데이터 이용과 인격권 보호

-개정 데이터 3법에 따른 개인정보 이용과 불법행위책임-

윤 태 영 (아주대 법전원 교수)

Ⅰ. 머리말

인터넷 서비스를 이용하기 위해 어떤 사이트에 가입하는 순간, 우리는 이미 '되돌아갈 수 없는 루비콘 강(Digital Rubicon)'을 건너게 된다.[1] 즉 이용자들은 필연적으로 개인정보를 제공하게 되고 이용자들이 제공한 빅데이터가 자신의 삶을 지배하게 된다는 의미이다. 각 회사들은 수집한 개인정보를 통해 개개인의 관심사를 추적 분석하여 맞춤형 광고나 서비스를 제공하는 등 편리함을 제공하기 때문에, 이용자의 입장에서도 그 편리함을 누리는 것은 큰 장점이 아닐 수 없다. 그러나 그러한 이용이 많을수록 그만큼 자신의 개인정보가 노출되고 프라이버시가 침해될 위험이 크다. 더구나 대부분의 경우 이용자는 자신의 어떤 개인정보가 어떻게 수집되고 거래되어 활용되는지 추측하기도 힘들다. 따라서 인터넷 이용자는 본인이 원치 않아도 개인정보 보호와의 싸움에 직면하게 된다.

지금까지 데이터의 무분별한 활용을 막고 개인정보의 노출로 인한 피해로부터 정보 주체를 보호하기 위해 개인정보 보호법제가 역할을 해왔다. 그런데 최근에는 4차 산업혁명 시대의 신성장동력인 빅데이터 산업의 발전에 맞추어 이러한 보호법제가 큰 변화에 직면하고 있다. 종전에는 개인정보 보호에 보다 비중을 두어 왔다면 최근에는 개인정보를 최대한 활용할 수 있는 방향으로 패러다임을 전환한다는 것이다. 2020년 1월 9일 국회에서 이른바 '데이터 3법'이 통과된 것도 이러한 차원에서 이루어진 입법적 조치이다.

'데이터 3법'은 「개인정보 보호법」, 「신용정보의 이용 및 보호에 관한 법률(이하 '신용정보보호법'이라 함)」, 「정보 통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 함)」의 개정법이다. 종전과 달리 특히 주목할만한 것은 이들 법(이하 '데이터 3법 개정법'이라 함)이 '가명처리'를 통해 생성된 '가명정보'의 활용에 대한 법적 근거를 마련하는 등 최대한 데이터를 활용할 수 있는 근거를 마련했다는 점이다. 특히 가명정보를 통해 개인정보의 식별성을 낮춤으로써 개인정보의 활용을 막고 있는 규제완화를 도모하겠다는 것이 핵심이다. 이러한 입법적 조치는 우리나라에서 처음 시작된 것이 아니라 유럽연합(EU), 미국, 일본 등 국제적인 흐름에 보조를 맞춘 것이다.

이러한 입법 조치들은 기존의 엄격한 보호에만 머물렀던 개인정보 보호 법제를 빅데이터 시대에 맞췄다고 평가받고 있다. 이번 개정으로 데이터산업 활성화의 촉매제 역할을 하게 되어

1) Jeff Chester, Cookie wars: how new data profiling and targeting techniques threaten citizens and consumers in the 'big data' era. In: Gutwirth S et al (eds) European data protection: in good health? Springer, Dodrecht (2012) p.58.

개인정보 보호와 활용의 균형추를 맞췄다는 것이다.[2] 그러나 개인정보를 활용하면 할수록 그만큼 개인정보의 침해 위험이 커지는 것은 당연하다. 데이터 3법이 통과하기까지 가장 많이 참고되고 언급된 것이 EU의 일반개인정보보호규정(GDPR)인데, 데이터 3법에서 개인정보 활용은 GDPR 수준으로 허용했지만, 개인정보 보호장치와 관련해서는 GDPR에 비해 현격히 부족한 수준이라고 비판받고 있다.[3]

개인정보의 이용에 대해 스스로 결정하는 것 자체가 인격의 발현이라고 볼 수 있으므로,[4] 제3자에 의해 개인정보가 다양하게 활용될수록 그만큼 인격권이 침해될 여지는 커지게 된다. 주지하는 바와 같이, 개인정보 보호와 관련하여 미국에서는 정보 프라이버시권의 개념을 발전시켰고, 독일의 경우 일반적 인격권의 한 내용으로서 정보자기결정권 내지 개인정보 자기결정권을 인정하였다.[5] 특히 새로 개정된 데이터 3법은 민간 분야에서의 정보의 적극적인 활용의 길을 열어주었고, 빅데이터의 활용은 개인의 인적사항 외에도 금융·위치·의료·재산 등의 각종 정보를 포함하고 있으므로, 개정법에 따라 인격권 침해로 인한 불법행위책임에 대한 분쟁의 여지는 그만큼 더 커질 것으로 예상된다.

그렇다고 하여 이제 와서 개인정보 보호만을 강조하거나 빅데이터 시대 이전의 상태로 되돌릴 수도 없다. 오히려 바람직한 빅데이터 활용을 도모하면서도 개인의 인격권 침해를 최소화하고 역기능을 억제하도록 법적으로 대응해 나가는 것이 필요하다. 이 점과 관련하여 민법학에서는 개인정보를 활용하는데 있어 어느 경우에 불법행위책임을 인정할 것인지 그 판단기준을 명확하게 제시할 필요가 있다고 생각된다. 종래 개인정보 침해에 관련하여서는 주로 유출로 인한 인격권 침해에 대한 불법행위책임 논의가 주를 이루어 왔는데 비해[6], 익명이나 가명처리 등으로 활용할 경우에 대한 논의는 거의 없기 때문이다. 개인정보의 보호와 개인정보의 활용 사이의 조화를 꾀할 수 있는 비교형량에 의한 적절한 기준을 제시하지 못한다면 개인정보 침해의 두려움으로 인하여 정보의 활용도 적절히 이루어지지 못하고 법제도 개혁의 목적에 부흥하지 못할 수 있다. 따라서 이하에서는 이러한 관점에서, 개정된 데이터 3법에 따른 개인정보의 이용에 있어서의 불법행위책임, 나아가 인격권의 보호방안에 대해 논하고자 한다.

Ⅱ. 개정 데이터 3법의 주요내용과 국제적 동향

1. 개인정보의 구체화 및 가명정보의 도입

현행 개인정보 보호법에서 규정하는 개인정보의 개념 정의에 따르면, 기본적으로 개인의 식별가능성을 그 주된 개념적 징표로 하되, 해당 정보 그 자체로부터의 직접적인 식별성이 인정되는 경우(개인 식별 정보)뿐만 아니라, 다른 정보와 쉽게 결합하여[7] 식별성이 인정되는 경우(개인 식별가능 정보)[8]를 포함하고 있다.[9] 그런데 여기서 식별가능성이라는 추상적 기준만을

2) 박주희, “민간부문 개인정보보호를 위한 약관 통제”, 성균관법학 제32권 제1호, 2020, 32면.
3) 김윤정, “개인정보를 위협하는 데이터 3법”, 월간 한국노총 통권 558호, 2020, 28면.
4) 권태상, “개인정보 보호와 인격권-사법(私法) 측면에서의 검토”, 법학논집 17권 4호, 2013, 93면.
5) 이에 관한 자세한 내용에 대해서는, 권태상, 전게논문, 77면 이하 참조.
6) 이와 달리 퍼블리시티권을 소재로 인격권 침해에 대한 부당이득반환 문제를 논한 문헌으로는, 안병하, “인격권 침해와 부당이득반환-침해구제의 측면에서 본 퍼블리시티권 도입 불필요성” 민사법학 제68호, 2014, 495면 이하 참조.
7) ‘쉽게 결합하여’의 의미는 결합 대상이 될 정보의 입수가능성과 결합가능성을 따진다고 한다(김태선, “자율주행과 데이터보호”, 비교사법 제26권 제4호, 2019, 11면.
8) ‘개인 식별 정보’를 ‘직접식별 개인정보’로, ‘개인 식별 가능 정보’를 ‘간접식별 개인정보’로 표현하기

가지고 어느 정보가 이에 해당하는지 논란이 있어 왔다.[10] 이에 개정된 「개인정보 보호법 개정법」은 개인정보에 대하여, “살아 있는 개인에 관한 정보로서, ① 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보, ② 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보, 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.”고 규정하고 있다(개정법 제2조제1호). ①의 정보는 종전의 개인식별 정보를, ②는 개인 식별 가능 정보를 보다 구체화한 것이다. 여기에 개정된 데이터 3법에서 가장 중요한 내용으로 평가받는 가명처리와 가명정보라는 개념을 추가하였다.[11] 즉 ‘가명처리’에 대하여는 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 것이라고 하고 있고, ‘가명정보’에 대해서는 가명처리 함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보라고 하고 있다(개정법 제2조제1호다목 및 제1호의2).

개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집 목적을 달성할 수 있는 경우, 먼저 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다(개정법 제3조제7항). 가명정보는 복원가능성이 있기 때문에 개인정보에 대한 규제가 적용될 여지가 남아 있는데 반해, 익명정보는 복원이 불가능해 법적으로 개인정보가 아닌 것으로 보고 있다.[12] 한편, 개정 신용정보보호법도 가명처리 및 가명정보에 대한 규정을 신설하였다. 추가정보를 사용하지 않고는 특정 개인을 알아볼 수 없도록 처리(가명조치)한 개인 신용정보로서 가명정보의 개념을 도입하고 있다. 이에 반해, 개정된 정보통신망법은 종전에 개인정보보호법과 다소 다르게 규정하고 있던 제2조제1항제6호[13]를 삭제함으로써 개인정보에 관한 정의 조항을 개인정보 보호법으로 일원화하였다.[14]

개정법은 기존에 비판받던 ‘쉽게 결합’에 관한 기준을 ‘다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려’라고 구체화한 한편, 가명정보 개념을 도입하여 개인정보의 이용을 활성화하고자 한 것이다.

2. 개인정보 이용을 위한 정보주체의 사전 동의제도 개정

개인정보 자기결정권을 보호하기 위해서는 먼저 자신의 개인정보가 어떻게 이용되는지 파악

도 한다(권건보, “유비쿼터스 시대의 개인정보 침해와 법적 대응방안”, 공법연구 제32집 제5호, 2004, 164면 참조).

9) 김정현, “빅데이터 시대의 개인정보 보호법제 개선방안”, 법학논총 제46집, 2020, 117면.

10) 문재완, “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 2014, 72면 등 참조.

11) 비식별화 대신에 가명처리 또는 익명처리라는 용어로 통일할 필요가 있다는 입장으로는 백승엽·김일환, “개인신용정보 비식별조치의 내용과 한계에 관한 연구”, 성균관법학 제29권 제4호, 2017, 91면.

12) 전승재·주문호·권헌영, “개인정보 비식별 조치 가이드라인의 법률적 의미와 쟁점”, 정보법학 제20권 제3호, 2016, 269-270면.

13) “개인정보”를 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함)”로 정의하고 있다.

14) 당초 ‘정보통신망법 개정안’은 “가명처리”와 “가명정보”에 관한 규정을 두고 있었으나, 과학기술정보방송통신위원회는 2019년 12월 4일 기존의 개정안을 본회의에 부의하지 않고, 정보통신방송법안 심사소위원회가 마련한 대안을 위원회안으로 제안하기로 의결하였다. 대안이 개정법으로 통과되었고, 이에 따르면 「정보통신망법」에 규정된 개인정보 보호에 관한 사항을 삭제하고 「개인정보 보호법」으로 이관하였다. 따라서 「정보통신망법」은 더 이상 개인정보 보호에 관한 규정을 두지 않게 되었다.

할 수 있도록 하는 것이 전제되어야 한다. 이를 위한 제도가 바로 사전 동의제도이다. 개인정보 보호법상 개인정보의 수집·이용과 제공, 목적 외 이용·제공, 그리고 민감정보 처리를 가능하게 하는 조항마다 그러한 처리의 전제 조건 중 하나로 정보주체의 동의를 요하는 것도 정보주체의 개인정보 자기결정권을 최대한 존중하려는 데에 있다. 개정된 개인정보 보호법도 현행 개인정보 보호법과 마찬가지로, 개인정보 처리자가 개인정보를 수집·이용하거나(제15조제1항), 제3자에게 제공하는 경우(제17조제1항) 원칙적으로 사전 동의를 요구하고 있다. 사전 동의제도가 개인정보 보호의 기본 규제방식인 셈이다. 따라서 빅데이터 수집과정에서 수집 대상인 정보가 이미 개인 식별 정보 혹은 개인 식별 가능 정보에 해당하는 경우에는 원칙적으로 동의의 대상이 된다고 할 것이다. 다만 이에 대해서는 예외규정을 두고 있다. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 등이 이에 해당한다. 한편, 정보주체의 사전 동의를 받은 경우, 다른 법률에 특별한 규정이 있는 경우, 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우 등에는 예외적으로 목적 외의 용도로 이용하거나 제3자에게 제공하는 것이 허용된다(제18조 제2항).

그런데 빅데이터의 이용 및 활용의 특성상 현행법에서 요구하는 사전 동의를 전제로 개인정보 빅데이터의 제3자 제공은 빅데이터의 특성과 상충하므로, 사전 동의제도가 빅데이터의 이용 및 활용을 하는 데 장애요인이 될 수 있다는 비판이 있어 왔다.[15] 따라서 개정법에서는 정보주체의 동의 없이 개인정보의 수집·이용·제공이 가능하도록 그 활용범위를 확대하였다. 개인정보 처리자는 '당초 목적과 합리적으로 관련된 범위'에서 정보주체의 불이익 발생여부, 안전성 조치여부 등을 고려해 동의를 받지 않고 개인정보를 처리할 수 있게 되었다. 데이터산업 활성화에 대비할 수 있도록 동의 및 처리의 유연화가 이루어진 셈이지만, 그만큼 개인정보 자기결정권 침해의 가능성은 훨씬 커졌다고 할 수 있다.

나아가 가명정보의 경우에는 개인정보 처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 처리할 수 있다. 다만, 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 안 된다(개정법 제28조의2). 그리고 개인정보 처리자는 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령이 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용 및 제공할 수 있다(개정법 제15조 제3항 및 제17조 제4항). 한편 개정된 신용정보보호법도 통계작성(시장조사 등 상업적 목적의 통계작성을 포함), 연구(산업적 연구를 포함), 공익적 기록보존 등을 위해서는 가명정보를 신용정보주체의 동의 없이도 이용하거나 제공할 수 있도록 함으로써 금융분야에서 빅데이터 분석·이용을 활성화하도록 하고 있다(개정법 제2조제15호·제16호 및 제32조제6항제9호의2·제9호의4).

3. 국제적 동향

개인정보를 이용한 데이터 이용의 활성화 추세는 우리나라에 국한된 문제가 아닌 세계적인 추세라고 할 수 있다. 이에 관하여 살펴보면 다음과 같다.

---

15) 김정현, 전게논문, 122면.

(1) 유럽연합(EU)의 '일반 개인정보 보호규정'(GDPR)

EU에서는 1995년 제정된 '개인정보 보호지침(Data Protection Directive, 95/46/EC)'을 대체하여 2018년 5월 25일부터 '일반 개인정보 보호규정(GDPR, General Data Protection Regulation)'이 발효되었다.[16] 지침과 달리 규정은 EU 회원국들에게 일괄 적용되어 개별 회원국 차원의 입법이 필요치 않다. 사업체로 통칭되는 기업이나 기관이 EU 주민들의 개인정보를 수집, 처리, 이용, 공유하거나, 웹사이트를 방문하는 EU 주민들의 온라인 행태를 추적하고 분석한다면 국적이나 지리적 위치와 상관없이 GDPR이 적용되므로, 우리나라에 있어서도 이 GDPR이 주는 영향은 크다.

1) 개인정보 구체화 및 가명처리

GDPR이 적용되는 개인정보는 '식별된 또는 식별 가능한 개인(정보주체)과 관련된 일체의 정보'를 의미한다(제4조제1항). 이름, 주소, 식별 번호, 위치정보, 온라인 식별자, 생체 인식 정보, 문화 정보, 유전자 정보 등을 비롯해, 유럽사법재판소(CJEU)의 'Breyer' 사건[17]을 계기로 그간 논란을 빚어 왔던 인터넷 IP주소도 개인정보로 분류된다. 또한 '민감 개인정보'와 '특정 범주 개인정보'에 대해서도 규정하고 있는데, "인종이나 민족, 정견, 종교나 철학적 신념, 노조 가입 여부가 드러나는 개인정보의 처리 및 유전자 정보, 개인을 특정해 식별할 수 있는 생체정보, 건강 정보, 성생활, 성적 취향에 관한 정보의 처리는 금지된다(제9조).

GDPR에서도 역시 주목할 만한 것은 가명처리에 관한 규정이다. '가명처리'란 추가적 정보의 이용 없이 개인정보가 더 이상 특정 정보주체에게 귀속될 수 없는 방식으로 처리하는 것(제4조제5호)을 의미하는데, 비식별화 처리 정도가 낮은 상태이기 때문에 가명처리를 했더라도 여전히 개인정보로 파악한다. 한편, 가명처리는 익명처리와 다른데, 익명처리는 비식별화 처리 정도가 매우 높기 때문에, 익명처리한 정보는 개인정보가 아니라고 본다. 이 조항에 따르면, 공익을 위한 기록보존 목적·과학 또는 역사 연구 목적·통계 목적의 개인정보 처리의 경우에는 정보주체의 동의가 없어도 추가적 처리가 가능하다. 다만, 가명처리 등 안전장치가 있어야 한다(제5조제1항(b)).

2) 개인정보 이용에 관한 규정

GDPR도 역시 사전 동의를 원칙으로 하고 있는데, GDPR 제정 과정에서 그 동의가 유효하기 위해 자유로운 선택 상황에서 범위의 특정화, 충분한 고지, 명시적 동의일 것 등 매우 세

16) EU의 GDPR에 대한 상세한 내용 소개는, 김상현, 「유럽연합의 개인정보보호법, GDPR」, 커뮤니케이션북스, 2018 참조.

17) CJEU Judgement Case 2016. 10. 19., C-582/14. 이 사건에서 유럽사법재판소는 해당 주소가 인터넷서비스사업자(ISP)의 수중에 있다면 개인정보로 간주되지만, 개인의 신원을 식별하는데 적절히 사용할만한 수단이 없는 주체의 수중에 있다면 개인정보로 간주되지 않는다고 판결하였다. 즉 적절한 기술과 인프라, 시스템을 갖춘 ISP 사업자라면 가입자의 IP 주소가 접속할 때마다 바뀌더라도 가입자의 신원과 위치를 쉽게 파악할 수 있는데 반해, 그렇지 않은 사업자는 IP주소 만으로는 해당 정보주체의 신원을 파악하기 불가능하다는 점을 감안한 판결이다(이 판결에 대한 자세한 분석은, 문수미, "유동 IP주소의 이용행위에 관한 온라인서비스제공자(OSP)의 책임-CJEU 'Breyer' 사건(Case C-582/14)의 개인정보성 판단 기준을 중심으로", 지식재산연구 제14권 제3호, 2019. 9, 151면 이하 참조).

부적인 지침을 별도로 제시했다.[18] 반면 GDPR 제6조에서는 이익형량의 관점에서 '정당한 이익'(legitimate interests) 추구를 위해 필요한 경우에는 개인정보를 처리할 수 있는 길을 열어주고 있는데, 개인정보 처리자와의 관계에서 정보주체가 합리적으로 예상하는 바를 고려하여 정보주체의 이익 또는 기본권 및 자유가 우선시 되지 않는다면 적법한 처리가 된다고 하고 있다. 또한 당초의 수집목적을 극대화하기 위하여 GDPR은 '양립가능성'(compatibility)이라는 개념을 도입하였는데, 원래의 수집목적과 양립가능한 범위라면 추가 처리에 있어서 별도 동의나 다른 적법처리 요건이 필요하지 않다.[19] 정보주체의 개인정보를 수집한 상태임을 전제로 추가 처리 시 양립가능성을 판단하기 때문에, 개인정보 처리자의 개인정보 목적 외 이용·제공을 폭넓게 허용하는 것이다.[20]

한편 데이터 주체에 대하여 프로파일링을 비롯하여, 자기에게 법적 효과를 가져오거나 그것에 유사한 중대한 영향을 가져오는 경우, 자동적 수단에 의한 결정에 반대할 권리를 부여하고 있다(제22조). 프로파일링이란, 개인적인 특성을 평가하기 위해 수행되는 모든 형태의 자동화된 개인정보 처리로서, 대출자격, 고용기회, 대학입학 등 개인의 법적 지위나 권리에 변동을 주거나 정보주체에 지속적인 영향을 미치는 결정[21] 등과 같은 경우에는 정보주체가 이에 반대하면 언제든지 그 처리가 중단되어야 함을 규정하고 있다. 프로파일링 그 자체를 규제하려는 것은 아니며, 정보주체와 개인정보 처리자간 계약 체결 또는 이행에 필요하거나, 정보주체의 명백한 동의가 있으면 예외적으로 허용된다.

(2) 미국 캘리포니아주 소비자 프라이버시법(CCPA)

미국에서는 연방법 차원에서의 포괄적인 개인정보 보호법은 존재하지 않는다. 기업에 의한 자율규제를 기본으로 하면서도, 기밀한 처리가 요청되는 분야에 대하여 개별법으로 규제가 이루어지고 있다. 예를 들어, 아동 보호를 위한 '아동 온라인 프라이버시 보호법'(COPPA: Children's Online Privacy Protection Act)이나, 사기나 도난으로부터 의료정보를 보호하기 위한 목적으로 제정된 '건강보험 이동성 및 법적 책임에 관한 법률(HIPAA: Health Insurance Portability and Accountability Act)이 그것이다. 여기서 자율규제라고 하더라도, 연방거래위원회법(FTC: Federal Trade Commission Act) 제5조(a)(1)에서 말하는 '불공정·기만적 행위 또는 관행'에 소비자의 프라이버시 침해가 포함된다고 해석되는 것에 의해 개인정보의 보호를 담보하고 있다. 즉 기업은 자율적으로 개인정보를 다룰 수 있지만, 소비자에 대한 불공정·기만적 행위로 평가받는다면 FTC법 위반에 대한 막대한 책임을 지게 된다.

그런데 2018년 6월 28일에 캘리포니아주에서 '소비자 프라이버시법'(CCPA: California Consumer Privacy Act)이 제정되어 2020년 1월부터 시행되었다. 그리고 복수의 주에서 이 CCPA를 모델로 하여 개인정보보호에 관한 법률안이 제출되고 있다. 나아가 이 CCPA의 시행을 계기로 미 연방 차원의 개인정보보호를 위한 입법 요구가 높아지는 가운데, 데이터와 프라

18) Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/67 9", (2018).

19) GDPR Article 6 (4)에 따르면, 양립가능성은, 수집목적과 추가처리 목적 사이의 연관성, 정보주체와 개인정보처리자간 관계를 고려하여 개인정보가 수집된 상황, 민감정보 및 범죄 기록 처리여부 등 처리되는 개인정보의 성격, 추가 처리가 정보주체에게 미칠 결과, 암호 처리 또는 가명처리 등 적절한 안전성 조치 여부를 고려하여 인정된다.

20) 박주희, 전게논문, 37면.

21) 예를 들면 The Article 29 Data P rotection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation" (2017) pp.23~24.

이버시를 규율하기 위한 연방 법률안이 제안되어 상원에서 논의 중이다.[22] 이러한 영향을 보여주고 있기 때문에 미국의 법제도를 검토함에 있어서는 이 CCPA를 분석할 필요가 있다.

1) 개인정보의 정의 및 비식별화

CCPA에서는 개인정보의 정의로서, "특정 소비자 또는 가구를 식별, 관련, 설명, 연관시킬 수 있거나 직접 또는 간접적으로 연결될 수 있는 정보"로 규정하고 있어[23], 개인정보 관련 미국의 다른 법령보다 광범위하게 정의하고 있고, GDPR과 유사하다. CCPA에서는 이메일주소 등과 같은 식별자뿐만 아니라, 구매내역 등을 포함한 상업적 정보, 인터넷 검색기록, 소비자의 선호도, 습관, 행동, 태도, 지능, 적성을 반영하여 소비자에 관한 프로파일을 생성하기 위한 식별 정보로부터 도출된 추론사항 등도 개인정보로 보고 있다. 이것들은 예시에 불과하여 광범위하게 규정하고 있음을 알 수 있다.

CCPA에서도 암호화 및 가명화에 대해 규정하고 있는데, 우리나라나 GDPR과 규정방식이 다르다. 별도로 비식별화에 대한 규정을 두고 있지 않고, 개인정보 유출 등이 발생했을 때의 금지청구나 손해배상청구에 대해 규정하고 있는 §1798.150에서 규정하고 있다. 또한 청구의 대상이 되는 정보는 §1798.81.5(d)(1)(A)에서 정하는 개인정보, 즉 (ⅰ) 사회보장번호, (ⅱ) 운전면허증 번호 또는 주 ID번호, (ⅲ) 은행 계좌번호와 신용카드 번호, 체크카드 번호 및 계좌에 접근할 수 있는 비밀번호, 접근코드나 비밀번호를 결합시킨 것, (ⅳ) 의료정보, (ⅴ) 건강보험정보, (vi) 바이오 메트릭스 데이터이다. 이러한 정보에 대해 암호화하지 않거나 비식별화(redacted)[24]하지 않은 채 유출된 경우에 한하여 책임을 지게 된다.

2) 개인정보 이용 관련

개인정보 처리에 관하여는, 종래 미국의 다른 개인정보 취급 관련 법제도에서 취하고 있는 입장과 마찬가지로, 소비자가 자신의 개인정보를 제3자에게 판매하는 사업자에게 자신의 개인정보를 판매하지 말 것을 지시할 권리인 옵트 아웃 권리(Opt-out)를 가지는 형식으로 규정하고 있다. 다만 제3자에게 소비자의 개인정보를 판매하는 사업자는 소비자에게 본인의 개인정보가 판매될 수 있으며, 본인의 개인정보 판매를 옵트 아웃 할 수 있는 권리를 가진다는 내용을 소비자에게 고지해야만 하도록 하였다. 사업자는 법에 따라 웹사이트에 명료하고 눈에 잘 띄는 방식으로 '자신의 개인정보를 판매하지 말 것'이라는 제목으로 개인정보 판매를 거부할 수 있는 기능을 제공하는 링크를 제공해야 한다(§1798.120.)

이러한 방식은 2010년대 초반부터 이어져 온 미국의 데이터 관련 정책과 그 맥락을 같이 한다. 일찍이 2014년 백악관에서는 빅데이터 관련 정책에서, 빅데이터 환경에서는 개인정보의 '수집'보다는 '이용'과 '재가공'에 정책의 방점이 두어져야 한다고 강조했다[25].

---

22) 연방차원에서의 입법 논의에 대해서는, 이규엽·엄준현, "미국 개인정보보호법 입법 동향: 국내 개정법과의 비교 및 시사점", KIEF 오늘의 세계경제 제20권 제3호, 2020, 2면 이하 참조.

23) Cal. Civ. Code §1798.140(o)

24) 'redacted'는 보통 '****'와 같은 방식을 말하지만 익명화 또는 가명화로 단적으로 정의하기 곤란한 점이 있어 여기에서는 이 양자보다 포괄적 개념인 비식별화로 표기한다.

25) The White House, "Big Data and Privacy: A Technological Perspective", "Big Data: Seizing Opportunities, Preserving Values" (2014).

4. 개정 내용에 대한 검토

온라인 데이터 관련 기술과 산업은 전세계적으로 공히 발전하고 있지만, 개인정보 관련 데이터의 활용과 이에 대한 보호 및 규제 정책은 국가에 따라 상당히 다른 입장을 보여 왔다.

먼저 미국은 전통적으로 규제를 하지 않는 방향이었고, 현재까지 드러난 문제를 해결하기 위한 최적의 해법으로 '통지와 동의에 의한 소비자의 선택'을 원칙으로 삼아 왔다. 미국에서 개인정보 이슈는 이용자가 스스로의 비용과 편익을 고려하여 결정하면 되는 개인적 이슈로 여겨져 왔다.[26] 그동안 옵트 아웃(Opt-out)의 입장을 취한 것도 이러한 정책에서 비롯된다.

이와 달리 EU는 기업에 개인정보의 위험을 취소화하기 위한 사전의무를 부과해 왔다. 이용자가 동의를 한 경우에 한하여 개인정보를 활용할 수 있는 옵트 인(Opt-in) 방식을 기본으로 하여, 사업자의 의무를 강화하고 있다. 개개의 정보제공자는 자신이 제공한 정보가 어떻게 활용되어 어떤 일이 일어날지 알기 힘들며, 설사 안다고 해도 적절히 대처할 수 없는 것이 그 이유였다.[27] 더구나 개인정보의 이용은 매출의 증가로 기업에 돌아가지만, 그 피해는 대부분 개인에게 귀결되므로, 기업과 개인 간에 존재하는 이러한 불균형 때문에 국가가 적극적으로 개입해 왔다. 그런데 EU는 GDPR에서 익명처리, 가명처리를 통해 데이터의 활용을 도모함으로써 미국과의 간극을 어느 정도 좁히게 된 것이다.

우리나라는 EU와 동일한 방식을 취해 왔다. 그리고 개정 데이터 3법에서도 GDPR과 마찬가지로 개인정보 관련 개념 체계를 개인정보, 가명정보, 익명정보로 구분하였으며, 익명정보는 개인정보 보호법의 적용 대상에서 제외시키면서 가명정보에 대해 규제하고 있다. 여기서 상업적 목적의 통계작성을 비롯한 통계 작성, 과학적 연구 및 공익적 기록 보존 등을 위해 정보주체의 동의 없이 가명정보 사용 및 제3자에게의 제공이 가능하다. 다만 가명처리에 대해서는 새로운 것이기 때문에 개정법의 시행 과정에서 가명정보의 처리 방법과 활용 방법과 관련하여 명확한 가이드라인을 마련할 필요가 있다.

GDPR의 '원래의 수집목적과 양립가능한 범위'와 유사하게, 개정 개인정보 보호법에서도 처음 수집목적과의 '합리적 관련성'이 인정되는 경우에는 동의 없이 개인정보를 처리할 수 있도록 하고 있다. 그러나 '합리적 관련성'에 대해서는 그 범위에 대하여 구체적인 논의가 필요하다고 본다.

데이터의 수집단계에서는 개인 식별성을 갖지 않는 정보라 하더라도 데이터의 처리 과정에서 사후적으로 특정 개인에 대한 식별성이 발생할 경우 어떤 개인정보 보호조치를 취할 것인가도 중요한 쟁점이다. 이 경우 데이터 처리 과정에서 생성되는 개인정보에 대해서도 정보주체에게 사전 동의권을 인정할지, 동의권을 인정할 경우 데이터 처리의 어떤 단계에서 인정되는 것으로 볼 것인지의 문제가 생긴다. 이러한 사전 동의제도와 관련하여 대법원은 이미 정보주체의 동의가 있을 경우 객관적으로 인정되는 범위 내에서 별도의 동의가 필요 없다고 본 바 있지만,[28] 활용을 전제로 하는 개정 데이터 3법 하에서도 이러한 법리를 그대로 유지하기는

---

26) 황주성, "빅데이터 환경에서 프라이버시 문제의 재조명", 「빅데이터와 위험 정보사회」, 커뮤니케이션북스, 2013, 228면.

27) 황주성, 전게서, 229면.

28) 대법원 2016. 8. 17. 선고 2014다235080 판결에 따르면, "법률정보 제공 사이트를 운영하는갑 주식회사가 공립대학교인 을 대학교 법과대학 법학과 교수로 재직 중인 병의 사진, 성명, 성별, 출생연도, 직업, 직장, 학력, 경력 등의 개인정보를 위 법학과 홈페이지 등을 통해 수집하여 위 사이트 내 '법조인' 항목에서 유료로 제공한 사안에서, 갑 회사가 영리 목적으로 병의 개인정 보를 수집하여 제3자에게 제공하였더라도 그에 의하여 얻을 수 있는 법적 이익이 정보처리를 막음으로써 얻을 수 있는 정보주체의 인격적 법익에 비하여 우월하므로, 갑 회사의 행위를 병의 개인정보자기결정권을 침해하는 위

위험한 측면이 있다. GDPR에서는 개인정보의 이동 시 해당 데이터에 대한 액세스 권한을 취소할 수 있도록 하는 권리를 부여하고 있고, 프로파일링에 대한 반대 권한을 보장하고, 잊혀질 권리를 규정화함으로써 이러한 문제를 해결하고 있는데 반해, 개정된 데이터 3법에서는 이러한 점들은 규정하지 않았다. 이 점이 개인정보 보호장치와 관련하여서는 GDPR에 현저히 못 미친다고 비판받는 주된 이유이다.

Ⅲ. 개정 데이터 3법에 따른 불법행위책임의 판단

1. 개정 데이터 3법에서의 개인정보 보호를 위한 문제점

(1) 불법행위책임 판단기준으로서의 데이터 3법

개인정보 자기결정권 침해로 인한 불법행위책임을 판단함에 있어 데이터 3법은 중요한 기준이 된다. 종래 개인정보의 유출이 문제된 사건에서, 판례는 인터넷 서비스 제공자가 수집한 이용자의 개인정보 등이 분실·도난·유출·변조 또는 훼손되지 않도록 개인정보 등의 안전성 확보에 필요한 보호조치를 취하여야 할 정보통신서비스 이용계약상 의무를 다하였는지 여부를 계약상 책임 또는 불법행위책임의 판단기준으로 삼고 있는데, 그 기준이 개인정보 보호법제에서 정하는 조치를 다했는지 여부이기 때문이다.[29)]

물론 불법행위책임을 판단할 때 법률 등에서 정한 기준에 국한되는 것은 아니고, 합리적으로 기대 가능하다고 인정되는 범위에서 준수할 만한 사항을 위반한 경우에도 불법행위책임을 질 수 있다. 소위 '네이트·사이월드 회원들의 개인정보 유출로 인한 손해배상 청구사건'에서는, 개인정보 취급자가 작업 종료 후 로그아웃을 하지 않아 개인정보가 유출되었는데, 이 사건에서 대법원은, "정보통신서비스 제공자가 정보처리시스템에 접속한 개인정보 취급자로 하여금 작업 종료 후 로그아웃을 하도록 하는 것은, 비록 '개인정보의 기술적·관리적 보호조치 기준'(방송통신위원회 고시 제2011-1호)에서 정하고 있는 기술적·관리적 보호조치에는 해당하지 않으나, 정보통신서비스 제공자가 마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치에 해당하므로, 정보통신서비스 제공자가 이러한 보호조치를 미이행하여 정보처리시스템에 접속권한이 없는 제3자가 손쉽게 시스템에 접속하여 개인정보의 도난 등의 행위를 할 수 있도록 하였다면 이는 불법행위에 도움을 주지 말아야 할 주의의무를 위반한 것으로써 이러한 방조행위와 피방조자의 불법행위 사이에 상

법한 행위로 평가할 수 없고, 갑 회사가 병의 개인정보를 수집하여 제3자에게 제공한 행위는 병의 동의가 있었다고 객관적으로 인정되는 범위 내이고, 갑회사에 영리 목적이 있었다고 하여 달리 볼 수 없으므로, 갑 회사가 병의 별도의 동의를 받지 아니하였다고 하여 개인정보 보호법 제15조나 제17조를 위반하였다고 볼 수 없다"고 한다.

29) "정보통신서비스 제공자가 구 정보통신망법 제28조 제1항 및 정보통신서비스 이용계약에 근거하여 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 여부를 판단할 때에는 해킹 등 침해사고 당시 일반적으로 알려져 있는 정보보안 기술 수준, 정보통신서비스 제공자의 업종과 영업 규모, 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술 수준과 정보보안기술 발전 정도에 따른 피해 발생 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보 누출로 인하여 이용자가 입게 되는 피해 정도 등의 사정을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 하여야 한다."(대법원 2018. 12. 28. 선고 2017다256910 판결)

당인과관계가 인정된다면 공동불법행위자로서 책임을 면할 수 없다"고 하였다.[30]

종래에 개인정보 보호와 관련하여 민사책임이 문제되는 경우는 주로 유출과 관련한 사고였다. 이러한 유출과 관련한 상황에서는 개인정보가 유출되었는지, 그리고 그 유출 자체에 필요한 보호조치를 제대로 취하지 않았는지 여부가 불법행위책임의 1차적인 판단기준이었다.[31]

그런데 데이터 이용과 관련하여서는 이러한 기준이 그대로 적용되기는 어렵다. 데이터 유출에서는 그 유출에 과실이 있었다는 점이 문제되지만, 익명 또는 가명 처리된 정보는 이용을 전제로 하므로, 이러한 정보는 유출 자체만으로 불법행위책임이 곧바로 문제되지 않기 때문이다.[32] 오히려 가명처리된 정보에 대해 암호화 등 안전성 확보에 필요한 조치를 다하였는지 여부가 보다 중요한 판단기준으로서, 이러한 처리를 잘못하여 개인의 신원이 드러나게 되었는지가 불법행위책임의 판단기준이 될 것으로 보인다.

(2) 목적 외 이용과 제3자 제공에 따른 문제점

개인정보 보호법에서는 개인정보의 목적 외 이용이나 제3자 제공의 경우 원칙적으로 본인의 동의가 필요한 것을 전제로 하고 있다. 그러나 빅데이터 시대에서의 2차이용은 처음부터 전제로 하지 않고 그때그때 필요에 의해 발생할 수도 있으므로, 데이터를 최초에 수집하는 시점에서는 2차이용을 상정하고 본인 동의를 취득하는 것은 어렵다. 따라서 결국 처음부터 무조건적으로 2차이용에 대한 동의를 받는 경우가 많은데, 이러한 관행이 바람직하지 않은 것으로 여겨져 왔다. 따라서 개인정보를 익명화 또는 가명화 하는 것에 의해 본인 동의 없이 목적 외 이용이나 제3자 제공을 하겠다는 요청이 산업계에서 나와 개정까지 이어진 것이다.

개정법에 따르면, 개인정보를 익명 처리한 경우에는 보호대상에서 제외되므로 제3자에게 보다 자유롭게 제공할 수도 있으며, 가명처리한 경우에도 상당히 이용범위가 넓어진다. 그렇지만 여전히 다음과 같은 문제를 가지고 있다.

첫째, 익명화 또는 가명화에 의해 개인정보를 가지고 특정 개인을 식별할 수 없도록 한다는 것인데, 완전하게 비개인정보로 하는 것이 기술적으로 가능한가 하는 것이 문제이다. 둘째, 익명화 또는 가명화를 한 개인정보 취급 사업자로서는 사업을 지속하기 위하여, 가공의 기초자료가 된 개인정보를 폐기하지 않고 계속 보유하는 경우가 많을 것인데, 그러한 경우에는 가공원자료인 개인정보와 익명화 정보를 용이하게 조합하여 개인을 식별할 위험성이 존재한다. 특히 개정된 신용정보보호법에는 해당 정보주체와의 상거래관계가 종료된 날로부터 최장 5년 이내(그 이전에 목적이 달성된 경우, 목적이 달성된 날로부터 3개월 이내)에 개인신용정보를 삭제할 의무를 부과하고 있으나, 가명 처리된 개인 신용정보의 경우에는 이에 대한 예외가 인정

---

30) 대법원 2018. 1. 25. 선고 2015다24904, 24911, 24928, 24935 판결. 그런데 이 사건에서도 "해킹사고 당시 해커가 이미 키로깅을 통하여 DB 서버 관리자의 아이디와 비밀번호를 획득한 상태였기 때문에 갑 회사의 DB 기술팀 소속 직원이 자신의 컴퓨터에서 로그아웃을 하였는지 여부와 무관하게 언제든지 게이트웨이 서버를 거쳐 DB 서버에 로그인을 할 수 있었던 것으로 보이므로, 위와 같은 보호조치의 미이행과 해킹사고의 발생 사이에 상당인과관계가 인정되지 아니하여 갑 회사의 손해배상책임이 인정되지 않는다."고 판단하였다.

31) 개인정보 유출과 관련하여 위법성이 인정되어도 정신적 손해 발생이 인정받기 어려워 불법행위책임이 인정되기 어려움에 대해서는, 윤태영, "위치정보 침해에 대한 불법행위책임", 민사법학 제81호, 2017, 166면 이하 참조.

32) 대법원 2012. 12. 26, 선고 2011다59834 판결에서는, 개인의 성명, 주소, 전화번호 등 신원을 나타내는 정보가 유출되었다고 하더라도 그것만으로 곧바로 위자료를 배상할만한 정신적 손해가 발생한 것은 아니고, 그 밖에 여러 가지를 고려하여 불법행위책임을 지는지 여부를 판단하고 있다.

된다(개정법 제20조의2). 셋째, 제3자에게 제공한 경우가 더욱 문제이다. 빅데이터 이용의 관점에서는 목적 외 이용보다도 오히려 제3자에게 제공하고 싶은 요청이 강하기 때문에 이 점에 대한 논의가 더욱 활발하게 진행되어 왔다. 개인정보를 익명화한 사업자가 당해 익명화 정보를 제3자에게 제공하는 경우에 문제로 되는 것은, 개인 식별성의 유무에 대하여 제공자를 기준으로 판단할 것인지, 제공받은 자를 기준으로 판단할 것인지 하는 점이다. 여기서 문제로 되는 점은 익명화를 한 제공자에게는 개인정보이지만, 제공받은 자에게 있어서는 그것이 익명화에 의한 비개인정보로 되어 있는 경우에 개인정보 보호법의 어느 범위까지 적용될 것인가 하는 점이다. 중요한 것은 본인 동의 없이 제3자 제공이 인정되기 위해서는, 익명화 정보가 제공자 또는 제공받는 자에게 있어서 비개인정보로 되어 있어야 하는 것이 필요하다. 문제는 개인정보를 익명화하는 것에 의해 그것을 완전하게 비개인정보로 하는 것이 기술적으로 가능한가 하는 점이다.

2. 익명 및 가명처리에서의 불법행위책임 판단 기준

(1) 익명처리의 경우

개인정보 이용에 있어 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다는 점(개정법 제3조제7항)을 앞에서 살펴본 바 있다. 그 이유로서는, 익명 처리된 정보는 복원이 불가능해 법적으로 개인정보가 아닌 경우라고 할 수 있기 때문이라는 것이다. 가명 처리한 정보는 비식별화 처리 정도가 낮은 상태이기 때문에 여전히 개인정보로 보는 반면, 익명처리는 비식별화 처리 정도가 매우 높기 때문에, 익명 처리한 정보는 개인정보가 아니라고 본다. 그렇다면 개인정보를 익명처리 하였다고 하여 이용에 있어 불법행위책임이 문제될 소지는 없을까?

지금까지 인터넷서비스 제공업체 측에서는 개인정보의 수집 이후 저장·처리과정에서 익명화를 거치기 때문에 인격권 침해가 문제되지 않음을 주장해 왔다. 익명화란 행위정보 데이터베이스에서 데이터의 주체를 판독하기 어렵도록 개인식별정보를 제거하는 것이기 때문에, 민감한 정보라 하더라도 익명화만 거치면 크게 문제되지 않는다고 주장하였고, 이것은 개인정보 활용의 근거가 되어 왔다. 프라이버시 문제를 해결하면서도 기업의 마케팅이나 사회적으로 유용한 연구와 혁신 등에 사용될 수 있다는 이익형량의 관점에서, 이러한 익명화 기술은 개인정보의 취득과 활용에 따른 프라이버시 침해 논쟁을 효과적으로 잠재워 왔다.[33)]

그러나 재식별화 기술(Reidentification Technique)의 진보에 의해 이러한 익명화 방법은 더 이상 신뢰할 수 없다고 할 수 있다.[34)] 실제로 익명 처리한 데이터가 재식별화 되어버린 유명한 사건으로서 2006년에 일어난 '아메리카 온라인(AOL) 사건'과 '넷플릭스(Netflix) 사건'이 자주 언급되고 있다. 아메리칸 온라인은 2006년 65만 이용자의 3개월간 검색기록을 공개하여 오픈리서치를 촉구하는 AOL리서치를 시작하였다. 검색 정보는 유저명이나 IP주소가 삭제된 일정한 익명처리 후에 공개되었다. 그러나 단 3일 만에 뉴욕타임스의 두 리포트가 한 할머니가 어떤 검색을 했는지 밝혀냈고[35)], 이 익명화 데이터에 대해서는 복수의 검색 정보를 조합시

33) 황주성, 전게서, 231면 참조.
34) Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010)
35) 델마 아놀드(Thelma Arnold)라는 할머니가 손가락 저림' '60세 싱글 남자', '아무 데서나 오줌 누는

키는 것에 의해 개인을 특정시킬 수 있다는 것이 드러났다.[36]

넷플릭스 사건도 유사하다. 넷플릭스사는 자사가 보유한 추천시스템의 알고리즘을 개선하기 위해 유저에 의한 영화 평점자료를 식별정보의 삭제 등의 익명처리를 한 후에 공개하였다. 그러나 이 데이터에 대하여도 가입자의 영화의 선호도에 대하여 약간의 외부정보만 있으면, 그 가입자를 재식별화 하는 것이 가능하다는 것이 밝혀졌다.[37] 이러한 일련의 사건으로부터 특히 인터넷상에 산재하는 '외부정보'와의 결합에 의한 재식별화의 위험성이 강조되고 있다.[38]

이러한 점에서 볼 때, 익명처리를 하였다는 것만으로 면책되는 것은 아님이 분명하다. 어찌 보면 개인정보의 활용에 있어 익명화라는 것은 피할 수 없는 본질적 한계를 가지고 있기 때문에 가명정보라는 개념을 도입했을지도 모른다. 따라서 완전한 익명화와 불완전한 익명화라는 두 가지 선택적 관계가 아니라, 꽤 안전성 높은 익명화로부터 개인정보 침해 위험이 높은 익명화까지 수많은 단계가 존재한다고 볼 수 있다.[39] 익명화라 하더라도 재식별화에 의해 인격권 침해 위험이 발생할 여지가 있고, 그로 인한 책임에 대해서는 개인정보의 종류, 특성, 이용 목적, 상황, 영역 등에 따라 케이스 바이 케이스의 판단이 필요하다.[40] 즉 익명처리를 한 자라도 그것이 재식별화되지 않도록 얼마나 최선을 다했는지에 따라 책임 유무가 달라질 수 있을 것으로 보인다.

(2) 가명처리의 경우

가명정보는 실명이나 주민등록번호처럼 신원이 드러나는 개인정보가 암호화 처리되어 개인을 식별할 수 없는 수준의 정보이므로, '30대 미혼 남성' 같은 익명정보보다는 구체적이다. 가명정보는 소득·나이·결제금액 같은 개인 신상 정보를 포함할 수 있고, 건강·금융·유통 같은 다른 영역의 정보와 같이 모아서 볼 수도 있다. 따라서 빅데이터로서 익명정보보다도 가치가 있으므로 정보의 활용을 극대화할 수 있는 반면, 익명화보다 훨씬 더 재식별화 할 수 있는 위험성이 높아진다.

따라서 익명처리보다 더 재식별화할 수 없도록 조치를 취해야 할 의무를 부담한다. 개인정보 보호법 제28조의5 제1항에서도 "누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다."고 규정하고 있고, 제2항에서는 "개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다."고 규정하고 있다. 그런데 그러한 의무를 다했는지 여부에 대해 익명정보와 마찬가지로 케이스 바이 케이스로 판단한다고 할 때, 어느 정도로 대응하면 좋을까 판단하는 것은 어렵다. 이럴 경우 역으로 이러한 조치의 부담으로 인해

개' 등의 검색어를 입력한 사실을 밝혀낸 것이다.

36) ZD Net Korea, "AOL, 사용자 검색 데이터 유출에 사과" 2006. 8. 18.자 기사 참조. https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=092&aid=0000009306

37) 중앙SUNDAY, "가명정보 빅데이터 산업 숨통…개인정보 침해 논란은 여전" 2020. 2. 8.자 기사 참조. https://news.joins.com/article/23700865

38) Ohm, supra note 34, at 1752.

39) 村上康二郎,「現代情報社会におけるプライバシー個人情報の保護」、日本評論社、2017, p. 231.

40) 범용적 익명화방법은 존재하지 않지만, 케이스 바이 케이스, 즉 개인정보의 종류·특성, 이용 목적 등에 따라 기술·대상을 적절하게 선택하는 것에 의해 식별비특정정보와 비식별비특정정보로 가공하는 것은 불가능하지는 않다는 의견도 있다. President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective (2014), p. 38-39.

빅데이터를 이용한 서비스를 포기하게 되고, 결국 새로운 개정법은 의의를 갖지 못할 수도 있다. 따라서 가능한 한 어느 정도 법적 기준을 제시할 필요가 있는데, 이제 제도를 시행하려는 단계에서 이런 기준을 명확하게 제시하기는 어렵다.

여기서 이러한 기준으로 될 만한 것을 비교법적으로 참고하기 위해, 종래 미국에서 개인정보 보호의 대상에서 제외되는 익명처리된 정보로 되기 위해 어떤 조치를 요구하고 있는지 살펴보는 것은 의미가 있다고 생각한다. 미국의 경우 원칙적으로 개인정보 데이터 활용을 원칙으로 하면서 개인정보 보호를 위해 소비자의 옵트 아웃을 보장하는 정책을 취하고 있으므로, 가명정보의 활용을 원칙으로 하는 개정법에서 많은 참고가 되기 때문이다. 미국에서 이러한 기준이 되는 것은 미국 연방거래위원회(FTC)가 제시하는 3요건인데,[41] 여기에서는 프라이버시 보호의 대상으로부터 제외되기 위해 다음의 3가지 요건이 필요하다고 한다. 즉, ① 사업자가 데이터의 비식별 처리를 위해 합리적인 조치를 취해야 한다는 점, ② 사업자가 데이터를 비식별적으로 유지 관리하고 데이터를 재식별 하려고 시도하지 않을 것, ③ 사업자가 서비스 제공업체든 다른 제3자이든 관계없이 다른 사업자가 이러한 비식별데이터를 사용할 수 있게 하는 경우 해당 사업자가 데이터를 재식별하려고 시도하는 것을 계약적으로 금지할 것이 그 내용이다. 물론 이러한 요건들이 시사하는 바가 적지는 않지만, 다음과 같은 한계도 가지고 있다. 먼저 ①에서 합리적으로 익명처리를 취해야 한다고 하지만, 어느 정도 익명화하면 좋은가 하는 점에 불명확한 점이 남아 있다. 한편, 한국과 미국의 법제도적 차이에서 도입에 효력이 의문시되는 것도 사실이다. 미국에서는 이 FTC 3요건, 특히 ②와 ③의 요건이 실효성을 꽤 담보할 수 있는데, 왜냐하면 이에 대한 위반이 있는 경우에는 앞에서도 언급한 FTC법 제5조의 불공정 또는 기만적인 행위 또는 관행으로서 제재를 가하는 것이 가능하기 때문이다. 이 제재조치는 강력한데 반해, 우리나라에서는 이러한 수준에는 미치지 못하기 때문이다. 따라서 이러한 제도의 도입을 위해 입법적 대응이라는 과제가 남아 있지만, 불법행위책임을 면하기 위해 최대한의 조치를 취했는가 하는 판단을 위해 시사점을 주는 것은 분명하다.

3. 재식별화 금지를 위한 조치

가명화는 개인정보 노출 위험에 직면할 가능성이 크다. 따라서 가명처리 과정에서, 데이터를 유출당하거나 비정상적 공격에 의한 해킹의 경우에도 민감한 개인 데이터에 접근할 수 없고, 민감한 개인 데이터의 원소스로 쉽게 추적할 수 없도록 조치해야 한다.[42] 이를 위해 최근 데이터의 활용을 도모하기 위한 개인정보 보호법제의 개정과 병행하여 온라인 행위추적에 대해 규제를 강화하는 입법적 조치들이 해외에서 이루어지고 있다.

온라인 행위추적(online behavioural tracking)이란, 로그 정보 등 웹 이용행위에 대한 데이터를 토대로 개개인의 관심사를 분석하여 맞춤형 광고를 하기 위해 데이터를 수집하는 모집 과정이다.[43] 광고가 개인의 필요에 정밀하게 맞춰질수록 광고를 보고 구매할 확률이 높아지기

41) Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), p. 21-22. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

42) 김정선, “가명 데이터 활용연구-기술적 처리방법 및 기업의 활용방향을 중심으로”, 정보보호학회논문지 제30권 제2호, 2020, 256면.

43) Pamela L. Alreck, Robert B. Settle, Consumer reactions to online behavioural tracking and targeting, in: Database Marketing & Customer Strategy Management, Vol. 15, 1 (2007) p.11.

때문에 기업들은 앞 다투어 이 행위추적 기술을 엄청난 속도로 발전시켜 왔다. 가장 대표적인 행위추적 수단이 쿠키(Cookie)인데, 이것은 처음에는 서로 다른 웹페이지 간에 이용자 정보를 공유함으로써 반복적인 방문자 인증 등의 불편함을 해소하기 위해 개발되었지만, 이것이 인터넷 업체들이 그것을 맞춤형 광고를 위한 개인정보의 수집 수단으로 활용해 왔다. 최근에는 서로 다른 웹사이트를 넘나들면서, 광고네트워크 기업들이 보유한 이용자 프로파일을 동기화함으로써 사생활 침해의 위험이 훨씬 더 커진 상태이다.

최근 금융위원회는 개정된 신용정보법 시행에 앞서 금융회사의 빅데이터 업무를 활성화하기 위한 주요 조치로서, 데이터 분석·컨설팅 등 신용정보법이 허용한 빅데이터 업무를 금융회사도 영위할 수 있게 하였다. 이에 따라 소득·소비성향 같은 금융 데이터와 매출·학군·상권 등 비금융 데이터를 결합·활용해 맞춤형 금융상품을 개발할 수 있게 된 것이다.[44] 그런데 여기서 미국의 서브프라임 금융사태가 맞춤형 광고로 인해 발생한 것일지도 모른다는 의미심장한 발언을 되새겨볼 필요가 있다.[45] 서브프라임 금융사태가 발생하기 전인 2005~2007년 사이에 온라인 담보대출 기업의 광고 지출이 3배가량 증가하고, 주요 온라인 광고 고객이 담보대출 금융기관이라는 점을 바탕으로, 행위추적에 의한 맞춤형 광고정보를 통해 주택담보대출을 필요로 하는 잠재고객을 정확히 찾아내 과도한 구매가 이루어졌다는 것이다.

행위추적은 이러한 위험성을 내포하고 있기 때문에, EU와 미국은 행위추적을 금지하는 법제도를 마련하고 있다. 먼저 EU에서는, GDPR에 더하여 전자통신서비스 영역에서의 프라이버시를 대상으로 하는 e프라이버시 지침(ePD: e-Privacy Directive)이 이에 대해 규율하고 있다.[46] 여기에서는 쿠키의 취득·이용에는 원칙적으로 데이터 주체의 '동의'를 얻어야 하고(ePD 제5조제3항), 적법한 동의라고 하기 위해서는, GDPR 제4조 제11호에서 요구하는 엄격한 기준, 즉 ① 임의로 이루어져야 하고, ② 특정되어야 하고, ③ 정보제공을 받은 후에 이루어져야 하고, ④ 불명료하지 않을 것을 충족할 필요가 있다.

최근 이와 관련한 판결도 있었는데, 2019년 10월 1일 유럽사법재판소는, 독일의 온라인 게임 기업 Planet49에 의한 쿠키 동의의 취득 방법이 ePD가 요구하는 요건을 충족하지 않았다고 판결하였다.[47] 이 판결은 동의하는데 있어 미리 체크가 된 채 표시되어 있는 체크상자에 의한 쿠키 동의는 유효한 동의로서 인정되지 않는다고 하였다. GDPR은 데이터 주체에 의한 자발적인 동의를 요구하는 바, 미리 체크되어진 박스에 의해 부지불식간에 이루어진 동의는 자발적이라고는 할 수 없다는 것이다.[48]

미국에서도 앞에서 언급한 FTC법이 제5조(a)에서 '불공정 또는 기만적인 행위 또는 관행'을 금지하고 있는 것을 근거로, 쿠키가 개인정보에 해당하는 범위에 있는 경우 규제를 하고 있다. 특히 옵트 아웃권을 행사했음에도 불구하고 실행되지 않은 경우 개인정보의 침해로 본다. 최근에는, 복수의 유저가 Google에 대해 유저가 브라우저 설정에서 쿠키의 이용을 거부하고 있었음에도 불구하고, Google이 유저의 정보를 추적할 목적에서 쿠키를 이용하였다고 주장하

---

44) 중앙SUNDAY, 전게 뉴스 "가명정보 빅데이터 산업 숨통…개인정보 침해 논란은 여전" 참조.

45) Jeff Chester, "Role of Interactive Advertising & the Subprime Scandal: Another wake-up call for FTC", Digital Destiny. August 28 (2007) http://www.democraticmedia.org/jcblog/?p=349

46) 맞춤형 광고에 대한 ePD의 규율내용과 관련한 상세 소개는, 정다영, "빅데이터 시대의 개인정보 자기결정권", IT와 법 연구 제14집, 2017, 175면 이하 참조.

47) Case C-673/17 Verbraucherzentrale Bundesverband v. Planet49, [2019] ECLI:EU:C:2019:801

48) 이 판례에 대한 자세한 내용과 비판은, Cristiana Santos, Nataliia Bielova, Célestin Matte, Are cookie banners indeed compliant with the law?, CoRR abs/1912.07144 (2019) 참조.

면서 집단소송을 제기하였다. 이 사건에서 2017년에 Google이 같은 브라우저에 있어서의 쿠키의 이용을 정지하는 것 및 원고단체에게 550만 달러를 지급하는 것을 내용으로 하는 화해안이 델라웨어 연방지방법원에서 승인되었지만 2019년 8월 항소심에서 이 사건이 파기환송되어 재논의 중이다.[49]

국내에서도 이러한 세계적 동향은 많은 시사점을 제공한다. 온라인 행위추적에 대해 금지할 수는 없지만, 익명화 또는 가명화에 의해 개인정보의 활용을 허용한 만큼 무분별한 행위추적을 규제할 필요가 있다고 본다. 현행법 하에서도 정보주체의 동의를 얻지 않은 행위추적이나 이미 이루어진 행위추적에 대해 거부했음에도 불구하고 계속되는 행위추적은 위법하므로 불법행위책임을 질 수 있다고 본다.

4. 개인정보 처리행위의 적법화 근거로서의 '동의'에 대한 과제

법영역에서 동의는 예를 들어 불법행위법에서의 위법성 조각사유로서, 또는 계약법에서의 합의라는 형태로서 그 의미가 큰 개념이다.[50] 개인정보 보호법제에 있어서도 정보 주체의 동의는 개인정보의 처리행위에 대한 적법화의 근거로서 중요한 기능을 가지는 것으로 설계되어 있다. 개인정보 보호법 제3장(개인정보의 처리) 제15조 이하의 각 조문마다 개인정보의 수집, 이용, 제공 등을 함에 있어 우선 '정보주체의 동의를 받은 경우'를 규정하고 있는 것을 보면 이 동의의 중요성이 어느 정도인지 잘 보여준다고 할 수 있다. GDPR 제6조제1항에서도 '처리의 적법성'이라는 표제 하에, 처리는 다음 조건의 어느 하나를 충족한 경우에만 적법하다고 하면서, 같은 항 (a)에서 데이터 주체가 하나 이상의 특정한 목적을 위해 자기의 개인 데이터의 처리에 대하여 동의를 부여하고 있는 경우를 규정하고 있다.

개인정보 보호법제에서의 동의는 소위 개인정보 자기결정권을 실현하기 위한 구조로서 이해할 수 있다.[51] 그렇지만 현재의 상황에서는 인터넷을 이용하는데 있어 동의절차가 자동적으로 이루어지거나, 동의를 하지 않으면 다음 단계로 진행되지 않아 인터넷 이용 목적을 달성할 수 없어 반강제성을 띄는 경우도 자주 경험하는 상황이다. 개인정보 보호법제에서의 동의가 개인정보 처리행위의 적법화 근거로서의 기능, 즉 동의가 없을 때에는 위법한 개인정보의 처리행위라도 동의만 있으면 적법화 될 수 있는 기능을 부여하고 있는 것에 비추어보면, 이러한 법적 기능을 부여하는데 가치를 둘만한 동의로서 정보주체의 실질적 의사를 반영하는 동의, 즉 실질적인 동의가 되는 것이 필요하다. 더구나 가명정보의 이용이 활성화되는 상황에서는 개인정보가 하나하나 드러나게 될 위험이 클 수 있으므로 형식적인 동의나 반강제적인 동의만으로는 위법성 조각사유로 삼아서는 안 된다고 본다.

개정 데이터 3법에서는 익명정보는 물론, 가명정보가 될 경우 정보주체의 동의를 생략하도록 하고 있는데, 개인을 식별할 수 없었던 데이터들도 활용 과정에서 개인을 식별할 수 있는 민감정보로 되는 상황도 배제할 수 없다. 이 경우 사업자들이 정보 주체에게 고지하고 동의를

---

49) https://www.mercurynews.com/2019/08/07/appeals-court-voids-google-cookie-privacy-settlement-that-paid-users-nothing/

50) Neil M. Richards, Woodrow Hartzog, The Pathologies of Digital Consent, 96 Wash. U. L. Rev. 1461, 1467 (2019).

51) GDPR에서도 개인 데이터에 대한 결정권이 현저히 드러나는 것이 동의에 관한 규정이라는 견해에 대해서는, van Ooijen, Helena U. Vrabec, Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective, 42 J. Consumer Policy, 91, 94 (2019).

받도록 하는 절차를 보장하지 않는다면 개인정보 자기결정권의 침해 문제를 막지 못할 위험성이 크다. 이 문제에 대한 GDPR과 같은 입법화 논의를 떠나, 이러한 경우에도 우리 개인정보 보호법 제22조의 동의를 받는 방법을 준수하도록 해석상 인정하여야 할 것고, 불법행위책임의 판단에 있어 이러한 조치를 취했는지 여부를 중요한 기준으로 삼아야 할 것이다.

Ⅳ. 맺음말

빅데이터, AI, IoT 등의 기술 진보 및 관련 산업 발전을 위해 개인정보를 포함한 데이터를 적절하게 이용하는 것이 세계적인 흐름이고, 국경을 넘어선 데이터 유통을 고려하여 모든 국가들이 이 흐름에 동참하고 있다. 이러한 시점에서 개인정보의 완벽한 보호만을 강조할 수도 없고, 이용과 보호라는 둘 사이의 균형을 좀 더 정치하게 잡아나갈 필요가 있다. 데이터 3법의 개정에 따라 익명처리 또는 가명처리를 통해 개인정보의 적극적인 이용의 활성화를 도모하였다고는 하나, 사업자가 이것으로 인격권 침해의 문제에서 자유로울 수는 없다. 오히려 재식별화로 인해 인격권 침해가 발생할 여지가 더 커진 만큼 익명 및 가명처리를 하였다고 하더라도, 비식별 처리 후 양도된 새로운 정보가 그 이전에는 없었던 다른 차원의 인격권 침해를 야기할 가능성이 없는지 주의를 기울여야 한다. 이 때문에 비식별 처리된 정보에 대해 암호화 등 안전성 확보에 필요한 최선의 조치를 다하였는지 여부가 불법행위책임의 가장 중요한 판단기준이 될 것으로 보인다.

데이터 3법의 개정이, 국제사회의 흐름에 맞춰 다양한 비식별정보를 폭넓게 이용할 수 있도록 하는 산업발전 측면에 무게를 두다 보니, 개인정보 침해에 대한 방어수단에 있어서는 GDPR에 비추어 미흡한 감이 있다. 향후 입법적 보완이 이루어질 것으로 기대되나, 개정법상 인격권 침해로 인한 불법행위책임을 판단하는데 있어서는 보다 적극적인 해석이 필요할 것으로 보인다. 이를 위해 본고에서는 행위추적 기술에 대한 법적 조치, 위법성 조각사유로서의 동의 제도를 고려하여 불법행위책임의 판단기준에 대한 몇 가지 방향성을 제시해 보았다.

데이터 3법의 개정 과정에서 많은 우려, 반대와 진통이 있었던 만큼, 시행 과정에서 또 다른 문제점이 부각될 가능성이 높고, 개인정보 보호와 관련한 후속 입법이 예상되기도 한다. 각국이 개인정보의 적극적 활용을 도모하면서도 개인정보 자기결정권에 심각한 위험을 끼치는 행위를 규제하는 법제도를 두어 균형을 맞추고자 한 점은 우리에게 많은 시사점을 준다.

<참고문헌>

권건보, “유비쿼터스 시대의 개인정보 침해와 법적 대응방안”, 공법연구 제32집 제5호, 2004.

권태상, “개인정보 보호와 인격권-사법(私法) 측면에서의 검토”, 법학논집 17권 4호, 2013.

김상현,「유럽연합의 개인정보보호법, GDPR」, 커뮤니케이션북스, 2018.

김윤정, “개인정보를 위협하는 데이터 3법”, 월간 한국노총 통권 558호, 2020.

김정선, “가명 데이터 활용연구-기술적 처리방법 및 기업의 활용방향을 중심으로”, 정보보호학회논문지 제30권 제2호, 2020.

김정현, “빅데이터 시대의 개인정보 보호법제 개선방안”, 법학논총 제46집, 2020.

김태선, “자율주행과 데이터보호”, 비교사법 제26권 제4호, 2019.

문재완, “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 2014.

박주희, “민간부문 개인정보보호를 위한 약관 통제”, 성균관법학 제32권 제1호, 2020.

백승엽·김일환, “개인신용정보 비식별조치의 내용과 한계에 관한 연구”, 성균관법학 제29권 제4호, 2017.

안병하, “인격권 침해와 부당이득반환-침해구제의 측면에서 본 퍼블리시티권 도입 불필요성” 민사법학 제68호, 2014.

윤태영, “위치정보 침해에 대한 불법행위책임”, 민사법학 제81호, 2017.

이규엽·엄준현, “미국 개인정보보호법 입법 동향: 국내 개정법과의 비교 및 시사점”, KIEF 오늘의 세계경제 제20권 제3호, 2020.

전승재·주문호·권헌영, “개인정보 비식별 조치 가이드라인의 법률적 의미와 쟁점”, 정보법학 제20권 제3호, 2016.

정다영, “빅데이터 시대의 개인정보 자기결정권”, IT와 법 연구 제14집, 2017.

황주성, “빅데이터 환경에서 프라이버시 문제의 재조명”,「빅데이터와 위험 정보사회」, 커뮤니케이션북스, 2013.

村上康二郎,「現代情報社会におけるプライバシー個人情報の保護」、日本評論社、2017.

Article 29 Data Protection Working Party, “Guidelines on Consent under Regulation 2016/67 9”, (2018)

Cristiana Santos, Nataliia Bielova, Célestin Matte, Are cookie banners indeed compliant with the law?, CoRR abs/1912.07144 (2019)

Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012)

Jeff Chester, “Role of Interactive Advertising & the Subprime Scandal: Another wake-up call for FTC”, Digital Destiny. August 28 (2007)

Jeff Chester, Cookie wars: how new data profiling and targeting techniques threaten citizens and consumers in the 'big data' era. In: Gutwirth S et al (eds) European data protection: in good health? Springer, Dodrecht (2012)

Neil M. Richards, Woodrow Hartzog, The Pathologies of Digital Consent, 96 Wash. U. L. Rev. 1461 (2019)

Pamela L. Alreck, Robert B. Settle, Consumer reactions to online behavioural tracking and targeting, in: Database Marketing & Customer Strategy

Management, Vol. 15, 1 (2007)
Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010)
President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective (2014)
The Article 29 Data P rotection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation" (2017)
The White House, "Big Data and Privacy: A Technological Perspective", "Big Data: Seizing Opportunities, Preserving Values" (2014)
van Ooijen, Helena U. Vrabec, Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective, 42 J. Consumer Policy, 91 (2019)