嘉泉法學 제10권 제3호 (2017. 9. 30.)
Gachon Law Review Vol. 10 No. 3 (Sep. 30 2017)
pp.3~38
http://dx.doi.org/10.15335/GLR.2017.10.3.001

「정보통신망법」상 민감정보의 규율방안에 대한 검토

김 현 경*

< 차 례 >

* 서울과학기술대학교 IT정책전문대학원 교수, 법학박사.
이 연구는 서울과학기술대학교 교내연구비의 지원으로 수행되었습니다.

< 국문요약 >

민감정보는 '사생활 침해의 현저성' 등을 이유로 일반적인 개인정보와 달리 취급하도록 요구된다. 「개인정보 보호법」과 「정보통신망법」은 각각 민감정보에 대하여 규율하고 있으나 그 유형 및 기준이 조금씩 다르다. 특히 최근 정보통신서비스 제공과정에서 생체정보나 개인영상정보 등이 많이 활용되고 있는바 그러한 정보가 민감정보에 해당되는지, 그렇다면 일반적인 개인정보와 달리 특별히 규율할 필요성이 있는지에 대하여 검토할 필요가 있다. 또한 정보통신서비스 제공자와 이용자 간의 관계를 규율하는 「정보통신망법」은 개인정보에 대한 일반법이라 할 수 있는 「개인정보 보호법」과의 정합성, 해외 입법과의 조화, 정보통신서비스의 특수성을 반영하여 규율되어야 한다. 따라서 본 고에서는 정보통신서비스 제공과정에 있어서 민감정보의 활용쟁점을 검토한 후 현행법상 민감정보 규율 내용과 한계를 분석하고 「정보통신망법」상 민감정보 규율의 개선방안을 제안하였다. 그 주요내용으로 법률의 명확성, 개인정보 보호법과의 정합성 측면에서 "민감정보" 규정방식을 한정적 열거방식으로 수정할 것을 제안하였다. 또한 민감정보의 유형으로서 생체정보, 건강 · 성생활 · 성적 성향에 대한 정보, 유전정보 등이 추가되어야 하며, 민감정보 처리의 허용을 무조건 법률에 위임할 것이 아니라 일정한 기준에 부합하는 경우에만 다른 법률에서 처리할 수 있는 방안을 제안하였다. 또한 민감정보의 관리, 보관, 파기 등에 있어서 특칙 필요성을 검토하였다.

주제어 : 민감정보, 개인정보, 생체정보, 사생활 침해, 정보통신망법, 개인정보 보호법

Ⅰ. 서 론

"민감하다"라는 의미는 " ~ 한 자극에 빠르게 반응을 보이거나 쉽게 영향을 받음"을 의미한다.[1] 「개인정보 보호법」은 '민감정보'라는 표현을 사용하여

1) 국립국어원, 표준국어대사전.(http://stdweb2.korean.go.kr/search/List_dic.jsp, 2017.8.18. 확인).

‘사생활 침해의 우려’가 통상의 다른 개인정보에 비해 높은 정보로 정의하고 있으며(제23조), 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 “정보통신망법”이라 한다)은 ‘민감정보’라는 표현을 하고 있지 않으나, “개인정보의 수집 제한 등”이라는 조문 제목으로 “개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보”를 특별히 규율하고 있다. 또한 개인정보 중 ‘고유식별정보’에 대하여 「개인정보 보호법」은 민감정보로 분류하고 있지 않으나 그 불변성과 전파성 등에 비추어 특별히 규율하고 있다. 뿐만 아니라,‘주민등록번호’에 대하여도 ‘민감정보’라고 규율하고 있지는 않으나 그 고유성과 오남용·유출로 인한 사회적 폐해로 인하여 역시‘법령의 규정’에 의한 경우에만 그 처리를 허용하도록 특별히 규율하고 있다. 앞으로 유럽국가와의 교역에서 개인정보 처리와 관련해 우리나라에 미칠 영향이 지대할 것으로 예상되는 EU의 ‘일반정보보호규정(General Data Protection Regulation, 이하 “GDPR”이라 한다, 2018년 5월 28일 발효)’ 역시‘민감정보’라고 표현하고 있지는 않으나, ‘특수한 유형의 개인정보’에 대하여 다른 개인정보와 구분하여 특별히 규율하고 있다.

이처럼 통상의 개인정보와 다르게 특별히 취급하기 위해서는 그 타당성이 인정되어야 한다. 또한 다르게 취급하는 모든 개인정보를 ‘민감정보’라고 할 수 있을지에 대하여는 그 정보의 쓰임과 방식에 따라 달라질 수 있다. 따라서 개인정보 중에서도 특정 개인정보에 대하여 각별히 더 강력하게 규율하는 경우 그 기준과 한계가 정해져 있어야 한다. 현행법은 ‘사생활 침해의 현저성’을 공통된 기준으로 제안하고 있으나, 「개인정보 보호법」과 「정보통신망법」상 기준이 조금씩 다르며, 민감정보의 유형 또한 다르다.

특히 최근 정보통신서비스 제공과정에서 ‘생체정보’나 ‘개인영상정보’등이 많이 활용되고 있으며 그 특별한 규율필요성에 대하여 검토할 필요가 있음이 제기되고 있다. ‘개인영상정보’에 대하여는 이미 특별법 형태로 추진하고자 하는 정부안이 진행 중이며,[2] ‘생체정보’역시 그 민감성, 불변성 등을 이유로 특별히 규율하자는 주장이 제기되고 있다.[3]

---

2) 2016년 12월 16일 행정자치부는 「개인영상정보 보호법」 제정법률(안)을 입법예고 한 바 있다(행정자치부공고 제2016-370호).

3) 김일환외, 앞의 “생체인식기술 등 첨단정보보호기술의 이용촉진을 위한 법제도적 방안연구”,

따라서 이하에서는 정보통신서비스 제공과정에 있어서 민감정보의 활용쟁점을 검토한 후 현행법상 민감정보 규율 내용과 한계를 분석하여「정보통신망법」상 민감정보 규정의 개선방안을 제안하고자 한다.

Ⅱ. 정보통신서비스와 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 범주의 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 범주의 개인정보’(GDPR), ‘배려를 요하는 개인정보’(일본)등으로 표현되기도 한다.

우리나라에서 1994년 제정되어 1995년 1월 8일 시행된 「공공기관의개인정보보호에관한법률(법률 제4734호)」에 의하면 특별히 민감정보라는 표현으

한국정보보호진흥원, 2004.10월, 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.

로 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.[4] 이러한 부분이 후일 「개인정보 보호법」의 민감정보 규정의 전신이라고 할 수 있다. 따라서 「공공기관의개인정보보호에관한법률」은 ‘기본적 인권을 침해할 우려’를 민감정보의 기준으로 설정한 것으로 보인다.

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.”[5]고 결정하여 ‘개인정보자기결정권’의 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.[6] 이렇게 볼 때 개인정보의 보호의 헌법적 근거는 일반적 행동자유권에서 비롯

4) 예외적으로 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 수집이 가능하도록 규정하였다(공공기관의개인정보보호에관한법률 제4조 후문).
5) 헌재 2012. 12. 27. 2010헌마153.
6) 헌재 2015. 7. 30. 2014헌마340·672, 2015헌마99(병합); 헌재 2016. 3.31. 2015헌마688; 헌재 2016. 4. 28. 2012헌마630.

된 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‘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.

2. 정보통신서비스와 민감정보 활용

「정보통신망법」은 정보통신서비스 제공자의 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, ②정보제공자 및 ③정보제공매개자의 세 가지 행위주체가 모두 포함된다. ①은 인터넷접속사업자(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 융합 산업군으로 전망되기도 한다.[7] 다음으로 '불변성 · 영구성'이다. 주민등록번호나 비밀번호 등 각종의 개인정보는 변경이 가능하나, 생체정보는 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.[8] 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.[9] 따라서 '개인영상정보'를 포함한 생체정보는 '정보주체의 자유와 사생활을 현저히 침해할 우려'가 강하다.

대체적으로 정보통신서비스 제공자가 이러한 정보를 직접 수집하여 이용하는 경우는 본인 확인을 위한 인증의 경우가 대다수라고 할 수 있다. 이러한 본인확인을 위한 인증의 경우, 성인인증, 결제서비스, 기기인증 등에서 활용된다. 대면중심의 오프라인에서는 본인인증이 특별히 문제될 것이 없다. 주로 주민등록증/운전면허증 소지와 대면인식이 함께 이루어지므로 본인인증을 위한

---

7) 조규범, "생체정보보호를 위한 입법론적 대응방안", 국회도서관회보」, 제45권제9호(통권 352호), 50면.

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

9) 김일환, 전게논문, 359-360면.

특별한 기술적 이슈가 존재하지 않는다. 그러나 비대면인 온라인상에서는 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 SNS서비스제공과정에서 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 개인영상정보의 수집처리 가능성은 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 처리과정에서 개인의 사적으로 내밀한 영역까지 침해 가능하다. 이동형 영상정보처리기기의 운영과정에서 무분별하게 수집될 수 있는 개인의 전신 · 얼굴 · 옷차림새 · 활동 등의 개인영상정보는 개인의 프라이버시와 민감하게 관련

되며, 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 규율범위에서 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 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.[10] 최근 미국 식품의약국(Food and Drug Administration, FDA) 및 한국 식약처에서 의료기기로서의 규제를 받지 않아도 된다고 정의한 건강관리용 제품들, 일명 "웰니스"제품들도

10) 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.

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.[11]

생체정보 또는 건강정보들은 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.[12] 클라우드컴퓨팅을 이용하여 개인용 의료 히스토리(PHR, EMR)를 모으는 형태와, SNS서비스로 구성되어 이용자들이 자발적으로 자신들의 의료 기록 및 정보를 공유하는 형태가 있다.[13] 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 플랫

11) 이진수, 전게논문, 4면.
12) 이진수, 전게논문, 4~5면.
13) 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.

폼 사업자들이 이 영역에서 성과를 낼 수 있을 것으로 생각된다. 정보통신서비스제공자의 생체정보 활용과 관련된 부분이 바로 이 플랫폼 사업자 영역이라고 할 수 있다.[14]

Ⅲ. 민감정보 규율현황과 법적 쟁점

1. 국내 규율현황

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 일정한 업무수행을 위하여 처리하는 경우에는 민감정보로 보지 아니하므로,[15] 이 경우에는 정보주체로부터의 별도 동의 없이 처리가 가능하다.

---

14) 김수영·김현경, 디지털헬스케어환경에서 개인정보의 활용과 규제의 합리적 조화방안 연구, IT와 연구 제12집(2016. 2), 219~258면.

15) i)개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우, ii) 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우, iii) 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우, iv) 법원의 재판업무 수행을 위하여 필요한 경우, v) 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우 등이다.

현행「정보통신망법」은 '민감정보'라고 명확히 규율하고 있지 않다. 다만 제23조 제1항에서 '정보통신서비스 제공자는 ①사상, 신념, ②가족 및 친인척관계, ③학력(學歷)·병력(病歷), ④ 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」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」상 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. 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.

2. 국외 규율현황

(1) EU

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

GDPR은 우리나라처럼 "민감정보"라고 명백히 표현하고 있지 않으나 "특정

범주의 개인정보 처리(Processing of special categories of personal data)"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. 1995년 개인정보보호지침과[16] 비교하여 GDPR은 이러한 '특정 범주의 개인정보'의 범위를 상당히 확대하였다. 유전데이터, 자연인을 고유하게 식별하는 목적의 생체데이터, 자연인의 성적성향에 관한 데이터를 '특정 범주의 개인정보'에 추가하였다.[17]

또한 범죄경력 및 범죄행위에 관한 개인정보의 처리에 대하여는 제10조에서 별도로 정하고 있다.[18] 이러한 개인정보는 제9조의 특정범주의 개인정보에 해당되지 않으며, 공공기관의 규제 하에서만, 또는 회원국 법률에 승인되는 경우에만 처리 가능하므로 '특정범주의 개인정보' 보다 더 엄격하게 규율하고 있다고 볼 수 있다.

---

16) 1995년 개인정보보호지침은 '특별한 유형의 개인정보 처리(The processing of special categories of data)'(제8조제1항)에서 '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'고 규정하고 있다(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).

17) GDPR Article 9 특별한 유형의 개인정보 처리(Processing of special categories of personal data)
1. 인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 또는 노조가입을 드러내는 개인정보의 처리, 및 **유전데이터, 자연인을 고유하게 식별하는 목적의 생체인식정보,** 건강에 관한 데이터 또는 자연인의 성생활 **또는 성적 성향에 관한 데이터**의 처리는 금지되어야 한다.(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.).

18) 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.

GDPR은 특정 범주의 개인정보에 대하여 더 높은 보호를 받아야 하며[19] 그 이유는 '기본권과 자유 침해의 리스크'라고 밝히고 있다. 또한 각국의 자의적 입법에 의한 허용을 금지하기 위해 GDPR에서 구체적으로 허용되는 경우를 열거하고 있다.[20] 이렇듯 특정 범주의 개인정보 처리를 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 특정 범주의 개인정보 중 건강관련 정보의 처리가 가능한 '공중보건'의 범위에 대하여는 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.[21]

이러한 특정범주의 개인정보에 대하여는 처리금지가 원칙이며, ①정보주체의 명시적 동의 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 공

19) GDPR 전문 (53) '더 높은 수준의 보호를 받아야 하는 특정범주의 개인정보는'....으로 시작한다.

20) GDPR 전문 (51) 기본권과 자유와 관련해 특히 민감한 개인정보는 기본권 및 자유 침해의 리스크를 야기할 수 있기 때문에 구체적인 보호를 받아야 한다. 이러한 정보에는 인종 또는 민족출신을 드러나는 개인정보도 포함되어야 하며...(중략)...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 안 된다.

21) GDPR 전문(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.

개한 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(제9조제2항). 즉 제9조 제2항이 열거하고 있는 10가지의 예외 조항 중 하나에 명시적으로 해당하는 경우에만 이러한 정보를 취급할 수 있다. 제9조 제2항의 자세한 내용은 다음과 같다.

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[22] 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 건강 정보에 대해서는 더 엄격한 제한 기준을 설정할 가능성을 열어 두고 있다. 뿐만 아니라 대규모로 처리되는 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.[23]

---

22) 제9조제2항 (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 사회 복지 제도 및 서비스의 관리를 위해 처리가 필요한 경우.

23) GDPR 제35조 개인정보보호 영향평가
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 범죄 행위에 관련된 개인정보에 대한 처리.

(2) 독일

독일은 세계 최초의 개인정보보호법으로 제정된 1970년 Hessen 주의 정보보호법과 1974년 Rheinland-Pfalz 주의 정보남용금지법에 이어 1977년에는 "연방데이터보호법(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.[24]

이 법은 연방헌법법원의 인구조사판결, 정보통신기술의 발달, 연방데이터보호법의 적용을 통하여 제기된 문제점으로 인해 개정의 필요성이 제기되어 1990년 12월에 개정되었고, 2003년 1월 14일 유럽연합의 개인정보보호지침을 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)[25]고 규정하고 있다. 특히 특별한 종류의 개인관련 정보가(제3조제9항) 수집, 가공, 이용되어지는 경우에, 이러한 정보에 대해서는 명시적으로 동의가 행하여져야 한다(제4a조).[26] 일반적인 개인정보와는 달리 명시적 동의를 요구하고 있다.

(3) 일본

일본의「개인정보의 보호에 관한 법률」은 민간에 적용되는 일반법으로,

---

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

25) §3 Weitere Begriffsbestimmungen
(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugeh□rigkeit, Gesundheit oder Sexualleben.

26) §4a Einwilligung
(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung dar□ber hinaus ausdrücklich auf diese Daten beziehen.

2003년에 제정되고 2015. 9. 9. 최종 개정되었다. 그 개정취지는 빅데이터, 사물인터넷 등 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 경제사회와 풍요로운 국민생활의 실현에 이바지하는 것이라는 점 외에] 개인정보의 有用性을 고려하면서 개인의 권리이익을 보호하는 것을 목적으로 한다"고 밝히고 있다.

개정 전에는 일반적인 개인정보와 민감정보의 구분이 없이 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 정령(政令)으로 정하는 기술(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[27]는 이러한 "배려를 요하는 개인정보"를 '① 사전에 정

27) "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 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.

보주체의 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 대하여 협력할 필요가 있는 경우로서, 본인의 동의를 얻게 되면 당해 사무의 수행에 지장을 초래할 우려가 있는 때, ⑥ 당해 "배려를 요하는 개인정보"가 본인, 국가기관, 지방자치단체, 제76조 제1항 각 호에 열거된 자 및 그밖에 개인정보보호위원회규칙으로 정하는 자에 의해 공개되고 있는 경우, ⑦ 그밖에 전 각 호에 열거된 경우에 준하는 것으로서 政令으로 정하는 경우'에만 취득할 수 있다(법 제17조제2항).

다만 일본의 「개인정보의 보호에 관한 법률」은 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 방식(사후동의 방식)을 부분적으로 채택하고 있는 것이다. 그러나 '배려를 요하는 개인정보'는 이러한 opt-out의 적용대상에서 제외된다.

3. 법적 쟁점

민감정보의 규율과 관련된 법적 쟁점 우선 민감정보의 대상과 관련된 문제이다. 앞서 검토하였듯이 생체정보나 개인영상정보 등 현재 그 활용이 증대되면서 정보주체의 자유와 사생활의 현저한 침해가능성이 문제되고 있으나 현행법상 일반 개인정보로 취급되고 있는 것들에 대한 부분이다. 즉 개인영상정보를 포함한 생체정보를 일반적인 개인정보와 분리하여 '민감정보'에 포함시킬 것인가 하는 것이 문제된다. 일반적인 개인정보는 「정보통신망법」에 의해 i) 동의, ii)법률의 규정, iii)계약의 이행, iv)요금정산을 위해 수집, 이용할 수 있

으며, 「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 가능하게 된다.

다음으로 민감정보의 규정방식이다. 현재 「개인정보 보호법」은 민감정보의 유형에 대하여 한정적 열거방식을 채택하고 있다. 다만 사생활을 현저히 침해할 우려가 있는지 여부에 대한 해석의 여지가 크기 때문에 민감정보로 특별히 보호할 필요가 있다고 사회적 합의가 이루어진 정보를 상황에 맞게 규정할 수 있도록 대통령령에 부분적으로 위임하는 방식을 취하고 있다. 반면 「정보통신망법」은 민감정보의 유형을 예시적 방식으로 규정하고 있다. 즉 제시된 민감정보의 유형은 예시에 불과하며 해석에 따라 추가적으로 예시된 것 이외의 정보가 민감정보에 해당될 수 있다. 이러한 규율방식은 새로운 유형의 민감정보가 나타날 때 마다 법을 개정할 필요가 없으므로 법률의 현실적 응성에 있어서 일응 바람직한 부분이 있으나, '사생활 침해 및 개인의 권리·이익 침해'라는 기준의 해석의 다의성, 법원을 통한 해석을 구해야 한다는 불편함 등에 비추어 볼 때 수범자인 정보주체나 정보통신서비스제공자 입장에서는 불편하고 혼란스러울 수 있다.

세 번째 쟁점은 관리, 보관, 파기 등에 있어서 특칙 필요 여부이다. '관리'단계에서 정보통신서비스제공자는 '개인정보 보호책임자'를 지정하고, '개인정보처리방침'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 '민감정보'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 방지 조치, v) 컴퓨터바이러스에 의한 침해 방지조치, vi)기타 안전성 확보를 위하여 필요한 보호조치를 규정하고 있다. 민감정보에 대하여 이에 추가할 만한 법률상의 조치가 필요한지에 대한 검토가 이루어져야 한다.

Ⅳ. 「정보통신망법」상 민감정보 규율 개선방안

1. “민감정보” 규정방식의 수정

현재 「정보통신망법」은 민감정보에 해당되는지 여부를 판단함에 있어서 융통성을 발휘하기 위하여 ‘예시적 방식’으로 규정하고 있다. 예를 들어 최근 유출되어 논란이 되었던 숙박앱[28] ‘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 차별적 규율은 수집등 처리단계에서 이루어지며, 현재 침해에 대한 가벌성은 동일(5년 이하의 징역 또는 5천만원 이하의 벌금, 제71조 제1항 제1호, 제2호)하다. 따라서 수집 등 처리단계에서 차별화할 수 있는 정보가 아닌 한 민감정보로 규율 실익이 없다.

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

28) 2017년 3월 숙박업체 O2O 앱 '여기어때'는 최근 발생한 내부 데이터베이스(DB) 해킹으로 고객 91만 명의 이용자명, 휴대전화번호와 숙박 이용정보 323만 건이 유출됐다고 밝힌 바 있다. 해커는 빼낸 정보를 이용해 피해자들에게 민감한 내용의 문자메시지까지 보냈다. 확인된 피해만 총 4천여 건이다. 해커는 한 문자 발송 업체의 시스템도 뚫은 뒤 “○월○일 ××(숙박업소명)서 즐거우셨나요”라는 내용의 문자를 전송했다. 더불어 해커는 '여기어때' 운영사인 위드이노베이션에 이메일을 보내 수 억원의 금전(비트코인)을 요구하기도 했다.

수 있으나 기본취지는 한정적 열거방식을 취하는 것이 바람직하다.

2. 생체정보의 민감정보 해당성

우선 현행법상 생체정보는 민감정보에 해당된다고 보기 곤란하다. 앞서 언급하였듯이 한정적 열거방식을 채택하고 있는「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 친인척관계, 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.

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 포함되지 않는다고 보는 것이 타당하다. 생체정보는 민감정보에 해당되지 않으므로 개인정보의 수

집 · 이용, 수집제한, 제3자 제공, 관리, 보호조치, 파기 등과 관련하여 통상의 개인정보와 동일하게 규율을 받는다.

단순히 서비스제공과정에서 처리되는 모든 생체정보를 민감정보를 규율한다면, 전혀 사생활 침해적 요소나 행동의 자유침해의 위험성이 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 볼 수 있다. GDPR에서도 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술적 수단을 통해 처리되는 경우에 한해서만 특수한 범주의 개인정보에 해당되기 때문에, 민감정보로 분류되지 않는다.[29] 즉 본인을 인증 또는 확인하기 위한 수단으로 사용되지 않는 한 생체정보는 민감정보로 규율하지 않는 것이 바람직하다.

이렇게 규율할 경우 각종 디지털헬스케어 서비스를 통하여 실시간 이동되는 심박정보나 맥박정보 등은 민감정보에서 제외되며, 페이스북 등 각종 SNS나 플랫폼서비스를 통해 이용되는 개인영상정보도 민감정보에서 제외된다. 따라서 민감정보에 해당되는 생체정보가 되기 위해서는 '개인정보로서 얼굴, 지문 등 개인의 신체적, 생리적, 행동적 특성에 관한 정보로서 개인을 인증 또는 확인하기 위하여 특별히 기술적으로 처리한 정보'여야 한다. 따라서 일반적인 개인정보인 생체정보와 구분하기 위해 '생체인식정보'라 칭하는 것이 바람직하다. 즉 민감정보에는 생체를 '인증 혹은 확인 대상'으로 이용하려는 목적성이 포함되어 있다는 점을 전제로 볼 때 일반적인 개인정보로 인정되는 '생체정보'와 구분되도록 '생체인식정보'라는 용어가 바람직하다.[30]

---

29) GDPR 전문 (51).

30) 용어와 관련하여 '바이오정보', '바이오인식정보', '생체정보', '생체인식정보' 등의 용어가 제안된다. 생체정보는 '생체실험'이 연상되는 등 부정적 어감이 존재하며, 바이오정보는 유전정보, 건강정보 또는 의료정보 등으로 오해 가능하다는 의견도 있을 수 있다. 그러나 생체정보와 '생체실험'의 연상에 대하여는 입증된 바 없으며, '바이오'는 외국어로서 국어기본법

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.

3. 그밖에 민감정보의 대상이 되는 개인정보 유형

(1) 인종이나 민족적 출신을 드러내는 정보, 정치적 견해

과거 우리나라는 단일민족으로 구지 인종이나 민족을 드러내는 정보가 개인에게 민감성을 가지지 않았다. 그러나 다문화 가족의 확산, 해외 노동인구의 국내 유입 등으로 다른 피부색과 다른 얼굴 형태를 가진 인종에 대한 사회적 편견과 차별이 심각한 사회문제로 대두되고 있다. 따라서 이제 인종이나 민족정보를 민감정보로 규율할 필요가 있다고 본다.

우리나라는 「개인정보 보호법」,과 「정보통신망법」에서 '사상 · 신념'을 민감정보로 규율하고 있으며, 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.

이나 「법령 제정 · 개정 업무 지침」에 의해 한글전용의 원칙을 규정하고 있는바 타당하지 않다.

(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, 예시방식을 폐지하고 '한정적 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 안 되는 정보이며, 특히나 사생활 침해와 관련이 깊은 민감성이 강한 정보이다. 「정보통신망법」에서 민감정보로 추가할 필요가 있다. '건강정보(data concerning health)'는 의료 서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신건강에 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

「개인정보 보호법」은 '범죄경력에 관한 정보'로 GDPR은 '범죄유죄판결 및 범죄행위에 대한 정보'를 민감정보에 포함하고 있다. '범죄유죄판결 및 범죄행위'는 당연히 '범죄경력'에 해당되므로 현행 「개인정보 보호법」은 더 넓은 개념이다. 「정보통신망법」상 '기타 사회활동 경력'에 해당될 수 있으나, 규정의 모호성, 불확실성, 열거주의의 폐지 등을 전제로 볼 때'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 타당하다.

4. 민감정보 처리 기준의 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 규정으로 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 경우이다(법 제22조 제1항). 또한「개인정보 보호법」의 보충적 적용에 의해 ' ⑤ 정보주체 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))' 개인정보를 수집, 이용할 수 있다. 그러나 「정보통신망법」상 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 "명시적 동의" 수준을 요구하고 있으며, 반드시 별도의 동의일 것을 요구하고 있지 않으므로 구지 「정보통신망법」의 동의방식을 「개인정보 보호법」처럼 "별도의" 동의로 개정할 필요는 없다고 본다. 「개인정보 보호법」은 민감정보처리의 허용 근거로서'명시적 동의'의 일 유형으로'별도의 동의'로 규율하고 있는 듯하다. 정보통신서비스 제공자가 서비스 과정에서의 동의의 방식은 대체로 웹페이지 창을 통한 고지 및 클릭을 통해 이루어지는 바'별도의 동의'를 구하도록 하는 것은 동의 클릭을 하나 더 추가하는 것에 불과하다. 또한 현행 정보주체의 동의가 주로 정보통신 서비스 제공과정에서 깨알같은 글씨의 웹페

이지 클릭을 통해 습관적, 관행적으로 이루어지고 있음에 비추어 볼 때 이러한 별도의 동의 방식이 유용한지에 대하여는 의문이다. 따라서 '별도의 동의'로 규정하기 보다는 정보주체의 명백한 인지와 표시를 전제로 하는'명시적 동의'로[31] 규정함이 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 타당하다고 생각된다. 또한 '법률의 규정'에 의한 민감정보의 처리 허용은 각 영역의 입법활동이 모두 개인정보 보호를 위해 초점이 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 "법령"에 의해 허용되는 경우에 대한 구체적 기준이 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. 그러나 이러한 기준은 정보통신서비스 제공과정에 있어서 수집처리 근거이기 보다는 개인정보 수집처리에 있어

31) GDPR는 일반적인 '동의'의 개념에 대하여 용어정의에서 "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 있다. 그러나 특정 범주의 개인정보에 대하여는 '명시적 동의(explicit consent)'를 요구하고 있으나, '명시적 동의'에 대하여는 별도로 용어 정의하고 있지 않다. 다만 영국에서 발간한 GDPR 설명 보고서에 의하면 진술에 의해 확인될 수 있으면 '명시적 동의'이나, 정보주체의 행위로부터 암시되는 동의는 명시적 동의라고 볼 수 없다. 즉 '동의'의 용어정의에 의하면 '동의'가 표시되는 방법으로 '진술' 또는 '긍정적 행위' 두 가지 이나, 명시적 동의가 되기 위해서는 반드시 '진술'에 의하여야 하며, '긍정적 행위' 만으로는 부족하다(UK Information Commissioner's Office, Consultation: GDPR consent guidance pp. 24~25 (March 2017) 참조.).

서 일반적 사항에 해당되므로 「정보통신망법」의 개정 보다는 「개인정보 보호법」의 개정을 통해 반영되는 것이 바람직하다.

5. 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. 현재 우리나라는 「개인정보 보호법」에서 개인정보 영향평가를 규율하고 있으며, 그 의무 시행은 공공기관에만 적용된다. 민간 사업자인 정보통신서비스제공자가 대규모 민감정보를 처리하는 경우 개인정보영향평가를 실시하도록 법률을 개정하여야 하는지가 문제될 수 있다. 정보통신서비스 제공자는 민감정보를 직접 수집 등 처리하는 경우도 있으나, 이용자의 민감정보 처리를 서비스를 통해 매개만 하는 경우도 다반사다. 따라서 이 부분에 대하여는 사업자게 미치는 영향, 개인정보 침해가능성 등을 고려하여 좀 더 신중한 접근이 필요하다.

‘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 특정, 세분화 할 수 없다. 따라서 파기의 기술적 조치는 지침 또는 가이드라인을 통해 기술변화에 연동하여 구체화 하는 것이 바람직하다.

‘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 보호조치를 규

정하고 있다. 생체인식정보의 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.

Ⅴ. 결 론

향후 개인정보 제도를 둘러싼 첨예한 쟁점은 합리적 활용과 보호의 조화라고 할 수 있다. 빅데이터, 4차산업혁명 등에서 제시하는 대부분의 IT서비스는 개인정보의 활용 없이는 불가능하다. 따라서 사생활 또는 자유 침해 위험성이 적은 일반 개인정보에 대하여는 지나친 보호보다는 합리적 활용과 관련된 제도적 방안이 고민될 필요가 있다. 그러나 현재 민감정보라 불리 우는 특수한 유형의 개인정보에 대하여는 사생활 및 자유 침해의 현저한 위험성이 전제된 것이니 만큼 그 보호의 체계화가 중요하다. 특히 정보통신서비스 제공자와 이용자 간의 관계를 규율하는 「정보통신망법」은 개인정보에 대한 일반법이라 할 수 있는 「개인정보 보호법」과의 정합성, 해외 입법과의 조화, 정보통신서비스의 특수성을 반영하여 규율되어야 한다. 그러한 규율방안으로서 본 연구의 결과를 요약하면 다음과 같다.

첫째, 「정보통신망법」상 민감정보의 대상을 구체화하고 예시규정에서 열거규정으로 개정하는 것이 타당하다. 「개인정보 보호법」과의 정합성 차원에서 또한 국외 규율방식에 비추어 볼 때 한정적 열거방식을 취하는 것이 바람직하다. 열거대상의 '민감정보'로는 ①인증 또는 확인목적의 생체정보(즉 생체인식정보)뿐만 아니라 ②사상·신념, ③노동조합·정당의 가입·탈퇴, ④정치적 견해, ⑤건강·성생활·성적 성향을 드러내는 정보, ⑥유전정보, ⑦범죄경력에 대한 개인정보를 포함시킬 필요가 있다. 다만 기존에 민감정보로 규율되

었던 '학력'은 민감한 개인정보의 오남용으로 인한 문제라기보다는 사회적 차별의 문제라고 할 수 있고, 정보통신서비스 제공과정에서 '학력'에 대한 개인정보의 처리가 민감하게 작용될 여지는 극히 제한적이므로 삭제하는 것이 타당하다고 생각된다.

둘째, 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 위한 목적의 생체정보 즉 생체인식정보'로 제한하여 규정하는 것이 바람직하다.

셋째, 현행법에 의할 경우 민감정보는 '사전동의'와 '법률에 특별한 규정'이 있는 경우에만 수집 및 이용이 가능하다. 「개인정보 보호법」은 민감정보에 대하여 다른 개인정보와 구분하여 별도의 동의를 받도록 규율하고 있으나, 「정보통신망법」은 이러한 규율이 없는 바, 다른 개인정보와 함께 일괄적으로 동의를 받아도 무방하다. GDPR에서도 "명시적 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 강화해야할 실익이 없는 한 이는 기본법 수준에 부합하는 것이 타당하다고 생각된다. 그리고 민감정보의 취지를 고려하지 않은 자의적 개별 입법에 의한 민감정보의 처리를 불허하기 위해 일정한 기준에 부합하는 경우에만 법령에 의해 민감정보의 처리가 가능 가능하도록 규율하는 것이 타당하다. 사회보장, 공중보건, 공익적 기록보존 · 연구목적 · 통계, 소송상 공격방어수단으로 처리되는 경우 등이 기준으로 제시될 수 있다.

넷째, 관리, 보관, 파기 등에 있어서 민감정보에 대한 특칙은 불필요하다. 다

만 GDPR과의 관계에서 대규모 민감정보의 처리에 대하여 개인정보 영향평가의 실시를 규정하고 있는바 국내법에의 도입에 대하여는 그 필요성, 사업자에게 미칠 영향 등을 고려한 좀 더 신중한 검토가 필요하다. 그밖에 파기의 기술적 기준, 기술적·관리적 조치에 대한 특별한 사항은 기술발전의 현실적응성 등을 고려할 때 고시나 지침을 통해 구체화하는 것이 바람직하다.

【참 고 문 헌】

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

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

권영빈, 생체인식산업 활성화를 위한 법제도 조사·연구, 정보통신부, 2004.

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

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

김수영 · 김현경, 디지털헬스케어환경에서 개인정보의 활용과 규제의 합리적 조화방안 연구, IT와 法연구 제12집(2016. 2)

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

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

, “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.

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

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

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

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

정연덕, “생체인식기술(biometrics)의 효과적 활용과 문제점”, 지식재산 21 제85호, 2004. 7.

정연덕, “생체인식여권(bio passport)의 활용과 문제점”, 인터넷법률 통권 제24호, 2004. 7.

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.

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.

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.

Kenneth P. Nugar, “Biometric Applications: Legal and Societal Considerations,” <http;//www.engr.sjsu.edu/biometrics/publications_consideration.html>.

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

内閣官房 IT総合戦略室 (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/).

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

日本経済新聞 (2015). 販売· 開発に個人情報活用, 2015. 8. 28.

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

【Abstract】

Study on the examination of regulation measures of sensitive data in "Act On Promotion Of Information and Communications Network Utilization and Information Protection, etc."

Kim, Hyun Kyung
Professor of Seoul National University of Science and Technology,
Ph.D. in Law

Sensitive data is required to be handled differently from general personal data because of the 'seriousness of privacy invasion' and so on. 「The Personal Information Protection Act」 and 「Act On Promotion Of Information and Communications Network Utilization and Information Protection, etc.」 regulate sensitive data, respectively. However, the types and standards of sensitive data defined by each law are slightly different. In particular, biometric data and personal image data are widely used in the process of providing information and communication services. It is necessary to examine whether such data corresponds to sensitive data, and if so, it is necessary to specially regulate unlike general personal data. In addition, 「Act On Promotion Of Information and Communications Network Utilization and Information Protection, etc.」 regulates providers of information and communications services and users. This Act shall be governed by the compatibility with the 「The Personal Information Protection Act」, which is the general law of personal data, harmonization with foreign legislation, and the specificity of information and communication

services. Therefore, this study examines the issues of using sensitive data in the process of providing information and communication services, analyzes the current status and limitations of sensitive data discipline, and suggests ways to improve sensitive data discipline in 「Act On Promotion Of Information and Communications Network Utilization and Information Protection, etc.」. In the main content, it is suggested that "sensitive data" should not be defined in an illustrative manner but in a limited enumeration method in terms of clarity of law and compliance with the Personal Information Protection Act. In addition, as a type of sensitive information, biometric information, information on health, sexual life, sexual orientation, and genetic information should be added. Currently, sensitive information processing is permitted without any condition if it is based on the law, but it suggests a way to deal with it only if it meets certain criteria.

Key Words : Sensitive data, Personal data, Biometric data, Invasion of privacy, 「Act On Promotion Of Information and Communications Network Utilization and Information Protection, etc.」, 「The Personal Information Protection Act」.

° 투고일 : 2017. 8. 18.
° 심사일 : 2017. 9. 18.
° 게재확정일 : 2017. 9. 26.