적으로 채택하고 있는 것이다. 그러나 배려를 요하는 개인정보는 이러한 opt-out의 적용대상에서 제외된다.

제3절 우리나라 민감정보제도 쟁점과 현안

1. 현행 민감정보 규율내용과 한계

현행「개인정보 보호법」제23조에 의하면 '민감정보'란 ①사상·신념, ②노동조합·정당의 가입·탈퇴, ③정치적 견해, ④건강, 성생활 등에 관한 정보, ⑤ 유전정보 ⑥ 범죄경력(형의 선고·면제 및 선고유예, 보호감호, 치료감호, 보호관찰, 선고유예의 실효, 집행유예의 취소 등)에 관한 정보를 의미한다(⑤, ⑥은 시행령 제18조).

'사상·신념'이란 개인의 가치관에 기초로 하여 형성된 사유체계, 개인이 굳게 믿고 지키고자하는 믿음・생각 등을 말하는 것으로 각종 이데올로기 또는 사상적 경향, 종교적 신념 등을 말한다. '노동조합·정당의 가입·탈퇴'란 노동조합 또는 정당에의 가입・탈퇴에 관한 정보로 반드시 적법한 노동조합이거나 정당일 필요는 없다. '정치적 견해'란 정치적 사안에 대한 입장이나 특정 정당의 지지 여부에 관한 정보를 의미하며, '건강 및 성생활 등에 관한 정보'란 개인의 과거 및 현재의 병력(病歷), 신체적·정신적 장애(장애등급 유무 등), 성적 취향 등에 관한 정보이며, 혈액형 등 건강과 무관한 정보는 이에 해당되지 않는다. 다만 시행령에 따른 민감정보(유전정보, 범죄경력에 관한 정보)는 공공기관이 다음의 업무수행을 위하여 처리하는 경우에는 민감정보로 보지 아니하므로, 이 경우에는 정보주체로부터의 별도 동의 없이 처리가 가능하다.

< 공공기관이 업무수행을 위하여 처리하는 경우 민감정보로 보지 않는 경우 >

- 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
- 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
- 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
- 법원의 재판업무 수행을 위하여 필요한 경우

- 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

현행「정보통신망법」은 '민감정보'라고 명확히 규율하고 있지 않다. 다만 제23조 제1항에서 '정보통신서비스 제공자는 ①사상, 신념, ②가족 및 친인척 관계, ③학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 타 개인정보에 비하여 특별히 규정하여 이러한 정보에 대하여는 원칙적으로 수집을 금지하되 ①이용자의 동의를 받거나 ②다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에만 필요한 범위에서 최소한으로 수집할 수 있도록 규정하고 있다.

〈표 2-3〉 개인정보 보호법과 정보통신망법상 민감정보

	개인정보 보호법	정보통신망법
민 감 정보	① 사상·신념 ② 노동조합·정당의 가입·탈퇴 ③ 정치적 견해 ④ 건강, 성생활 등에 관한 정보 ⑤ 유전정보 ⑥ 범죄경력에 관한 정보	① 사상, 신념 ② 가족 및 친인척관계 ③ 학력(學歷)·병력(病歷) ④ 기타 사회활동 경력
	열거규정	예시규정
판 단 기준	사생활을 현저히 침해할 우려가 있는지 여부	개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는지 여부

「개인정보 보호법」이 민감정보의 판단기준을 "사생활 침해 우려"만 규정하고 있는 반면, 「정보통신망법」은 민감정보의 판단여부를 "사생활 침해" 뿐만 아니라 "개인의 권리·이익 침해"까지 포함하고 있으므로 「정보통신망법」민감정보의 범위가 더 넓어 질 수 있다.

또한 「개인정보 보호법」은 사생활을 현저히 침해할 우려여부에 대한 해

석의 여지가 크기 때문에 민감정보로 특별히 보호할 필요가 있다고 사회적 합의가 이루어진 정보를 상황에 맞게 규정할 수 있도록 대통령령에 위임하여 현재 6가지 종류의 정보를 민감정보로 열거하고 있다. 반면「정보통신망법」은 "기타 ~~등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보"라고 규정함으로서 앞에 제시된 정보는 예시적 사항이며 추가적 민감정보가 법률상 포섭될 수 있도록 규정하고 있다.

〈표 2-4〉「개인정보 보호법」과 「정보통신망법」의 규율현황

	개인정보 보호법	정보통신망법	비고
수집·이용	- 정보주체의 동의 - 계약의 체결 및 이행 - 법률에 특별한 규정, 법령상 의무 준수 - 공공기관의 소관 업무 수행 - 정보주체·제3자의 급박한 생명, 신체, 재산의 이익 - 개인정보처리자의 정당한 이익을 달성	- 정보주체의 동의 - 계약의 이행, 요금정산 - 법률에 특별한 규정	「개인정보 보호법」이 「정보통신망법」 규정 포괄
동의에 의한 수집 시 고지사항	- 수집·이용 목적 - 개인정보의 항목 - 보유·이용 기간 - 동의 거부 권리가 있다는 사실 등	- 수집·이용 목적 - 개인정보의 항목 - 보유·이용 기간	「개인정보 보호법」이 「정보통신망법」 규정 포괄
개인정보수집 제한	- 필요최소한 수집 원칙 - 불필요한 정보 수집 거부에 대하여 서비스 제공 거부 불가 - 불필요한 개인정보 수집에는 동의하지 아니할 수 있다는 사실 고지	- 필요최소한 수집 원칙 - 불필요한 정보 수집 거부에 대하여 서비스 제공 거부 불가	「개인정보 보호법」이 「정보통신망법」 규정 포괄

민감정보	- 원칙: 수집금지 - 예외 : **별도의** 동의, 법령의 요구 또는 허용	- 원칙 : 수집금지 - 예외 : 동의, 법률에 의해 허용된 경우	「개인정보 보호법」이 「정보통신망법」 규정 포괄
제3자 제공	- 정보주체의 동의 - 법률에 특별한 규정, 법령상 의무 준수 - 공공기관의 법령상 소관 업무 수행 - 정보주체·제3자의 급박한 생명, 신체, 재산의 이익	- 정보주체의 동의 - 법률에 특별한 규정 - **요금정산을 위하여 필요한 경우**	「정보통신망법」 상 특별규정 존재
관리	- 개인정보 보호책임자 지정 - 개인정보처리방침 공개 - 개인정보 보호 인증 - 개인정보 영향평가	- 개인정보 보호책임자 지정 - 개인정보처리방침 공개	「개인정보 보호법」이 「정보통신망법」 규정 포괄
파기	- 보유기간의 경과 - 처리 목적 달성 - 기타 개인정보가 불필요하게 되었을 때	- 보유기간 경과 - 수집·이용목적달성 - **사업의 폐업** - **1년 동안 미이용자 정보**	「정보통신망법」 상 특별규정 존재
개인정보누출 통지·신고	- 지체 없이 해당 정보주체에게 통지 - 행정자치부장관 또는 전문기관에 신고	- 24시간 이내에 이용자에게 통지 - 방송통신위원회 또는 한국인터넷진흥원에 신고	규정 내용 대동소이 신고기관만 다름
보호조치	기술적·관리적·물리적 조치 - 내부 관리계획 수립·시행 - 접근 통제 및 권한 제한 조치 - 안전하게 저장·전송할 수 있는 암호화 기술의 적용 - 접속기록 보관, 위·변조 방지 조치 - 보안프로그램 설치 및 갱신 - 보관시설 마련, 잠금장치	기술적·관리적 조치 - 내부 관리계획 수립·시행 - 접근 통제장치의 설치·운영 - 안전하게 저장·전송할 수 있는 암호화 기술의 적용 - 접속기록 위·변조 방지 조치	「개인정보 보호법」이 「정보통신망법」 규정 포괄

	의 설치 등 물리적 조치	- 컴퓨터바이러스에 의한 침해 방지조치 - 기타 안전성 확보를 위하여 필요한 보호조치	
정보주체의 권리	- 열람청구권 - 정정삭제청구권 - 처리정지요구권	- 열람·제공·정정 요구권 - 수집·이용·제공 등의 동의 철회권 - **개인정보의 이용내역을 주기적으로 통지**	「정보통신망법」 상 특별규정 존재
손해배상	- 법정손해배상 청구(300만원 이하) - 징벌적 손해배상 규정	-법정손해배상 청구(300만원 이하)	「개인정보 보호법」이 「정보통신망법」 포괄

2. 정보통신서비스분야 민감정보 규율 개선방안

가. “민감정보” 규정방식의 수정 : 한정적 열거방식

현재 「정보통신망법」은 민감정보 해당성의 융통성을 발휘하기 위하여 ‘예시적 방식’으로 규정하고 있다. 예를 들어 최근 유출되어 논란이 되었던 숙박앱 ‘여기어때’의 개인정보(고객 이름, 전화번호, 숙박이용정보) 는 현재의 「정보통신망법」에 예시되어 있지는 않으나 해석여부에 따라 ‘민감정보’에 해당될 수 있다. 그러나 한정적 열거방식의 경우 명시적으로 규정하지 않는 한 ‘민감정보’에 해당되지 않게 된다. ‘숙박이용정보’의 민감성은 개개인에 따라 다를 수 있으며, ‘범죄경력정보·성생활·건강정보’ 등 누구에게나 보편타당하게 민감한 정보라고 보기는 곤란하다. 민감정보 해당성 여부가 개개인의 주관적 성향에 따라 달라진다면 법적 안정성이나 명확성 측면에서 바람직하지 않으므로, 한정적 열거방식이 타당하다. 또한 일반 개인정보와 민감정보에 대한 차

별적 규율은 수집등 처리단계에서 이루어지며, 침해에 대한 가벌성은 동일(5년 이하의 징역 또는 5천만원 이하의 벌금, 제71조 제1항 제1호, 제2호)하므로 수집 등 처리단계에서 차별화할 수 있는 정보가 아닌 한 민감정보로 규율 실익이 없다.

따라서 현행 「정보통신망법」상 민감정보에 대하여 우선 한정적 열거방식이 아니라 예시방식으로 규율하는 것은 타당하지 않다. 사생활침해, 개인의 권리·이익의 침해 여부는 지극히 주관적이며 이를 일일이 판례를 통해 규명하는 것도 용이하지 않다.

개인정보 법역의 기본법인 「개인정보 보호법」도 이러한 점을 반영하여 대통령령 위임을 통해 한정적 열거방식을 채택하고 있으며, GDPR의 경우도 열거방식을 채택하고 있다. 불가피하게 융통성을 두고자 한다면 현행 「개인정보 보호법」과 같이 기준을 정하여 대통령령에 위임하는 방안도 검토될 수 있으나 기본취지는 한정적 열거방식을 취하는 것이 바람직하다.

나. 민감정보의 대상이 되는 개인정보 유형

(1) 인종이나 민족적 출신을 드러내는 정보

과거 우리나라는 단일민족으로 구지 인종이나 민족을 드러내는 정보가 개인에게 민감성을 가지지 않았다. 그러나 다문화 가족의 확산, 해외 노동인구의 유입등에 비추어 볼 때 또한 다문화 가족에 대한 사회적 편견과 차별은 현재 심각한 사회문제로 대두되고 있다. 따라서 이제 인종이나 민족정보를 민감정보로 규율할 필요가 있다고 본다.

우리나라는 「개인정보 보호법」,과 「정보통신망법」에서 '사상·신념'을 민감정보로 규율하고 있으나 이를 GDPR에서는 '종교적 또는 철학적 믿음을 드러내는 정보'라고 표현하고 있는 듯하다. 한편 '정치적 견해'를 「개인정보 보호법」과 GDPR은 민감정보로서 별도로 규정하고 있으나, 「정보통신망법」에 이를 민감정보에 포함시키고 있지 않다. 법 제정 시 '정치적 견해'를 '사상·

신념'에 포함된다고 해석할 수 도 있으나, 「개인정보 보호법」과 GDPR이 별도로 규율하고 있는 바, 또한 법률의 명확성, 구체성 차원에서 이를 '정치적 견해'를 「정보통신망법」에 민감정보로 명확히 규정하는 것이 바람직하다. 또한 '사상·신념'을 '종교적·철학적 믿음을 드러내는 등 사상·신념에 대한 정보'로 구체화 하는 것도 바람직하다.

(2) 노동조합·정당의 가입·탈퇴

이는 「개인정보 보호법」과 GDPR이 모두 민감정보로 규율하고 있는 바 「정보통신망법」에 추가할 필요가 있다. 「정보통신망법」은 한정적 열거주의가 아니라 예시주의 규정방식을 취하고 있는바 '기타 사회활동 경력'에 포함된다고 볼 수 있으나, 예시주의을 폐지하고 '열거주의'로 규정한다고 할 때 '기타 사회활동 경력'이라는 모호한 정보는 폐지하는 것이 마땅하다.

(3) 유전정보

유전정보는 개인의 유전적 결함, 장애 등과 밀접하게 관련되며, 그 활용영역도 다채로운 만큼 그 오남용으로 인한 개인의 권리와 자유 침해적 요소가 심각하다. 따라서 「개인정보 보호법」과 GDPR이 모두 민감정보로 규율하고 있는 바「정보통신망법」에서 민감정보로 추가할 필요가 있다.

(4) 건강·성생활·성적 성향에 대한 정보

「개인정보 보호법」과 GDPR이 모두 민감정보로 규율하고 있는 바, 정보주체의 의사와 무관하게 사용되어서는 안되는 정보이며, 특히나 사생활 침해와 관련이 깊은 민감성이 강한 정보이다. 「정보통신망법」에서 민감정보로 추가할 필요가 있다.

'건강정보(data concerning health)'는 의료 서비스의 제공을 비롯하여 개인

의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보이다. '심전도' 자체가 생체정보라면, '심전도를 측정한 값(이 주는 의미)'은 건강정보에 해당된다. '홍채'가 생체정보라면 '홍채가 의미하는 신체 또는 건강상태'는 건강정보에 해당된다.

(5) 범죄경력

이와 관련하여 「개인정보 보호법」은 '범죄경력에 관한 정보'로 GDPR은 '범죄유죄판결 및 범죄행위에 대한 정보'로 표현하고 있다. '범죄유죄판결 및 범죄행위'는 당연히 '범죄경력'에 해당되므로 더 현행 「개인정보 보호법」은 더 넓은 개념이다. 「정보통신망법」상 '기타 사회활동 경력'에 해당될 수 있으나, 규정의 모호성, 불확실성, 열거주의의 폐지 등에 비추어 '기타 사회활동 경력'을 폐지하고 '범죄경력에 관한 정보'를 추가하는 것이 타당하다.

(6) 학력(學歷)·병력(病歷)

병력은 민감정보에 해당되며, '건강·성생활·성적 성향에 대한 정보'에 포함된다. 따라서 '건강·성생활·성적 성향에 대한 정보'를 「정보통신망법」상 민감정보에 포함시킬 경우 구지 별도로 규정할 필요는 없다고 본다.

다만 '학력'을 '민감정보'에 포함시킬 것인가에 대하여는 의문의 여지가 있다. '학력'으로 인해 불합리하게 자유와 기본권을 침해당할 수 있다면 이는 민감한 개인정보의 오남용으로 인한 문제라기보다는 사회적 차별의 문제이다. 또한 개인의 역량이나 재능을 판단하기 위한 객관적 기준으로 처리될 수밖에 없는 바, 건강정보, 성생활과 동일하게 그 민감성을 취급하는 것도 곤란하다. 그러나 다른 나라에 비해 학벌만능주의가 팽배하여 사회에 미치는 해악이 크다면 이 또한 민감정보라 하지 않을 수 없다. 다만 정보통신서비스 제공과정에서 '학력'에 대한 개인정보의 처리가 민감하게 작용될 여지는 극히 제한적이므로 삭제하는 것이 타당하다고 생각된다.

(7) 생체정보

단순히 서비스제공과정에서 처리되는 모든 생체정보를 민감정보를 규율한다면, 전혀 프라이버시침해적 요소나 권리와 자유침해의 리스크가 없음에도 불구하고 과도한 규율이 된다. 따라서 민감정보에 해당되는 생체정보는 본인인증등의 목적으로 제한할 필요가 있다. 이에 대하여는 제3장에서 후술한다.

다. 민감정보 처리 규정의 구체화

민감정보는 원칙적으로 처리가 금지되며 ①(별도로) 정보주체의 동의를 받은 경우와 ②법령(정보통신망법은 "법률")에서 민감정보의 처리를 요구하거나 허용하는 경우에 한해 그 처리를 허용한다(「개인정보 보호법」 제23조제1항, 「정보통신망법」 제23조 제1항). 별도로 정보주체의 동의를 받은 경우라 함은 제15조제2항 각 호 또는 제17조 제2항 각 호의 사항을 정보주체에게 알리고 다른 개인정보의 처리에 대한 동의와 분리해서 민감정보 처리에 대한 동의를 받은 경우를 의미한다. 법령에서 처리를 요구하거나 허용하는 경우라 함은 법령에서 민감정보의 종류를 열거하고 그 처리를 요구하고 있는 경우로서 법정서식에 민감정보 기재사항이 있는 경우도 포함된다. 「개인정보 보호법」 제23조는 개인정보 처리에 관하여 특별한 규정이므로 제15조, 제17조 및 제18조 등 개인정보 처리에 관한 다른 규정에 우선하여 적용되므로, 민감정보의 경우에는 제23조 제1항 각호에서 정하는 예외 사유가 존재하는 경우에 한하여 처리할 수 있다.

「정보통신망법」 상 개인정보의 수집과 이용은 원칙적으로 ①'사전동의'를 득함으로서 가능하며 그 이외의 경우에는 ②정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, ③ 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 ④ 다른 법률에 특별한 규정이 있는 경우 이다

(법 제22조 제1항). 또한「개인정보 보호법」의 보충적 적용에 의해 ' ⑤정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, ⑥개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우(이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다)(개인정보 보호법 제15조 제1항 제5호 및 제6호))' 생체정보를 수집, 이용할 수 있다. 그러나 현행법에 의할 경우 민감정보의 경우 ①'사전동의'와 ④ 다른 법률에 특별한 규정이 있는 경우에만 수집 및 이용이 가능하다(제23조 제1항). 따라서 '개인을 인증하기 위한 목적의 생체정보'가 민감정보에 해당된다고 명시적으로 규정할 경우 계약이행을 위해 필요한 경우(②)와 요금정산을 위해 필요한 경우(③), 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 경우(⑤), 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우(⑥)에는 개인정보를 수집/이용할 수 없다. 「개인정보 보호법」은 민감정보에 대하여 다른 개인정보와 구분하여 별도의 동의를 받도록 규율하고 있으나, 「정보통신망법」이러한 규율이 없는 바, 다른 개인정보와 함께 일괄적으로 동의를 받아도 무방하다. GDPR에서도 "명백한 동의" 수준을 요구하고 있으며, 반드시 별도의 동의일 것을 요구하고 있지 않으므로 구지 「정보통신망법」의 동의방식을 「개인정보 보호법」처럼 "별도의" 동의로 개정할 필요는 없다고 본다.

또한「정보통신망법」은 민감정보 수집의 정당화 근거를 "법률"로 제한하고 있으나, 「개인정보 보호법」은 대통령령을 포함한 "법령"으로 그 범위를 넓히고 있다. 「정보통신망법」에서 특별히 더 수집, 이용의 근거를 더 강화해야 할 실익이 없는 한 이는 기본법 수준에 부합하는 것이 타당하다고 생각된다.

이는 GDPR보다도 더 높은 수준으로 생체정보의 보호수준을 규율하는 것이며 생체정보의 활용영역에 비추어 볼 때 이용에 있어서 더 큰 제약이 될 수 있다. 따라서 생체정보를 허용하는 범위를 좀 더 구체화 할 필요가 있다.

또한 '법률의 규정'은 각 영역의 입법활동이 모두 개인정보 보호를 위해 초점

이 맞추어져 있지 않는 한 오히려 그 활용영역을 임의적으로 확대할 수 있다. 이처럼 자의적 입법에 의한 허용을 금지하기 위해 GDPR에서 구체적으로 허용되는 경우를 열거하고 있다. 이러한 취지에 비추어 "법률"에 의해 허용되는 경우에 대한 구체화가 필요하다. 복지, 산업, 교육 등 각 영역의 개별법에 의해 민감정보의 처리가 무작위적으로 허용되는 것을 막기 위해서 단순히 "법률"의 규정에 의한 처리의 허용을 규정하는 것이 아니라, 특정한 사안의 경우 법률에 의해 가능하도록 기준을 수립할 필요가 있다. 그러한 기준으로 i)기본권을 보호를 위한 사회보장제도의 실행을 위한 경우(고용법, 사회보장법, 의료보장법, 건강보험법 등), ii)전염병, 건강안보, 공중보건 등(공중보건법, 전염병관리법 등) iii)공익적인 기록보존, 연구 목적, 통계목적을 위해 허용(기록물관리법, 통계법 등) iv)소송상 공격방어 수단으로 처리되는 경우 등이 제안될 수 있다.

라. '고유식별정보'와 유사하게 취급하는 방법

모든 생체정보가 반드시 '민감정보'인 것은 아니다. 그러나 생체정보의 정보주체와의 관계에 있어서 지참성, 생체정보의 불변성 등으로 인해 오·남용되었을 경우 통상의 개인정보와 개인정보에 비해 그 권리침해적 요소가 더 클 수 있다. 이와 유사한 성격으로 인해 특별히 규율하고 있는 개인정보가 '고유식별정보'이다.

「개인정보 보호법」상 고유식별정보는 원래 공익목적으로 개인에게 부여된 것이나 그 편리성 때문에 공공부문은 물론 민간영역에서도 광범위하게 수집·이용되고 있다. 고유식별정보란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보를 말한다. 법령에 의해서 개인에게 부여된 것이어야 하므로 기업, 학교 등이 소속 구성원에게 부여하는 사번, 학번 등은 고유식별정보가 될 수 없다. 또 법인이나 사업자에게 부여되는 법인등록번호, 사업자등록번호 등도 고유식별정보가 될 수 없다.

「개인정보 보호법」상 고유식별정보는 민간 분야에서 DB매칭키 등으로 남용되어 개인 프라이버시 침해가능성이 높은 정보를 중심으로 규정하고 있는

데 시행령에서는 고유식별정보의 범위를 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호로 정하고 있다.

고유식별정보는 원칙적으로 처리할 수 없다. 다만, 별도로 정보주체의 동의를 받은 경우와 법령에서 고유식별정보의 처리를 요구하거나 허용하고 있는 경우에는 고유식별정보를 처리할 수 있다(다만, 고유식별정보 중 주민등록번호의 처리에 관하여서는 제24조의 2에서 별도 규정하고 있다)(법 제24조제1항).

정보주체의 별도의 동의를 받는 경우에 개인정보처리자는 제15조제2항 각 호 또는 제17조 제2항 각 호의 사항을 정보주체에게 알리고 다른 개인정보의 처리에 대한 동의와 분리해서 고유식별정보 처리에 대한 동의를 받아야 한다. 법령에서 구체적으로 처리를 요구하거나 허용하는 경우란, 원칙적으로 법령에서 구체적으로 고유식별정보의 종류를 열거하고 그 처리를 요구하거나 허용하고 있는 것을 말한다. '법령'에 의한다고 규정하고 있으므로 법률 외에 시행령, 시행규칙이 포함되며 이에 첨부된 별지 서식이나 양식도 포함된다.

개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다(제24조제3항). 고유식별정보의 안전성 확보조치는 그 외의 일반적 개인정보에 대한 안전성 확보조치와 거의 유사하므로, 대통령령은 고유식별정보의 안전성 확보조치에 관해서 일반적 개인정보에 대한 안전성 확보조치(영 제30조)를 준용하도록 하였다(영 제21조). 대통령령에 따라 행정자치부장관이 고시한 「개인정보의 안전성 확보조치 기준」에서는 고유식별정보의 암호화 등을 별도로 규정하고 있다.

행정자치부장관은 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다(제24조제4항). "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 i)공공기관과 ii) 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자를 말한다(시행령 제21조제2항). 행정자치부장관은 이러한 개인정보처리자에 대하여 법 제24조제4항에 따라 안전

성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사하여야 한다(시행령 제21조제3항).

모든 생체정보가 반드시 민감정보에 해당되는 것은 아니므로 그 법적 취급을 '고유식별정보'와 유사하게 하는 방안도 고려될 수 있다.

마. 관리, 보관, 파기 등에 있어서 특칙 필요성

'관리' 단계에서 정보통신서비스제공자는 '개인정보 보호책임자'를 지정하고, '개인정보 처리방침'을 공개하여야 한다. 민감정보의 경우 특별히 문제될 수 있는 사항은 현재 공공기관의 정보처리의 경우에만 의무화 하고 있는 '개인정보 영향평가' 도입에 관한 사항이다. 앞에서 검토하였듯이 GDPR은 대규모 민감정보의 처리나 범죄경력 및 범죄 행위에 관련된 개인정보의 처리에 대하여는 영향평가를 실시하도록 규정하고 있다. 정보통신서비스제공자가 민감정보에 대하여 개인정보영향평가를 의무적으로 실시하여야 하는지가 문제될 수 있다. 이 부분에 대하여는 사업자에게 미치는 영향, 개인정보 침해가능성 등을 고려하여 좀 더 추가적 연구가 선행될 필요가 있다.

'파기'와 관련하여「정보통신망법」은 i)보유기간 경과, ii)수집·이용목적달성, iii) 사업의 폐업, iv)1년 동안 미이용자 정보를 파기하도록 규율하고 있다. 이와 관련하여 '민감정보'에 특별히 규율한 사항이 있는지에 대한 검토가 필요하다. 특히 민감정보의 파기와 관련된 기술적 보호조치의 기준 제시가 필요하다는 견해가 있을 수 있으나, 이는 비단 민감정보에만 국한된 문제가 아니며, 법률은 기술중립성에 기반하여 '파기'에 대하여 규정할 수 있을 뿐 그 파기 기술의 수준까지 세분화 할 수 없다. 따라서 파기의 기술적 조치는 지침 또는 가이드라인을 통해 기술변화에 연동하여 구체화 할 문제이다.

'기술적·관리적 조치'와 관련하여 「정보통신망법」은 i)내부 관리계획 수립·시행, ii) 접근 통제장치의 설치·운영, iii) 안전하게 저장·전송할 수 있는 암호화

기술의 적용, iv) 접속기록 위·변조 방지 조치, v) 컴퓨터바이러스에 의한 침해 방지조치, vi)기타 안전성 확보를 위하여 필요한 보호조치 를 규정하고 있다. 생체정보의 기술적·관리적 조치에 대한 특별한 사항은 이 이에 추가할 만한 법률상의 조치가 필요한지에 대한 검토가 이루어져야 한다. 이용자 식별이 가능한 ID와 생체정보의 분리 운영(물리적, 논리적)이 기술적·관리적 조치와 관련하여 필요하다면 이는 법률 위임에 따라 시행령에 의해 규율될 수 있다. 「정보통신망법」시행령 제15조제6항에서는 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하도록 규정하고 있는 바, 특수한 민감정보의 조치와 관련하여 특이사항은 이러한 고시를 통해 규율하는 것이 바람직하다.

제3장 생체정보 규율현안과 입법과제

제1절 서 론

최근 개인정보의 특수한 유형으로서 '생체정보', '개인영상정보' 등에 대한 특별한 규율필요성에 대하여 검토할 필요가 있음이 제기되고 있다. 특히 '개인영상정보'에 대하여는 이미 특별법 형태로 추진하고자 하는 정부안이 진행 중이며, '생체정보' 역시 그 민감성, 불변성 등을 이유로 특별히 규율하자는 주장이 일응 타당성 있기도 하다.

이러한 개인정보를 다른 개인정보와는 다르게 특별히 규율하는 경우는 그 기본권 및 자유의 침해가능성, 사생활 침해가능성에 비추어 그 보호실익이 각별히 요구되는 경우 '민감정보'로 규율하고 있다. 또한 '고유식별정보' 역시 그 불변성과 전파성 등에 비추어 특별히 규율하고 있다. 뿐만 아니라, 우리나라와는 '주민등록번호'라는 고유한 식별번호의 부여와 그 오남용/유출로 인한 사회적 폐해가 극심한 바 이에 대하여는 '정보주체의 동의'와 무관하게 그 수집을 원천적으로 금지하고 '법령의 규정'에 의한 경우에만 그 처리를 허용하고 있다.

이처럼 통상의 개인정보와 다르게 특별히 취급하기 위해서는 그 타당성이 인정되어야 한다. 2018년 발효 예정은 GDPR은 앞으로 유럽국가와의 교역에서 개인정보 처리와 관련해 우리나라에 미칠 영향이 지대할 것으로 예상되고 있다. GDPR은 '생체정보'를 특별한 유형의 정보, 즉 우리나라의 '민감정보'에 해당하는 범주에 포함시켜 규율하고 있다. 최근 국내에서도 인증, 스마트 헬쓰케어 기기, 각종 영상정보 서비스 등 생체정보를 활용한 서비스가 확산되고 있는 바, 이에 대한 특별 규율의 필요성을 검토할 필요가 있다. 특히 '생체정보'는 항상 정보주체가 지니고 있으며, 그 속성이 쉽게 변하지 않는 다는 특성으로 인해 보안성이 강한 식별자로 취급되고 있으나, 한번 유출되거나 침해되었을 경우 이러한 불변성, 지참성 등으로 인한 정보주체의 권리 및 자유의 침해 요인도 크다.

따라서 이하에서는 '생체정보'가 활용되는 유형에 대하여 검토하여 그 활용과 관련된 법적 쟁점을 검토한 후, 「정보통신망법」의 개선방안을 제안하고자 한다.

제2절 생체정보의 속성

1. 생체정보의 개념

'생체정보'에[17] 대하여 혹자는 '사람의 고유한 신체적, 행동적 특징을 이용하여 개인의 신원을 확인할 수 있게 하는 정보로서, 지문, 홍채, 망막, 정맥패턴, 얼굴, 음성, 서명패턴 등 개인을 직접 나타내는 정보를 말한다'고 한다.[18] TTA는 생체정보에 대하여 '지문·얼굴·홍채·정맥 등 개인의 신체적 또는 행동적 특징에 관한 정보로서 특정 개인을 식별할 수 있는 것'을 말한다고 한다. EU GDPR은[19] '생체정보(Biometric data)'를 안면 영상이나 지문 정보와 같이 개인

17) Biometric data를 "생체정보" 혹은 "생체인식 정보" 또는 "생체정보"라는 용어에서 "생체"가 주는 부정적 인식 때문에 "바이오정보"라고 사용하는 경우가 있으나 본고에서는 "생체정보"라 명한다.

18) 김일환, 앞의 "생체인식기술 등 첨단정보보호기술의 이용촉진을 위한 법제도적 방안연구", 65-66면; 이민영, "생체정보의 보호에 관한 법제도적 정책방향", 「정보통신정책」, 제16권제21호(통권제359호), 정보통신정책연구원, 2004. 11. 16, 41면; 심우민, 심우민, "스마트 시대의 생체정보 보호를 위한 입법과제", 「이슈와 논점」, 국회입법조사처, 제1129호, 2016. 3. 3, 1면; 박정훈, 앞의 "바이오매트릭스의 이용에 따른 법적 과제", 401-402면; 조규범, "생체정보보호를 위한 입법론적 대응방안", 「국회도서관회보」, 제45권제9호(통권352호), 2008. 10, 49면 및 "생체정보 보호를 위한 입법론적 고찰", 「공법연구」, 제37집제1-2호, 2008. 183면; 연광석, "생체인식정보 보호에 관한 연구(비교법적 검토를 중심으로)", 「법제현안」, 제2005-4호(통권제173호), 국회사무처 법제실, 2005. 9, 5면; 박정훈・김행문, "생체정보 프라이버시의 쟁점 및 정책 시사점-전자여권 사례를 중심으로-", 「정보화정책」, 제15권제3호, 2008 가을호, 86면.

19) '일반개인정보보호규칙 (General Data Protection Regulation, GDPR)'은 2018년 5월 28일자로 발효하며, 기존 1995년 개인정보보호지침(Data Protection Directive 95/46/ec)을 대체하게 된다. GDPR은 유럽연합의 입법 형식 가운데 규칙(regulation)의 형식을 취하고 있으므로, 모든 회원국에서 직접적으로 적용된다. 1995년 개인정보보호지침 이후 21년 만에 채택된 GDPR은 그 동안의 인터넷 등 과학기술적 발전을 적극적으로 반영하였다.

고유의 식별을 허용 또는 확인하는 해당 개인의 신체적, 생리적, 행동적 특성에 관한 특정 기술 처리로 발생하는 개인정보를 의미한다.[20]

이러한 용어정의들에 비추어 봤을 때 "생체정보"라 함은 "개인의 신체적, 생리적, 행동적 특성에 관한 사항들이 특별한 기술적 처리를 통해 개인을 식별하거나, 식별할 수 있게 된 정보의 총체"를 의미한다고 할 수 있다. 생체인식(Biometrics)이라 함은 개인의 신체적 또는 행동적 특징을 이용하여 개인을 식별할 수 있는 방법을 의미하므로 그 자체는 개인정보에 해당되지 않는다.

이를 분설하면, 우선 특정 개인을 식별하거나 식별할 수 있는 정보 즉 개인정보이어야 한다. 따라서 특정인을 식별하지 않거나 식별가능성이 없는 신체적, 생리적, 행동적 특징은 논할 여지가 없다.

다음으로 개인정보 중에서도 신체적, 생리적. 행동적 즉 생체 특성에 관한 정보이다. 여기에는 가공되지 않은 '원본정보'와 기술적 처리를 통해 원본정보로부터 생성된 '특징정보'가 모두 포함된다. 통상 원본정보는 감지장치를 통하여 직접 사람의 신체나 행동방식에서 취득하는 정보를 말한다. 사진기에 촬영된 사진이나, 녹음된 목소리 등이 이에 해당된다. 특징정보란 원본정보를 기반으로 생체특징 추출 알고리즘을 이용해서 만든 디지털 정보를 의미한다. 따라서 통상 이러한 특징정보 만으로는 개인정보라 할 수 없으며 이러한 정보는 추가적 식별정보와 별정보가 합쳐져야 개인정보가 된다.[21]

한편 생리적 특성과 행동적 특성 사이에는 그 차이가 있다. 지문, 손모양, 홍채패턴 등 '생리적 특성'(physiological characteristic)은 상대적으로 안정적인 생체적 특성을 의미한다고 볼 수 있다. 그 측정값은 근본적으로 변화하지도 수

---

20) 제4조(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

21) 김일환, 생체정보보호법제 정비방안에 관한 고찰, 토지공법연구 제33집, 2005년 11월, 360면. 이 논문에서는 '원본정보'를 '생체인식 原데이터'로, '특징정보'를 '생체형판(biometric template)'이라는 용어를 사용한다.

정하지도 못한다. 이에 반해 서명, 목소리 등 '행동적 특성'(behavioral characteristic)은, 개인의 심리적 기질을 반영하며 유동적일 수 있다. 예를 들어 목소리인식의 경우 성대(voice chord) 모양 또는 서명인식의 경우 손과 손가락의 기민성(dexterity)에 따라 유동적이다. 즉 개인에게 발생하는 변화의 정도는 생리적 특성이 행동적 특성 보다 적다. 지문은 매일 동일한 형태로 유지되지만, 서명은 심리적 요인은물론 기타의 요인에 의하여서도 많은 영향을 받는다.

또한 생체 특성에 관한 정보가 특별한 기술적 처리를 거쳐야 한다. 이러한 기술적 처리를 거치지 아니한 경우 영상정보, 심박정보 등 사생활과 무관한 단순 서비스제공과정에서의 생체정보도 규율대상에 포함되어 그 규율범위가 지나치게 확대되게 된다.

2. 생체정보의 특성

우선 개인생체정보는 다음과 같은 특성을 지닌다. 우선 "지참성"이다. 항상 본인과 함께 존재한다. 별도로 보관할 필요가 없으며 다른 정보와 달리 도난이나 분실의 우려가 거의 없다. 이러한 편리성과 경제성으로 인해 고도의 부가가치를 창출할 바이오와 정보기술의 새로운 융합 산업군으로 전망되기도 한다.[22]

다음으로 '불변성·영구성'이다. 주민등록번호나 비밀번호 등 각종의 개인정보는 변경이 가능하나, 개인생체정보는 변경할 수 없다. 따라서 일단 유출이 되고 나면 다른 생체정보로 대체하지 않는 이상 그 생체정보를 사용할 수가 없게 된다. 생체정보는 다른 개인정보와는 달리 살아있는 동안 그 사람과 결합되어 있기 때문에 이름이나 주소, 식별번호, 암호와 같이 변경할 수 없다는 특수성을 가진다.[23]

이러한 특성으로 인해 생체정보는 여타 개인정보에 비해 더 엄격하게 보호

---

22) 조규범, 앞의 "생체정보보호를 위한 입법론적 대응방안", 50면.

23) 김일환, "정보사회에서 생체정보의 보호에 관한 헌법적 고찰", 인권과 정의 제344호, 2005.4., 23면 이하 참조.

되어야 한다고 주장된다. 즉 생체인식기술은 개인이 가진 신체 특징은 태어나서 죽을 때까지 변하지 않는다는 점에 착안한 기술로, 생체정보는 다른 개인정보와는 달리 정보 그 자체가 개인을 나타낼 수 있으므로 다른 개인정보보다 그 보호를 강화할 필요가 있다고 한다.[24]

24) 김일환, 전제논문(각주 5), 359-360면

제3절 생체정보제도 입법현안과 개선방안

1. 정보통신서비스제공자의 생체정보의 활용 유형

정보통신서비스제공자가 생체정보를 활용하는 유형은 생체정보를 직접 수집하여 이용하는 경우와, 타인에 의해 수집된 생체정보를 매개만 하는 경우로 나누어 볼 수 있다. 대체적으로 정보통신서비스제공자가 직접 수집하여 이용하는 경우는 본인 확인을 위한 인증의 경우가 대다수라고 할 수 있다. 이러한 본인확인을 위한 인증의 경우, 성인인증, 결제서비스, 기기인증 등에서 활용된다. 타인에 의해 수집된 정보를 매개만 하는 경우는 온라인동영상서비스 및 SNS 서비스제공과정에서 이루어지는 개인영상정보의 경우가 대표적이다. 그밖에 최근 디지털 헬스케어플랫폼 서비스 제공과정에서는 직접 수집과 매개가 동시에 이루어지는 양상을 보인다. 이하에서는 정보통신서비스제공자와 관련된 대표적 생체정보 활용현황을 '인증', '디지털헬스케어 플랫폼', '개인영상정보 활용' 중심으로 검토해 본다.

가. 인증(본인 확인)

대면중심의 오프라인에서는 본인인증이 특별히 문제될 것이 없다. 주로 주민등록증/운전면허증 소지와 대면인식이 함께 이루어지므로 본인인증을 위한 특별한 기술적 이슈가 존재하지 않는다. 그러나 비대면인 온라인 상에서는 필수적으로 본인확인 즉 인증이 중요한 기술적 제도적 이슈가 될 수 밖에 없다. "온라인 인증[Authentication]"이라 함은 여러 사람이 공유하고 있는 컴퓨터 시스템이나 통신망의 경우 이를 이용하려는 사람이나 장치 및 응용프로그램의 신분(identification)을 확인하여 불법적인 사용자가 들어올 수 없도록 시스템 보안을 유지하는 방법을 의미한다. 영기서 "본인확인"이란 정보통신망을 통하여 정보시스템 또는 행정정보를 이용하는 업무담당자, 민원인 또는 시스템 관리자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것을 의미

한다. 구별개념으로 “실명확인”이 있으며 이는 사용자가 사용한 명의가 실제로 존재하는 자의 명의인가 여부를 확인하는 것을 의미한다.

〈표 3-1〉 본인 확인 관련 법률규정

구분		관련 법률	주요내용
실명 확인		공직선거법 제82조의6(인터넷언론사 게시판·대화방 등의 실명확인)	실명확인이라 함은 사용자가 사용한 명의가 실제로 존재하는 자의 명의인가 여부를 확인하는 것을 말함
본인확인	민원인 등의 본인확인	전자정부법 제10조(민원인 등의 본인 확인) 전자정부법 시행령 제12조(민원인 등의 본인 확인)	전자정부법에서는 민원인등의 본인확인에 대하여 규정하고 있다. 본인확인의 방법으로 법률에서는 전자서명법 제2조제3호에 따른 공인전자서명을 제안하고 있음
	게임과몰입·중독 예방조치를 위한 본인인증	게임산업진흥에 관한 법률 제12조의3(게임과몰입·중독 예방조치 등) 게임산업진흥에 관한 법률 시행령 제8조의3(게임과몰입·중독 예방조치 등)	게임물 이용자의 게임과몰입과 중독을 예방하기 위하여 과도한 게임물 이용 방지 조치로서 ‘게임물 이용자의 회원가입 시 실명·연령 확인 및 본인 인증’을 하도록 규정

이러한 본인확인 즉 인증 수단으로는 다음과 같이 지식기반, 소지기반 및 생체기반의 인증수단으로 분류된다.

〈표 3-2〉 분류별 인증수단

분류	종류	설명
지식기반	ID/Password	서버에 저장된 아이디와 아이디에 매칭되는 비밀번호로 본인을 인증방식

	I-PIN	명의도용이 쉬운 주민등록번호를 대신하여 이용자에게 부여되는 인터넷 개인식별번호
	보안카드	비밀번호 도용에 의한 금융사고를 방지를 위해 사용하며 35개의 표에 4자리숫자들이 기록되어 있는 형태의 카드
	진위확인	식별정보를 이용하여 문서의 진위를 확인해주는 서비스
소지기반	공인인증서	공인인증기관이 인증한 전자서명으로 법령에서 서명 또는 기명날인을 요구한 경우에 공인전자서명은 이의 요건을 충족한 것
	보안토큰(HSM)	소프트웨어 형태의 토큰을 안전하게 보관하기 위해 고안된 하드웨어형 토큰
	OTP	로그인할 때마다 그 세션에서만 사용할 수 있는 1회성 패스워드를 생성하는 보안서비스
	휴대폰 SMS 인증	입력한 주민등록번호와 휴대폰번호 + 휴대폰 가입시 등록한 가입자 주민등록번호가 맞는지를 이동통신사를 통해 확인하는 서비스
	2채널인증	임의로 생성된 1회용 비밀번호를 반드시 사용자의 전화에서 입력하는 인증을 거쳐야만 거래가 가능하도록 하는 서비스
	PC등록 인증	사전에 등록된 PC에 한하여 거래가 가능하도록 하는 서비스
생체기반	바이오인증	이용자의 바이오정보(지문인식, 얼굴인식, 전자펜서명인식등)의 바이오정보를 이용하여 본인 확인을 하는 서비스

특히 생체기반 인증은 사용자가 가지고 있는 고유한 지문이나 홍체, 정맥등과 같은 생체적 특징을 이용하여 인증하는 방식으로 이용자의 생체정보(지문인식, 얼굴인식, 전자펜서명인식등)를 이용하여 본인 확인을 하는 방식이다. 얼굴구조, 지문, 홍채, 정맥 등 생체적 특징을 이용한 방식과, 목소리, 타이핑리듬 등 행동적 특징을 이용한 방식이 있다.

분실, 변경의 위험이 없어 타인증수단 보다 보안성이 높다는 장점이 있으나, i)생체정보를 인식할 시스템이 필요하여 비용이 많이 소요되고, ii)생체정보 이용에 대한 거부감이 있을 수 있으며, iii)변경이 불가능하여 유출시 복구가 불가능하다는 단점이 있다. 생성주기는 다음과 같다.

〈표 3-3〉 인증수단으로서 생체정보 생성주기

구분	설 명
발급	- 별도의 과정이 없음
등록	- 생체정보의 원본 정보 영상을 디지털화하고 이것의 특징 정보를 생성하여 저장
인증	- 데이터베이스에 저장된 값과 비교하여 검증
갱신	- 별도의 갱신 과정이 없음
폐기	- 이용자가 요청하거나 정보가 필요하지 않는 경우

나. 헬스케어 플랫폼 서비스

우선 헬쓰케어 영역에서 생체정보는 개인건강기기(Personal Health Device)를 통해 수집된다. 이러한 개인건강기기는 가정용 또는 휴대용기기에 센서를 내장하여 언제 어디서나 개인의 건강상태를 측정할 수 있는 웨어러블 디바이스 등을 말한다. 주요 제품으로는 Fitbit Flex(핏비트), Fuel Band(나이키), Shine(미스핏), Gear Series(삼성전자) 등이 있다.[25] 최근 미국 식품의약국(Food and Drug Administration, FDA) 및 한국 식약처에서 의료기기로서의 규제를 받지 않아도 된다고 정의한 건강관리용 제품들, 일명 “웰니스”제품들도 이에 해당된다. “웰니스”제품의 경우에는 건강관리용으로서 맥박, 수면 장애 등을 점검하여 사용자에게 정보를 알려줄 수는 있으나 본 데이터는 질병 진단의 목

25) 이진수, “디지털 헬스케어 플랫폼과 주요기업 동향”, 보건산업브리프 vol 140, 한국보건산업진흥원, 2014. 9, 4면.

적을 가질 수 없기 때문에 의료용으로 사용할 수 없다. 또한 의료기기로서 규제를 받으나 ICT의 기술을 활용하는 심전도 측정 제품, 유전자 분석 제품들 또한 이에 해당한다. 이렇게 수집된 정보들은 스마트기기에 내장된 카메라 센서 및 앱세서리(앱과 연결된 악세서리를 이용하여 개인의 건강상태를 측정·관리할 수 있는 어플리케이션)인 PHA(Personal Health Application)를 통해 전송된다. 주요 PHA 제품으로는 Nike Move(나이키), S-헬스(삼성전자), RunKeeper(피트니스키퍼) 등이 있다.[26]

두 번째로는 각 기기들로부터 측정된 결과가 집결되는 데이터 관리의 영역이다. 생체정보를 비롯한 개인건강정보들은 각각의 정보를 통합하여 저장·관리할 수 있는 데이터 플랫폼이 필요하며, 이를 '개인건강정보 플랫폼(PHI Platform)' 또는 '디지털헬스케어 플랫폼'이라 한다. 외부사업자들이 개발한 헬스케어 제품들로부터 수집된 생체정보 또는 개인건강정보들은 이러한 하나의 플랫폼에서 통합·관리함으로서 개인의 건강상태를 종합적으로 분석할 수 있다. 개인건강정보(PHI)를 효율적으로 관리할 수 있는 플랫폼을 중심으로, 개인의 건강정보를 수집하는 제품공급자(PHD, PHA)와 건강관리·의료서비스 제공자가 참여함으로써 디지털헬스케어 생태계의 구현이 가능하다.[27] 클라우드컴퓨팅을 이용하여 개인용 의료 히스토리(PHR, EMR)를 모으는 형태와, SNS서비스로 구성되어 이용자들이 자발적으로 자신들의 의료 기록 및 정보를 공유하는 형태가 있다.[28] 개인건강정보 플랫폼 서비스의 특성상 다양한 공급자와

---

26) 이진수, 전게논문, 4면.

27) 이진수, 전게논문, 4~5면.

28) SNS를 통해 의료정보를 공유하는 대표적 케이스로 'PatientsLikeMe'가 있다. 'PatientsLikeMe'는 2004년 29살의 젊은 나이로 희귀 질환인 루게릭병에 걸린 형제를 위해 3명의 MIT출신 엔지니어가 모여서 만든 환자들의 SNS로 2011년까지 루게릭병, 파킨슨씨병 등 22가지 만성 질환에만 제한적으로 새로운 멤버들을 받아들이다가, 이후로는 완전히 공개하여 암이나 당뇨병등 여타 다른 질병에 대한 환자들의 가입도 허용하고 있다. 이렇게 환자들을 통해 쌓인 데이터를 바탕으로 기존의 의학계 연구를 정면으로 반박하는 논문을 Nature Biotechnology 에 출판하기도 하였으며 매우 희귀한 질병을 가진 환자들을 서로 이어줌으로써, 학계와 제약업계

참여자(소비자)를 수용할 수 있는 사업자가 유의미한 개인건강정보 플랫폼 사업자로서 참여할 수 있어 애플, 구글과 같이 많은 이용자의 트래픽을 유도할 수 있는 플랫폼 사업자들이 이 영역에서 성과를 낼 수 있을 것으로 생각된다. 정보통신서비스제공자의 생체정보 활용과 관련된 부분이 바로 이 플랫폼 사업자 영역이라고 할 수 있다.

(1) 애플의 HealthKit

'애플'은 클라우드컴퓨팅을 기반으로 헬스앱을 통해 수집한 개인건강정보와 EMR정보의 통합을 통해 새로운 디지털헬스케어서비스를 제공하고자 종합적인 개인건강정보 통합 플랫폼 구축을 시도하고 있다. 애플의 HealthKit은 외부의 다양한 디바이스 어플리케이션을 통해 개인건강정보를 수집하고 이를 통합 저장·관리하는 시스템이다.[29] 이를 위해 애플은 헬스케어 시장에 다양한 외부사업자(Third party service)들을 끌어들여 개방형 헬스케어 생태계를 구축할 계획을 추진하고 있으며, 이와 동시에 iOS 어플리케이션을 개발하기 위한 iOS SDK(Software Development Kit)의 프레임워크로 HealthKit을 제공, 외부사업자는 애플의 앱스토어에 입점한 iOS 어플리케이션으로 한정함으로써 통제권을 발휘하고자 한다. 아울러 헬스어플리케이션을 통해 의료기관, EHR 시스템과 연계 및 의료서비스와 접목을 시도하고 있는데 지난 5년간 미국 의료기관인 Mayo Clinic과 협력을 통해 헬스어플리케이션을 공동으로 개발함으로써 단순한 건강데이터의 관리뿐 아니라 기존의 의료시스템과 통합까지 사업영역을 확대하고 있다. 또한 미국 최대 EHR 회사인 Epic과의 제휴를 통해 다양한 대형 의료기관 환자들의 의료기록을 HealthKit과 통합함으로써 플랫폼 활용도를 극

에서 아직 연구가 되지 않은 해당 질병을 파악하기 위한 방도로도 많이 이용되고 있다.

29) 애플은 2014년 6월 3일, 자사의 개발자 행사인 WWDC 2014를 통해 모바일 운영체제 차기 버전 iOS8를 발표하고 디지털 헬스케어 플랫폼 HealthKit과 어플리케이션 Health를 탑재함으로써 디지털헬스분야 진출을 본격화하였다.

대화 하고자 하는 움직임을 보이고 있다. 여기서 헬스케어 플랫폼을 제공하는 '애플'은 우리법에 의할 경우 정보통신서비스제공자에 해당된다.

(2) 얼라이브코(AliveCor)

'얼라이브코(AliveCor)'가 제공하는 '얼라이브 인사이트(Alive insight)'서비스는 사용자가 자신이 측정한 데이터를 미국 내 의사 면허를 갖고 있는 심혈관계 전문의(cardiologist) 및 심장 관련 테크니션(cardiac technician)에게 전송하는 원격 진단 서비스라고 할 수 있다. 사용자가 스마트폰으로 측정한 ECG(심전도)데이터를 일정한 금액을 지불하고 원격으로 의료 전문가에게 전송하면, 일정 시간 후 그 데이터에 대한 해석 및 진단을 받아볼 수 있다.[30] 심장 기기 테크니션에게 데이터를 보내는 서비스는 지불하는 금액에 따라 30분 내, 혹은 24시간 내에 결과를 받아볼 수 있으며[31] 심혈관계 전문의에게 데이터를 보내면 24시간 내에 상태가 얼마나 심각한지를 나타내어주는 결과 및 권고 사항을 받아볼 수 있다. '얼라이브코(AliveCor)'는 미국 내 가장 큰 전자건강기록(EHR)[32] 기업 중 하나인 '프랙티스 퓨전(Practice Fusion)'과 연동하여 측정된 데이터를 의료기관의 의료진이 진료에 활용할 수 있도록 제공하고 있다. '프랙티스 퓨전(Practice Fusion)'의 EMR에 '얼라이브코(AliveCor)'가 연동되면서,

---

30) 최윤섭, "이미 시작된 미래 헬스케어 이노베이션", 클라우드 나인, 2014, 98면

31) 각각 서비스의 가격은 5달러, 2달러이다.

32) 모든 의료 기관의 전자 의료 기록(EMR)을 네트워크로 통합하여 공유하는 첨단 의료 정보화. 현재 각 의료 기관별로 개별 관리되고 있는 환자의 진료 관련 자료들을 통일 또는 호환성을 향상시키고, 시스템 및 서비스 표준화를 통해 중복 투자와 낭비를 줄이며, 임상 진료의 효과를 향상시킨다는 것이 주 목적이다. 전자 건강 기록(EHR)은 환자에 대한 처방 및 임상 실험, 진료 의사 결정뿐만 아니라 환자의 의료 정보에 대한 장기적 관리를 가능하게 해 주는 장점을 가지고 있으며, 네트워크화된 시스템은 진료 정보에 대한 저장뿐만 아니라 원격 진료, 치료, 처방, 건강 관리 및 분석과 기록을 가능하게 함으로써 의료의 질을 향상시킬 수 있는 기회를 제공한다. (IT용어사전, 한국정보통신기술협회)

환자들이 측정한 ECG 데이터를 실시간으로 전송하여 EMR에 저장할 수 있고, 이 결과를 의사들이 일상적인 진료에 활용할 수 있다. 이제 의사들은 기존의 다른 일반적인 의료 테스트 결과와 함께, 환자들이 매일 측정한 ECG 데이터 또한 진료실에서 EMR을 통해 간편하게 확인하고 진료에 이용할 수 있다. '프렉티스 퓨전'은 미국에서 매달 10만 명의 의사가 사용하는 대규모 EHR이기 때문에 그 파급효과는 더욱 클 것으로 예상 된다. 의사들은 비용대비 효과적인 방법으로 환자들의 심장을 언제, 어디서나 측정하고, 이 데이터를 즉시 EMR로 받아들일 수 있으며, 환자들의 ECG(심전도)데이터를 '얼라이브코(AliveCor)'와 AliveInsight를 통해서 무선으로 기록 및 저장, 열람하고 이를 해석하여 전송하는 것이 가능하다. 또한 측정한 데이터는 클라우드컴퓨터 내에서 언제 어디서나 안전하게 저장할 수 있으며, 환자의 측정 결과 및 분석 레포트, 전문가 리뷰를 EMR과 함께 동기화 할 수 있다. 여기서 헬스케어 플랫폼을 제공하는 '얼라이브코(AliveCor)'는 우리법에 의할 경우 정보통신서비스제공자에 해당된다.

다. 개인영상정보 활용서비스

최근 다양한 분야에서 드론(Drone)기기·웨어러블(Wearable)기기·차량용블랙박스등 '이동형 영상처리기기'의 이용이 점차 확산되고 있다. 과거와 달리 폐쇄회로텔레비전(CCTV) 등의 '고정형 영상정보처리기기' 뿐만 아니라, 차량용(Black box)영상처리기기·무인항공기(Drone)영상처리기기·웨어러블(Wearable)영상처리기기 등과 같이 누구나 언제어디서든 촬영이 가능한 이동형 영상정보처리기기의 급격한 이용과 확산으로 인하여 개인의 사적인 정보가 침해될 위험성이 증폭되고 있다. 초기 드론·스마트글래스·차량용블랙박스 등 이동형 영상정보처리기기는 정찰용·방범용·방송용·군사용 등 특정목적을 위해 공공분야에서 주로 사용되어 왔지만 최근 그 판매가격과 이용비용이 낮아지면서, 레저용·농업용·택배용 등 민간의 여러분야로도 그 이용이 점차 확대되고 있다. 특히, 개인영상정보는 개인일상생활의 전체과정을 포함하고 있어, 그 처리과정에

서 개인의 사적으로 내밀한 영역까지 침해가 가능하다. 이동형 영상정보처리기기의 운영과정에서 무분별하게 수집될 수 있는 개인의 전신·얼굴·옷차림새·활동 등의 개인영상정보는 개인의 프라이버시와 민감하게 관련되며, 이동형 영상정보처리기기는 이동성·휴대성·융합성·은밀성·연계성·첨단성 등의 특징으로 말미암아 과거에 비해 개인영상정보가 침해될 위험성이 높다.

〈표 3-4〉 이동형 영상정보처리기기의 특성

구분	특성
이동성	폐쇄회로 텔레비전(CCTV: Closed Circuit Television) 등과 같이 일정한 공간에 지속적으로 설치되는 고정형 영상정보처리기기와는 다르게 언제어디서든 누구나 손쉽게 그 이동이 가능
휴대성	한 지역에서 다른 지역으로 빠르게 이동할 수 있음은 물론 개인이 소지가 가능해 많은 사람이 방송촬영·개인사진촬영 등의 개인휴대용을 이유로 이용하고 있으며 그 수도 파악 곤란
융합성	나노기술(NT), RFID기술 등과 결합할 경우 눈에 잘 안보일 정도로 초소형화할 수 있거나 대량의 개인영상정보는 물론 많은 정보가 수집·유출될 수 때문에 개인영상정보가 침해될 위험성이 급증
은밀성	제3자에 의해 개인영상정보가 촬영되는 상황을 인식하기가 곤란
연계성	스마트폰, 컴퓨터, 노트북, 태블릿 등의 수많은 전자기기들과 연결할 수 있고 연계된 전자기기에 다운로드한 다양한 앱들의 기능도 함께 사용이 가능하여 한번 개인영상정보가 수집되고 저장된 후 개인영상정보를 통제하기 곤란
첨단성	첨단화된 기기들로 지상 수십미터에서도 고정밀로 촬영이 가능한 고성능 카메라장치를 장착할 수 있을 정도로 발전속도가 매우 빠르며 상업화로 인해 매년 새로운 기능이 장착된 많은 제품이 양산

현행「개인정보 보호법」제25조는 고정형 영상정보처리기기에 관한 사항만 규율하고 스마트폰, 블랙박스, 드론 등 이동형 영상정보처리기기는 규율 범위에서 제외된다. 사람・사물을 촬영할 수 있는 영상정보처리기기는 매우 다양하며, 기기들의 사용을 모두 엄격하게 규제할 경우 사회생활이나 경제활동에 제약을 가져올 수 있기 때문에, 이 법에 따른 영상정보처리기기의 종류는 대통령령으로 정하는 기기만을 인정하고 있다. 따라서 개인정보 보호법 시행령 제3조에서느 영상정보처리기기를 '폐쇄회로 텔레비전'과 '네트워크 카메라'로 규율하고 있다. '폐쇄회로 텔레비전'이라 함은 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 이를 유·무선 폐쇄회로 등의 전송로를 통해 전송 또는 저장매체에 녹화·기록할 수 있도록 하는 장치를 의미하며, '네트워크 카메라'는 일정한 공간에 지속적으로 설치된 촬영기기로 수집한 영상정보를 유·무선 인터넷을 통하여 어느 곳에서나 수신・ 조작・저장 등의 처리를 할 수 있도록 하는 장치를 말한다.

따라서 이동형 영상정보처리기기에 의한 개인영상정보의 수집, 처리에 대하여는 '개인정보 처리자'에 해당될 경우 '개인정보 보호법'의 일반규정이 적용되는 것인지 모호하며, 이동형 영상정보처리기기를 통해 개인정보를 처리하는 자들이 '개인정보 처리자'에 해당될 경우, 현재 일상적인 블랙박스 사용자 등 수많은 범법자가 발생하게 된다. 이러한 점을 규율하고자 '개인영상정보 보호법(안)'이 현재 입법추진중이다.

정보통신서비스 제공자가 처리하는 개인영상정보는 크게 3가지로 구분할 수 있다. 첫째, 정보통신서비스 제공자가 직접 수집·이용하는 개인영상정보이다(예 : 구글의 스트리트뷰 또는 카카오의 로드뷰 등을 통하여 수집된 개인영상정보). 둘째, 일반인이 수집하여 정보통신서비스 제공자를 통해 제공된 개인영상정보이다(예 : 보배드림의 블랙박스영상 또는 유튜브의 개인영상). 셋째, 정보통신서비스 제공자의 플랫폼을 이용하여 생성되는 개인영상정보이다 (예 : 아프리카TV 등의 인터넷개인방송).

일반 공중이 수집하는 개인영상정보는 대면 또는 통신수단을 통해서 제3자에게 제공될 우려가 없는 것은 아니지만, 그 확산성은 높지 않다고 할 것이나.

이에 반해 정보통신서비스 제공자가 처리하는 개인영상정보는 널리 전파될 위험이 매우 높고 영리목적으로 사용될 가능성이 높다. 또한 개인영상정보를 직접 수집/유통하는 정보통신서비스제공자와 단순히 매개서비스만 제공하는 정보통신서비스제공자에 대한 규율은 달라져야 한다.

개인영상정보에 대하여는 제4장에서 후술한다.

2. 법적 쟁점

우선 첫 번째 쟁점은 생체정보를 통상의 개인정보와 분리하여 '민감정보'에 포함시킬 것인가 하는 것이 문제된다. 통상의 개인정보는 「정보통신망법」에 의해 i)동의, ii)법률의 규정, iii)계약의 이행, iv)요금정산을 위해 수집, 이용할 수 있으며, 「개인정보 보호법」에 의해 i)정보주체·제3자의 급박한 생명, 신체, 재산의 이익 ii) 개인정보처리자의 정당한 이익을 달성을 위해서도 수집, 이용할 수 있다. 만약 생체정보를 명시적으로 민감정보에 포함할 경우 그 수집, 이용은 i)정보주체의 동의, ii) 법률의 규정에 의해서만 정당화 된다.

두 번째 쟁점은 관리, 보관, 파기 등에 있어서 특칙 필요 여부이다.

'관리' 단계에서 정보통신서비스제공자는 '개인정보 보호책임자'를 지정하고, '개인정보 처리방침'을 공개하여야 한다. '파기'와 관련하여「정보통신망법」은 i)보유기간 경과, ii)수집·이용목적달성, iii) 사업의 폐업, iv)1년 동안 미이용자 정보를 파기하도록 규율하고 있다. 이와 관련하여 '생체정보'에 특별히 규율한 사항이 있는지에 대한 검토가 필요하다. '기술적·관리적 조치'와 관련하여 「정보통신망법」은 i)내부 관리계획 수립·시행, ii) 접근 통제장치의 설치·운영, iii) 안전하게 저장·전송할 수 있는 암호화 기술의 적용, iv) 접속기록 위·변조 방지조치, v) 컴퓨터바이러스에 의한 침해 방지조치, vi)기타 안전성 확보를 위하여 필요한 보호조치를 규정하고 있다. 생체정보에 대하여 이에 추가할 만한 법률상의 조치가 필요한지에 대한 검토가 이루어져야 한다.

3. 생체정보의 특칙필요성 검토

가. 민감정보 포함 여부

우선 현행법상 생체정보는 민감정보에 해당된다고 보기 곤란하다. 현행「개인정보 보호법」제23조에 의하면 '민감정보'란 ①사상·신념, ②노동조합·정당의 가입·탈퇴, ③정치적 견해, ④건강, 성생활 등에 관한 정보, ⑤ 유전정보 ⑥ 범죄경력(형의 선고·면제 및 선고유예, 보호감호, 치료감호, 보호관찰, 선고유예의 실효, 집행유예의 취소 등)에 관한 정보를 의미한다(⑤, ⑥은 시행령 제18조).

현행「정보통신망법」은 '민감정보'라고 명확히 규율하고 있지 않다. 다만 제23조 제1항에서 '정보통신서비스 제공자는 ①사상, 신념, ②가족 및 친인척 관계, ③학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 타 개인정보에 비하여 특별히 규정하여 이러한 정보에 대하여는 원칙적으로 수집을 금지하되 ①이용자의 동의를 받거나 ②다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에만 필요한 범위에서 최소한으로 수집할 수 있도록 규정하고 있다.

「개인정보 보호법」은 사생활을 현저히 침해할 우려여부에 대한 해석의 여지가 크기 때문에 민감정보로 특별히 보호할 필요가 있다고 사회적 합의가 이루어진 정보를 상황에 맞게 규정할 수 있도록 대통령령에 위임하여 현재 6가지 종류의 정보를 민감정보로 열거하고 있다. 반면「정보통신망법」은 "기타 ~~등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보"라고 규정함으로서 앞에 제시된 정보는 예시적 사항이며 추가적 민감정보가 법률상 포섭될 수 있도록 규정하고 있다.

따라서 '생체정보'는 「개인정보 보호법」상 민감정보에 해당되지 않으나,

「정보통신망법」상 민감정보 해당될 여지도 있다. 그러나 「개인정보 보호법」과 「정보통신망법」이 민감정보의 해당여부에 대한 공통된 기준으로 '사생활을 현저하게 침해할 우려가 있는 개인정보'를 제시하고 있으며 이는 해당 정보를 수집·처리함으로써 「헌법」상 보장된 프라이버시권의 본질적 내용이 침해될 우려가 있는 것을 의미한다. 따라서「개인정보 보호법」에서 생체정보를 특별히 '민감정보'로 규정하지 않은 바 정보통신서비스제공자에 의한 프라이버시 침해 우려가 특별히 더 인정된다고 입증할 만한 사유가 없는 한 「정보통신망법」상 민감정보에 해당된다고 보기 어렵다. 그밖에 「정보통신망법」상 생체정보의 수집/이용이 "개인의 권리·이익을 뚜렷하게 침해할 우려가 있는지 여부"에 대하여는 별도의 검토가 필요하다. 따라서 현행 「개인정보 보호법」 및 「정보통신망법」상 '생체정보'는 '민감정보'에 해당되지 않는다.

생체정보는 민감정보에 해당되지 않으므로 개인정보의 수집·이용, 수집제한, 제3자 제공, 관리, 보호조치, 파기 등과 관련하여 통상의 개인정보와 동일하게 다음과 같은 규율을 받는다.

단순히 서비스제공과정에서 처리되는 모든 생체정보를 민감정보를 규율한다면, 전혀 프라이버시침해적 요소나 권리와 자유침해의 리스크가 없음에도 불구하고 과도한 규율이 된다. 따라서 생체정보를 민감정보에 포함시킨다면 GDPR의 경우처럼 모든 생체정보가 아니라 '개인을 고유하게 식별하는 목적의 생체정보(biometric data for the purpose of uniquely identifying a natural person)'로 제한하는 것이 타당하다. 모든 개인정보는 '식별가능성'이 핵심이며 '식별가능성'이 없으면 개인정보가 아니다. 그럼에도 불구하고 GDPR에서 민감정보로서 '생체정보'에 대하여는 '개인을 식별하기 위한 목적으로 사용되는 경우'로만 한정하는 것은 결국 '인증' 이나 본인확인을 목적으로 생체정보를 활용하는 경우를 의미한다고 보여 진다. GDPR 에서도 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술적 수단을 통해 처리되는 경우에 한해서만 생체정보의 정의에 해당되기 때문에, 시스템적으로 민감처리로 분류되지 않는다.[33] 즉 본인을 확인하기 위한 수단으로 사용되지 않는 한 생체정보는 민

감정보로 규율하지 않는 것이 바람직하다.

각종 디지털헬스케어 서비스를 통하여 실시간 이동되는 심박정보나 맥박정보 등은 이러한 생체정보에서 제외되며, 페이스북 등 각종 SNS나 플랫폼서비스를 통해 이용되는 개인영상정보도 생체정보에서 제외된다. 따라서 "생체정보"란 '개인정보로서 얼굴, 지문 등 개인의 신체적, 생리적, 행동적 특성에 관한 정보로서 개인을 인증 또는 확인하기 위하여 특별히 기술적으로 처리한 정보'로 규율될 수 있다.

생체정보에는 수집되어 처리되는 과정에서 원본정보와(지문, 얼굴 이미지 등) 이러한 원본정보에서 추출한 특징정보(feature)가 포함된다. 원본정보는 감지장치를 통하여 직접 사람의 신체나 행동방식에서 취득하는 정보를 말한다. 사진기에 촬영된 사진이나, 녹음된 목소리 등이 이에 해당된다. 특징정보란 원본정보를 기반으로 생체특징 추출 알고리즘을 이용해서 만든 디지털 정보를 의미한다. 따라서 통상 이러한 특징정보 만으로는 개인정보라 할 수 없으며 이러한 정보는 추가적 식별정보와 특징정보가 합쳐져야 개인정보가 된다. 양자는 개인정보에 해당되는 한 동일하게 생체정보로 규율되어야 하며, 법률상 다른 취급을 할 실익은 없다.

나. 관리, 보관, 파기 등에 있어서 특칙 필요성

'관리' 단계에서 정보통신서비스제공자는 '개인정보 보호책임자'를 지정하고, '개인정보 처리방침'을 공개하여야 한다. 생체정보의 경우 특별히 문제될 수 있는 사항은 현재 공공기관의 정보처리의 경우에만 의무화 하고 있는 '개인정보 영향평가' 도입에 관한 사항이다. 앞에서 검토하였듯이 GDPR은 대규모 민감정보의 처리나 범죄경력 및 범죄 행위에 관련된 개인정보의 처리에 대하여는 영향평가를 실시하도록 규정하고 있다. 정보통신서비스제공자가 생체인증 방식으로 본인확인을 하고자 한다면 개인정보영향평가를 의무적으로 실시

33) GDPR 전문 (51)

하여야 하는지가 문제될 수 있다. 이 부분에 대하여는 사업자에게 미치는 영향, 현재 정보통신서비스제공자가 인증목적의 생체정보를 활용하고 있는 규모와 현황, 개인정보 침해가능성 등에 대한 사전적 조사를 통하여 도입에 신중을 기하여야 할 것이다.

'파기'와 관련하여「정보통신망법」은 i)보유기간 경과, ii)수집·이용목적달성, iii) 사업의 폐업, iv)1년 동안 미이용자 정보를 파기하도록 규율하고 있다. 이와 관련하여 '생체정보'에 특별히 규율한 사항이 있는지에 대한 검토가 필요하다. 생체인식 서비스의 알고리즘 고도화를 위해 개인식별 ID를 분리한 원본 정보의 활용 필요성이 제기되기도 한다. ID를 분리한 원본정보를 파기에 대한 예외 규정으로 둘 필요가 있는지에 대하여는 추가적 논의가 필요하다. 그러나 원본정보의 무분별 활용 및 장기 보관은 그 오남용 및 프라이버시 침해 위협을 증대시키므로, 원본정보는 원칙적으로 현행「정보통신망법」상 파기 사유에 해당되면 파기하도록 하는 것이 타당하다고 생각된다.

특히 생체정보의 파기와 관련된 기술적 보호조치의 기준 제시가 필요하다는 주장이 있다. 그러나 이는 비단 생체정보에만 국한된 문제가 아니며, 법률은 기술중립성에 기반하여 '파기'에 대하여 규정할 수 있을 뿐 그 파기 기술의 수준까지 세분화 할 수 없다. 따라서 파기의 기술적 조치는 지침 또는 가이드라인을 통해 기술변화에 연동하여 구체화 할 문제이다.

'기술적·관리적 조치'와 관련하여 「정보통신망법」은 i)내부 관리계획 수립·시행, ii) 접근 통제장치의 설치·운영, iii) 안전하게 저장·전송할 수 있는 암호화 기술의 적용, iv) 접속기록 위·변조 방지 조치, v) 컴퓨터바이러스에 의한 침해 방지조치, vi)기타 안전성 확보를 위하여 필요한 보호조치 를 규정하고 있다. 생체정보의 기술적·관리적 조치에 대한 특별한 사항은 이 이에 추가할 만한 법률상의 조치가 필요한지에 대한 검토가 이루어져야 한다. 이용자 식별이 가능한 ID와 생체정보의 분리 운영(물리적, 논리적)이 기술적·관리적 조치와 관련하여 필요하다면 이는 법률 위임에 따라 시행령에 의해 규율될 수 있다. 「정

보통신망법」시행령 제15조제6항에서는 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하도록 규정하고 있는 바, 생체정보의 조치와 관련하여 특이사항은 이러한 고시를 통해 규율하는 것이 바람직하다.

제4절 소결

우선, 현행법상 생체정보는 민감정보에 해당된다고 보기 곤란하다. 그러나 GDPR등 국제적 흐름에 비추어 볼 때, 생체정보의 특성 및 활용 확장성에 비추어 볼 때 생체정보를 민감정보의 일 유형으로 규정할 필요가 있다. 다만 모든 생체정보를 민감정보로 규율하는 것은 사생활 침해 가능성·정보주체의 자유와 권리침해의 리스크 등에 비추어 볼 때, 개인정보처리자에 대한 과도한 제한이 될 수 있다. 따라서 본인을 인증 또는 확인하기 위한 수단으로 사용되지 않는 한 생체정보는 민감정보로 규율하지 않는 것이 바람직하다. 민감정보에 해당되는 생체정보를 '특정인을 인증 또는 확인하기 위해 기술적으로 처리된 생체정보' 제한하여 규정하는 것이 바람직하다.

다음으로 관리, 보관, 파기 등에 있어서 생체정보에 대한 특칙은 불필요하다.

다만 GDPR과의 관계에서 대규모 민감정보의 처리에 대하여 개인정보 영향평가의 실시를 규정하고 있는바 국내법에의 도입에 대하여는 좀 더 고민이 필요하다. 그밖에 파기의 기술적 기준, 기술적·관리적 조치에 대한 특별한 사항은 고시나 지침을 통해 구체화하는 것이 바람직하다.

제4장 개인영상정보 규율현안과 입법과제

제1절 서 론

최근 다양한 분야에서 드론(Drone)이나 웨어러블(Wearable), 차량용블랙박스와 같이 영상을 촬영하여 정보통신망을 통해 전송될 수 있는 영상정보처리기기의 보편화가 이루어졌다. 이로 인하여 공공과 민간에 대한 손쉽게 영상정보처리기기를 구입할 수 있고 타인의 개인영상정보고 귀결되는 영상을 시간과 장소 등에 구애됨이 없이 촬영할 수 있게 되었다.

이러한 영상정보처리기기의 보편화는 드론이나 웨어러블 기기 등의 신산업 영역에서는 새로운 길을 열었으나, 개인영상정보주체에 대하여서는 자신이 촬영되었다는 점을 인지하지 못하여 정보자기결정권을 행사하지도 못할 뿐만 아니라, 유출·노출 및 사생활 침해 등에 그대로 방치되는 등 사회적 문제를 야기했다. 이로 인해 행정안전부는 2015년부터 '개인영상정보'를 안전하게 보호할 수 있도록 개인영상정보 보호법안을 마련하여 입법추진 노력이 한창 진행중이다.

따라서 이하에서는 정보통신서비스 환경에서의 '개인영상정보'가 의미하는 바와 그 개념적 특징을 살피고, 국내외의 산업 현황과 입법 동향을 검토함으로써 행정안전부가 마련한 개인영상정보 보호법 제정안에 대한 주요 내용과 법적 쟁점·한계를 분석함으로써 정보통신망법의 개정 방향을 모색해 보기로 한다.

제2절 정보통신서비스와 개인영상정보

1. 개인영상정보의 개념 및 특성

가. 개인영상정보의 개념

개인영상정보란 개인정보 보호법 제2조제7호에 따라 “일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치”에 의하여 촬영된 개인을 알아볼 수 있는 영상자료를 말한다. 구체적으로 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송 또는 녹화・기록하는 폐쇄회로 텔레비전(CCTV), 혹은 그 기기를 설치·관리하는 촬영된 영상정보를 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있는 네트워크 카메라 장치 등 영상정보처리기기[34]에 의하여 촬영·처리되는 영상정보 중 개인의

34) 개인정보 보호법 시행령 제3조는 ‘폐쇄회로 텔레비전’과 ‘네트워크 카메라’가 개인정보보호법 제25조에 따른 영상정보처리기기에 해당한다는 것을 명문화해 왔다. 그러나 최근 행정안전부가 입법예고한 개인영상정보 보호법 제정안에 따르면 영상정보처리기기는 기능에 따라 영상의 촬영을 주된 기능으로 하는 ‘영상촬영기기’와 PC, USB, WiFi 등 녹화・분석・전송 기능만을 수행하는 경우가 아니라 녹화·전송·분석을 주된 기능으로 하는 ‘기타 영상처리기기’로 세분화했고, 폐쇄회로 텔레비전(일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치 또는 그렇게 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치)과 네트워크 카메라(일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치)로 구분되었던 것을 구체적인 설치・운영 형태에 따라 특정 장소에 고정 설치된 폐쇄회로 텔레비전(CCTV)이나 네트워크 카메라와 같이 일정한 공간에 지속적으로 설치・운영되는 “고정형 기기”와 스

초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.

특히 최근에 입법 예고된 행정안전부의 개인영상정보 보호법 제정안에 따르면 개인의 식별 가능한 범위가 확장되었음을 알 수 있다. 제정안은 개인영상정보에 대하여 “개인영상정보란 영상정보처리기기에 의하여 살아있는 개인 또는 해당 개인과 관련된 사물을 촬영된 정보로서 초상이나 형태, 행동 등을 통하여 해당 개인을 알아볼 수 있는 정보를 말하며, 해당 영상만으로는 특정 개인을 알아 볼 수 없더라도 다른 정보와 쉽게 결합하여 알아 볼 수 있는 것을 포함하는 것으로 한다고 정의”하고 있기 때문이다. 즉, 육안을 통해 특정 개인을 알아볼 수 있는 영상자료는 물론이고 직관적으로 특정 개인을 알아볼 수 있는 개인이나 물건이 나온 영상자료, 얼굴이 나타나지 않거나[35] 알아보기 힘든 경우 등 직·간접적으로 특정 개인을 알아볼 수 없는 경우에도 착용하고 있는 의상이나 물건 등에 비추어 해당 개인이 누구인지 알아볼 수 있다면 개인영상정보에 해당한다는 것이다.

마트 안경·시계 등 웨어러블과 같이 사람의 신체에 착용하거나 스마트폰, 캠코더, 디지털카메라 등과 같이 휴대할 수 있는 이동성 있는 물건에 부착하여 운영하는 경우와 블랙박스, 주차단속 카메라, 드론 등 이동성 있는 물건에 부착하여 운영하는 “이동형 기기”로 다시 분류하면서 영상정보처리기기의 범위를 확대시켰다. ‘기타 영상처리기기’는 영상촬영기기와 전자회로 또는 유무선 네트워크로 연결되어 촬영된 영상을 녹화, 전송 또는 분석하는 기기를 포함하지만, 영상촬영기기와 연결된 기기로 제한되므로 녹화된 영상을 별도로 복사하여 다른 기기에서 저장·분석하는 경우는 제외되는 것으로 보고 있다.

35) 행정안전부는 개인영상정보에 대한 정의규정을 신설하는 과정에서 개인에 대한 사진이나 동영상의 범위에 대하여, 성명이나 연락처 등 ‘문자’를 촬영한 영상자료는 ‘살아있는 개인’ 또는 ‘해당 개인과 관련한 사물’에 대한 촬영은 아니고 개인정보보호법 상의 개인정보인 것으로 보고 있다. 한편 일반적으로 개인정보성이 있다고 보기 어려운 ‘건물’을 촬영하는 경우에 대하여 특정 유명인의 소유로 알려진 건물을 촬영한 사진과 같이 해당 사물의 소유자를 쉽게 식별할 수 있다면 개인영상정보에 해당할 수 있는 것이라 덧붙여 개인영상정보에 대한 범위가 상당히 폭넓게 설정되어 있음을 밝혔다.(개인영상정보 보호법안 제·개정이유서 참조)

특히, 물건에 대한 영상자료에 대해서도 결합가능성을 인정하고 있는데, 특정 개인과 직접적인 관련성이 있음을 전제하고 있는 물건이 사진이나 동영상 속에 나타나 있고, 그 물건을 통하여 특정 개인을 알아볼 수 있는 등 특정인에 대한 정보를 쉽게 알아낼 수 있다면, 해당 물건과 관련성 있는 개인이 영상정보주체[36]가 되는 것으로 해석하고 있기 때문에 '물건' 자체는 개인정보는 아니지만 그 사진은 개인영상정보에 해당할 수 있다는 결론이 도출되는 등 상당히 폭넓게 개인영상정보를 인정하고 있음을 알 수 있다.

결합용이성, 식별성, 식별성 등은 '개인정보'의 매우 특징적인 요소인데 개인영상정보 보호법 제정안은 '개인정보'를 정의하고 있는 우리나라의 개인정보 보호 법제에서 흔히 볼 수 있는 방식[37]으로 개인영상정보를 정의하고 있다. 예를 들면 개인정보 보호법이 "개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼

---

36) 행정안전부는 영상정보주체를 처리되는 영상정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다고 하여, 개인정보 보호법이 "처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람"을 정보주체라고 정의하는 것과 같은 형태로 정의내리고 있다. 위치정보의 보호 및 이용에 관한 법률의 개인위치정보주체(개인위치정보에 의하여 식별되는 자)나 신용정보의 이용 및 촉진에 관한 법률의 신용정보주체(처리된 신용정보로 식별되는 자로서 그 신용정보의 주체가 되는 자)의 정의규정과도 마찬가지의 형태이지만, 종전의 각 법률 상의 정보주체는 나타나 있는 개인과 관련된 정보들을 바탕으로 해당 정보의 주체가 되는 것이었으나, 영상정보주체는 영상자료에 나타난 개인이 아닌 '물건'이 특정인의 소유라고 하여 해당 물건의 소유자를 개인영상정보주체라고 하고 있어 위치정보법에서 개인위치정보주체에 '이동성 있는 물건의 소유자'를 개인위치정보주체로 보지 않는 것과 차이가 있다.

37) 위치정보의 보호 및 이용에 관한 법률에 따라 "개인위치정보라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)"를 말하며, 신용정보의 이용 및 촉진에 관한 법률에 따라 "개인신용정보란 신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보"라고 정의 되어 있다.

수 있는 것을 포함한다)를 말한다."고 정의하고 있는 것처럼 말이다.

나. 정보통신서비스 환경에서의 개인영상정보의 특성

과거 고정된 장소에 설치되는 것이었던 영상정보처리기기가 휴대성을 갖추고 IT 기술력과 융합하여 지능화를 이루어 낸 대표적인 사례는 제4차 산업혁명의 핵심적 요소인 인공지능(AI)[38] 이라고 할 수 있을 것이다. 인공지능 기술은 언어에 대한 자동분석・변환, 법조・의료 등 전문성 보유, 카메라와 오디오의 영상・음성 분석・변환, 이론증명, 두뇌역할을 하는 신경망(네트워크) 등 다섯 가지의 기능을 보유하고 있다.[39] 특히 인공지능 기기에 장착되어 있는 영상정보처리기기는 인간의 눈처럼 보면서 동시에 분석 자료의 하나인 사진이나 동영상 등을 생산해 낸다.

특정인의 얼굴 사진이나 동영상 등 영상자료를 통하여 누군가를 알아볼 수 있다는 점에서 개인영상정보는 생체정보[40]에 해당한다고 볼 수도 있을 것이지

38) 1956년에 광학판독 정도를 인공지능으로 보았다는 점에서 인공지능은 사회적 환경변화 또는 과학기술 및 정보통신기술 발전의 정도에 따라 달리 정의될 수 있다. (특허청, 인공지능(AI)분야 산업재산권 이슈 발굴 및 연구, 부산대학교 산학협력단 위탁연구, 2016.12., 14면)

39) 인간의 지능으로 할 수 있는 사고, 학습, 자기 개발 등을 컴퓨터가 할 수 있도록 하는 방법을 연구하는 컴퓨터 공학 및 정보기술의 한 분야로서, 컴퓨터가 인간의 지능적인 행동을 모방할 수 있도록 하는 것을 인공지능이라고 말하고 있다. 또한 인공지능은 그 자체로 존재하는 것이 아니라, 컴퓨터 과학의 다른 분야와 직간접으로 많은 관련을 맺고 있다. 특히 현대에는 정보기술의 여러 분야에서 인공지능적 요소를 도입하여 그 분야의 문제 풀이에 활용하려는 시도가 매우 활발하게 이루어지고 있다. (네이버 지식백과 - (두산백과) 인공지능 artificial intelligence)

40) 제3장에서 생체정보의 개념에 대한 검토한 내용에 비추어 개인의 신체적, 생리적, 행동적 특성에 관한 사항들이 특별한 기술적 처리를 통해 개인을 식별하거나, 식별할 수 있게 된 정보의 총체인 것으로 생체정보를 정의할 수 있으며, 지문, 홍채, 망막, 정맥패턴, 얼굴, 음성, 서명패턴 등 사람의 고유한 신체적・생리적 특징과 같이 개인을 직접 나타내는 정보를 예로 들 수 있을 것이다.

만 주로 본인임을 확인하거나 의료서비스 등 생체정보의 주체를 위한 목적으로 생성・추출・가공 되는 생체정보와는 태생부터 다르다고 볼 수 있다. 왜냐하면 개인영상정보는 CCTV・네트워크 카메라 또는 차량용블랙박스, 드론(Drone), 웨어러블(Wearable) 등 다양한 영상정보처리기기를 통해 무차별적으로 생성되어 불특정 다수에 대하여 개인의 사생활 침해문제가 발생할 수 있다는 점이 바로 그 근본적인 차이라고 볼 수 있다.

본래 영상정보처리기기는 범죄의 예방이나 수사, 시설안전 및 화재 예방, 교통단속 또는 교통정보의 수집·분석 및 제공 등을 목적으로 설치・운영되어왔다.[41] 특히 CCTV나 블랙박스 영상이 범죄 행위의 입증이나 범인 검거에 결정적인 단서를 제공하기 때문에 민간 영역에서도 그 설치가 빠르게 확산되었고 2014년에 이미 CCTV 795만여대, 블랙박스 643만여대가 설치・운영되는 것에 이르렀다.[42] 뿐만 아니라 각종 산업의 지능화가 진행되면서 영상정보처리기기는 IT 기술이 접목된 다양한 산업군에서 빠지지 않는 요소가 되었고, 결국 일일 평균 83번씩 CCTV에 노출(파이낸셜뉴스, 2015.2월)되는 결과로 이어졌다. 심지어 스마트폰이나 블랙박스를 통해 분별없이 촬영된 영상정보에 대하여서는 그 숫자를 가늠할 수조차 없어 그저 길을 걷고 있을 뿐인 행인은 자신이 촬영되었다는 사실도 모른 채 개인영상정보 오남용과 유출, 노출의 위험에 무방비로 노출되게 된 셈이다.

정보통신서비스 환경에서 개인영상정보는 크게 정보통신서비스 제공자가 직접 수집·이용하는 경우[43]와 일반인이 수집하고 정보통신서비스 제공자는 공개를 매개하는 경우[44] 등 두 가지로 분류할 수 있을 것인데 이러한 점은 개인영

41) 개인정보보호법 제25조 참조

42) 2015 정보화 통계집

43) 구글맵 또는 네이버 지도, 카카오 지도 서비스와 같이 정보통신서비스 제공자가 직접 개인영상정보를 수집하는 경우를 말한다.

44) 유투브와 같이 일반인들이 촬영한 영상을 업로드하여 공개하는 경우나 아프리카TV처럼 인터넷개인방송과 같이 정보통신서비스 제공자가 마련한 장을 통해 일반인이 자신이 보유하고 있거나 촬영한 영상정보를 공개하는 경우를 말한다.

상정보가 일단 노출되면 그 피해는 빠르게 확산된다는 점을 알 수 있을 것이다. 이러한 점으로 말미암아 정보통신서비스 환경에서의 개인영상정보는 특정인의 외모, 신체적 특징, 옷차림, 행태 등 사생활과 밀접하다는 점, 시간과 장소에 구애받지 않는 등 노출 위험도가 높다는 점, 각종 스마트기기와의 연계성에 의하여 피해가 빠르게 확산된다는 점이 주요 특징이라고 정리할 수 있겠다.

2. 개인영상정보 관련 해외규제동향

가. 미국

미 고속도로교통안전청(The National highway Traffic Safety Administration)에서는 2006년에 차량의 주행 속도, 안전벨트 및 에어백 상태 등 안전한 운행을 위한 정보를 수집하는 블랙박스 의무 장착에 관한 규제안을 발표하고, 2012년에는 경차의 경우 2014년부터 바로 적용할 수 있도록 하는 법안을 제안하기도 하였다.[45] 뿐만 아니라 2014년에는 미국 상원에서 블랙박스를 통해 수집된 개인영상정보가 회수되는 경우에 대하여 제한할 수 있는 운전자 프라이버시법(The S1925-Driver Privacy Act)가 제안되기도 했다. 또한 2017년에는 캘리포니아 주 차량국(DMV)에서 일반도로(public road)에서 무인 자율주행차량의 시험주행을 허용하는 법안을 제안하여(2017.3.10) 관련 규정에 대한 정비[46]를 마치고 현재 시행 중(2017.10.11.)이다.

---

45) 개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 158면

46) 차량을 통해 촬영되는 영상에서 개인에 대한 사생활 침해 등이 발생할 수 있기 때문에 제조사사가 차량 소유자 등에게 문서로써 동의를 받아 승인을 얻은 경우가 아니면 안전운행을 위한 정보를 제외한 개인정보는 모두 익명화 하도록 의무화 하는 규정을 포함하고 있다.(김경환, 캘리포니아주 공중운행 법안 제228.24조) Information Privacy, 방송통신위원회 자율주행차 제도개선 연구반 제2차 회의 발표자료)

한편, 미 연방항공청(Federal Aviation Administration, FAA)은 드론 시장 활성화를 위한 소형무인기 규정안 제안 공고(Small UAS Notice of Proposed Rulemaking)를 발표(2015.2월)하여 무게・운영시간・비행고도・속도 등의 제한 및 조종사의 자격, 항공기 규격 및 모델 등 일정 사항을 충족하는 경우에 별도 허가 없이 누구나 자유롭게 드론을 활용할 수 있도록 하였고, 이후 무인항공기의 통합관리, 면허관련 비행 테스트 도입, 비행구역 확대 등의 내용으로 법안이 추가 발의되기도 했다.[47]

미 법무부(Department of Justice)는 신체 부착 카메라 프로그램 추천과 교훈이라는 보고서(2014년 발간)에서 경찰의 법집행에 필요한 촬영 시 공정성 담보 원칙을 제안하였는데, 착용형 카메라의 허용 근거와 기준, 사용 조건 등을 명확히 하는 등 경찰의 웨어러블 기기 사용에 대한 기록을 의무화 하여 증거자료로 활용하는 방안을 추진 중이다.([48]

나. 유럽연합(EU)

유럽은 교통사고 발생 시, 신속한 구조가 가능하도록 2018년부터 모든 승용차와 소형 VAN에 사고 발생 시 운전자 운행 정보・습관, 사고 일시・장소・규모, 에어백 상태 등의 정보가 인근 응급센터와 보험회사 등에 전송되는 블랙박스를 장착해야 한다.(의회 통과, 2015.4월)[49]

---

47) Commercial UAS Modernization Act 법안은 뉴저지 민주당 의원 코리 부커와 노스타코타 공화당 의원 존 호벤에 의하여 발의되었으며, 2015년 2월의 드론 허용기준을 보완하였다.(개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 163면)

48) 개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 167에서 재인용

49) EU 집행위원회는 개인영상정보에 대한 사생활 침해 문제를 방지하기 위하여 블랙박스 의무화에 대한 개인영상정보 보호 원칙을 발표하였는데, 다른 정보와의 결합으로 개인을 알아볼 수 있는 경우가 아니라면 블랙박스로 촬영된 영상정보는 개인영상정보라고 할 수 없고, 해당 영상의 소유자는 원칙적으로 차주이며, 해당 영

한편, 민간영역의 드론산업 육성을 위하여 유럽연합은 비전 2020 프로젝트를 2014년 9월부터 추진해 오고 있는 중이며, 유럽항공안전기구는 드론규제 가이드라인을 발표(2015.3월)하여 소형 무인기에서부터 대형 항공기까지 포괄할 수 있게 했으면서 동시에 사고발생과 같은 위험상황이나, 촬영・농업・택배 등을 구분하여 서로 다른 규제가 적용되도록 하였다.[50]

다. 기타 국가

영국 정보보호위원회(ICO)는 2014년 감시카메라와 개인정보 사용 관련 정보보호 규정을 제정하여 드론에 의한 영상정보 처리 시 개인정보보호에 관한 원칙을 준수하게 했으며, CCTV code of practice를 발표하여 사전에 사용의 적절성・타당성・정당성을 철저하게 검토하고 사생활 침해를 최소화 할 수 있도록 했다[51]. 프랑스는 25Kg 미만 상업용 드론에 대한 규제를 대폭 완화하여 시장 활성화에 기여하고 있으며, 독일의 경우에는 개인 사유지 비행 금지와 여가목적으로 드론 운행 중에 타인을 촬영할 수는 있어도 타인의 영상정보를 공개하는 것은 제한하는 규제정책을 유지하고 있다. 오스트리아는 2014년에 드론법을 제정하여 장난감과 모형비행기에 대해서는 규제를 적용하지 않도록 하고 있다.[52]

상에 대한 접근은 원칙적으로 OBD에 접근할 수 있는 자이며, 해당 영상정보 활용 시 개인을 알아볼 수 있는 정보인 경우에는 EU 개인정보지침을 준수하도록 하는 내용이다.(차량용 블랙박스의 비용과 혜택에 관한 최종보고서에 대하여 개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 159면에서 재인용)

50) 강정수, 미국과 유럽 드론 산업정책과 규제정책에서 서로 다른 길을 걷다, 파워리뷰, 한국인터넷진흥원 2015년 5월 25면; 개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 164면에서 재인용

51) 개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 168~169면

3. 정보통신서비스와 개인영상정보의 보호

이상에서 영상정보처리기기가 국내외에서 법・제도적 지원을 받으면서 종래의 CCTV, 차량용 블랙박스 등에서부터 자율주행차, 헬스케어, 드론, 웨어러블 기기, 개인비서 등 ICT 융합 산업의 다양한 영역에서 활용되고 있음을 확인하였다. 최근에는 인공지능 기술이 접목되면서 지능화된 맞춤형 서비스가 가능해지는 수준이 이르렀다. 가령 국내의 사례를 예로 들자면, 최근 사회적으로 큰 파장을 일으켰던 학교폭력사건에 대하여 지능형 폐쇄회로텔레비전(CCTV)가 대안으로 활용되고 있다.[53] 인공지능(AI)이 촬영된 영상에 나타난 폭행 등의 특정 행동을 파악하면 경찰에 신고가 되기 때문이다. 한편 드론(Drone)은 방범 등 치안목적 또는 정찰・군사목적 등 공공분야의 특수 영역에서 이용되어 왔던 것이 최근에는 키덜트 제품에서부터 물류・배송, 중계방송・촬영 등 민간영역에서 드론(Drone)산업[54]이 활성화 되고 있다.

그러나 영상정보처리기기의 지능화와 보편화가 이루어지면서 개인영상정보 주체들은 더 은밀한 영역까지 정밀하게 촬영될 수 있다는 점에서 그 침해의 정

52) 강정수, 미국과 유럽 드론 산업정책과 규제정책에서 서로 다른 길을 걷다, 파워리뷰, 한국인터넷진흥원 2015년 5월 25~26면; 개인정보보호위원회, 영상정보처리기기 확대에 따른 개인정보보호 대책, (사)개인정보보호협회 위탁연구, 2015.10., 166에서 재인용

53) 중앙Sunday, 인공지능으로 동영상 분석해 학교폭력·자살 등 예방, 201710.15자 언론보도

54) 드론은 무선전파로 조종할 수 있는 무인 항공기다. 카메라, 센서, 통신시스템 등이 탑재돼 있으며 25g부터 1200kg까지 무게와 크기도 다양하다. 드론은 군사용도로 처음 생겨났지만 최근엔 고공 촬영과 배달 등으로 확대됐다. 이뿐 아니다. 값싼 키덜트 제품으로 재탄생돼 개인도 부담 없이 드론을 구매하는 시대를 맞이했다. 농약을 살포하거나, 공기질을 측정하는 등 다방면에 활용되고 있다. (네이버 지식백과, (용어로 보는 IT) 드론 - 군사용에서 키덜트 제품까지)

보가 더욱 강화되어 가는 추세다. 그럼에도 불구하고 점차 소형화 되어가는 영상정보처리기기로 인하여 정보주체들은 그 사실조차 알지 못하고 있다. 다음 절에서는 정보통신 서비스 환경에서의 개인영상정보의 안전성을 확보하기 위하여 방안으로서 개인영상정보 보호법 제정안을 검토하고, 정보통신서비스 제공자에 대한 규율방안을 모색해보고자 한다.

제3절 개인영상정보제도 입법현안

1. 개인영상정보 보호법안의 주요내용

가. 개인영상정보 보호의 범위 명확화

업무를 목적으로 개인영상정보를 처리하는 공공기관, 민간사업자, 비영리단체 등을 수범자로 하고 영상정보처리기기를 영상정보처리기기 중 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 등을 촬영하는 기기를 고정형 영상촬영기기로, 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 등을 촬영하는 기기를 이동형 영상촬영기기로 각각 분류하고, 기능에 따라 영상촬영기기와 기타 영상처리기기로 구분하는 등 대상을 명확화 했다. 개인영상정보처리자는 영상정보주체의 동의를 받거나 영상정보주체와의 계약 체결 및 이행을 위하여 불가피한 경우 등에 해당하면 이동형 영상촬영기기로 개인영상정보를 촬영할 수 있다.[55] 뿐만 아니라 고정형 영상정보처리기기에 대한 안내판 설치 의무와 같이 이동형 영상정보처리기기에도 불빛, 소리 등의 방법에 따라 촬영 사실을 표시토록 함으로써 영상정보주체의 자기정보결정권을 보장하도록 명문화 하였다.

나. 개인영상정보의 이용·제공 등 처리절차

55) 도로, 공원 등 불특정한 다수의 사람들이 출입하거나 이용하는 장소 또는 회의, 공연, 행사 등 사생활을 침해할 가능성이 적은 장소에서 촬영하는 경우로서 촬영 사실을 표시하였음에도 불구하고 촬영 거부 의사를 밝히지 않거나 영상정보주체가 촬영 사실을 알 수 있었음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우에도 개인영상정보를 촬영할 수 있다. 다만, 이 경우에도 영상정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정한다.

개인영상정보처리자는 영상정보처리기기의 설치 목적 범위에서 개인영상정보를 이용할 수 있고, 그 설치 목적 범위에서 불가피한 경우로서 영상정보주체 등의 이익을 부당하게 침해할 우려가 없는 경우에만 개인영상정보를 제3자에게 제공할 수 있다. 개인영상정보를 제3자에게 제공하는 경우 이용 목적 및 이용 방법의 제한, 폐기 기한의 설정 등 개인영상정보의 안전성 확보를 위하여 필요한 조치를 취하여야 한다.

다. 개인영상정보 등의 안전한 관리를 위한 조치

개인영상정보처리자는 개인영상정보가 분실, 도난, 유출 등이 되지 아니하도록 영상정보처리기기 및 개인영상정보의 안전성 확보에 필요한 기술적·관리적·물리적 조치하여야 한다. 영상정보처리기기를 설치·운영하는 공공기관과 그 밖에 대통령령으로 정하는 개인영상정보처리자는 매년 개인영상정보의 처리 현황에 대한 자체 점검을 실시하고, 그 점검 결과를 행정안전부장관에게 제출하여야 한다. 지방자치단체가 영상정보처리기기 통합관제시설을 운영하려는 경우 영상정보주체의 권리 침해 가능성 등을 고려하여 개인정보 영향평가를 하도록 하고, 그 결과를 행정안전부장관에게 제출하도록 하였다.

라. 영상정보주체 등의 권리 보장

개인영상정보의 열람, 출처 확인, 사본의 교부, 보관, 촬영 및 이용·제공의 중단 또는 삭제를 요구할 수 있는 권리를 부여하고, 그 권리행사 방법 등을 규정하는 등 영상정보주체의 정보자기결정권 행사에 대한 실현을 보장하였다. 개인영상정보처리자는 열람 및 사본의 발급을 하는 경우 열람 등을 요구한 자 외의 자를 알아볼 수 없도록 하는 기술적 조치를 하고, 개인영상정보를 삭제할 때에는 복구되거나 재생되지 아니하도록 하여야 한다.

마. 기타

개인영상정보가 침해되는 경우 등의 사고가 발생하면 행정안전부에 그 침해 사실을 신고하거나 권리 구제의 상담 등을 요청할 수 있도록 하고, 행정안전부는 관련 업무를 수행하기 위한 전문기관을 지정하여 운영할 수 있게 하였다. 또한 개인영상정보처리자가 동 법률안을 위반하는 행위를 하거나 개인영상정보가 침해되었다고 판단할 상당한 근거가 있는 경우에는 해당 개인영상정보처리자에게 침해 행위의 중지 등 시정명령·개선권고를 할 수 있도록 하였다.

2. 개인영상정보 보호법안의 한계

가. 정보통신서비스 제공자의 개인영상정보의 처리

일반 개인이 수집하는 개인영상정보는 대면 또는 그 밖의 통신수단을 통해서 제3자에게 제공될 우려가 없는 것은 아니지만, 그 확산성은 높지 않다고 할 수 있다.[56] 이에 반하여 정보통신서비스 제공자가 개인영상정보를 직접 처리하거나 매개하는 경우에는 그 개인영상정보는 널리 전파될 위험이 매우 높고 영리목적으로 사용될 가능성 또한 높다.

개인영상정보의 확산가능성과 침해회복의 어려움, 개인영상정보의 유통을 통한 직간접적인 영리취득 등을 고려할 때, 일반인의 개인영상정보 수집·이용과 달리 정보통신서비스 제공자의 개인영상정보 처리에 관한 특칙을 마련하여, 개인영상정보의 수집·이용의 요건과 절차, 적절한 관리를 위한 기준 등을 제시함으로써 이용자의 신뢰를 확보할 필요가 있다. 또한, 영리를 목적으로 하는 기업인 정보통신서비스 제공자의 부적절한 개인영상정보 처리로 인한 피해의 사전적 예방과 신속한 차단 그리고 실효적 구제를 위한 제도적 장치를 마련할 필요가 있다.

---

56) 일반인이 수집하는 개인영상정보가 넓은 전파성을 보이는 경우는 대부분 정보통신서비스를 통한 경우로 제한될 것으로 예상된다.

나. 정보통신서비스 제공자의 개인영상정보 처리의 특성

정보통신서비스 제공자가 처리하는 개인영상정보는 3가지 유형으로 구분할 수 있다. 첫째, 정보통신서비스 제공자가 직접 개인영상정보를 수집·이용하는 직접처리 유형이다. 예컨대 구글의 스트리트뷰 또는 카카오의 로드뷰 등을 통하여 수집된 개인영상정보가 이에 해당할 수 있다. 둘째, 정보통신서비스 이용자가 개인영상정보를 수집하여 정보통신서비스 제공자를 통해 제공되는 매개유형이다. 예컨대 보배드림의 블랙박스영상 또는 유튜브의 개인영상 등이 이에 해당할 수 있디. 셋째, 정보통신서비스 제공자의 플랫폼을 이용하여 생성되는 개인영상정보이다. 예컨대 아프리카TV 등의 인터넷개인방송의 콘텐츠 등이 이에 해당할 수 있다. 그런데, 정보통신서비스 제공자의 개인영상정보의 처리는 그 유형에 따라 동일한 규제방식을 적용하기 어려운 측면이 있다.

일례로 「개인영상정보 보호법(안)」 제19조와 제20조는 영상정보주체등[57]이 개인영상정보처리자에게 개인영상정보에 대한 열람, 출처 확인, 사본의 발급, 보관, 처리의 전부·일부 정지 또는 삭제를 요구할 권리를 규정하고, 이러한 요구에 따른 개인영상정보처리자의 조치의무를 규정하고 있지만, 개인영상정보를 직접 촬영하거나 수집하지 아니하고, 오직 정보통신서비스 이용자가 촬영하거나 수집한 개인영상정보를 매개만 하는 정보통신서비스제공자에게 이를 적용하는 것은 불가능하다. 즉, 정보통신서비스제공자는 열람등을 요청하는 영상정보처리주체와 개인영상정보를 수집·게재한 이용자와의 이해관계의 고려 없이 무조건 열람등의 요구에 응할 수 없다. 또한 정보통신서비스제공자는 개인영상정보주체와 정당한 이해관계에 있는 자가 누구인지 알 수 없으며 이를 판단하는 것 자체가 과도한 부담이 될 수밖에 없기 때문에 해당 규정을 직접 적용하는 것은 불합리하며, 정보통신서비스제공자의 매개자로서의 특수성을 반영한 별도의 특칙을 마련할 필요가 있다.

57) 영상정보주체 및 개인영상정보에 대한 정당한 이해관계가 있는 자를 말한다.

또한, 정보통신서비스 제공자의 개인영상정보처리가 매개유형에 해당하는 경우에는 「개인영상정보 보호법(안)」 제16조에 따른 개인영상정보의 처리 이력 관리도 이행이 어렵다. 동조는 개인영상정보처리자에게 개인영상정보의 안전한 관리 및 영상정보주체의 권리 보호를 위하여 촬영, 이용, 제공, 공개, 열람, 삭제, 폐기 등 개인영상정보의 처리 이력을 관리하도록 규정하고 있으나, 개인영상정보를 직접 촬영하지 않은 정보통신서비스 제공자는 촬영이력 자체를 알 수 없다.

다. 정보통신서비스 제공자에 대한 특칙의 필요성

정보통신서비스 제공자가 개인영상정보를 직접 촬영하는 경우에는 「개인영상정보 보호법(안)」에 따른 일반적인 규율이 가능할 수 있지만, 유튜브, 네이버 블로그 등 정보를 직접 수집하지 아니하고 정보의 매개서비스만을 제공하는 정보통신서비스제공자는 개인영상정보를 직접적으로 수집·이용하지는 않기 때문에 직접 개인영상정보를 촬영하는 등 개인영상정보의 처리에 관한 실질적 통제력 가지는 개인영상정보처리자를 규율대상으로 상정하고 있는 「개인영상정보 보호법(안)」의 규정들은 그 적용이 적합하지 않다. 이러한 점을 고려하여 「개인영상정보 보호법(안)」은 매개유형의 정보통신서비스 제공자에 대해서는 일부 규정의 적용을 제외하는 조문을 마련하고 있다. 동 법안 제23조 제5항은 "「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 따른 정보통신서비스 제공자가 같은 항 제4호에 따른 이용자 또는 다른 정보통신서비스 제공자의 개인영상정보를 매개(媒介)하는 경우에는 제3장부터 제5장까지를 적용하지 아니한다."고 함으로써 개인영상정보를 매개하는 정보통신서비스 제공자에 대해서는 "개인영상정보의 이용 및 제공 등"에 관한 제11조부터 제13조까지와 "영상정보처리기기 및 개인영상정보의 안전한 관리"에 관한 제14조부터 제18조까지, "영상정보주체 등의 권리 보장"에 관한 제19조부터 제22조까지는 적용되지 않도록 규정하고 있다.

그런데. 「개인영상정보 보호법(안)」은 정보통신서비스 제공자의 매개유형의

개인영상정보 처리에 대한 적용제외를 규정하고 있을 뿐, 이에 관한 적절한 규율방안을 제시하고 있지는 않다. 따라서 정보통신서비스 제공자의 개인정보 처리에 관하여 규율하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 정보통신서비스 제공자가 개인영상정보를 매개하는 경우에 정보통신서비스 제공자의 역할과 정보통신서비스를 이용하여 개인영상정보를 처리하는 정보통신서비스 이용자의 책무 그리고 정보통신서비스를 통하여 매개되는 개인영상정보의 주체의 보호방안 등에 관한 제도적 장치를 마련하여 보완할 필요가 있다.

3. 정보통신망법 개정방안[58)]

가. 이용자 개인영상정보 처리지침 마련 및 준수(안 제27조의4)

이용자에 의해 수집된 개인영상정보를 플랫폼을 통해 공개 또는 유포하는 사업자는 이용자에 의해 처리되는 모든 개인영상정보를 개별적으로 모니터링 할 수는 없으나 해당 정보의 매개를 통하여 수익을 창출하는 사업자이므로 개인영상정보를 처리하는 이용자가 영상정보주체의 권익을 침해하지 않도록 일정한 지침을 제공하고 준수하도록 할 필요가 있다.

즉, 정보통신서비스 제공자는 정보통신서비스를 이용하여 개인영상정보를

58) 본 연구는 그 수행과정에서 개인영상정보를 비롯한 개인정보에 대한 정보통신서비스 제공자의 처리 및 매개에 관하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 통해 통일적으로 규율하는 방안을 모색함으로써 "정보통신서비스 제공자의 개인영상정보 수집근거 마련"(안 제22조의3)과 "이용자(개인영상정보주체) 보호"(안 제32조, 제32조의2, 제32조의4부터 제32조의6까지) 등의 개정안을 검토한 바 있다. 그러나 재입법예고된 「개인영상정보보호법(안)」이 정보통신서비스제공자가 개인영상정보를 매개하는 경우만 제외하고, 직접 촬영하는 경우 등 매개에 해당하지 않는 경우는 「개인영상정보보호법(안)」의 적용을 받도록 하고 있기 때문에 기술에서 제외하기로 한다.

처리하는 이용자로 하여금 준수해야 하는 일정한 지침을 마련하여 사전에 개인영상정보 침해 위험에 대비하도록 할 필요가 있다. 이를 위해서 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망을 이용하여 개인영상정보를 처리하는 이용자가 준수하여야 하는 사항을 담은 이용자개인영상정보처리지침을 정하고 이를 공개하도록 하고, 이용자개인영상정보처리지침에 수록될 내용은 영상정보주체의 권리보장에 대한 것으로 그 구체적 내용은 대통령령에서 규정하도록 한다. 이용자 영상정보처리지침에 담길 내용으로는 개인영상정보주체의 권리보장방법과 개인영상정보주체에 대한 이용자의 의무, 정보통신서비스제공자에 대한 이용자 준수사항, 개인영상정보의 삭제요청 등에 대한 적절할 처리절차 등과 그밖에 영상정보주체의 권리를 보장하기 위해 필요한 사항이 될 것으로 예상된다. 다만, 이용자의 가독성과 사업자의 지침마련의 불편성 등을 고려하여, 정보통신서비스제공자가 정보통신망법 제27조의2에 따른 개인정보 처리방침을 수립하는 경우에는 별도로 영상정보처리지침을 만들기보다는 개인정보 처리방침에 포함하여 정할 수 있도록 허용할 필요가 있다.

그리고 이용자가 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하여 개인영상정보를 처리하는 경우에는 제1항에 따른 이용자 영상정보처리지침을 준수하도록 한다.

한편, 정보통신서비스 제공자에 대하여 “이용자 영상정보처리지침”을 마련할 의무를 직접 부여하는 방안 이외에 “이용자 영상정보처리지침”을 마련해 둔 자에 한하여 책임을 감경할 수 있도록 하는 방안도 고려할 수 있을 것이다. 이에 따라서 개인영상정보처리지침은 정보통신서비스 제공자로 하여금 이를 수립하도록 하는 방안(수립의무)과 수립 및 공개하도록 하는 방안(수립·공개의무), 수립 또는 수립·공개를 선택적으로 이행하도록 하는 방안(임의규정), 수립하고 이를 이용자에게 권고하도록 의무화하는 방안(수립·권고의무) 등 대안적 구성이 가능할 수 있다.

나. 개인영상정보의 삭제요청 등(안 제27조의5)

정보통신서비스의 전파성, 신속성 등에 비추어 볼 때 영상정보주체의 원치 않는 개인영상정보의 유출에 대한 신속한 권리구제 방안이 필요하다. 사진, 동영상 등의 개인영상정보에 대한 원치 않는 공개를 당한 경우에 반론과 토론을 통한 자정작용이 사실상 무의미한 경우가 적지 않을 것이다. 또한, 빠른 전파 가능성으로 사후적 손해배상이나 형사적 제재만으로는 피해자의 손상된 인격이나 사생활 등이 회복하기 어려운 사례를 배제할 수 없는데, 반박내용 게재 또는 링크・스크랩・검색노출 기능 차단 등의 조치만으로는 사실상 개인영상정보주체를 보호하기에는 미흡하므로 개인영상정보 공개의 잠정적 차단 등의 권리보호 장치가 요구된다.

개인영상정보의 원치 않는 처리로부터 개인영상정보주체를 보호하기 위한 입법적 방식은 세 가지를 고려할 수 있다. 첫째, 정보통신망법 제44조의2[59]의

59) 제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등”이라 한다)를 요청할 수 있다.
② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제・임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.
③ 정보통신서비스 제공자는 자신이 운영・관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.
④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 “임시조치”라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다.
⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용・절차 등을 미리 약관에 구체적으로 밝혀야 한다.
⑥ 정보통신서비스 제공자는 자신이 운영・관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면

삭제·임시조치 등의 대상을 확대하는 방안이다. 제44조의2 개정을 통하여 영상정보의 공개로 인하여 사생활 침해나 명예훼손 등 자신의 권리가 침해된 자가 그 사실을 소명하여 정보통신서비스 제공자에게 해당 개인영상정보의 처리를 중단하거나 삭제, 영상정보주체를 알아볼 수 없도록 하는 기술적 조치(비식별화)를 할 것을 요구할 수 있도록 한다. 즉, 제44조의2 제1항을 “정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제, 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기술적 조치 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다.”로 한다. 이 경우 삭제 또는 처리정지 등의 요구를 받은 정보통신서비스 제공자는 경우에는 즉시 그 개인영상정보 처리의 중단 등 필요한 조치를 하고 요청자에게 그 사실을 통보하게 되고, 그 개인영상정보를 공개 또는 유통한 이용자에게도 이를 통보하여야 한다. 이에 따라 일정한 조치를 취한 정보통신서비스 제공자에 대하여 배상책임을 줄이거나 면제받을 수 있다. 둘째, 개인영상정보가 본인의 의사에 반하여 공개되었다면, 개인영상정보주체에게 있어서는 공개된 사실 자체가 침해에 해당되므로 굳이 침해에 대한 별도의 소명절차를 요구할 필요가 없다는 점을 고려하여 별도의 간이한 요건의 절차를 마련하는 방안이다. 일차적으로 당사자(개인영상정보 게재자와 개인영상정보주체) 간 개인영상정보의 게재 여부에 대하여 합의할 기회를 주되, 합의가 원만히 되지 않을 경우 임시조치 등의 수단을 발동하도록 한다. 구체적으로는 우선 “정보통신서비스 제공자가 제공하는 정보통신서비스를 통하여 개인영상정보가 공개됨에 따라 자신의 개인정보에 관한 권리가 침해됨을 주장하는 자(이하 ”권리주장자”라 한다)는 그 사실을 소명하여 정보통신서비스 제공자에게 그 개인영상정보의 삭제 또는 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기술적 조치(이하 “삭제등”이라 한다)를 요청할 수 있다“는 점을 명시한다. 그리고 요청을 받은 정보통신서비스 제공자는 그 요청사실을

제받을 수 있다.

해당 개인영상정보를 공개한 이용자에게 지체 없이 알리고 합의하도록 권고하도록 한다. 정보통신서비스 제공자는 해당 개인영상정보를 게재한 자에게 요청사실을 통지할 수 없거나 당사자 간 합의가 이루어지지 않는 경우에는 해당 개인영상정보에 대한 접근을 임시적으로 차단하는 조치를 할 수 있도록 하고, 임시조치의 사실 및 기간[60]을 당사자들에게 지체 없이 통지하도록 한다. 다만, 해당 개인영상정보를 게재한 자에게 통지할 수 없는 경우 해당 게시판에 공시하는 등의 방법으로 알리도록 한다. 정보통신서비스제공자는 임시조치 기간 만료 후 해당 개인영상정보를 삭제하도록 하고, 임시조치 기간 내에 정보게재자와 권리주장자 간 해당 개인영상정보처리에 대한 합의가 이루어진 경우에는 그 합의내용에 따른다. 정보통신서비스 제공자가 자신이 제공하는 정보통신서비스를 이용하여 처리되는 개인영상정보에 대하여 일련의 조치와 삭제를 한 경우에는 이로 인한 배상의 책임을 지지 않도록 한다. 셋째, 제44조의2와 유사한 개인영상정보에 관한 임시조치 등에 관한 제도를 도입하되, 법령 조문의 간소화라는 입법 경제적 측면을 고려하여 세부절차 등은 제44조의2를 준용하는 방안이다. "정보통신서비스 제공자가 제공하는 정보통신서비스를 통하여 개인영상정보가 공개됨에 따라 자신의 권리가 침해됨을 주장하는 자(이하 "권리주장자"라 한다)는 그 사실을 소명하여 정보통신서비스 제공자에게 그 개인영상정보의 삭제, 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기술적 조치(이하 "삭제등"이라 한다)를 요청할 수 있다."는 조문을 신설하고, 그 요청에 관하여는 제44조의2를 준용하는 규정을 둔다.

다. 가정용 CCTV(Home Security Camera)

최근 영상정보처리기기의 한 유형으로 이른바 홈캠 내지 가정용 CCTV의 활용이 늘고 있다. 이들 홈캠은 소비자가 정보통신서비스 제공자가 제공하는 서비스를 이용하는 경우와 개인이 필요설비를 구매·설치하여 정보통신망을 통해

60) 임시조치의 기간은 30일 이내로 한다.

서 처리하는 경우 등이 있다. 이러한 홈캠과 관련하여 최근 침해사고가 증가하면서[61] 개인영상정보의 보호에 관한 관심이 증가하고 있기 때문에 법률적 대응방안을 검토해 볼 필요가 있다. 이에 홈캠에 의해서 촬영되는 개인영상정보의 주체와 개인영상정보를 처리하는 자를 기준으로 세분하여 제도적 처리방안을 검토할 필요가 있다.

먼저 홈캠은 비록 가정용 실내 CCTV(폐쇄회로 텔레비전)으로 불리기도 하지만, 그 법적 개념은 대부분은 디지털 방식으로 네크워크에 연결된 IP 카메라이다. 즉, "일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치"[62]로서 「개인영상정보 보호법」에 예상하고 있는 고정형 영상정보처리기기에 해당한다.

다음으로 홈캠을 통해서 촬영되는 개인영상정보의 주체는 해당 홈캠이 설치된 주거공간의 거주자와 방문자로 구분할 수 있고, 거주자는 다시 해당 홈캠을 구매·설치하여 운용하거나 홈캠서비스의 이용계약자와 그 동거인(가족 등)으로 나눌 수 있다. 전자는 개인영상정보의 주체이기는 하지만 직접 개인영상정보를 촬영하거나 홈캐서비스를 신청한 본인이므로 개인영상정보의 처리에 따른 권리침해 또는 충돌의 문제는 발생하지 않는다. 하지만, 동거인(가족 등) 또는 방문자의 경우는 달리 볼 필요가 있다.

첫째, 정보통신서비스 제공자가 개인영상정보를 처리하는 경우에는 「개인영상정보 보호법」이 적용된다. 즉, 이용자와의 계약에 따라 정보통신서비스 제공자가 홈캠을 운용함으로써 스스로 개인영상정보를 촬영하는 것으로 볼 수 있는 경우라면, 이는 「개인영상정보 보호법(안)」의 적용대상으로 볼 수 있다. 이

61) 아시아경제, "가정용 캠 해킹사고 끊이질 않아…3년간 신고만 700건", 2017. 9. 22(http://www.asiae.co.kr/news/view.htm?idxno=2017092210015761460, 2017년 12월 17일 최종 접속); KBS 뉴스, ""집 안을 훤히" 가정용 CCTV 해킹 비상", 2017. 5. 1(http://news.kbs.co.kr/news/view.do?ncd=3473553&ref=A, 2017년 12월 17일 최종 접속)

62) 「개인정보보호법 시행령」 제3조 제1호 나목 참조.

용자가 가정 내에 위치한 홈캠 장비의 위치를 변경하는 등 일부 조작행위에 기여하더라도 이는 정보통신서비스 제공자의 영상정보 처리행위에 종된 행위로 볼 것이다. 그런데 정보통신서비스 제공자가 공개된 장소(여러 사람이 모이거나 다니는 장소)[63]가 아닌 곳에 홈캠을 설치하여 개인영상정보를 촬영하려면 원칙적으로 영상정보주체의 동의를 받아야 한다(안 제5조 제3항). 그런데 주거지 내에 범죄 예상을 위해서 설치하여 운용되는 홈캠으로 촬영되는 개인영상정보는 주거지 내에 설치를 신청 또는 동의한 자와 그 동거인은 물론 일시방문자의 것도 포함할 수 있는데, 일시방문자에게 개인영상정보 촬영에 대한 사전 동의를 받는다는 것은 사실상 불가능하다고 할 것이다.

둘째, 개인이 본인의 주거공간에서 스스로 개인영상정보를 촬영하는 경우라면 「개인영상정보 보호법(안)」의 개인영상정보저리자로 볼 수 없다. 「개인영상정보 보호법(안)」은 "(누구든지) 여러 사람이 모이거나 다니는 장소 외의 장소"에 고정형 영상촬영기기를 설치하여 개인영상정보를 촬영할 수 없도록 규정하고 있으나, 개인이 사유지에 사적 목적으로 고정형 영상촬영기기를 설치하여 개인영상정보를 촬영하는 경우는 제외하고 있다(안 제5조 제3항). 즉, 개인은 주거지 내에 홈캠을 설치하여 개인영상정보를 촬영할 수 있고, 해당 개인은 홈캠을 설치·운용함으로써 개인영상정보를 촬영하더라도 이는 업무목적에 해당하는 것으로 볼 수 없으므로 개인영상정보처리자에는 해당하지 않는다. 또한, 해당 개인과의 계약에 따라 정보통신회선 또는 저장공간 제공 등의 서비스를 제공하는 정보통신서비스 제공자가 스스로 개인영상정보를 촬영하는 자에 해당하지 않으므로, 「개인영상정보 보호법(안)」의 적용대상으로 볼 수 없다. 그러나 홈캠 서비스를 제공하는 정보통신서비스 제공자가 개인정보를 처리하는 행위는 정보통신망법의 적용대상이므로 홈캠서비스를 제공하는 정보통신서비스 제공자의 영상정보보호를 위한 관리조치방안 또는 이용자에 대한 가이드 등

63) ① 다중이용시설, 대중교통시설, 공공장소, 도로 등 불특정한 다수의 사람들이 출입하거나 이용하는 장소와 ② 집합건물의 복도 또는 계단, 주차장, 그 밖에 이에 준하는 장소로서 특정집단의 구성원이나 이와 관련된 방문객이 출입하거나 통행할 수 있는 장소를 말한다(「개인영상정보 보호법(안)」 제5조 제2항).

세부적 규율방안을 지침 등 하위법규를 통하여 고려할 필요는 있을 것으로 보인다.

한편, 개인이 자신의 주거지에 홈캠을 설치하거나 정보통신서비스 제공자의 서비스를 이용하여 개인영상정보를 촬영하는 경우에 동거인 또는 일시방문자의 보호와 관련해서는「개인영상정보 보호법」또는 「정보통신망법」에 따른 공법적 규율대상보다는 해당 개인과 동거인 및 방문자 간에 민사법적인 해결방안을 모색하여야 할 대상으로 볼 것이다.

제4절 소결

우선, 정보통신서비스 제공자의 개인영상정보 처리와 이에 대한 법률적 취급은 정보통신서비스 제공자가 개인영상정보 처리에 개입하는 방식에 따라서 차별적으로 접근할 필요가 있다. 정보통신서비스 제공자가 직접 개인영상정보를 촬영하는 경우에는 영상정보처리기기의 설치·운영 등에 관한 사항을 규율하는 「개인영상정보 보호법(안)」의 적용대상으로 하는 것이 가능할 것이다. 그러나 정보통신서비스 이용자가 개인영상정보를 촬영하여 정보통신서비스 제공자의 서비스를 통해 유통하는 매개유형의 경우에는 정보통신서비스 제공자가 영상정보처리기기의 설치·운영하는 것이 아니므로 「개인영상정보 보호법(안)」의 적용대상으로 적절하다고 보기 어렵다.

그런데 정보통신서비스 제공자가 직접 영상정보처리기기의 설치·운영하여 개인영상정보를 촬영하지 않더라도, 정보통신서비스를 통해서 개인영상정보가 유통되는 경우에 그 개인영상정보는 널리 전파될 위험이 매우 높을 뿐만 아니라 침해가 발생하는 경우에 회복이 어려울 수 있다. 따라서 정보통신서비스 제공자의 개인정보보호에 관한 정보통신망법의 보완을 통해 이를 예방하고 피해의 확대를 차단하도록 할 필요가 있다. 이용자가 촬영한 개인영상정보가 정보통신서비스 제공자의 서비스를 통해 매개되는 경우 그 개인영상정보를 개별적으로 모니터링할 수는 없으나, 해당 정보의 매개를 통하여 수익을 창출하는 정보통신서비스 제공자는 개인영상정보를 처리하는 이용자로 하여금 준수해야 하는 일정한 지침을 마련하여 사전에 개인영상정보 침해 위험에 대비하도록 하고, 정보통신서비스의 전파성, 신속성 등에 비추어 볼 때 영상정보주체의 원치 않는 개인영상정보의 유출에 대한 신속한 권리구제 방안을 마련하도록 한다.

제5장 결 론

이 연구는 민감정보와 관련된 「정보통신방법」 의 개정방안을 마련하는 것을 주된 연구의 범위로 한다. 그러나 최근 개인정보의 특수한 유형으로서 '생체정보', '개인영상정보' 등에 대한 특별한 규율필요성에 대하여 검토할 필요가 있음이 제기되고 있다. 특히 '개인영상정보'에 대하여는 이미 특별법 형태로 추진하고자 하는 정부안이 진행 중이며, '생체정보' 역시 그 민감성, 불변성 등을 이유로 특별히 규율하자는 주장 등이 제기되고 있다. 따라서 민감정보 중에서도 특히 '생체정보'와 '개인영상정보'에 대한 부분을 별도로 검토하였다. 연구의 결과를 요약하면 다음과 같다.

첫째, 현재 「정보통신망법」은 민감정보 해당성의 융통성을 발휘하기 위하여 '예시적 방식'으로 규정하고 있다. 그러나 민감정보 해당성 여부가 개개인의 주관적 성향에 따라 달라진다면 법적 안정성이나 명확성 측면에서 바람직하지 않으므로, 한정적 열거방식이 타당하다. 「개인정보 보호법」도 이러한 점을 반영하여 대통령령 위임을 통해 한정적 열거방식을 채택하고 있으며, GDPR의 경우도 열거방식을 채택하고 있다. 불가피하게 융통성을 두고자 한다면 현행 「개인정보 보호법」과 같이 기준을 정하여 대통령령에 위임하는 방안도 검토될 수 있으나 기본취지는 한정적 열거방식을 취하는 것이 바람직하다. 또한 「정보통신망법」은 민감정보 수집의 정당화 근거를 "법률"로 제한하고 있으나, 「개인정보 보호법」은 대통령령을 포함한 "법령"으로 그 범위를 넓히고 있다. 「정보통신망법」에서 특별히 더 수집, 이용의 근거를 더 강화해야할 실익이 없는 한 이는 기본법 수준에 부합하는 것이 타당하다.

둘째, '개인을 고유하게 하는 목적의 생체정보(biometric data for the purpose of uniquely identifying a natural person)'를 '민감정보'에 포함시키는 것이 타당하다. 현행 「개인정보 보호법」 및 「정보통신망법」상 '생체정

보’는 ‘민감정보’에 해당되지 않으므로 일반 개인정보로 취급된다. 한편 단순히 서비스제공과정에서 처리되는 모든 생체정보를 민감정보를 규율한다면, 전혀 프라이버시침해적 요소나 권리와 자유침해의 리스크가 없음에도 불구하고 과도한 규율이 된다. GDPR 역시 민감정보로서 ‘생체정보’에 대하여는 ‘개인을 식별하기 위한 목적으로 사용되는 경우’로만 한정하는 것은 결국 ‘인증’ 이나 본인확인을 목적으로 생체정보를 활용하는 경우를 의미한다고 보여 진다. 따라서 본인을 인증 또는 확인하기 위한 수단으로 사용되지 않는 한 생체정보는 민감정보로 규율하지 않는 것이 바람직하다. 민감정보에 해당되는 생체정보를 ‘특정인을 인증 또는 확인하기 위해 기술적으로 처리된 생체정보’ 제한하여 규정하는 것이 바람직하다.

한편 관리, 보관, 파기 등에 있어서 생체정보에 대한 특칙은 불필요하다. 다만 GDPR과의 관계에서 대규모 민감정보의 처리에 대하여 개인정보 영향평가의 실시를 규정하고 있는바 국내법에의 도입에 대하여는 좀 더 고민이 필요하다. 그밖에 파기의 기술적 기준, 기술적·관리적 조치에 대한 특별한 사항은 고시나 지침을 통해 구체화하는 것이 바람직하다.

세째, 정보통신서비스 제공자의 개인영상정보 처리와 이에 대한 법률적 취급은 정보통신서비스 제공자가 개인영상정보 처리에 개입하는 방식에 따라서 차별적으로 접근할 필요가 있다. 정보통신서비스 제공자가 직접 개인영상정보를 촬영하는 경우에는 영상정보처리기기의 설치・운영 등에 관한 사항을 규율하는 「개인영상정보 보호법(안)」의 적용대상으로 하는 것이 가능할 것이다. 그러나 정보통신서비스 이용자가 개인영상정보를 촬영하여 정보통신서비스 제공자의 서비스를 통해 유통하는 매개유형의 경우에는 정보통신서비스 제공자가 영상정보처리기기의 설치・운영하는 것이 아니므로 「개인영상정보 보호법(안)」의 적용대상으로 적절하다고 보기 어렵다.

이용자가 촬영한 개인영상정보를 정보통신서비스 제공자가 매개하는 서비스만 제공할 경우 정보통신서비스 제공자는 일일이 개인영상정보를 개별적으로 모니터링 할 수 없다. 따라서 타인에 의해 해당 정보의 매개를 통하여 수익을 창출하는 정보통신서비스 제공자는 개인영상정보를 처리하는 이용자로 하여금

준수해야 하는 일정한 지침을 마련하여 사전에 개인영상정보 침해 위험에 대비하도록 하는 방안을 「정보통신망법」의 개정을 통해 도입할 필요가 있다. 또한 정보통신서비스의 전파성, 신속성 등에 비추어 볼 때 영상정보주체의 원치 않는 개인영상정보의 유출에 대한 신속한 권리구제 방안을 마련하는 것이 타당하다.

<부 록> 「정보통신망법」 개정(안)

1. 생체인식정보 개념의 신설 및 민감정보에 포함

현행	개정안
제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다. 6의2.<신설>	제2조(정의)① 이 법에서 사용하는 용어의 뜻은 다음과 같다. **6의2. "생체인식정보"란 얼굴, 지문 등 개인의 신체적, 생리적, 행동적 특성에 관한 정보로서 개인을 인증 또는 식별하기 위하여 기술적으로 처리되는 개인정보를 의미한다.**

□ 개정이유

o 핀테크, 근태관리, 온라인 거래 등 다양한 분야에서 생체정보의 활용이 증가함에 따라 생체정보의 보호 및 안전한 활용을 위한 법제도 근거 마련 필요

o 특히 생체정보는 항상 정보주체가 지니고 있으며, 그 속성이 쉽게 변하지 않는다는 특성으로 인해 보안성이 강한 식별자로 취급되고 있으나,

한번 유출되거나 침해되었을 경우 이러한 불변성, 지참성 등으로 인한 정보주체의 권리 및 자유의 침해 요인도 크므로 민감정보에 해당

o '생체정보'를 민감정보의 일 유형으로 규율하기 위한 입법방안 마련 필요

□ 주요내용

o 용어정의의 개정을 통해 '생체인식정보'의 개념을 신설하고, 이러한 생체정보를 '정보통신망법' 제23조의 민감정보에 추가

o 생체인식정보를 ‘얼굴, 지문 등 개인의 신체적, 생리적, 행동적 특성에 관한 정보로서 **개인을 인증 또는 식별하기 위하여** 특별히 기술적으로 처리되는 개인정보’로 정의

- 단순히 서비스제공과정에서 처리되는 모든 생체정보를 민감정보로 규율한다면, 전혀 프라이버시침해적 요소나 권리와 자유침해의 리스크가 없음에도 불구하고 과도한 규율에 해당

- 따라서 민감정보에 해당되는 생체정보는 생체정보중에서도 **특히 ‘개인을 인증 또는 식별하기 위하여 특별히 기술적 조치를 수반한 경우’로** 제한하여 ‘생체인식정보’로 규정

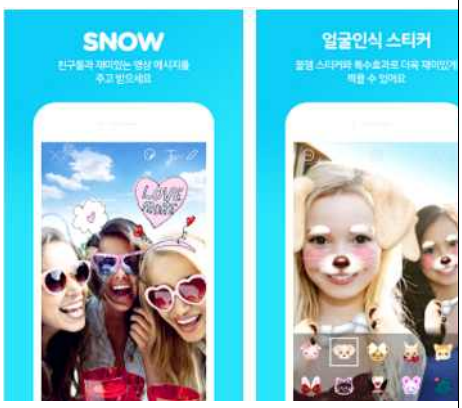
  * GDPR도 모든 생체정보가 아니라 ‘개인을 고유하게 식별하는 목적의 생체정보(biometric data for the purpose of uniquely identifying a natural person)’로 제한하고 있으며

  따라서 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술적 수단을 통해 처리되는 경우에 한해서만 생체정보에 해당되기 때문에, 시스템적으로 민감처리로 분류되지 않음(GDPR 전문 (51))

o 특정 개인을 인증하거나 확인할 목적 없이 단순히 서비스제공과정에서 처리되는 생체정보는 민감정보에서 제외

- 각종 디지털헬스케어 서비스를 통하여 실시간 이동되는 심박정보나 맥박정보 등은 민감정보로서 생체정보에서 제외되며, 페이스북 등 각종 SNS나 플랫폼 서비스를 통해 이용되는 개인영상정보도 제외

- 얼굴 사진, 영상 파일, 음성 파일 등 특정 개인의 생물학적·행동적 특징 자체를 의미하는 경우는 제외되나, 특정 정보주체를 인증 또는 확인하기 위한 목적으로 활용되는 경우 민감정보로서 생체인식정보에 포함

생체인식정보에서 제외되는 경우	생체인식정보에 해당되는 경우
- 네이버의 스노우는 사진·동영상 채팅 애플리케이션으로, 사용자가 스마트폰에 얼굴을 비추면 **자동인식**해 **스티커가 얼굴 위에 덧입혀지거나, 그림이 움직이는 등의 특수 효과**를 사용	- 삼성전자는 갤럭시 S5에서부터 **지문인식** 기술인 패스(Pass)를 도입하였으며, 갤럭시 S8에는 **안면인식**, **홍채인식** 기능을 탑재하여, 삼성월렛, 페이팔과 연동한 서비스를 출시
	

□ 쟁점사항

o 용어와 관련하여 '바이오정보', '바이오인식정보', '생체정보', '생체인식정보' 등의 용어가 제안

- 생체정보는 '생체실험'이 연상되는 등 부정적 어감이 존재하며, 바이오정보는 유전정보, 건강정보 또는 의료정보 등으로 오해 가능하다는 의견도 있을 수 있으나

- 생체정보와 '생체실험'의 연상에 대하여는 입증된 바 없으며, '바이오'는 외국어로서 국어를 원칙으로 사용토록 하고 있는 법령 제정·개정 업무지침에 타당하지 않음

「국어기본법」	제14조(공문서의 작성) ① 공공기관등은 공문서를 일반 국민이 알기 쉬운 용어와 문장으로 써야 하며, 어문규범에 맞추어 한글로 작성하여야 한다. 다만, 대통령령으로 정하는 경우에는 괄호 안에 한자 또는 다른 외국 글자를 쓸 수 있다.
「법령 제정·개정 업무 지침」	(한글 전용의 원칙) 법령안은 국어기본법과 행정업무의 효율적 운영에 관한 규정에 따라 한글 전용을 원칙으로 한다. 다만, 현재 한글·한자를 혼용한 법령에는 한글·한자를 혼용할 수 있다.

- 민감정보에는 생체를 '인증 혹은 확인 대상'으로 이용하려는 목적성이 포함되어 있다는 점을 전제로 볼 때 일반적인 개인정보로 인정되는 '생체정보'와 구분되도록 '생체인식정보'라는 용어가 타당

o 원본정보와 특징정보에 대한 별도의 개념정의 여부

- 원본정보와 특징정보를 구분하여 법률에서 달리 규율하지 않는다면 법률상 별도로 개념 정의를 할 실익은 없으므로 이를 별도로 규정하는 것은 불필요. 오히려 수범자의 혼란 야기

- 원본정보와 특징정보의 처리과정에 있어 구체적으로 기술적/관리적 보호조치 등의 차이는 하위법령이나 가이드라인 등을 통해 규율되는 것이 타당

<참고> 원본정보와 특징정보

o 생체정보에는 수집되어 처리되는 과정에서 원본정보와(지문, 얼굴 이미지 등) 이러한 원본정보에서 추출한 특징정보(feature)가 포함

- 원본정보는 감지장치를 통하여 직접 사람의 신체나 행동방식에서 취득하는 정보를 말하며, 사진기에 촬영된 사진이나, 녹음된 목소리 등이 이에 해당

- 특징정보란 원본정보를 기반으로 생체특징 추출 알고리즘을 이용해서 만든 디지털 정보를 의미. 따라서 통상 이러한 특징정보 만으로는 개인정보라 할 수 없으

며 이러한 정보는 추가적 식별정보와 특징정보가 합쳐져야 개인정보가 됨

o 「정보통신망법 시행령」 제9조의2에서 규정하는 ‘접근권한이 필요한 정보 및 기능’의 일 유형으로서 ‘바이오정보’와 「정보통신망법 개정안」에서 신설하고자 하는 민감정보로서 ‘생체인식정보’는 동일하다고 보기 곤란

- 정보통신서비스 제공자가 일정한 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 설치된 기능에 대하여 접근하는 것이므로

- ‘접근권한이 필요한 정보 및 기능’의 각 항목은 반드시 개인을 인증 또는 식별하기 위한 목적성을 가진 정보가 아니라 단순히 서비스제공을 위해 필요한 경우일 수 있음

* 예를 들어 ‘사진보정앱’을 실행하기 위해 단말장치에 저장되어있는 사진파일에 접근하여야 하는 경우 개인을 인증 또는 식별하기 위한 목적성이 결여되어 있으므로 「정보통신망법 개정안」의 민감정보에 해당되지 않으나 이러한 서비스를 제공하기 위해서 그 이용이 필요

- 다만 ‘보안/인증 앱’의 경우처럼 ‘개인을 인증 또는 확인하기 위한 목적성’을 가지고 단말기 내의 생체정보에 접근하고자 하는 경우에는 「정보통신망법 개정안」의 민감정보로서 생체인식정보에 대한 규율이 적용되므로 동의를 받거나, 법령의 근거가 있어야 할 것임

- 따라서 「정보통신망법 시행령」 제9조의2에서 규정하는 ‘접근권한이 필요한 정보 및 기능’의 일 유형으로서 ‘바이오정보’는 현행과 같이 시행령에 별도로 규정하는 것이 타당

□참조입법례(국내외)

법령	생체(바이오)정보 관련 규정	
개인정보의 기술적·관리적 보호조치 기준 (방송통신위원회고시 제2015-3호,2015.5.19.일부개정)	제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다 8. "바이오정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.	
전자서명법 (제2조 정의)	13. "**개인정보**"라 함은 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 **생체특성 등**에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.	
GDPR 제4조 (정의)	(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;	(14) '**생체정보(biometric data)**'는 안면 영상이나 지문정보와 같이 개인 고유의 식별을 허용 또는 확인하는 해당 개인의 신체, 생리, 행동 특성에 관한 특정 기술 처리로 발생하는 개인정보를 의미한다.
	(15) 'data concerning health' means personal	(15) '**건강관련 정보(data**

	data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;	**concerning health)**'는 의료 서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보를 의미한다.
EU WP29 Biometric data	biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.	비록 기술적인 측정 방법에 사용되는 패턴이 일정 정도 확률을 포함하고 있지만, 개인별로 **고유하고 측정 가능한 생물학적** 속성, **행태적** 측면, **생리** 특성, **생활 특성** 또는 **반복성이 있는 행동**
미국 NTSC 국가과학기술위원회 Biometric data	A catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and	생체인식 처리과정에서 생성된 컴퓨터 **데이터**들에 대한 포괄적 개념. 자동인식 과정에서 발생하는 원시 센서 관측, 샘플, 모형, 탬플릿, 유사성 점수를 포함. 생체인식 데이터(Biometric data)는 등록, 확인 또는 식별 과정 중에 수집된 정보를 설명하는데 사용되지만, 사용자 이름, 인구 통계학적 정보 및 인증 같은 최종 사용자 정보에는 적용되지 않음

	authorizations.	
국제표준화 기구(ISO) Biometric data	biometric sample, biometric feature, biometric model, biometric property, other description data for the original biometric characteristics, or aggregation of above data	바이오인식 샘플(Sample), 기능(Feature), 모델(Model), 속성(Property), 본래의 바이오인식 특징에 대한 기타 설명 데이터 또는 위 자료의 **<u>집합</u>**
미국 일리노이 생체정보 프라이버시 법 제10조(정의)	"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.	생체정보식별자(Biometric Identifier)는 망막 혹은 홍채, 지문, 성문, 손과 얼굴모양을 대상으로 한다. 이와 대조적으로 생체정보식별자에는 작성샘플(Writing Sample), 서명, 사진, 타당한 과학적 실험에 사용된 인간생물학 샘플(Human Biological Sample), 인구통계(Demographic data), 신장, 체중, 모발 색 또는 동공의 색과 같은 신체적 묘사는 포함되지 않는다.
	"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.	생체인식 정보(Biometric information)란, 어떻게 수집, 변환, 보관 또는 공유되는지에 관계없이, 특정 개인을 **<u>식별</u>**하기 위해서 사용되는 개인의 **<u>생체인식 식별자에 기초한</u>** 여하한 정보를 의미함 생체인식 정보에는 생체인식 식별자의 정의 상 제외되는 항목이나 절차로부터 나온 정보는 포함되지 않음

2. 생체정보를 포함한 민감정보의 유형 구체화

현행	개정안
제23조(개인정보의 수집 제한 등) ① 정보통신서비스 제공자는 사상, 신념, 가족 및 친인척관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다.	<1안> 제23조(개인정보의 수집 제한 등) <1-1안>① 정보통신서비스 제공자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강·성생활·성적 성향을 드러내는 정보, 인종이나 민족적 출신을 드러내는 정보, 유전정보, 생체인식정보, 범죄경력에 대한 개인정보 그밖에 이용자의 권리·이익이나 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <1-2안>① 정보통신서비스 제공자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강·성생활·성적 성향을 드러내는 정보, 유전정보, 생체인식정보, 범죄경력에 대한 개인정보 그밖에 이용자의 권리·이익이나 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당

	하는 경우에는 그러하지 아니하다. (1안) 1. 정보주체에게 제22조제1항 각 호 또는 제24조의2 제1항 각 호의 사항을 알리고 명시적으로 동의를 받은 경우 (2안) 1. 정보주체에게 제22조제1항 각 호 또는 제24조의2 제1항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우
	<2안> 제23조(개인정보의 수집 제한 등) ① <1안과 동일> 1. <1안>과 동일 2. 정보주체가 일반에게 공개한 것이 명백한 정보 3. 다음 각 목에 해당하는 경우로서 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 가. 고용, 의료, 건강보험 등 사회보장제도의 실행을 위한 경우 나. 전염병, 건강안보 등 공중보건을 위해 필요한 경우 다. 공익적인 기록보존, 연구목적, 통계목적을 위해 필요한 경우

	라. 소송상 공격방어 수단으로 처리되는 경우

□ 개정이유

o 「정보통신망법」 상 민감정보에 대한 “예시방식”을 “한정적 열거방식”으로 개선할 필요가 있음

- 사생활침해, 개인의 권리·이익의 침해 여부는 지극히 주관적이며 이를 일일이 판례를 통해 규명하는 것도 용이하지 않을뿐더러

- 개인정보 법역의 기본법인 「개인정보 보호법」 도 이러한 점을 반영하여 대통령령 위임을 통해 한정적 열거방식을 채택하고 있으며, GDPR의 경우도 한정적 열거방식을 채택

- 불가피하게 융통성을 두고자 한다면 현행 「개인정보 보호법」과 같이 기준을 정하여 대통령령에 위임하는 방안도 검토될 수 있으나 기본취지는 한정적 열거방식을 취하는 것이 바람직

o 민감정보의 대상이 되는 개인정보의 유형을 구체적이고 명확하게 수정 필요

- 현재 「정보통신망법」 상 민감정보의 유형은 ① 사상, 신념, ② 가족 및 친인척관계, ③ 학력(學歷)·병력(病歷), ④ 기타 사회활동 경력을 규정하고 있으나,

- ② 가족 및 친인척관계가 민감정보인지 여부 불명확하며, 특히 기타 사회활동 경력은 매우 모호함

- 생체정보를 비롯한 ‘노동조합·정당의 가입·탈퇴’, ‘건강·성생활·성적 성향에 대한 정보’ 등 민감정보의 추가 및 구체화 필요

o 현재 민감정보를 수집할 수 있는 경우에 대하여, 「개인정보 보호법」 등과의 정합성

에 비추어 재검토 필요

- 「정보통신망법」은 민감정보 수집의 정당화 근거를 “법률”로 제한하고 있으나, 「개인정보 보호법」은 대통령령을 포함한 “법령”으로 그 범위를 넓히고 있는바, 법률의 정합성 측면 등에서 검토 필요

□ 주요내용

o 「정보통신망법」상 민감정보를 ‘한정적 열거방식’으로 수정하되, 다만 개정의 융통성을 위해 대통령령에 위임할 수 있도록 규정하고, 민감정보의 대상 및 유형을 개인정보 보호법 및 GDPR등 국제규범에 부합하도록 구체화

- 민감정보를 ‘사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강·성생활·성적 성향을 드러내는 정보, 인종이나 민족적 출신을 드러내는 정보, 유전정보, 생체정보, 범죄경력에 대한 개인정보, 그밖에 이용자의 권리·이익이나 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보’로 규정

- 다만 “인종이나 민족적 출신을 드러내는 정보”가 현재 국내 실정상 민감정보로서 취급될 필요가 있는지는 불명확한 바, 「개인정보 보호법」과의 정합성 측면에서 법률에 열거하기 보다는 추후 대통령령을 통하여 융통성을 부여하는 방안도 바람직

<민감정보의 유형 신구대비>

현행	개정안	개정이유
사상·신념	현행 유지	-
가족 및 친인척관계	**<삭제>**	- 이용자의 권리이익/사생활 침해 현저성 불명확 - 입법례 없음
기타 사회활동 경력	**<삭제>**	- 예시주의을 폐지하고 ‘한정적 열거주의’로 규정한다고 할 때 ‘기타 사회활동 경력’은 그 개념이 지나치게 모호함 - 필요시 ‘그밖에 이용자의 권리·이익이나

		사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보'에 포섭가능
<신설>	노동조합·정당의 가입·탈퇴	- 「정보통신망법」은 한정적 열거주의가 아니라 예시주의 규정방식을 취하고 있는바 '기타 사회활동 경력'에 포함된다고 볼 수 있으나, 이를 폐지하므로 구체화 할 필요가 있음 - 「개인정보 보호법」과 GDPR이 모두 민감정보로 규율
<신설>	정치적 견해	- '정치적 견해'를 '사상·신념'에 포함된다고 해석할 수 도 있으나, 법률의 명확성, 구체성 차원에서 이를 '정치적 견해'를 「정보통신망법」에 민감정보로 명확히 규정하는 것이 바람직 - 개인정보 보호법」과 GDPR은 민감정보로서 별도로 규정
병력 <수정>	건강·성생활·성적 성향에 대한 정보	- 정보주체의 의사와 무관하게 사용되어서는 안 되는 매우 민감한 정보 - 「개인정보 보호법」과 GDPR이 모두 민감정보로 규율 - '건강정보(data concerning health)'는 의료서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보로 전술한 생체정보와 구분 * '심전도' 자체가 생체정보라면, '심전도를 측정한 값(이 주는 의미)'은 건강정보에 해당, '홍채'가 생체정보라면 '홍채가 의미하는 신체 또는 건강상태'는 건강정보에 해당
대 통 령	인종이나 민족	- 과거 우리나라는 단일민족으로 구지 인종

<u>령을 통해 규율 필요성에 대한 융통성 부여</u>	적 출신을 드러내는 정보	이나 민족을 드러내는 정보가 개인에게 민감성을 가지지 않았으나 - 다문화 가족의 확산, 해외 노동인구의 유입 등에 비추어 볼 때 또한 다문화 가족에 대한 사회적 편견과 차별은 현재 심각한 사회문제로 대두 - 따라서 이제 인종이나 민족정보를 민감정보로 추가 필요 - 다인종/다민족으로 구성된 유럽의 특성상 GDPR은 민감정보로 규율
<u><신설></u>	유전정보	- 개인의 유전적 결함, 장애 등과 밀접하게 관련되며, 그 활용영역도 다채로운 만큼 그 오남용으로 인한 개인의 권리와 자유 침해적 요소가 심각 - 「개인정보 보호법」과 GDPR이 모두 민감정보로 규율
<u><신설></u>	생체인식정보	- 앞의 내용 참조
<u><신설></u>	범죄경력에 대한 정보	- 「정보통신망법」상 '기타 사회활동 경력'에 해당될 수 있으나, 규정의 모호성, 불확실성, 열거주의의 폐지 등에 비추어 '기타 사회활동 경력'을 폐지하고 '범죄경력에 관한 정보'를 추가하는 것이 타당 - 「개인정보 보호법」과 GDPR이 모두 민감정보로 규율

o 민감정보 수집의 정당화 근거를 "법률"로 제한하고 있으나, 이를 대통령령을 포함한 "법령"으로 개정

- 「개인정보 보호법」은 대통령령을 포함한 "법령"으로 그 범위를 넓히고 있는 바 「정보통신망법」에서 특별히 더 수집, 이용의 근거를 더 강화해야할 실익이 없는 한 이는 기본법 수준에 부합하는 것이 타당

o 민감정보에 대한 행위유형을 '수집'에서 '처리'로 확대

- 현재는 민감정보를 ‘수집’ 단계에서만 규율하고 있으나, 수집 된 이후로는 다른 개인정보와 동일하게 취급

- ‘수집’단계에서 뿐만 아니라, 이용, 제3자 제공 등 ‘처리’ 전반에 있어서도 민감정보의 규율 특수성이 여전히 존재하므로 ‘수집’ 단계에서의 규율체계를 ‘처리’로 확대

- 「개인정보 보호법」, GDPR 역시 민감정보에 대한 규율행위태양을 ‘수집’에 국한하지 않고 ‘처리’ 전반으로 규율하고 있음

o 민감정보 처리의 허용사유로서 동의의 방식에 대한 ‘명시적 동의’ 또는 ‘다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우‘ 라고 규정할 것인지 여부

- GDPR과 「개인정보 보호법」의 규정에 비추어 볼 때 통상적인 동의보다는 좀 더 강화된 요건의 동의를 요구하는 것이 ‘민감정보’의 보호필요성에 비추어 볼 때 타당

- 다만 GDPR과 같이 ‘명시적 동의’로 규정할 것인지, 「개인정보 보호법」과 같이 ‘별도의 동의’로 규율할 것인지에 대하여는 검토 필요

*「개인정보 보호법」은 민감정보 처리의 허용 근거로서 ‘명시적 동의’의 하나의 방법으로 ‘다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우’로 규율

- 정보통신서비스 제공자가 서비스 과정에서의 동의의 방식은 대체로 웹페이지 창을 통한 고지 및 클릭을 통해 이루어지는 바 ‘별도의 동의’를 구하도록 함은 동의 클릭을 하나 더 추가하는 것이 불과

- 현행 정보주체의 동의가 주로 정보통신 서비스 제공과정에서 깨알같은 글씨의 웹페이지 클릭을 통해 습관적, 관행적으로 이루어지고 있음에 비추어 볼 때 이러한 별도의 동의 방식이 유용한지에 대하여는 의문

- 따라서 ‘별도의 동의’로 명시적 동의의 방식을 제한하기 보다는 정보주체의 명백한 인지와 표시를 전제로 하는 ‘명시적 동의’로 규정함이 바람직

<참고1> GDPR 동의의 개념과 의미

o 통상적인 개인정보에 대하여 요구되는 '동의'

- GDPR는 일반적인 '동의'에 대하여 "정보주체가 자신에 관련되는 개인정보의 처리에 대한 자신의 의도를 **자유롭게, 구체적이며, 고지에 입각하여 모호하지 않게** 나타내는 것을 의미하며 그러한 합의는 **진술로 또는 분명한 긍정적 행위로** 표시되어야 함"(GDPR 제4조(11))이라고 규율하고 있음

  * GDPR 제4조(11) 'consent': any **freely given, specific, informed and unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her

o 특수한 유형의 개인정보에 대하여 요구되는 '명시적 동의(explicit consent)'

- GDPR은 특수한 유형의 개인정보 즉 민감정보 처리의 허용요건으로서의 '동의'에는 **'명시적' 동의**라고 규정함으로서 문언적으로 볼 때 일견 동의의 요건을 강화한 것으로 보임(GDPR제9조제2항(a))

  * GDPR제9조제2항(a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law .....

o GDPR은 '동의'에 대하여는 정의하고 있으나 '명시적 동의'에 대하여는 별도로 정의하고 있지 않음

다만 영국에서 발간한 보고서에 의하면 (UK Information Commissioner's Office, Consultation: GDPR consent guidance pp. 24~25 (March 2017) 참조.)

- 진술에 의해 확인될 수 있으면 '명시적 동의'이나, 정보주체의 행위로부터 암시되는 묵지적 동의는 명시적 동의라고 볼 수 없음

" 일반적인 동의와 명시적 동의의 다른 점은 구두이든 서면이든 동의가 **분명한 진술에서 확인되어야 한다는 점**이라고 할 수 있음. 즉 동의는 정보주체가 자신의 개인정보 처리에 대한 합의의 표시인데, **진술에 의하면 명시적 동의가 될 것이고,** '분명한 긍정적 행위'에 의하면 명시적 동의가 되지 않음 " ..... " 정보주체의 행위로부터 암시되는 묵시적 동의는 명시적 동의가 되지 않으며, 명시적 동의는 단어로 분명하게 확정되어야 함"

* 묵시적 동의의 예:

A 백화점이 고객에게 이메일주소를 선택적으로 기재하게 하면서 "당신의 이메일을 이용하여 우리 상품과 특별 제공에 대하여 이메일을 보내겠습니다." 라는 정보를 제공한다. 이 경우 고객이 그 문구 옆의 빈 칸에 자신의 이메일 주소를 기재하면, 그러한 이메일에 합의하는 구체적이고, 고지에 입각하며 모호하지 않은 긍정적 행위가 되지만, 묵시적 동의라고 보아야 한다.[64] B백화점이 고객에게 체크박스와 함께 "나는 당신의 상품과 특별 제공에 대한 이메일을 수령하기를 동의합니다."라는 정보를 제공한다. 이 경우 고객이 체크박스에 체크하면, 그러한 처리에 명시적 동의를 한 것이다.[65]

<참고2> 현행 「개인정보 보호법」 상 동의의 의미(행정안전부, 개인정보 보호법 해설서, 2016)

o 이 법에서 정보주체의 동의는 명시적 동의를 의미, 다만 다음과 같은 경우 '명시

적'에 대한 해석이 모호함

- 명함을 주고받는 행위

· 특별한 조건을 명시하여 명함을 교부한 경우가 아니라면, 일반적으로 명함을 교환하는 행위에는 명함에 기재된 정보를 사용해도 된다는 동의가 내재되어 있다고 해석됨이 바람직

· 즉 명함을 준 정황에 비추어보아 명함을 교부한 목적에 부합하는 이용이라면 정보주체의 동의가 있었다고 인정되므로 개인정보처리자는 명함에 기재된 개인정보를 이용하기 위해서 반드시 정보주체의 동의를 받아야 할 필요가 없음

- 공개된 매체를 통한 동의의사 표시

· 인터넷 홈페이지 등 공개된 매체, 장소 등에 정보주체가 자신의 개인정보를 수집 이용해도 된다는 명시적인 동의의사를 표시하거나, 홈페이지의 성격, 게시물 내용에 비추어 동의의사가 있었다고 인정되면, 해당 정보주체의 개인정보는 동의 없이 수집·이용할 수 있음

<참고3> 참조판례

o 인터넷 인물정보 서비스와 공개된 개인정보의 수집·제공(대법원 2016. 8. 17. 선고 2014다235080 판결)

- 개인정보자기결정권이라는 인격적 법익을 침해·제한한다고 주장되는 행위의 내용이 이미 정보주체의 의사에 따라 공개된 개인정보를 그의 별도의 동의 없이 영리 목적으로 수집·제공하였다는 것인 경우에는, 그와 같은 같은 정보처리 행위로 침해될수 있는 정보주체의 인격적 법익과 그 행위로 보호받을 수 있는 정보처리자 등의 법적 이익이 하나의 법률관계를 둘러싸고

충돌하게 된다.

- 이 때는 정보주체가 공적인 존재인지, 개인정보의 공공성과 공익성, 원래 공개한 대상 범위, 개인정보 처리의 목적・절차・이용형태의 상당성과 필요성, 개인정보 처리로 인하여 침해될 수 있는 이익의 성질과 내용 등 여러 사정을 종합적으로 고려하여, 개인정보에 관한 인격권 보호에 의하여 얻을 수 있는 이익과 그 정보처리 행위로 인하여 얻을 수 있는 이익 즉 정보처리자의 '알 권리'와 이를 기반으로 한 정보수용자의 '알 권리' 및 표현의 자유, 정보처리자의 영업의 자유, 사회 전체의 경제적 효율성 등의 가치를 구체적으로 비교 형량하여 어느 쪽 이익이 더 우월한 것으로 평가할 수 있는지에 따라 그 정보처리 행위의 최종적인 위법성 여부를 판단하여야 하고, 단지 정보처리자에게 영리 목적이 있었다는 사정만으로 곧바로 그 정보처리 행위를 위법하다고 할 수는 없다(대법원 2011. 9. 2. 선고 2008다42430 전원합의체 판결, 대법원 2014. 7. 24. 선고 2012다49933 판결 등 참조).

o 홈플러스 판결(대법원 2017.4.7. 선고 2016도1326판결)

- 홈플러스는 고객들에 대한 경품행사를 통하여 고객들의 개인정보를 수집하고 제3자 제공에 관한 동의를 받았는데, 그 중 약 600만건을 보험회사들에 판매하여 약 119억원을 지급받음. 홈플러스는 경품 응모권 뒷면에 개인정보의 수집·이용목적, 제공받는 자 등 고지사항을 약 1mm크기의 글씨로 기재함

- 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 그 처리에 관한 동의를 받았는지 여부를 판단함에 있어서는 개인정보처리자가 그에 관한 동의를 받는 행위 그 자체만을 분리하여 개별적으로 판단하여서는 안 되고, 개인정보처리자가 개인정보를 취득하거나 처리에 관한 동의를 받게 된 전 과정을 살펴보아 거기에서 드러난 개인정보 수집 등의 동기와

목적, 수집 목적과 수집 대상인 개인정보의 관련성, 수집 등을 위하여 사용한 구체적인 방법, 개인정보 보호법 등 관련 법령을 준수하였는지 여부 및 취득한 개인정보의 내용과 규모 특히 민감정보·고유식별정보 등의 포함 여부 등을 종합적으로 고려하여 사회통념에 따라 판단하여야 한다..... 이 사건 경품행사를 위하여 사용된 응오권에 기재된 동의 관련 사항은 약 1mm 크기의 글씨로 기재되어 있어 소비자의 입장에서 보아 그 내용을 읽기가 쉽지 않다... 여기에 더하여 이 사건 광고를 통하여 단순 사은행사로 오인하고 경품행사에 응모하게 된 고객들의 입장에서는 짧은 시간동안 응모권을 작성하여 응모화면에 입력을 하면서 그 내용을 정확히 파악하여 잘못된 인식을 바로잡기가 어려울 것으로 보인다. **이러한 조치는 개인정보처리자가 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 하여야 한다는 개인정보 보호법상의 의무를 위반한 것이다.**

□ 쟁점사항

o 민감정보 해당성의 융통성을 발휘하기 위하여 '예시적 방식'의 규정이 타당하다는 다른 견해가 있을 수 있음

- 예를 들어 숙박앱 '여기어때'의 개인정보(고객 이름, 전화번호, 숙박이용정보) 유출사건 관련 숙박이용정보의 경우 현재의 「정보통신망법」에 의한 경우 '민감정보'에 해당될 수 있으나, 한정적 열거방식의 경우 명시적으로 규정하지 않는 한 '민감정보'에 해당되지 않음

---

64) UK Information Commissioner's Office, *Consultation: GDPR consent guidance* p. 24 (March 2017) 참조.

65) UK Information Commissioner's Office, *Consultation: GDPR consent guidance* p. 25 (March 2017) 참조.

- ‘숙박이용정보’의 민감성은 개개인에 따라 다를 수 있으며, ‘범죄경력정보·성생활·건강정보’ 등 누구에게나 보편타당하게 민감한 정보라고 보기 곤란

- 민감정보 해당성 여부가 개개인의 주관적 성향에 따라 달라진다면 법적 안정성이나 명확성 측면에서 바람직하지 않으므로, 한정적 열거방식이 타당

- 또한 일반 개인정보와 민감정보에 대한 차별적 규율은 수집등 처리단계에서 이루어지며, 침해에 대한 가벌성은 동일(5년 이하의 징역 또는 5천만원 이하의 벌금, 제71조 제1항 제1호, 제2호)하므로 수집 등 처리단계에서 차별화할 수 있는 정보가 아닌 한 민감정보로 규율 실익이 없음

o ‘정보주체가 일반에게 공개한 것이 명백한 정보’를 수집근거에 추가할 것인지 여부

- GDPR은 정보주체가 일반에게 공개한 것이 명백한 경우 구지 그 활용을 제한할 필요가 없으므로 이에 대한 수집, 이용 근거를 추가하고 있으나

- 정보주체가 아무리 일반에게 공개하였다 할지라도 정보주체가 허락한 이용 목적 및 범위를 초과하여 활용하여서는 아니므로, 수집처리 허용 근거로 규정하는 것을 바람직하지 않을 수 있음

- 특히 「정보통신망법」 제22조의 일반 개인정보의 수집등 처리와 관련하여서도 이러한 예외규정이 없는바, 보호를 더 강화해야 할 민감정보의 처리근거에 이를 추가하는 것은 법체계상 모순

- 개인정보 일반법인 「개인정보 보호법」에도 현재 이러한 규정이 없으므로 개인정보의 수집이용요건의 완화와 함께 체계정합적으로 논의될 필요가 있음

o 민감정보 수집 법령의 기준을 제안할지 여부

- ‘법령의 규정’은 각 영역의 입법활동이 모두 개인정보 보호를 위해 초점이 맞추어져 있지 않는 한 오히려 그 활용영역을 임의적으로 확대할 수 있음

즉, 복지, 산업, 교육 등 각 영역의 개별법에 의해 민감정보의 처리가 무작위적으로 허용되는 것을 막기 위해서 단순히 "법령"의 규정에 의한 처리의 허용을 규정하는 것이 아니라, 특정한 사안의 경우 법률에 의해 가능하도록 기준을 수립할 필요성 제기

- 자의적 입법에 의한 허용을 금지하기 위해 GDPR에서 구체적으로 허용되는 경우를 열거하고 있으며 이러한 취지에 비추어 "법령"에 의해 허용되는 경우에 대한 구체화가 필요

- 그러한 기준으로 i)기본권을 보호를 위한 사회보장제도의 실행을 위한 경우(고용법, 사회보장법, 의료보장법, 건강보험법 등), ii)전염병, 건강안보, 공중보건 등(공중보건법, 전염병관리법 등) iii)공익적인 기록보존, 연구 목적, 통계목적을 위해 허용(기록물관리법, 통계법 등) iv)소송상 공격방어 수단으로 처리되는 경우 등이 제안될 수 있음

- 다만 이는 정보통신서비스 제공자를 규율하는 「정보통신망법」이 아니라, 개인정보 보호의 일반법인 「개인정보 보호법」에서 규율하는 것이 더 타당한 측면도 있음

o 관리, 보관, 파기 등에 있어서 특칙 필요성

- 관리, 보관, 파기 과정에서의 기술적 보호조치의 기준 제시가 필요하다는 주장이 있을 수 있으나

- 법률은 기술중립성에 기반하여 '기술적 보호조치'에 대하여 규정할 수 있을 뿐 그 기술의 구체적 수준까지 세분화 할 수 없음

- 따라서 파기의 기술적 조치는 지침 또는 고시를 통해 기술변화에 연동하여 구체화하는 것이 타당

* 「정보통신망법」 시행령 제15조제6항에서는 방송통신위원회는 제1항부터 제5항까

지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하도록 규정하고 있는 바, 민감정보의 조치와 관련하여 특이사항은 이러한 고시를 통해 규율하는 것이 타당

□참조입법례(국내외)

o EU 1995년 지침 및 GDPR

1995년 개인정보보호지침	GDPR
Article 8 특별한 유형의 개인정보 처리(The processing of special categories of data)	Article 9 특별한 유형의 개인정보 처리 (Processing of special categories of personal data)
1. 회원국들은 인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 노조 가입을 드러내는 개인정보의 처리, 및 건강 또는 성생활에 관한 데이터의 처리를 금지해야 한다	인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 또는 노조가입을 드러내는 개인정보의 처리, 및 **유전데이터, 자연인을 고유하게 식별하는 목적의 생체데이터,** 건강에 관한 데이터 또는 자연인의 성생활 **또는 성적 성향에 관한 데이터**의 처리는 금지되어야 한다
1 . Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.	1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, **and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,** data concerning health or data concerning a natural person's sex

	life **or sexual orientation** shall be prohibited.

o 민감정보의 수집처리가 허용되는 경우 비교

	개인정보 보호법	정보통신망법	GDPR
민감 정보 유형	① 사상·신념 ②노동조합·정당의 가입·탈퇴 ③ 정치적 견해 ④ 건강, 성생활 등에 관한 정보 ⑤ 유전정보 ⑥ 범죄경력에 관한 정보	① 사상, 신념 **② 가족 및 친인척관계** ③ 학력(學歷)·병력(病歷) **④ 기타 사회활동 경력**	**① 인종적 또는 민족적 출신을 드러내는 정보** ② 정치적 의견을 드러내는 정보 ③ 종교적 또는 철학적 믿음을 드러내는 정보 ④ 노조가입을 드러내는 정보 **⑤ 유전데이터** **⑥자연인을 고유하게 식별하는 목적의 생체데이터** ⑦ 건강에 관한 데이터 ⑧ 성생활에 관한 데이터 **⑨ 성적 성향에 관한 데이터** **⑩ 범죄유죄판결 및 범죄행위**에 관한 개인정보
	열거규정	예시규정	열거규정
처리가 허용되는 경우	①**별도의** 동의 ②**법령**의 규정	① 동의 ② **법률**의 규정	①명시적 동의 ②고용, 사회 안보나 사회보장법 또는 단체협약에 따른 의무의 이행 ③ 동의무능력 정보주체의 중대한 이익의 보호 ④ 정치, 철학, 종교 목적을 지닌 비영리단체나 노동조합이 하는 처리 ⑤ 정보주체가 일반에게 공개한 것이 명백한 정보

			⑥ 법적 주장의 구성, 행사나 방어 ⑦ 중대한 공익을 위해 법률을 근거로 하는 처리 ⑧법률 또는 계약을 근거로, 예방 의학이나 직업 의학, 종업원의 업무능력 판정, 의료 진단, 보건·사회 복지·치료, 보건이나 사회복지 시스템의 관리 및 서비스 제공 ⑨공중보건 영역에서의 공익을 위해 필요한 경우 ⑩ 공익을 위한 저장, 과학적·역사적 연구 목적이나 통계 목적 **다만** '범죄경력 및 범죄행위'는 ①공공기관의 규제 하에서만 또는 ②법률의 규정에 의해서만 처리 가능

3. 이용자 개인영상정보 처리지침 마련 및 준수(안 제27조의4)

현행	개정안
<신 설>	**제27조의4(이용자 영상정보처리지침)** ① 정보통신서비스 제공자는 자신의 정보통신서비스를 이용하여 개인영상정보를 처리하는 이용자가 영상정보주체의 권리보장 등을 위하여 준수하여야 하는 사항을 담은 지침(이하 "이용자 영상정보처리지침"이라 한다)을 대통령령에 따라 정하여 공개하여야 한다. 다만, 정보통신서비스 제공자가 제27조의2에 따른 개인정보 처리방침을 수립하는 경우에는 그에 포함하여 정할 수 있

	다. ② 이용자는 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하여 개인영상정보를 처리하는 경우에는 제1항에 따른 이용자 영상정보처리지침을 준수하여야 한다.

□ 개정이유

o 유튜브, 네이버 블로그 등 정보를 직접 수집하지 아니하고 정보의 매개서비스만을 제공하는 정보통신서비스제공자는 개인영상정보를 직접적으로 수집, 이용하지는 아니하나, 이용자에 의해 수집된 개인영상정보를 플랫폼을 통해 공개 또는 유포

- 이들은 이용자에 의해 처리되는 개인영상정보를 일일이 모니터링 할 수 없으나, 그러한 정보의 매개로 수익을 창출하는 사업자 이므로, 개인영상정보를 처리하는 이용자가 영상정보주체의 권익을 침해하지 않도록 일정한 지침을 제공하고 준수하도록 할 필요가 있음

□ 주요내용

o 정보통신서비스를 이용하여 개인영상정보를 처리하는 이용자로 하여금 준수해야 하는 일정한 지침을 마련하여 사전에 개인영상정보 침해 위험에 대비

- 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망을 이용하여 개인영상정보를 처리하는 이용자가 준수하여야 하는 사항을 담은 이용자개인영상정보처리지침을 정하고 이를 공개하도록 함

- 이용자개인영상정보처리지침에 수록될 내용은 영상정보주체의 권리보장에 대한 것으로 그 구체적 내용은 대통령령에서 규정하도록 함

이용자 영상정보처리지침에 담을 내용(예)

1. 개인영상정보주체의 권리보장방법
2. 개인영상정보주체에 대한 이용자의 의무
3. 정보통신서비스제공자에 대한 이용자 준수사항
4. 개인영상정보의 삭제요청 등에 대한 적절할 처리절차 등
5. 그밖에 영상정보주체의 권리를 보장하기 위해 필요한 사항

- 다만, 정보통신서비스제공자가 제27조의2에 따른 개인정보 처리방침을 수립하는 경우에는 별도로 영상정보처리지침을 만들기 보다는 개인정보 처리방침에 포함하여 정할 수 있도록 규율하여, 이용자의 가독성, 사업자의 지침마련의 불편성 제고

o 이용자로 하여금 정보통신서비스 제공자가 수립·공개한 이용자개인영상정보처리지침을 준수하도록 함

□ 쟁점사항

o 이용자개인영상정보처리지침은 정보통신서비스 제공자로 하여금 이를 수립하도록 하는 방안(수립의무)과 수립 및 공개하도록 하는 방안(수립·공개의무), 수립 또는 수립·공개를 선택적으로 이행하도록 하는 방안(임의규정), 수립하고 이를 이용자에게 권고하도록 의무화하는 방안(수립·권고의무) 등 대안적 구성이 가능

- 대안으로 정보통신서비스 제공자로서 하여금 “이용자 영상정보처리지침”을 마련할 의무를 부여할 것이지 또는 “이용자 영상정보처리지침”을 마련하는 경우에 책임을 감경하도록 할 것인지에 대한 추가 분석이 요구됨

□ 참조입법례(국내외)

o 위반방지를 위한 고지의무

「방문판매 등에 관한 법률」 제28조(다단계판매업자의 책임) ① 다단계판매업자는 다단계판매원이 자신의 하위판매원을 모집하거나 다단계판매업자의 재화등을 소비자에게 판

매할 때 제23조 또는 제24조를 위반하지 아니하도록 다단계판매원에게 해당 규정의 내용을 서면이나 전자우편으로 고지하여야 한다.

② 다단계판매업자가 제1항에 따른 고지의무를 게을리한 경우에 다단계판매원이 제23조 또는 제24조를 위반하여 다른 다단계판매원 또는 소비자에게 입힌 재산상 손해는 대통령령으로 정하는 바에 따라 다단계판매업자가 배상 책임을 진다. 이 경우 다단계판매업자는 다단계판매원에게 구상권을 행사할 수 있다.

o 위험물 취급지침

「위험물 선박운송 및 저장규칙」

제23조(위험물 취급지침의 제공) ① 제204조제1항 각 호에 따른 위험물을 운송하는 선박과 산적액체위험물을 운송하는 선박의 소유자는 해당 위험물의 운송으로 발생하는 위험을 방지하기 위하여 해당 위험물에 관한 성질·상태, 작업의 방법, 재해발생 시의 조치나 그 밖의 주의사항을 상세히 기록한 위험물취급지침을 작성하여 해당 선박의 선장에게 제공하여야 한다.

② 선장은 제1항의 위험물취급지침에 기술된 사항을 해당 선박의 선원 및 해당 작업을 하는 작업원에게 주지시키고 이를 준수하게 하여야 한다.

③ 제1항의 위험물 외의 위험물을 운송하는 경우(국내항 간에 컨테이너 외의 수단으로 운송하는 경우는 제외한다)에 송하인은 선박소유자 또는 선장(위험물을 자동차에 적재하거나 컨테이너에 수납하여 운송하는 경우로서 선박소유자가 적재하거나 수납할 경우에는 선박소유자만 해당한다)에게 해당 위험물에 관하여 재해발생시의 조치에 관한 정보를 기재한 서류를 제출하여야 한다. 다만, 위험물을 적재하는 항만의 관할지방해양항만청장등이 안전에 지장이 없다고 인정한 경우에는 그러하지 아니하다.

④ 선장은 제3항의 서류(사본 등을 포함한다. 이하 이 조에서 같다)를 해당 운송이 종료할 때까지 선박 안에 보관하여야 한다.

⑤ 위험물을 다른 선박에 옮겨 실을 경우에는 옮겨 주는 선박의 소유자

또는 선장은 제3항의 서류를 옮겨 실을 선박의 소유자 또는 선장에게 내주어야 한다.

o 내부통제기준

「자본시장과 금융투자업에 관한 법률」 제117조의6(지배구조 등) ① 온라인소액투자중개업자는 대주주(제23조제1항의 대주주를 말한다)가 변경된 경우에는 이를 2주 이내에 금융위원회에 보고하여야 한다. ② 온라인소액투자중개업자는 그 임직원이 직무를 수행할 때 준수하여야 할 적절한 기준 및 절차로서 대통령령으로 정하는 사항을 포함하는 내부통제기준을 정하여야 한다. ③ 제28조, 제28조의2, 제29조, 제30조, 제31조는 온라인소액투자중개업자에 대하여 적용하지 아니한다.
「자본시장과 금융투자업에 관한 법률 시행령」 제118조의8(내부통제기준) ① 법 제117조의6제2항에 따른 내부통제기준(이하 "내부통제기준"이라 한다)에는 다음 각 호의 사항이 포함되어야 한다. 1. 업무의 분장과 조직구조에 관한 사항 2. 고유재산운용업무(제50조제1항에 따른 고유재산운용업무를 말한다)를 하는 과정에서 발생하는 위험의 관리지침에 관한 사항 3. 임직원이 업무를 할 때 준수하여야 하는 절차에 관한 사항 4. ~ 9. (생략) ② ~ ④ (생략)

o 이용조건

「여신전문금융업법」 제39조(거래조건의 주지 의무) 할부금융업자는 할부금융계약을 체결한 재화와 용역의 매수인(이하 “할부금융이용자”라 한다)에게 다음 각 호의 사항이 적힌 서면을 내주어야 한다. 다만, 할부금융이용자의 동의가 있으면 팩스나 전자문서(「전자문서 및 전자거래 기본법」 제2조제1호에

따른 전자문서를 말한다)로 보낼 수 있다. 1. 할부금융업자가 정하는 이자율, 연체이자율 및 각종 요율. 이 경우 각종 요율은 취급수수료 등 그 명칭이 무엇이든 할부금융이용자가 할부금융업자에게 지급하는 금액이 포함되도록 산정하여야 한다. 2. 할부금융에 의한 대출액(이하 “할부금융자금”이라 한다)의 변제방법 3. 그 밖에 총리령으로 정하는 사항

o 특수한 유형의 부가통신사업자

- 「전기통신사업법」 제22조는 특수한 유형의 부가통신사업자의 등록을 규정하고 있고, 같은 법 시행령 제29조제9항과 별표 3은 등록요건을 정함
- 동 등록요건의 하나로서 “저작권 위반 시 처리지침”과 “상습적 침해자 등에 대한 적절할 처리절차, 제재내용, 소요기간, 제재 대상자 자료보관 방안 등”을 포함하는 이용자보호계획서의 작성이 요구됨

4. 개인영상정보의 삭제요청 등(안 제27조의5)

<1안>

현 행	개 정 안
제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 **삭제** 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청	**제44조의2(정보의 삭제요청 등)** ①① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 **삭제, 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기**

할 수 있다. ② ~ ⑥ (현행과 같음)	**술적 조치** 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다. ② ~ ⑥ (현행과 같음)

<1-1안>

o 정보게재자의 이의제기권 신설 및 이와 관련한 분쟁조정 절차를 마련하고, 임시조치 이후 해당 정보에 대한 처리방법(이의제기가 없으면 삭제)을 명확히 규정하는 것을 내용으로 하는 정보통신망법 개정안이 국회에 계류 중임(의안번호 2000546)

현 행	개 정 안	재개정안
제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수	**제44조의2(임시조치 등)** ① ---------- ---------- ---------- ---------- ---------- -------- 권리를 침해받았다고 주장하는 자(이하 "권리주장자"라 한다)는 ----- ---------- ---------- ---------- 삭제를 ---------- -------.	**제44조의2(임시조치 등)** ① ---------- ---------- ---------- ---------- ---------- -------- 권리를 침해받았다고 주장하는 자(이하 "권리주장자"라 한다)는 ----- ---------- ---------- ---------- 삭제 또는 영상정보주체를 알아볼 수 없도록 하는 기술적 조치

현 행	개 정 안	재개정안
있다.		(이하 "삭제등"이라 한다)를 ----------.
② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제 등을 요청받으면 지체 없이 삭제·임시 조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.	② 정보통신서비스 제공자는 제1항에 따른 정보의 **삭제를** 요청받으면 지체 없이 그 정보에 대한 접근을 임시적으로 차단하는 조치(이하 "임시조치"라 한다)를 하고, 지체 없이 다음 각 호의 사항을 권리주장자 및 정보게재자에게 통지하여야 한다. 다만, 정보게재자에게 통지할 수 없는 경우에는 해당 게시판에 게시하여야 한다. 1. 임시조치의 사실 및 기간 2. 이의제기의 방법 및 절차 3. 이의제기 시 직권 조정절차에 회부된다는 사실	② ---------- **삭제등을** ----------. 1. ---------- 2. ---------- 3. ----------
③ 정보통신서비스	③ 정보통신서비스	(개정안과 같음)

현 행	개 정 안	재개정안
제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.	제공자는 임시조치를 한 사실을 해당 게시판에 게시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.	
④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 “임시조치”라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다.	④ 제2항에 따른 임시조치의 기간은 30일로 한다. 다만, 제5항에 따른 정보게재자의 이의제기가 있는 때에는 제44조의14제1항에 따른 직권조정절차가 종료되는 날까지로 한다.	(개정안과 같음)

현 행	개 정 안	재개정안
⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다.	⑤ 정보게재자는 제4항 본문에 따른 임시조치의 기간 내에 임시조치에 대하여 이의를 제기할 수 있다. 이 경우 정보통신서비스 제공자는 다음 각 호의 사항을 권리주장자에게 지체 없이 통지하여야 한다. 1. 정보게재자의 이의제기 사실 2. 직권조정절차에 회부된다는 사실 3. 직권조정결정의 절차	(개정안과 같음)
⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.	⑥ 제5항 각 호 외의 부분 본문에 따른 정보게재자의 이의제기가 있는 경우에는 제44조의14에 따른 직권조정절차에 회부된 것으로 본다. 이 경우 정보통신서비스 제공자는 대통령령으로 정하는 바에 따라 임시조치와 관련된 자료를 제44조의10에 따른 온라인명예훼손분쟁조정위원회에 지	(개정안과 같음)

현 행	개 정 안	재개정안
	체 없이 송부하여야 한다.	
<신 설>	⑦ 정보통신서비스 제공자는 제5항 각 호 외의 부분 본문에 따른 정보게재자의 이의제기가 없는 경우에는 제4항 본문에 따른 임시조치의 기간이 만료한 후 해당 정보를 즉시 **삭제하여야** 한다.	⑦ ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- **삭제하거나 영상정보주체를 알아볼 수 없도록 하는 기술적 조치를 하여야** ----.
<신 설>	⑧ 정보통신서비스 제공자는 정보의 삭제 요청, 임시조치에 관한 내용 및 절차 등을 미리 약관에 구체적으로 밝혀야 한다.	(개정안과 같음)
<신 설>	⑨ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항 및 제3항에 따른 조치와 제7항에 따라 해당 정보를 **삭제한** 경우에는 이로 인한	⑨ ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- **삭제하거나 영상정보주체**

현 행	개 정 안	재개정안
	책임을 면제받거나 감경받을 수 있다.	**를 알아볼 수 없도록 하는 기술적 조치를 한** ----------. ----------
<신 설>	⑩ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.	(개정안과 같음)

<2안>

현행	개정안
<신 설>	**제27조의5(개인영상정보의 삭제요청 등)** ① 정보통신서비스 제공자가 제공하는 정보통신서비스를 통하여 자신의 개인영상정보가 공개됨에 따라 개인정보에 관한 권

	리가 침해됨을 주장하는 자(이하 “권리주장자”라 한다)는 그 사실을 소명하여 정보통신서비스 제공자에게 그 개인영상정보의 삭제 또는 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기술적 조치(이하 "삭제등"이라 한다)를 요청할 수 있다.[66] ② 정보통신서비스 제공자는 제1항에 따른 요청을 받으면 지체 없이 요청사실을 정보통신서비스를 이용하여 해당 개인영상정보를 처리하는 이용자에게 알리고 권리주장자와 해당 개인영상정보의 처리에 관하여 합의하도록 권고하여야 한다. ③ 정보통신서비스 제공자는 다음 각 호의 경우에는 제1항의 개인영상정보에 대한 접근을 임시적으로 차단하는 조치(이하 “임시조치”라 한다)를 할 수 있다. 1. 제2항에 따라 권리주장자와 정보제개자 간의 합의가 이루어지지 않은 경우 2. 정보게재자에게 통지할 수 없는 경우 ④ 제3항에 따라 임시조치를 한 경우에는 지체없이 임시조치의 사실 및 기간을 정보게재자와 권리주장자에게 통지하여야 한다. 다만, 정보게재자에게 통지할 수 없는 경우 해당 게시판에 공시하는 등의 방법으로 알려야 한다. ⑤ 제3항에 따른 임시조치의 기간은 30일로 한다. ⑥ 정보통신서비스제공자는 임시조치 기

	간 만료 후 해당 개인영상정보를 삭제한다. 다만, 임시조치 기간내에 정보게재자와 권리주장자 간 해당 개인영상정보처리에 대한 합의가 이루어진 경우에는 그 합의내용에 따른다. ⑦ 정보통신서비스 제공자는 자신이 제공하는 정보통신서비스를 이용하여 처리되는 개인영상정보에 대하여 제2항부터 제4항까지에 따른 조치 및 제6항에 따른 삭제를 한 경우에는 이로 인한 배상의 책임을 지지 아니한다.

<3안>

현행	개정안
<신 설>	**제27조의5(개인영상정보의 삭제요청 등)** ①정보통신서비스 제공자가 제공하는 정보통신서비스를 통하여 개인영상정보가 공개됨에 따라 자신의 권리가 침해됨을 주장하는 자(이하 "권리주장자"라 한다)는 그 사실을 소명하여 정보통신서비스 제공자에게 그 개인영상정보의 삭제, 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기술적

66) 다음과 같은 대안을 고려할 수 있다.
① 정보통신서비스 제공자가 제공하는 정보통신서비스를 통하여 자신의 개인영상정보가 공개됨에 따라 자신의 권리가 침해됨을 주장하는 자(이하 "권리주장자"라 한다)는 그 사실을 소명하여 정보통신서비스 제공자에게 그 개인영상정보의 삭제 또는 처리정지, 영상정보주체를 알아볼 수 없도록 하는 기술적 조치(이하 "삭제등"이라 한다)를 요청할 수 있다.

	조치(이하 "삭제등"이라 한다)를 요청할 수 있다. ② 제2항에 따른 삭제등의 요청에 관하여는 제44조의2를 준용한다.

□ 개정이유

o 정보통신서비스의 전파성, 신속성등에 비추어 볼 때 영상정보주체의 원치 않는 개인영상정보의 유출에 대한 신속한 권리구제 방안 필요

o 사진, 동영상 등의 개인영상정보에 대한 원치 않는 공개의 경우 반론과 토론을 통한 자정작용이 사실상 무의미한 경우가 적지 않고, 빠른 전파가능성으로 말미암아 사후적인 손해배상이나 형사처벌로는 회복하기 힘들 정도의 인격 파괴가 이루어질 수도 있어,

- 정보의 공개 그 자체를 잠정적으로 차단하는 것 외에 반박내용의 게재, 링크 또는 퍼나르기 금지, 검색기능 차단 등의 방법으로는 개인영상정보주체의 보호에 미흡

□ 주요내용

<1안>

o (삭제·임시조치 등 대상 확대) 제44조의2 개정을 통하여 영상정보의 공개로 인하여 사생활 침해 등 권리가 침해된 자는 그 사실을 소명하여 정보통신서비스 제공자에게 해당 개인영상정보의 처리를 중단하거나 삭제, 상정보주체를 알아볼 수 없도록 하는 기술적 조치(비식별화)를 할 것을 요구할 수 있음

- 처리의 중단요구를 받은 경우에는 즉시 그 개인영상정보의 처리를 중단시키고 권리주장자에게 그 사실을 통보

- 이때, 정보통신서비스 제공자는 그 개인영상정보를 공개 또는 유통한 이용자에게도 이

를 통보하도록 함

- 이에 따라 일정한 조치를 취한 정보통신서비스 제공자에 대하여 배상책임을 줄이거나 면제받을 수 있도록 함

<2안>

o 개인영상정보주체는 본인의 개인영상정보의 원치 않는 공개 자체가 침해에 해당되므로 굳이 별도의 소명절차 불필요하므로 제44조의2와 별도의 절차 마련

- 일차적으로 당사자(정보게재자와 권리주장자) 간 개인영상정보의 게재 여부에 대하여 합의할 기회를 주되

- 합의가 원만히 되지 않을 경우 임시조치 등의 수단 발동

<3안>

o (삭제·임시조치 등의 준용) 유관 조문(개인영상정보를 처리하는 이용자에 관한 신설 조문안 제27조의4)과 함께, 개인영상정보에 관한 임시조치 등을 위한 제도를 마련

- 제44조의2와 유사한 제도를 도입하되, 법령 조문의 간소화라는 입법 경제적 측면을 고려하여 세부절차 등은 제44조의2를 준용하도록 함

□ 참조입법례(국내외)

o 정보통신망법 上 (정보통신서비스 제공자) 자신이 운영·관리하는 정보통신망

제44조② 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
제44조의2 ③ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.
제44조의2 ⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신

망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

제44조의3 ① 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다.

- 저작권법

제102조(온라인서비스제공자의 책임 제한) ① 온라인서비스제공자는 다음 각 호의 행위와 관련하여 저작권, 그 밖에 이 법에 따라 보호되는 권리가 침해되더라도 그 호의 분류에 따라 각 목의 요건을 모두 갖춘 경우에는 그 침해에 대하여 책임을 지지 아니한다.

1. 내용의 수정 없이 저작물등을 송신하거나 경로를 지정하거나 연결을 제공하는 행위 또는 그 과정에서 저작물등을 그 송신을 위하여 합리적으로 필요한 기간 내에서 자동적·중개적·일시적으로 저장하는 행위
   가. 온라인서비스제공자가 저작물등의 송신을 시작하지 아니한 경우
   나. 온라인서비스제공자가 저작물등이나 그 수신자를 선택하지 아니한 경우
   다. 저작권, 그 밖에 이 법에 따라 보호되는 권리를 반복적으로 침해하는 자의 계정(온라인서비스제공자가 이용자를 식별·관리하기 위하여 사용하는 이용권한 계좌를 말한다. 이하 이 조, 제103조의2, 제133조의2 및 제133조의3에서 같다)을 해지하는 방침을 채택하고 이를 합리적으로 이행한 경우
   라. 저작물등을 식별하고 보호하기 위한 기술조치로서 대통령령으로 정하는 조건을 충족하는 표준적인 기술조치를 권리자가 이용한 때에는 이를 수용하고 방해하지 아니한 경우
2. 서비스이용자의 요청에 따라 송신된 저작물등을 후속 이용자들이 효율적으로 접근하거나 수신할 수 있게 할 목적으로 그 저작물등을 자동적·중개적·일시적으로 저장하는 행위
   가. 제1호 각 목의 요건을 모두 갖춘 경우
   나. 온라인서비스제공자가 그 저작물등을 수정하지 아니한 경우
   다. 제공되는 저작물등에 접근하기 위한 조건이 있는 경우에는 그 조

건을 지킨 이용자에게만 임시저장된 저작물등의 접근을 허용한 경우

라. 저작물등을 복제·전송하는 자(이하 "복제·전송자"라 한다)가 명시한, 컴퓨터나 정보통신망에 대하여 그 업계에서 일반적으로 인정되는 데이터통신규약에 따른 저작물등의 현행화에 관한 규칙을 지킨 경우. 다만, 복제·전송자가 그러한 저장을 불합리하게 제한할 목적으로 현행화에 관한 규칙을 정한 경우에는 그러하지 아니한다.

마. 저작물등이 있는 본래의 사이트에서 그 저작물등의 이용에 관한 정보를 얻기 위하여 적용한, 그 업계에서 일반적으로 인정되는 기술의 사용을 방해하지 아니한 경우

바. 제103조제1항에 따른 복제·전송의 중단요구를 받은 경우, 본래의 사이트에서 그 저작물등이 삭제되었거나 접근할 수 없게 된 경우, 또는 법원, 관계 중앙행정기관의 장이 그 저작물등을 삭제하거나 접근할 수 없게 하도록 명령을 내린 사실을 실제로 알게 된 경우에 그 저작물등을 즉시 삭제하거나 접근할 수 없게 한 경우

3. 복제·전송자의 요청에 따라 저작물등을 온라인서비스제공자의 컴퓨터에 저장하는 행위

가. 제1호 각 목의 요건을 모두 갖춘 경우

나. 온라인서비스제공자가 침해행위를 통제할 권한과 능력이 있을 때에는 그 침해행위로부터 직접적인 금전적 이익을 얻지 아니한 경우

다. 온라인서비스제공자가 침해를 실제로 알게 되거나 제103조제1항에 따른 복제·전송의 중단요구 등을 통하여 침해가 명백하다는 사실 또는 정황을 알게 된 때에 즉시 그 저작물등의 복제·전송을 중단시킨 경우

라. 제103조제4항에 따라 복제·전송의 중단요구 등을 받을 자를 지정하여 공지한 경우

4. 정보검색도구를 통하여 이용자에게 정보통신망상 저작물등의 위치를 알 수 있게 하거나 연결하는 행위

가. 제1호가목의 요건을 갖춘 경우

나. 제3호나목부터 라목까지의 요건을 갖춘 경우

② 제1항에도 불구하고 온라인서비스제공자가 제1항에 따른 조치를 취하는 것이 기술적으로 불가능한 경우에는 다른 사람에 의한 저작물등의 복제·전송으로 인한 저작권, 그 밖에 이 법에 따라 보호되는 권리의 침해에 대하여 책임을 지지 아니한다.
③ 제1항에 따른 책임 제한과 관련하여 온라인서비스제공자는 자신의 서비스 안에서 침해행위가 일어나는지를 모니터링하거나 그 침해행위에 관하여 적극적으로 조사할 의무를 지지 아니한다.

-공공데이터의 제공 및 이용 활성화에 관한 법률

제36조(면책) ① 공공데이터의 제공에 관하여 해당 공공기관과 그 소속의 공무원 및 임직원은 공공데이터의 품질(고의 또는 중대한 과실이 있는 경우는 제외한다), 제20조에 따른 공공데이터 목록의 제외, 제28조에 따른 공공데이터 제공중단 및 업무상 사유의 공공데이터 일시적 제공중단 등으로 인하여 이용자 또는 제3자에게 발생한 손해에 대하여 민사상·형사상의 책임을 지지 아니한다.

참 고 문 헌

국내 문헌

고형석, “개인정보침해와 손해배상책임의 원칙”, 「저스티스」, 통권 제145호, 2014.12

곽영임, “개인정보유출사건판결에관한연구”, 「전자상거래학회지」, 제15권 제2호, 2014

권영준, “해킹(hacking) 사고에 대한 개인정보처리자의 과실판단기준”, 「저스티스」, 통권 제132호, 2012.10

권영빈, 생체인식산업 활성화를 위한 법제도 조사연구, 정보통신부, 2004.

김민호, 개인정보처리자에 관한 연구, 성균관법학 제26권 제4호 (2014. 12)

김일환, “정보사회에서 생체정보의 보호에 관한 헌법적 연구”, 인권과 정의 통권 제344호, 2005. 4.

김일환, “미국의 생체정보보호법제에 관한 연구”, 인터넷법률 제31호, 2005.9.

김일환, “생체정보보호법제 정비방안에 관한 고찰”, 토지공법연구 제33집, 2006. 11.

김현경, ‘개인정보’와 ‘사물정보’의 규제 차별성에 관한 연구 - 사물인터넷 환경 하에서 서비스를 중심으로 -, 성균관법학 第27卷 第3號, 2015.09.

박영철, “생체정보의 보호”, 헌법학연구 제10권 제4호, 2004. 12.

연광석, 생체인식정보 보호에 관한 연구(비교법적 검토를 중심으로), 국회사무처, 2005.

이민영, “생체정보의 보호에 관한 법제도적 정책방향”, 정보통신정책 제16권 제21호, 2004. 11.

이부하, 환자의 의료정보권, 한양법학 제17집, 2005, 178면 이하;이인영, 개정 의료법의 환자의 개인정보 보호규정에 관한 법리적 고찰, 한림법학 Forum 제11권, 2002.

이상명, “의료정보화와 의료정보보호”, 법학논총 제25집 제1호, 한양대 법학연구소, 2008.

이한주, “개인의료정보보호법 제정의 필요성과 입법방향”, 한국의료법학회지 제22권 제1호, 2014.

이한주, 의료영역에서의 개인정보보호의 문제점과 해결방안, 한국의료법학회지 제20권 제2호, 한국의료법학회, 2012.

이호용, 전자의무기록의 보관과 신뢰할 수 있는 제3의 기관의 활용, 한양법학 제24권 제4집(통권 제44집) 2013.11.

이주연 외, ‘대형 대학병원의 의무기록관리 현황분석 및 개선방안에 관한 연구’, 한국기록관리학회지 제13권 제1호, 2013. 4. 20.

이진수, “디지털 헬스케어 플랫폼과 주요기업 동향”, 보건산업브리프 vol 140, 한국보건산업진흥원, 2014. 9.

이태희・정영철, 의료분야에서의 정보기술 융합연구 동향과 시사점. 보건복지포럼,(209), 2014.

이준형, “생체인식정보 보호에 관한 미국의 입법례와 논의상황”, 통상법률 제50호, 법무부, 2003. 4.

이창범, “생체 프라이버시 보호원칙에 관한 연구”, 인터넷법률 제31호, 2005. 9.

정연덕, “생체인식기술(biometrics)의 효과적 활용과 문제점”, 지식재산 21 제85호, 2004.

정연덕, “생체인식여권(bio passport)의 활용과 문제점”, 인터넷법률 통권 제24호, 2004.

조규범, 생체정보 보호를 위한 법제 정비방향, 국회도서관 입법지식데이터베이스, 2006.5.1.

조규범(역), 사이버스페이스 프라이버시, 진한M&B, 2004.

최경진, 빅데이터와 개인정보 , 성균관법학 제25권 제2호, 2013.

최경진 외, 사물지능통신 활성화를 위한 법・제도 연구, 방송통신위원회, 2010.

최민석, 하원규, 김수민. 2013. 만물지능인터넷 관점으로 본 초연결사회의 상황 진단 및 시나리오. IT 이슈 리포트 2013-12. 대전: 한국전자통신연구원.

최승원, 유럽과 미국의 개인정보 보호정책 동향연구, 정보통신부, 2004.

한국전산원, IT 발전과 개인정보보호 관련 법적 현안 분석, 2004.

해외 문헌

European Commission Joint Research Centre, Biometrics at the Frontiers: Assessing the Impact on Society Fore the European Parliament

Committee on Citizens′ Freedoms and Rights, Justice and Home Affairs(LIBE), Institute for Prospective Technical Studies, 2005.

National Science and Technology Council, Privacy & Biometrics Building a Conceptual Foundation, 2006.9.15.

內閣官房 IT總合戰略室 (2015). 概要 (個人情報保護法改正部分), 2015. 4. (http://www.soumu.go.jp/main_content/000355092.pdf)

北野晴人 (2015). 個人情報保護法は何を改正するのか, ZD Net Japan, 2015. 6. 29.(http://japan.zdnet.com/article/35066449/).

每日新聞 (2015). 改正個人情報保護法：成立「匿名」加工で賣買自由, 2015. 9. 4.

日本経濟新聞 (2015). 販賣・ 開發に個人情報活用, 2015. 8. 28.

情報法制研究會 第2回シンポジウム(2015). 改正個人情報保護法の國會審議分析, 2015. 6. 28. (http://www.dekyo.or.jp/kenkyukai/data/2nd/20150628_doc1.pdf)

● 저 자 소 개 ●

김 민 호

· 현 성균관대학교 교수
· 현 (사)개인정보보호법학회 회장
· 현 중앙행정심판위원회 위원

김 현 경

· 현 서울과학기술대학교 조교수
· 현 개인정보 분쟁조정위원
· 현 법제처 법령해석심의위원회 위원

김 선 아

· 현 숭실대학교 초빙교수
· 전 경기연구원 비상임연구위원
· 전 경희대학교 후마니타스 칼리지 외래교수

방통융합미래전략체계연구 지정2017-21

정보통신서비스 분야의 민감정보 유형과 보호방안 연구

2017년 11월 일 인쇄
2017년 11월 일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
서울특별시 종로구 세종로 20
TEL: 02-2110-1323
E-mail: webmaster@kcc.go.kr
Homepage: www.kcc.go.kr