블록체인과 개인정보 규제 합리화 방안 검토

김 현 경*

〈요 약〉

개인정보에 대한 권리는 절대적 권리가 아니며, 비례성 원칙에 부합하도록 다른 기본권들과도 조화되어야 한다. 특히 개인정보 보호제도는 혁신적 기술에 장애가 되고자 고안된 제도는 아니다. 이러한 관점에서 본 연구는 최근 이슈가 되고 있는 블록체인 기술 및 서비스를 둘러싼 개인정보 규제 쟁점을 검토하고 그 개선방안을 모색해 보았다. 블록체인의 거래정보는 그 자체만으로는 개인의 식별이 곤란하다 할지라도 현행법상의 식별가능성의 판단에 비추어 볼 때 개인정보에 해당될 수 있다. 따라서 블록체인 서비스에 있어서 '거래정보'의 처리가 법 위반이 되지 않도록 '가명정보'의 이용근거 마련, 이에 상응하는 '재식별 금지' 규정의 도입 등이 필요하다. 또한 '퍼미션리스(permissionless) 블록체인'의 경우 거래의 참여자가 개인정보처리자에 해당될 수 있으나 그 수가 무제한이므로 실질적으로 개인정보처리자에게 규범준수를 강제하도록 설계하는 것이 곤란하다. 결국 블록체인 시스템 운영자(사업자)에게 일정한 책임을 부여하는 입법의 가능성이 있다. 이러한 경우 면책요건도 함께 규정하여 블록체인 시스템 운영자의 부담을 경감시킬 필요가 있다. 한편 블록체인의 기술적 특성에 비추어 볼 때 현행법상 '적법한 동의'의 요건을 충족하는 것은 상당히 곤란하다. 안정적 서비스가 가능하도록 현행법상 ' 동의' 규정의 개선이 필요하다. '블록체인'은 많은 영역에 새로운 가치와 서비스를 제공할 수 있고 이로부터 많은 혜택을 얻을 수 있다. 이러한 혜택에 개인정보 규제가 걸림돌이 되어서는 안 될 것이다.

[검색어] 블록체인, 개인정보, 개인정보처리자, 블록체인 시스템 운영자, 정보주체의 권리

---

* 서울과학기술대학교 IT정책전문대학원 교수, 법학박사

이화여자대학교 법학논집 제23권 제1호 통권 63호 (2018. 9)
Ewha Law Journal, vol. 23, no. 1 (2018. 9)

Ⅰ. 서 론

누가 뭐라 해도 최근 대세라 할 수 있는 기술적 이슈는 '블록체인'이다. 그러나 블록체인의 특성상 모든 참여자가 거래 내용이 기록된 원장을 보유하게 된다. 따라서 거래당사자 뿐만 아니라 블록체인 상의 모든 참여자가 거래 내용을 볼 수 있고 이 때 발생하는 원장정보의 공유가 현행 개인정보 보호법제와 부합하는지가 문제될 수 있다. 가장 기초적 문제로서 그러한 블록의 '원장정보'가 개인정보에 해당되는지 여부, 개인정보에 해당된다면 이러한 개인정보의 공유가 현행법상 합법적인지 여부 등이 문제될 수 있다. 설사 블록체인을 활용한 서비스와 관련하여 이러한 기술적 내용을 모두 이해하고 서비스 이용과 관련된 개인정보의 처리에 동의하였다 할지라도 그러한 포괄적 동의가 현행법상 유효한지 검토할 필요가 있다. 또한 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 등 개인정보보호법령에 의하면 개인정보의 수집 목적을 달성하거나 정보주체의 요청 시 수집된 개인정보를 삭제하여야 하는데 블록체인에 올라간 거래내역은 수정과 삭제가 불가능하므로 현행법과 갈등의 여지가 있다. 의료, 금융, 물류 등 사회 각 영역에서 블록체인 기술의 활용이 논의되고 있으나, 이러한 규제의 불안감이 해결되지 않는 한 서비스의 발전은 제한적일 수밖에 없다. 최근 방송통신위원회, (구)미래창조과학부, 행정안전부 등 6개 관계부처가 2016년 합동으로 마련한 '개인정보비식별조치 가이드라인'에 따라 비식별조치를 통해 '정보집합물 결합서비스'를 제공한 사안에 대하여 시민단체가 한국인터넷진흥원(KISA) 등 개인정보 비식별화 전문기관 및 20개 기업을 검찰에 고발한 바 있다.[1] 정부의 가이드라인에 따른 조치를 이행하였음에도 불구하고 송사(訟事)에 휘말릴 수 있다면 어떠한 기업도 규제불안감 속에서 혁신적 서비스를 개발하기를 꺼려할 수밖에 없다. 따라서 본고에서는 블록체인을 둘러싼 개인정보 규제 쟁점을 검토하고 그 개선방안을 모색해 보고자 한다.

---

1) 2017년 11월 9일, 참여연대 등 12개 시민단체는 서울중앙지검 정문 앞에서 공동기자회견을 열고 한국인터넷진흥원 등 개인정보 비식별화 전문기관과 이 기관들에 정보를 제공한 기업을 검찰에 고발한다고 밝혔다. 시민단체들에 따르면 이들 기관은 통신 3사와 보험사, 카드사 등 20여개 기업으로부터 고객 정보를 넘겨받아 이른바 '정보집합물 결합서비스'를 통해 3억4,000여 만 건의 정보결합물을 기업에 제공했다. 시민단체들은 "기업이 보유한 고객의 정보를 무단으로 제공하고 처리하도록 한 것은 개인정보보호법과 정보통신망이용촉진 및 정보보호등에 관한 법률, 신용정보보호법을 위반한 것"이라고 주장했다. ""前 정부때 지침 따랐을 뿐인데..." 고발당한 '개인정보 제공' 기업들", 「서울경제」, 2017년 11월 9일자.
http://www.sedaily.com/NewsView/1ONIHGZBQ7 (최종방문일 2018. 6. 6.).

Ⅱ. 블록체인 개념 및 유형

1. 개념

우리가 통상 '비트코인', '블록체인', 'DLT(distributed ledger technology)'를 동시에 사용하지만, 'DLT'는 탈중앙화 되고 분산된 모든 종류의 거래 원장에 대한 패밀리 이름이라고 할 수 있다. 블록체인은 블록 및 체인을 사용하여 거래기록을 저장하고 보호하는 DLT의 특수한 유형이다. 비트코인은 블록체인을 사용하여 모든 거래를 기록하는 '암호화폐 어플리케이션'이다. 즉 비트코인은 블록체인의 한 가지 유형이며 블록체인은 DLT의 한 유형이다.[2)]

기존 시스템은 장부를 중앙집중형으로 관리하므로 제3의 신뢰할 수 있는 기관(TTP : Trusted Third Party)을 설립하여 이러한 기관이 부여하는 인증 등의 방식을 통해 신뢰를 확보하고자 하였다. 이러한 중앙 집중 기관에서 문제가 발생하여 시스템에 대한 신뢰가 훼손되는 것을 예방하기 위해, 높은 관리비용을 소모하게 되며 그럼에도 불구하고 여전히 해킹의 위험은 상존한다. 그러나 블록체인은 서버나 클라이언트 없이 개인컴퓨터 사이를 연결하는 통신망인 P2P(Peer to Peer) 네트워크를 기반으로 한다. 즉, 거래정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하게 된다. 따라서 중앙 집중적 조직이나 공인된 제3자가 필요 없게 되므로 중앙집중형 시스템의 운영 및 유지보수, 보안, 금융거래 등에 필요한 비용을 절감할 수 있다.

블록체인은 P2P기반 분산처리 방식으로 인한 분산성, 누구나 참여할 할 수 있는 확장성, 모든 내용에 접근 가능한 투명성 등의 특성을 가지게 된다. 따라서 금융거래에서는 투명성, 추적 용이성이 보장되고, 문서기록에서는 데이터의 변조 문제를 해결하며 무결성을 보장한다는 장점이 있다.

블록체인의 아키텍처는 성사된 모든 거래가 원장에 기록되고 이러한 원장은 네트워크상에 있는 모든 참여자의 컴퓨터에 분산 처리된다. '동의(합의)'라는 기능이 작동하기 위하여 매우 복잡한 수학적 수단을 통해 확인되지 않는 한 어떠한 거래도 블록에 추가될 수 없다. 그 결과 블록에 있는 항목을 삭제하거나 변경할 수 없으며 해당 네트워크에

2) Chang, H. (2018). Is Distributed Ledger Technology Built for Personal Data? *Journal of Data Protection & Privacy.* 1(4). 1.
https://ssrn.com/abstract=3137606. (최종방문일 2018. 8. 21.).

연결된 모든 사람은 동일한 원장사본을 보유할 수 있다.

예를 들어, A가 B와 거래를 하는 경우, A와 B의 거래기록이 거래당사자 이름, 금액 등의 형태로 기록되는 것이 아니라 암호처리 되어 공식 주소(예컨대, 『15KGAfhff1B15nsrhbLYHH9WpHvpCaKPK5』와 같은 형식이다)의 형태로 공개된다. 이와 같이 공개된 암호기록에 대해 참여자들이 암호를 푸는 복잡한 계산을 수행함으로서(이 과정이 mining이다) 거래의 유효성을 확인한다. 거래가 계속될수록 암호화기록이 다수에게 분산된 형태로 추가된다. 따라서 일부 참여자가 블록체인상의 이러한 기록을 조작하더라도 다른 참여자가 보유하는 기록을 통하여 진위여부가 걸러질 수 있기 때문에 기록을 변조하는 것은 현실적으로 불가능하다.[3]

2. 유형

(1) 퍼블릭(Public) vs. 프라이빗(Private) vs. 컨소시엄

블록체인은 참여 네트워크의 성격, 범위, 거버넌스 체계 등에 따라 퍼블릭, 프라이빗, 컨소시엄 블록체인으로 구분할 수 있다.[4]

퍼블릭 블록체인은 공개형으로 누구나 참여할 수 있는 블록체인이다. 따라서 모든 참여자는 자유로운 자료 열람과 거래가 가능하지만 검증되지 않은 다수의 사용자가 참여하므로 고도화된 암호화 검증이 필요하여 네트워크의 확장이 어렵고 속도가 느리다. 퍼블릭 블록체인은 완벽한 분산형 구조를 이루고 있으며 네트워크 참여자가 익명성의 성격을 띠게 된다. 또한 퍼블릭 블록체인에서는 데이터가 투명하게 공개되기 때문에 문서의 무결성을 검증하는 데 유익할 수 있으나 기밀데이터를 포함한 모든 데이터가 공개된다는 점은 고려해 보아야할 문제이다.

프라이빗 블록체인은 한 기관이 모든 권한을 가지며 거래에 참여하는 모든 사람은 그러한 기관의 허가를 받아야만 하므로 분산장부의 장점을 이용한 중앙집권형 구조라고 할 수 있다. 익명성을 제공했던 퍼블릭 블록체인과 달리 참여자 식별이 가능하다. 또한 처리 속도가 빠르고 네트워크 확장이 용이하며 사용자가 원하는 대로 커스터마이징 할 수 있다. 프라이빗 블록체인은 블록체인을 생성하고 관리하는 자가 블록체인을 중앙 시

3) 김제완, "블록체인 기술의 계약법 적용상의 쟁점- '스마트계약(Smart Contract)'을 중심으로 -", 『法曹』(법조협회, 2018), 제67권 제1호, 157-158면.

4) 홍승필, "공공 및 전자정부 블록체인 활용방안 관련 개인정보보호 및 정책관련 동향 연구", 『전자정부민관협력포럼』(2017).

스템처럼 관리하고자 하는 경우에 적합하다. 예를 들어 모두가 자료를 읽을 수는 있으나 자료를 기록하는 것은 특정 주체만 가능한 경우, 또는 읽기와 쓰기(기록)는 모두 특정 주체만이 가능한 경우 등이다.

컨소시엄 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인의 중간 형태이며 미리 선정된 참여자들이 권한을 가지게 되는 블록체인이라고 할 수 있다. 따라서 컨소시엄 블록체인은 분산형 구조를 유지하면서 제한된 참여를 통해 보안을 강화할 수 있고 퍼블릭 블록체인에서 제기된 느린 거래 속도와 네트워크 확장성의 문제도 일정부분 해소시켜 줄 수 있다.

(2) 퍼미션(permissioned) 블록체인 vs. 퍼미션리스(permissionless) 블록체인

블록체인의 개방성은 체인이 연속된다는데 있다. 이러한 연속성은 극단적 기준으로 두 유형으로 분류될 수 있다. 승인여부와 관련 없이 누구나 참여자가 될 수 있는 '퍼미션리스(permissionless) 블록체인'과(대표적으로 비트코인이 그러하다), 허가된 즉 승인된 자만 참여할 수 있는 '퍼미션(permissioned) 블록체인'이다.

'퍼미션리스(permissionless) 블록체인'에서 개별 참여자는 거래의 유효성에 참여하게 된다. 따라서 개별 참여자는 모두 거래의 유효성에 대한 합의에 도달해야 하고, 이러한 참여자 모두 거래에 대하여 읽고 기록할 수 있는 권리(the right to read and write)를 가진다.

반면 '퍼미션(permissioned) 블록체인'에서는 선택된 그룹의 참여자만이 거래의 유효성에 참여할 수 있으며, 이들만이 기록할 수 있는 권리(the right to write)를 가진다.[5] '기록할 수 있는 권리(the right to write)'는 이들만이 보유하지만, 읽을 수 있는 권리(the right to read)는 '퍼미션리스(permissionless) 블록체인'처럼 모든 이들에게 인정할 수도 있고 선택된 그룹의 참여자로 제한할 수도 있다.

'퍼블릭 블록체인'에서는 '퍼미션리스(permissionless) 블록체인'과 '퍼미션(permissioned) 블록체인'의 유형을 모두 가질 수 있다. '퍼블릭 퍼미션리스(permissionless) 블록체인'의 경우 읽고 기록할 수 있는 권한은 참여자 누구에게나 보장된다. '퍼블릭 퍼미션(permissioned) 블록체인'의 경우 기록은 누나 읽을 수 있으나, 기록은 권한을 부여받은 자에게만 허용된다. 그러나 '프라이빗 블록체인'과 '컨소시움 블록체인'의 경우 특정수의 참여자만이 블록의 유효성 검증에 참여하게 되므로 '퍼미션(permissioned) 블록체인'이 가

5) R3(https://www.r3.com/)가 대표적인 이러한 컨소시움 블록체인이다.

능하다.

비트코인은 다른 많은 암호화폐와 마찬가지로 '퍼블릭 퍼미션리스(permissionless) 블록체인' 방식이다. 즉, 특정 당사자나 참여자에 의해 승인될 필요 없이 모든 참가자가 비트코인 네트워크에 참여할 수 있다는 것을 의미한다. 비트코인 참가자의 익명성을 감안할 때 단일 참여자는 신뢰할 수 없으며, 대다수가 음모를 꾸미는 것은 불가능하다는 개념에 기반 한다. 즉, 참여자가 악의적일 수 있지만 시스템을 속이는데 모든 참가자의 50% 이상이 합의한다는 것은 불가능하다. 따라서 비트코인 설계는 한 참여자의 원장 블록을 다른 모든 참여자의 원장에 복사함으로서 작동하며 따라서 이것이 작동하려면 모든 참여자가 원장을 읽을 수 있어야 한다.

반면 허가된 참여자로 제한하는 블록체인 유형의 경우 원장이 모든 참여자에게 복사될 필요가 없으며, 소수의 신뢰할 수 있는 참여자만이 유효성 검사 및 백업 작업에 할당될 수 있다. 이러한 '퍼미션(permissioned) 블록체인'의 구현에서는 전체 원장을 다른 모든 참여자의 블록에 복사 할 필요는 없으며 신뢰할 수 있고 지정된 참여자에게만 복사 할 수 있다.

<블록체인의 유형>

유형		읽기(Read)	기록(Write)
퍼블릭	퍼미션리스 (permissionless)	누구나 가능	누구나 가능
	퍼미션 (permissioned)	누구나 가능	권한이 부여된 참여자로 제한
컨소시움	퍼미션 (permissioned)	권한이 부여된 참여자로 제한	권한이 부여된 참여자로 제한
프리이빗	퍼미션 (permissioned)	제한된 범위의 참여자로 제한	블록체인 네트워크 운영자로 제한

(3) 블록체인과 프라이버시

비트코인 거래 시 주소의 반복적인 재사용은 사용자의 프라이버시를 침해할 수 있고 이용자들 역시 이에 대한 우려를 나타내고 있다.[6] 표면상 비트코인 참여자는 익명이고

6) Barcelo, J. (2007). User Privacy in the Public Bitcoin Blockchain. *Journal of LATEX. 6(1)*; Fabian, B., Ermakova, T., & Sander, U. (2016). Anonymity in Bitcoin – The Users Perspective. *Thirty Seventh International*

거래당사자의 실제 신원 정보와 연결되어 있지 않지만, 실제적으로 거래에 사용하는 주소와 해당 주소를 통해 거래당사자를 식별할 수 있을 가능성이 충분히 존재한다는 것이다. 거래 시 사용하는 주소는 특정 거래와 연결되어 있고 이러한 거래 내역은 결국 거래당사자와 관련된 것이기 때문이다. 또한 거래기록을 의미하는 주소의 누적은 거래당사자를 식별할 수 있는 데이터의 증가를 의미하므로 처음 비트코인을 고안한 사토시 나카모토 역시 그의 논문에서 주소의 재사용은 지양되어야 한다고 밝히고 있다.[7]

블록체인과 스마트 계약[8]의 표현방식과 이들 기술이 가진 속성에도 불구하고 현재의 형태로는 스마트계약에서 발생하는 모든 일련의 것들이 네트워크를 통해 전파되고 블록체인에 기록되어진다. 또한 블록체인의 모든 참여자가 볼 수 있다. 따라서 거래 참여자들이 익명성을 높이기 위해 새로운 공개키를 계속해서 재생성한다고 하더라도 각각의 공개키에 해당하는 모든 거래내역이 모두에게 공개되며, 이러한 거래내역을 이용하여 익명성을 제거하는 공격도 가능하다고 한다.[9]

Ⅲ. '원장정보'의 개인정보 해당성

1. 정보주체는 누구인가

이는 블록체인에서 누구의 프라이버시에 대하여 주의해야 하는가라는 문제와 연결된다. 블록체인 네트워크에 참여하고 있는 이용자(user) 즉 거래당사자의 프라이버시가 보호받아야 함은 명확한 것 같다. 그러나 GDPR을 비롯한 개인정보규제는 그러한 당사자뿐만 아니라 거래의 유효성을 검증하는 참여자들의 프라이버시와도 관련된다. 모순되게도 이용자 즉 거래당사자의 프라이버시가 더 잘 보호받기 위해서는 유효성을 검증하는 참여자들의 수가 더 많아야 하므로 이들의 프라이버시는 덜 보호되는 상황에 이르게 된다. 사실 특수한 거래 기법이 적용되지 않는 한, 거래 당사자의 신분은 항상 추적 될 수 있다.[10] EU에서도 「돈세탁금지지침」(the anti-money laundering directive)과 고객확인의무

Conference on Information Systems-Dublin. 1-2.

7) Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (최종방문일 2018. 8. 21.).

8) 스마트계약에 대하여는 후술한다.

9) Kosba, A. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. *IEEE Symposium on Security and Privacy (SP).*

10) Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex

(know your customer, "KYC")에 대한 사항은 GDPR이 적용되지 않는다. EC는 암호화폐(cryptocurrency)의 거래에 있어서 이용자를 식별할 것을 요구하도록 돈세탁금지지침을 개정하는데 동의하였다.[11] 고객확인의무 역시 거래대상과 거래자의 공개를 필수요건으로 한다. 따라서 블록체인 기반에서 이루어지는 암호화폐거래가 이러한 지침과 의무가 적용될 경우 모든 관련자에 대한 추적 및 식별이 가능하다.

그러나 매우 많은 숫자의 참여자들이 블록체인 네트워크상에 존재한다. '퍼미션리스(permissionless) 블록체인'의 경우 모든 거래의 유효성을 검증하는데 모두가 참여하는 것이 아니므로 누군가는 어떠한 거래에 있어서는 유효성검증의 참여자가 될 수도 있고 그렇지 않을 수도 있다. 따라서 일단 유효성 검증의 역할을 완료하였을 때 그들의 컴퓨터에 원장을 유지할 수도 있고 그렇지 않을 수도 있다. 이러한 '퍼미션리스(permissionless) 블록체인'에서 모든 참여자의 개인정보 보호와 프라이버시를 책임질 사람을 정확히 지목하고 그에게 책임을 부과하고자 하는 것은 현실적이지 않다.[12] 따라서 우선적으로 고려되어야 할 것은 '거래당사자의 프라이버시'라고 할 수 있다.

2. 원장정보의 '식별가능성'

(1) '식별가능성'의 의미

GDPR과 우리 개인정보 보호법령 모두 개인정보의 개념을 '식별가능성'을 기준으로 규정하고 있다. 다만 GDPR은 익명정보(anonymous information)에 대하여는 개인정보 보호원칙이 적용되지 않는다고 명시하고 있으나, 익명성에 대한 명확한 정의는 내리지 않고 있다. 단지 익명성이라는 단어가 가지는 사전적 의미에서 알 수 있듯이 식별되거나 식별가능한 자연인과 관련되지 않는 정보, 또는 개인정보이나, 정보주체가 식별되지 않거나 더 이상 식별될 수 없도록 조치한 정보를 의미한다고 기술하고 있다.[13] 제29조 실무 위원회(Working Party, 이하 "WP29")의 의견에 의하면 익명성이라 함은 '불가역적인

Cryptographia. *SSRN Electronic Journal*. 21. ; De Filippi, P. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production*. 7:Alternative Internets. 10-14. https://hal.archives-ouvertes.fr/hal-01382006/document (최종방문일 2018. 9. 27.).

11) Guarascio, F. (2017. 12). EU agrees clampdown on bitcoin platforms to tackle money laundering. *Reuters,* retrieved from https://www.reuters.com/article/uk-eu-moneylaundering/eu-agrees-clampdown-on-bitcoin-platforms-to-tackle-money-laundering-idUSKBN1E928M (최종방문일 2018. 8. 21.).

12) Salmensuu, C. (2018). The General Data Protection Regulation and the Blockchains. *Liikejuridiikka*. 2018(1). 10. https://ssrn.com/abstract=3143992 (최종방문일 2018. 8. 21.).

13) Recital 26 Articles 4 and 5 of the GDPR.

익명성(irreversible anonymisation)'을 의미한다고 한다. 즉 데이터 처리과정에서 개인정보로 추출하는 것이 불가능한 형태를 의미한다.

결국 핵심은 '식별가능성'의 유무이므로, '식별가능성'의 수준을 어디까지 요구할 것인가 하는 것이 익명화 판단의 핵심이다. 해당 정보로 인해 정보주체를 식별할 수 있는지는 상황에 따라 복잡하게 나타날 수 있다. 식별가능성 기준에 충족하는 지를 평가하는데 요구되는 판단의 방법에 대하여 '절대적 접근법'과 '상대적 접근법'으로 설명하는 견해가 있다.[14]

'절대적 접근법'에 의하면, 개인정보처리자등[15]이 들여야 하는 노력 혹은 비용을 불문하고 정보주체를 개별적으로 식별하기 위해 취할 수 있는 모든 가능성과 기회들이 고려되어야 한다.[16] 이러한 접근법에 의할 경우 "누군가가 데이터 세트를 해독 할 수 있는 한", 개인정보처리자등이 그러한 해독키를 소지하고 있지 않다 할지라도 책임을 부담하게 된다.[17] 그러나 '상대적 접근법'에 의하면 개인정보처리자등에게 정보주체를 식별하기 위해 요구되는 필수적 비용과 노력만이 고려된다.[18] 이러한 의미에서 볼 때 개인정보처리자등이 데이터셋을 해독할 수 있거나 적어도 해독키를 획득할만한 합리적 기회가 있는 경우에만 법의 적용을 받는다.[19]

GDPR이 어떠한 견해를 따르는 지는 모호한 부분이 있다. "자연인이 식별가능한지 결정하기 위해서는 개인정보 통제자(data controller) 또는 다른 누군가가 자연인을 직접 또는 간접적으로 식별하기 위해 합리적으로 사용될 수 있는 모든 수단을 고려하여야 한다"고 기술하고 있다.[20] 개인정보 통제자 뿐만 아니라 제3자의 수단까지 고려해야 하므로 절대적 접근법을 취하고 있다고 보는 견해도 있으나,[21] 합리적으로 사용될 수 있는

14) Spindler, G., & Schmechel, P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. *JIPITEC*. 2016(7). 14. https://www.jipitec.eu/issues/jipitec-7-2-2016/4440/spindler_schmechel_gdpr_encryption_jipitec_7_2_2016_163.pdf (최종방문일 2018. 8. 21.).

15) 우리법은 '개인정보처리자', GDPR은 개인정보 통제자와 개인정보처리자의 개념을 분류사용하고 있다. 본고에서는 이를 통칭하여 '개인정보처리자등'이라 한다.

16) Spindler, G., & Schmechel, P., 앞의 논문(주 14), Supra note 17. 165.

17) *Ibid.*

18) *Ibid.*

19) Spindler, G., & Schmechel, P., 앞의 논문(주 14), 165면.

20) Recital 26.3 은 다음과 같이 기술하고 있다.
"(…) to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

21) Borgesius, F. J. Z. (2016). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer law & Security review*. 9.

수단(“the means reasonably likely”)에 제한하고 있으므로 상대적 접근법을 취하고 있다고 보는 견해도 있다.[22]

유럽사법재판소는 the Breyer case[23]에서 ‘유동 IP주소(dynamic IP address)가 개인정보에 해당하는가와 관련하여, “IP주소만으로는 해당 네트워크에 연결된 디바이스를 작동하는 특정인이 누구인지 식별할 수 없으므로, IP주소는 인터넷서비스제공자(ISP)가 정보주체를 식별할 수 있는 법적 수단을 가지고 있는 경우에만 개인정보에 해당 된다”고 밝힌 바 있다. 이는 사실상 특정 데이터가 동시에 개인정보일 수 도 있고 그렇지 않을 수도 있다는 모호성이 있음을 인정한 것이라 볼 수 있다.[24] 이러한 판시에 따르면 IP주소가 개인정보로 규율되기 위해서는 IP주소가 특정인을 식별하는데 있어 의미를 가질 수 있도록 다른 정보를 획득할 법적 수단을 가지고 있어야 한다. 즉 여기서 이러한 법적 수단은 특별히 법에 의해 금지되지 않으면서 가능한 수단을 의미한다.[25]

WP29는 ‘식별’이라 함은 단지 개인의 이름, 주소 등을 찾아낼 수 있는 가능성과만 관련된다고 생각되어 져서는 안 되며, 추출, 연계, 참조 등에 의한 잠재적 식별가능성을 포함한다고 한다.[26] 또한 유럽에서는 데이터에 대한 정보, 즉 메타데이터 역시 개인정보에 해당된다.[27] 정보주체는 반드시 이름이나 주소 없이도 인식될 수 있다. 또한 GDPR의 Recital 30은 “자연인은 응용 프로그램 등 기타 장치를 통해 IP주소, 쿠키 식별자 또는 무선 주파수 식별 태그와 같은 온라인 식별자와 연관 될 수 있다. 서버로부터 수신된 유일한 식별자와 다른 정보들이 합쳐져서 흔적을 남길 수 있고 특정인을 식별하고 프로파일링 하는데 사용될 수 있다”고 기술하고 있다. 따라서 GDPR의 Recital 30에 의할 경우 IP주소뿐만 아니라 IoT(Internet of Things) 기술환경에 의해 생성된 수많은 데이터들도 그러한 데이터들이 단순히 기계정보에 불과한 속성데이터임에도 불구하고 개인정보로 취급될 수 있다.[28]

---

22) Esayas, S. Y. (2015). The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the ‘all or nothing’ approach. *European Journal of Law and Technology*. 6(2). 6.

23) Patrick Breyer v Bundesrepublik Deutschland 35 ECJ, Case C-582/14.

24) El Khourya, A. (2017). Dynamic IP Addresses Can Be Personal Data, Sometimes. A Story of Binary Relations and Schrodinger’s Cat. *European Journal of Risk Regulation (EJRR)*. 8(1). 191-197.

25) Salmensuu, C., 앞의 논문(주 12), 16-17면.

26) Article 29 Working Party, 2014 on the Anonymisation Techniques, WP 216.

27) Article 29 Working Party, ‘Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes’ WP 215.

28) Spindler, G., & Schmechel, P., 앞의 논문(주 14), 168면.

(2) 블록 거래정보의 식별가능성

WP29의 설명과 개인정보에 대한 유럽사법재판소의 판결에 비추어 볼 때 블록체인의 데이터가 완전히 암호화 되고 본질적으로 그러한 데이터를 정보주체와 연계시킬 수 없을지라도, 메타데이터를 포함하고 있는 한 i) 개인을 식별하는데 필요한 접근수단이 법에 의해 특별히 금지되어 있지 않고, ii) 그러한 정보가 획득되는 과정이 특별히 복잡하지 않으면 개인정보로 판명 될 수 있다.[29] 데이터셋에서 특정인을 추출해 낼 수 있는 정도에 따라서 '가명정보'와 '익명정보' 여부가 결정된다. GDPR에 의하면 "가명성"이라 함은 "추가 정보를 사용하지 않고는 개인정보가 특정 정보 주체에게 더 이상 귀속 될 수 없도록 개인정보를 처리하는 것을 의미하며, 그러한 추가 정보는 별도로 보관되며 개인정보가 식별된 또는 식별될 수 있는 자연인에게 귀속되지 않도록 하는 기술적·조직적 조치"를 의미한다.[30] WP29의 견해로, '가명화'는 정보주체의 원래 신원과 데이터 집합의 연결 가능성을 감소시키는 반면, 자연인은 여전히 간접적으로 식별 될 가능성이 있다고 한다.[31]

블록체인상의 정보가 온라인상에서 익명성을 유지한다고 할지라도 네트워크 밖의 다른 정보와 결합되어 그러한 익명성이 훼손될 수 있는 가능성은 항상 존재한다. 네트워크 밖의 정보들은 이메일 주소, 배송지 주소, 신용카드번호, 은행계좌 등이 포함된다. 예를 들어 비트코인을 결재수단으로 승인할 경우 당사자들을 통해 접근가능 한 IP주소도 포함될 수 있다. 즉 과거의 거래와 관련된 IP 주소를 공개할 수 있는 비트코인 수신자의 공개키와 연계시켜 이용자를 식별할 수 있는 정보를 얻을 수도 있다고 한다.[32] 결론적으로 외부정보를 사용함으로서 공개키를 서로 연계시키게 된다면 '익명성'은 비트코인의 특성이 될 수 없다.[33] 비트코인이 현금과 동일한 수준의 익명성을 유지할 수 없다면, 점점 스마트해지는 알고리즘은 정보주체를 식별할 수 있는 개인정보를 획득하기 위하여 지속적으로 외부정보와 연계시키기 위한 패턴을 만들어낼 것이다.[34] 따라서 비트코인상의 원장정보는 익명정보라 할 수 없다.

한편 '퍼미션리스(permissionless) 블록체인'에서 참여자들이 유효성 검증을 요청받은

29) Salmensuu, C., 앞의 논문(주 12), 17면.
30) GDPR Article 4(5).
31) Article 29 Working Party, 2014 on the Anonymisation Techniques, p. 21.
32) Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. New York: Springer Link. 15-17.
33) *Ibid.*
34) Narayanan, A., Bonneau, J., Felten, E. W., Miller, A., Goldfeder, S., & Clark, J. (2016). Bitcoin and Cryptocurrency Technologies, A Comprehensive Introduction. Princeton University Press. 14.

거래라는 사실을 인식하고 있는 상태를 유지하면서, 데이터를 완전히 불가역한 상태로 익명화시키는 것은 불가능하다. 따라서 블록체인상의 거래정보는 완전히 익명화 될 수 없으므로 GDPR의 적용을 받는 개인정보이며, 다만 가명화는 가능하다고 보여진다.

3. 개인정보의 분리보관과 '해시(hashes)'

블록체인과 개인정보 규제와의 갈등을 해결하기 위해 일각에서는 기술적 방식을 통한 해결을 제안하기도 한다. 개인정보 보호를 위해 체인 밖의 별도의 저장소를 만드는 방안이다. 즉 개인정보를 암호화하여 블록 밖의 외부 데이터베이스에 별도로 저장하되, 블록에는 개인정보의 해시가 저장될 수 있다. 이러한 경우 블록 밖의 외부 데이터베이스에 저장된 개인정보는 보유목적이 더 이상 유효하지 않을 때 삭제될 수 있다. 즉 정보주체의 삭제권은 보장될 수 있다. 거래 후 블록에 저장되기 전, 즉 블록 형태로 기록되기 전에 임시 저장소를 통해 식별성이 있는 개인정보에 대해서는 비식별화 기술을 적용하고, 생성되는 개인정보에 대해서는 계약의 기간 동안에만 저장 및 활용되고 이후에는 파기될 수 있도록 정보의 유효기간을 지정하는 방안도[35] 이와 유사한 기술적 원리를 적용한 것이라 할 수 있다.

그러나 이러한 기술적 방안을 사용한다 할지라도 "외부저장소에 있는 개인정보로부터 생성된 블록상의 '해쉬'는 '개인정보'에 해당되는가"라는 문제에 직면하게 된다. 컴퓨터 과학자들은 해시가 도로 개인정보로 되돌려 질 수 없는 '일방 변형'이라고 주장한다. 그러나 원래의 데이터를 '추측'할 수 있는 방법이 있다. 결국, 해시의 주요 목적 중 하나는 해시가 생성 된 정보를 검증할 수 있는지 확인하는 것이다.[36] 일례로 해시의 가장 일반적인 사용은 패스워드를 저장하는 것이다. 허가되지 않은 접근/공개의 우려로 패스워드를 일반 텍스트로 저장하는 대신 패스워드의 해시를 저장한다. 사용자가 다시 로그온하려면 새로 입력 한 패스워드가 해시화 되고 같은 방식으로 이미 저장된 해시와 비교된다. 일치하면 새로 입력 한 암호가 원래 암호와 동일하고 사용자에게 접근이 허용됨을 의미한다. 그러나 이러한 해시를 계산하는 데 단지 몇 가지 표준 방법만 있기 때문에 충분한 시간과 끝없는 조합의 노력만 주어지면 패스워드가 깨지고 밝혀 질 수 있다. 패스워드가 최대 8자까지만 가능한 경우처럼 패스워드 패턴이 알려지면 현실적으로 더 쉽게

35) 이수현·김혜리·홍승필, "개인정보보호를 고려한 블록체인 데이터 설계 방안 연구", 『한국통신학회 학술대회논문집』(한국통신학회, 2018), 478-479면.
36) Chang, H., 앞의 논문(주 2), 5면.

패스워드를 알 수 있다. 마찬가지로, 사회보장번호, 생년월일, 은행 계좌 번호 등과 같이 외부 데이터베이스에 저장된 개인정보의 패턴이 알려지면 해시에 액세스하는 것은 실제적으로 개인정보에 액세스하는 것을 의미한다. 이러한 일체의 작업이 합리적인 시간 내에 완료 될 수 있다.[37]

이렇게 볼 때 해시 자체는 현재 식별되지 않는 정보라 할지라도 '식별가능성'이 있다면 '개인정보'에 해당될 수 있다. 앞서 언급한 바와 같이 블록체인상의 데이터가 완전히 암호화 되고 본질적으로 그러한 데이터를 정보주체와 연계시킬 수 없을지라도, 블록체인 데이터는 메타데이터를 포함하고 있는 한 i) 개인을 식별하는데 필요한 접근수단이 법에 의해 특별히 금지되어 있지 않고, ii) 그러한 정보가 획득되는 과정이 특별히 복잡하지 않으면 개인정보로 판명 될 수 있다.[38] 따라서 해시정보는 합리적 노력을 통해 식별되는 한 개인정보에 해당될 여지가 크다.

해시가 개인정보에 해당되지 않기 위해서는 해시의 식별가능성을 완전히 제거할 수 있는 기술적 방안이 강구되어야 한다. 그러나 완전한 식별제거가 불가능하다면 규범적으로 해시에 식별가능성을 차단하는 일정한 기술적 조치가 취해진 경우 가명정보로 취급하여 개인정보 규정의 적용에서 제외시켜 줄 필요도 있다.[39] 또는 개인정보의 추론에 비현실적인 시간이 걸리도록 기술적 조치를 하는 경우에도 가명정보로 취급하여 개인정보 규제에서 일정부분 면제할 필요가 있다. 외부 데이터베이스에 저장된 개인정보를 복잡하게 만들고 복잡한 개인 데이터 집합에 대해 하나의 해시만 저장할 경우 현실적으로 복잡한 개인정보를 추론하는데 지극히 많은 시간이 필요할 수밖에 없다고 한다.[40] 이러한 경우 재식별 금지 및 재식별 금지 위반에 대한 제재가 동반되어야 할 것이다.

---

37) *Ibid.*

38) Salmensuu, C., 앞의 논문(주 12), 17면.

39) 예를 들어 암호처리기법의 하나인 솔트(salt)를 사용하는 것이다. 해시 메커니즘에 비밀 '솔트'를 넣어 해시 정보를 복잡하게 한다. 솔트를 알지 못하는 외부인은 현실적으로 개인정보를 추론해 낼 수 없다. 즉, 외부 데이터베이스에 저장된 개인정보를 확인하기 위해 해시를 사용해야하는 블록체인의 참가자는 검증을 수행하기 위해 솔트를 제공해야한다. 솔트는 소금이 기본 양념이듯 원문에 가미하여 암호문을 다른 값으로 만드는 것이다. 이것은 일정한 결과값을 내며, 원문 복원이 불가능한 해시 함수에서 많이 쓰인다.
https://namu.wiki/w/salt (최종방문일 2018. 5. 17.).

40) Chang, H., 앞의 논문(주 2), 5-6면.

Ⅳ. 블록체인에서 '개인정보처리자'

1. 개인정보처리자의 개념

개인정보를 처리하는 수많은 응용 프로그램에서 누군가는 개인정보의 처리과정에 있어서 책임을 져야 하며, 이를 통상 개인정보처리자등이 수행하게 된다. 우리 개인정보보호법도 이러한 책임을 부과하기 위해 개인정보처리자의 개념을 도입하고 있다. 개인정보처리자란 "업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등"을 말한다.[41] GDPR역시 우리법상 개인정보처리자에 상응하는 개념으로 개인정보통제자(data controller)의 개념을 규정하고 있다. "개인정보 통제자"라 함은 개인정보 처리의 목적과 수단을 결정하는 자를 의미하며, 공동 개인정보 통제자(joint controller)도 인정한다. 개인정보를 통제한다는 것은 특정 데이터 처리 활동이 왜 그리고 어떻게 발생하는지에 대한 결정을 내리는 것을 의미 한다.[42] WP29는 개인정보통제자를 결정하는 요인들에 대하여 설명한다. 그러나 그러한 요인들이 법률에 규정되어있다 할지라도, 개인정보 통제자를 결정하는 것은 특정당사자를 일방적으로 지정하는 것이 아니라, 각 상황을 고려하여야 한다. 따라서 개인정보통제자를 결정하는 것은 심도 있는 조사가 필요하며 실제적으로 미치게 될 영향을 고려하여야 한다.[43]

2. 블록체인에서 개인정보처리의 책임

블록체인에서 개인정보처리자등은 개인정보를 블록체인에 넣을지 또는 제3자에 의해 제공되거나 스스로 가지고 있는 데이터베이스에 넣을지 등을 결정한다. 이 경우 블록체인 작동은 개인정보처리자등의 작업의 일부로 간주 될 수 있다. 개인정보처리자등은 저장된 개인정보가 보안 및 오남용으로부터 적절한 보호를 받을 수 있도록 보장할 책임이 있다.

---

41) 「개인정보 보호법」 제2조 제5호.

42) Article 29 Working Party, 'Opinion 01/2010 on the concepts of "controller" and "processor"', p. 8.

43) Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

(1) 프라이빗(퍼미션) 블록체인

‘프라이빗(퍼미션) 블록체인’에서 개인정보처리의 목적과 수단을 결정하는 것은 블록체인 시스템의 운영자이다. 따라서 GDPR상의 ‘개인정보 통제자’는 블록체인 시스템 운영자가 될 것이다. 그러나 우리 「개인정보 보호법」은 “업무를 목적으로 개인정보파일을 운용하기 위하여 개인정보를 처리하는 자”를 개인정보처리자로 규정하고 있다. 개인정보 “처리”란 “개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위”를 말한다. 처리는 법률상 정의에서 규정한 행위 외에도 ‘그 밖에 이와 유사한 모든 행위’가 포함되는데, 이에는 개인정보의 전송, 전달, 열람, 이전, 공유, 위탁 등이 포함될 수 있다. 다만, 다른 사람이 처리하고 있는 개인정보를 단순히 전달, 전송 또는 통과만 시켜주는 행위는 처리에 해당하지 않는다. 예컨대 우편배달사업자나 인터넷서비스제공자는 다른 사람의 개인정보를 단순히 전달 또는 전송하는 업무만 담당하게 되는데 이 때 우편배달사업자 등의 전달 또는 전송 행위는 개인정보의 처리로 보지 않는다.[44] 개인정보처리자가 되기 위해서는 ‘업무를 목적으로’ 개인정보를 처리하여야 한다. ‘업무’란 “직업상 또는 사회생활상의 지위에 기하여 계속적으로 종사하는 사무나 사업의 일체를 의미하는 것으로 보수 유무나 영리 여부와는 관계가 없으며, 단 1회의 행위라도 계속·반복의 의사가 있다면 업무로 볼 수 있다”고 한다.[45] 순수한 개인적인 활동이나 가사활동을 위해서 개인정보를 수집·이용·제공하는 자는 개인정보처리자가 아니다. 예를 들어 사적인 친분관계를 위하여 휴대폰에 연락처 정보, 이메일 주소록 등을 저장하는 경우는 당연히 개인정보처리자에 해당하지 않는다.[46]

이렇게 볼 때 우리 「개인정보 보호법」에 의하면 프라이빗 퍼미션 블록체인의 경우 ‘블록체인 시스템의 운영자’ 뿐만 아니라 ‘원장을 보유한 참여자 모두’가 개인정보처리자에 해당 될 수 있다. 참여자는 원장을 통해 개인정보에 해당되는 거래정보를 수집/보유하게 된다. 이는 개인정보를 처리하는 행위이며, 이러한 행위가 직업상 또는 사회생활상의 지위에 기하여 계속적으로 종사하는 사무나 사업의 일체를 의미하는 것이라면, 보수 유무나 영리 여부와는 관계가 없이, 단 1회의 행위라도 계속·반복의 의사가 있다면 업무로 볼 수 있다.

---

44) 행정안전부, 『개인정보보호법 해설서』(2016), 16-17면.
45) 행정안전부, 앞의 자료집(주 44), 20면.
46) 또한 업무란 직업상 또는 사회생활상 지위에 기하여야 하므로, 예를 들어 지인들에게 모임을 안내하기 위해 전화번호 및 이메일주소를 수집하는 행위나 결혼을 알리기 위해 청첩장을 돌리는 행위 등은 업무를 목적으로 한 것이 아니다. 행정안전부, 앞의 자료집(주 44), 20면.

(2) 퍼미션리스(permissionless) 블록체인

‘퍼미션리스(permissionless) 블록체인’의 참여자는 개인정보 규제의 적용과 관련하여 불확정성이 가장 크다. 개인정보에 대한 관리 및 통제가 부족한 시스템에 개인정보를 위탁할 뿐만 아니라, 개인정보의 파기·오용 등에 대하여 책임을 지게 될 수도 있다. 블록체인의 탈중앙화 및 분산이라는 특성으로 인해 개인정보에 대한 통제는 모든 참여자들 간에 공유되며, 그러한 모든 참가자, 특히 식별되고 위치 할 수 있는 모든 참가자는 공동으로도 개별적으로도 책임이 있다고 여겨질 수 있다. 이 경우 참가자는 자신이 통제 할 수 없는 다른 참가자가 보유한 개인정보의 유출 또는 오용에 대해서도 책임을 지게 되며, 이는 매우 불행한 문제라 하지 않을 수 없다.[47]

GDPR상 개인정보처리의 실질적 지배력(통제력)을 가져야 개인정보 통제자로 인정될 수 있다면, ‘퍼미션리스(permissionless) 블록체인’에서 어떠한 참여자도 이러한 요건을 충족할 수 없거나, 혹은 분산원장의 사본을 가지고 있는 모든 참여자가 이러한 요건을 충족한다고 보는 결론에 이르게 될 수 있다.[48] 우리나라의 경우 「개인정보 보호법」상 모든 참여자는 ‘개인정보처리자’에 해당될 수 있다. 즉 ‘퍼미션리스(permissionless) 블록체인’에서 개인정보를 안전하게 관리할 책임은 시스템 운영자로부터 개개의 이용자/참여자들에게 이전되게 된다.[49] 혹자는 이러한 데이터에 대한 책임소재가 EU가 추구하는 데이터 및 프라이버시 보호 추세에 부합하는 것이라고 평가하기도 한다.[50] 그러나 실제로 이러한 평가가 가능하기 위해서는 해당 기술에 대한 정교한 지식을 가지고 있어서 이러한 기술이 가지는 잠재적 위해로부터 그들 자신을 보호하기 위한 유용한 기술들에 대하여 알고 있는 이용자/참여자들이 전제되어야 한다. 그러나 과연 EU의 평균적인 소비자가 이러한 지식을 가진 이용자에 해당하는지에 대하여는 논쟁의 여지가 다분하다.

이러한 상황에서 규제당국은 누구에게 책임을 부여할 것인가에 대한 합의를 도출하기가 곤란할 수밖에 없다. 따라서 규제 당국 입장에서는 모든 참여자에게 책임을 부과한다 할지라도 집행의 곤란함으로 인해 블록체인 시스템 운영자에게 최소한 어느 정도의 책임을 할당 할 가능성이 더 크다고 보여 진다. 즉 다른 사람이(이용자들이) 정보를 저장

---

47) Zetzsche, D., Buckley, R. & Arner, D. (2017). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review*. https://ssrn.com/abstract=3018214 (최종방문일 2018. 8. 21.).

48) Matthias, B., & Malgorzata, S. (2016). Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers. *European Data Protection Law Review*. 2. *422, 426*. 425.

49) De Filippi, P., 앞의 논문(주10), 15면.

50) Recital 7 은 명백하게 GDPR은 자연인 개인에게 그 자신에 대한 정보 통제권을 부여하는 것을 기반으로 한다고 기술하고 있음을 근거로 한다. Salmensuu, C., 앞의 논문(주 12), 12면.

하거나 공개하도록 오직 공간만을 제공하는 제3자, ISP(intermediary service providers , ISPs)에게 책임을 부여하는 것이다. 사실 이러한 예는 이미 존재한다. EU의 경우 GDPR 제17조 잊힐 권리의 도입을 통해 ISP의 책임을 규정하고 있다. 또한 저작권법의 경우에도 P2P서비스를 특수한 유형의 온라인서비스 제공자로 규율하고 있으며 불법저작물 유통에 대하여 방조책임을 인정하고 있다. 즉 이들은 데이터가 어떻게 처리될 것인지를 결정하는데 참여하지 않음에도 불구하고 일정한 정도의 책임이 부과된다. 그러나 더 중요한 것은 이들에게 책임만을 부과한 것이 아니라 일정한 기술적·관리적 조치를 통해 면책규정을 부여하였다는 것이다.

블록체인 데이터를 처리하는 과정에서 ISP(또는 블록체인 시스템 운영자)의 역할이 자동화된 기술적 처리에 그치는 지극히 수동적 속성만 지니고 있다면 이들에게 책임을 부과하는 것 자체에 신중할 필요가 있다. 설사 일정부분 책임이 부과되더라도 반드시 면책요건이 함께 고려되어야 한다.

실제 유럽 개인정보보호 감독기구는[51]는 '퍼미션리스(permissionless) 블록체인'과 관련해서 책임의 주체, 데이터 보호의 적법성, 정보주체 등 보안과 프라이버시 문제에 대한 조사할 것을 요구한 바 있다.[52] 이처럼 블록체인에서 개인정보 처리자의 문제는 개인정보 보호에 대한 책임을 할당하는 것뿐만 아니라 보호적·예방적 조치를 수행함에 있어서도 매우 중요한 문제이므로 EDPS의 이러한 요구는 우리나라에서도 검토될 필요가 있다.

결국 개인정보처리자는 법에서 보안 및 사용 제한 등의 요구 사항을 준수하여야 한다. 이를 위해 개인정보에 대한 조직, 통제, 보안 및 데이터 보호 정책이 적용되어야 하므로 개인정보규제의 틀 안에서 서비스를 합법적으로 운영하려면 권한 있는 자만이 참여할 수 있는 '퍼미션(permissioned) 블록체인'만을 사용할 것을 고려하게 된다.[53]

---

51) EDPS(European Data Protection Supervisor).
52) European Data Protection Supervisor. (2016). 2016 Annual Report of the EDPS. 111-112.
53) Chang, H., 앞의 논문(주 2), 7-8면.

Ⅴ. 정보주체의 권리 보장 규범과 갈등

1. 동의

(1) '적법한 동의'의 방식

정보주체의 동의는 개인정보의 수집, 제공 등의 처리를 정당화 시켜준다. '동의'는 개인정보처리자가 개인정보를 수집·이용하는 것에 대한 정보주체의 자발적인 승낙의 의사표시로서 동의여부를 명확하게 확인할 수 있어야 한다.[54] 동의와 관련하여 법규를 살펴보면 다음과 같다.

첫째, 사전고지사항으로 규정된 것을 명확히 고지하여야 한다. 즉 일정한 사항들을 동의 받기 전에 정보주체에게 알려야 한다(제15조제2항). 개인정보처리자가 정보주체의 동의를 받을 때에는 정보주체가 동의의 내용과 의미를 명확히 알 수 있도록 미리 "①개인정보의 수집·이용 목적, ② 수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용 기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용"을 정보주체에게 알려야 한다.

둘째, 포괄적 동의를 받아서는 안 된다. 즉 각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각의 동의를 받아야 한다(제22조제1항).

셋째, 법령이 정하는 동의의 대상과 동의의 내용을 표시하는 구체화된 방법을 준수하여야 한다. 즉 개인정보처리자는 전자문서를 포함하여 서면으로 동의를 받을 때에는 i) 개인정보의 수집·이용 목적, ii)수집·이용하려는 개인정보의 항목, iii) 민감정보, iv)여권번호, 운전면허의 면허번호 및 외국인등록번호 v) 개인정보의 보유 및 이용 기간, vi)개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적을 행정안전부령으로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다. 여기서 "행정안전부령으로 정하는 방법"이란 i) 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것, ii)글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것, iii)동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것 등이다(「개인정보 보호법 시행규칙」 제4조).

---

54) 행정안전부, 앞의 자료집(주 44).

넷째, 재화나 서비스 홍보 등을 위해 동의 받으려는 경우 정보주체가 이를 명확히 인지할 수 있도록 알리고 동의를 받아야 하고(제22조제4항), 개인정보처리자는 정보주체가 선택적 동의사항에 동의하지 않는다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 안 된다(제22조제5항). 이는 어떤 정보가 필요 최소한의 정보이고 필요 최소한의 정보가 아닌지를 정보주체가 쉽게 알아볼 수 있게 구분해서 고지해야 하고, 필요 최소한의 정보가 아닌 정보에 대해서는 재화 또는 서비스의 이용에 방해를 받음이 없이 자유롭게 동의를 거부할 수 있음을 알려야 함을 의미한다.

동의와 관련하여 이러한 사항을 모두 준수하여야 '적법한 동의'가 된다.

(2) 블록체인에서 '적법한 동의'의 실현가능성

'블록체인'에서 거래의 유효성을 검증하는 참여자들은 개인정보에 해당되는 거래기록을 원장에 보유하게 된다. 이러한 행위가 적법하게 이루어지기 위해서는 앞서 언급하였듯이 '정보주체의 동의'가 있거나 정보처리자와의 합당한 '이용계약'이 있어야 한다. 또는 법적 의무를 수행하거나 공익 또는 공권력에 근거한 업무의 수행과정에서 개인정보가 처리되어야 한다.[55] '퍼미션(permissioned) 블록체인'에서 대체로 유효성을 검증하는 참여자들이 법적 의무를 수행하는 공공기관에 해당되는 경우 정보주체의 동의는 면제된다. 그러나 그 외의 경우 '퍼미션(permissioned) 블록체인'에서 거래 유효성을 검증하는 참여자들은 원장에 개인정보에 해당하는 거래기록이 담기기 위해서는 정보주체의 동의를 받아야 한다.

이는 '퍼미션리스(permissionless) 블록체인'도 마찬가지다. 블록체인의 기술적 구조에서 블록체인 시스템 운영자는 개인정보를 수집하지 않는다. 따라서 정보주체의 동의를 득해야 하는 자는 엄격히 이들이 아니라, 원장을 보유하는 블록체인의 참여자들이다. 이들이 본인들의 블록 원장에 개인정보를 수집하게 되기 때문이다. 합법적 동의가 되기 위해서는 원장을 보유하는 참여자들이 개인정보처리자로서 위와 관련된 합법적 동의 요건을 준수하여야 한다.

우선, 고지사항에 대하여 명확한 인지가능성을 부여하고 동의를 받아야 한다. 이용자의 동의가 형식적이지 않고 실질적인 동의라고 보려면 "미리" 법정 고지사항에 관하여 일반적으로 예상되는 방법을 사용하여 이해하기 쉽고 "명확하게 표시"하여 이를 이용자에게 알린 상태에서 동의를 받은 것이라고 평가할 수 있어야 한다. 그러나 블록체인에서

55) Art. 6(c) and Art.6(e) of the GDPR , 「개인정보 보호법」 제15조, 제17조.

개인정보의 수집은 통상 다른 거래과정에서 수반되어 이루어진다. 일례로 비트코인의 거래과정에서 거래와 동시에 거래정보에 해당되는 개인정보의 수집이 이루어지는데 사전에 일일이 고지사항들(①개인정보의 수집·이용 목적, ② 수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용 기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용)을 법령에서 정하는 표시방식(글자크기, 색깔 등)에 따라 고지할 수 있을지는 의문이다.

또한 '보유 및 이용 기간'을 구체적으로 정해서 알려야 하고, 보유 및 이용 기간을 특정할 수 없는 경우에는 보유 및 이용 기간을 결정하는데 사용되는 기준을 알려야 한다.[56] 그러나 원장정보는 거의 파기되지 않고 무한 보유되어야 하므로 '보유 및 이용기간의 적시'가 가능할 지, 가능하다 할지라도 어떤 의미가 있을지 의문이다.

한편 이러한 동의는 블록체인에 기반 한 거래당사자와 원장을 보유하는 참여자 간에 이루어져야 하는데, '퍼블릭 퍼미션리스(permissionless) 불록체인'에 기반 할 경우 실질적으로 참여자는 거래당사자가 누구인지 알 수 없는 경우도 존재한다. 이 경우 블록체인시스템 운영자는 개인정보를 처리하지 않음에도 불구하고 실제 개인정보의 처리과정에서 '동의'를 중재하여야 하는 입장에 있을 수 있다. 이러한 경우 후일 '동의'의 유효성 문제가 다투어질 경우 그 책임에서 자유로울 수 없다.

(3) 스마트 계약과 '동의'

'동의'를 전제로 하는 정보처리의 정당성은 대부분 '사적거래'에서 이루어지게 된다. 공공영역에서의 개인정보 처리는 행정기관 등이 공익적 업무수행을 위하여 국민의 개인정보를 처리하는 것이다.[57] 반면 사적거래영역의 개인정보의 처리는 정보주체의 동의에 의해 이루어지도록 규율하고 있으며 동의에 기하지 않은 정보의 수집 및 이용이 정당화되기 위해서는 법령의 규정에 의한 경우에 한한다. 특히 계약의 체결을 위한 개인정보의 제공 역시 개인정보 제공을 내용으로 하는 별도의 계약으로 볼 수 있으며 실무상으로는 대부분 약관이라는 계약절차에 의해서 이루어진다.[58]

블록체인에 기반 한 서비스 실행을 위한 개인정보의 수집 등이 스마트계약[59]을 통해

---

56) 행정안전부, 앞의 자료집(주 44).

57) 김민호, "공공부문 개인정보보호법제의 현황과 과제", 『토지공법연구』(한국토지공법학회, 2007), 제37집 제1호, 213면.

58) 김현경, "개인정보보호제도의 본질과 보호법익의 재검토", 『성균관법학』(성균관대학교 법학연구소, 2014), 287-289면.

59) 스마트 계약은 1994년 Nick Szabo에 의해 처음 소개된 개념이다. Nick Szabo는 스마트 컨트랙트를

이루어질 경우 이러한 '동의 규정'의 적용은 곤란해 질 수 있다. 스마트계약이라 함은 계약이 전자적으로 체결될 뿐 아니라, 계약의 이행까지도 인간의 관여 없이 자동적으로 이행되는 것을 말한다.[60] 즉 계약의 성립과 이행이라는 두 과정을 블록체인 기술을 이용하여 하나로 합친 것이다.[61] 스마트계약은 블록체인 플랫폼에서 실행되는 일련의 소프트웨어 코드로서, 미리 정의된 조건이 충족된다면 블록체인에 담겨진 자산에 대하여, 계약의 내용이 자동적으로 이행되는 것을 의미한다.[62] 스마트계약이 최초로 활용된 대표적 예는 '이더리움'[63]이다.[64]

이러한 스마트계약의 특성은 그 계약내용이 프로그램 코드로서의 형식을 가진다는 것이다. 즉, 계약 조항이 컴퓨터 코드로 만들어진다. 형식이 이러하므로 계약으로서의 성격이 배제되는가가 문제될 수 있으나 종이문서인 '계약서' 역시 계약이 발현된 형식일 뿐 그 자체가 계약은 아니며, 계약의 본질은 '당사자 간의 합의'이므로 종이 문서에 의하든, 전자문서에 의하든, 나아가 암호화된 블록체인 데이터에 의하든, 당사자 간에 의사의 합치가 이루어지고, 그에 따라 권리관계의 변동을 일으킨다면 이는 계약이라고 볼 수 있다.[65]

그러나 '동의'를 득하기 위한 개인정보의 수집/이용 계약은 일반계약과는 달리 i)사전 고지사항의 명확화, ii)포괄적 동의 금지, iii)동의의 대상과 동의내용을 표시하는 방법의 구체화 등을 통해 동의의 형식을 엄격히 법정화하고 있다. 스마트계약을 통한 동의가 이러한 '동의'의 법정요건을 충족하는지는 의문이다. 포괄동의의 금지규정을 준수하기 위

"계약에 필요한 요소들을 코드화하여 스스로 실행되게 하는 전산화된 거래 프로토콜"이라 정의하였으며, 이를 통하여 신뢰할 수 있는 제3자의 필요성과 혹 발생할 수 있는 사고의 가능성을 최소화할 수 있다고 제안하였다. Szabo, N. (1997). The Idea of Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (최종방문일 2018. 8. 21.).

60) Amuial, S., Dewey, J. N., & Seul, J. (2016). The Blockchain: A Guide for Legal & Business Professionals. Legal Works. (Westlaw Database, October 2016 Update), § 2:2. Smart contracts—Basics.

61) Levy, K. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*. 2017(3). 3.

62) Savelyev, A. (2016). Contract Law 2.0: «Smart» Contracts As the Beginning of te End of Classic Contract Law. *Higher School of Economics Research Paper. No. WP BRP71/LAW/2016*. 15.

63) 2014년 캐나다인 비탈리크 부테린이 개발한 가상화폐. 단위로 이더(ETH)을 쓴다. 계약서, 전자투표, e-mail 등 다양한 프로그램에 적용할 수 있는 확장성을 제공하는 Smart contract 기능을 구현할 수 있어서 다양한 금융 애플리케이션을 투명하게 운영할 수 있다. 비트코인과 마찬가지로 블록체인(데이터 분산저장 기술)을 활용한 화폐다. 비트코인에 비해 발전된 기술을 사용해 거래 속도가 빠르다. 한경 경제용어사전, 한국경제신문/한경닷컴[네이버 지식백과] '이더리움 [Ethereum]'.

64) 김제완, 앞의 논문(주 3), 152면.

65) 김제완, 앞의 논문(주 3), 166면.

해 현실에서는 약관으로 통칭되어 분류될 수 있는 성질의 문서를 수집・이용 동의, 제3자 제공 동의, 국외 제3자 제공 동의, 마케팅 목적 처리 동의 등 여러 개의 개별 동의사항으로 나누어 동의를 받도록 하고 있고, 실제 이용자들은 하나의 웹사이트에 회원으로 가입하는 과정에서 수차례에 거쳐 '동의합니다'창에 동의를 표시해야 하는 것이 보통이다.[66] 계약의 형식이 프로그램코드로 구현된 스마트계약 하에서 이러한 고지의 유효성이 유지되는 것은 곤란하다. 사실 이러한 '동의'가 과연 정보주체의 개인정보자기결정권을 보장하는가에 대한 의문은 별론으로 하더라도 스마트 계약의 실행과정에서 개인정보의 수집이 발생하는 경우 위의 동의요건들을 모두 스마트계약 내에 프로그램코드로 구현할 수 있는지, 구현한다 할지라도 정보주체가 이해할 수 있는 명확한 고지 요건을 충족할 수 있는지는 의문이다.

사실 이러한 동의 요건을 절대적인 합법성 기준으로 설정한 입법배경에는 사전 동의가 합리적으로 가능한 상황이 전제되어 있었다. 회원중심의 인터넷 서비스 제공 및 운영이 그러하다. 회원가입 시 이용자가 직접 제공해 주는 정보를 수집하는 경우만을 상정한 때문인 것으로 보인다. 그러나 블록체인, IoT환경 등 기술의 적용은 수집되는 정보의 시간적 간격이 다르다. 부지불식간에 실시간으로 정보가 생성되고 전달된다. 정보전달의 당사자자 또한 다르다. 기존의 인터넷 환경에서는 정보주체가 본인이 가지고 있는 개인정보를 서비스제공자에게 전달하는 체계였다(사람-사람 또는 사람-서비스). 그러나 새로운 기술 환경에서는 정보전달의 상대방을 특정할 수 없는 경우도 부지기수다. 따라서 블록체인에서 개인정보 처리의 '동의'규정의 내용은 수정될 필요가 있다.

2. 정정·삭제

(1) 정보주체의 정정·삭제권의 내용

「개인정보 보호법」상 정보주체는 개인정보처리자에게 그 개인정보의 처리정지, 정정 또는 삭제를 요구할 수 있다(제36조 및 제37조). 다만 "i) 법률의 규정 또는 법령상 의무를 준수하기 위하여 불가피한 경우, ii) 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우, iii)공공기관이 법률에서 정하는 소관 업무를 수행할 수 없는 경우, iv)계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우"에는 처리정지 요구를

66) 김현경, 앞의 논문(주 58).

거절할 수 있다(제37조제2항). 또한 정보주체는 “다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우”에는 그 삭제를 요구할 수 없다(제36조제1항). 개인정보처리자는 이러한 정정·삭제 요구를 받은 경우 “개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야” 한다(제36조 제2항). 또한 “개인정보처리자가 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야” 한다(제36조 제3항).

GDPR 역시 제16조에 의하면 개인은 그 정보가 부정확하거나 불완전한 경우 해당 개인정보를 정정 할 권리가 있다.[67] 또한 제17조에 의하면 정보주체는 계속해서 개인정보를 처리해야 할 강력한 사유(*compelling reason)*가 존재하지 않는 한 개인정보 삭제를 요청할 권리를 보유한다.

(2) 블록체인 거래정보의 정정·삭제

블록체인상의 장부에서 정보를 삭제하는 기능은 구현하기가 어려우며, 일반적으로 다수의 거래 참여자가 원장의 정보를 보유하고 있으므로 모든 정보가 삭제되었음을 입증하는 것 또한 어렵다.[68] 즉 변경할 수 없다는 것은 블록체인의 핵심 기능이다. 블록 내부의 정보를 변경하거나 제거하면 블록 안의 모든 기록이 더 이상 신뢰할 수 없게 되다. 기록 관리라는 측면에서 볼 때 중요한 기능이지만, 원래의 개인정보 수집에 대한 법적 근거가 더 이상 유효하지 않고 개인정보를 삭제해야 하거나 정보주체가 삭제 권한을 행사하고자 할 때 문제가 발생할 수밖에 없다. 결국 개인 식별이 가능한 데이터를 체인에 저장하는 블록체인 애플리케이션은 분산된 플랫폼의 불변성으로 인해 정보주체의 삭제권 및 정정권과 충돌하게 된다.[69]

정보주체가 자신의 개인정보를 삭제 또는 정정하길 원한다면 GDPR에 의하든 「개인정보 보호법」에 의하든 그 이행이 면제되기 힘들다. ‘동의’로 인해 개인정보 처리가 합법화되었다면, 동의라는 행위 자체가 쉽게 취소가능하고, 정보주체에 의한 정보의 삭제 또는 정정 요구에 대한 면제가 인정되지 않기 때문이다. 그러나 계약의 이행을 위해 개인정보의 보유가 필요하다면 정보주체의 삭제 요구에 대항할 수 있다. GDPR의 Recital

67) Article 16 GDPR.

68) ENISA. (2016). Distributed Ledger Technology & Cybersecurity- improving information security in the financial sector. Greece:ENISA(European Union Agency for Network and Information Security). 15. 21. https://www.enisa.europa.eu/publications/blockchain-security (최종방문일 2018. 9. 27.).

69) Chang, H., 앞의 논문(주 2).

65에서도 “개인정보 보유를 연장하는 것은 법적 의무를 준수하는 데 필요한 경우에는 합법적인 것으로 인정되어야 한다”고 기술하고 있다.[70] 그러나 정보주체가 합당한 이유로 계약을 철회하길 원하는 경우 문제될 수 있다. 이러한 경우 개인정보처리자등의 ‘합법적 이익’과 ‘개인정보를 보유를 지속할 필요성’을 근거로 삭제권을 무력화 할 수 있다고 본다.

블록체인의 아키텍처 자체가 기록의 불변성을 요구/강제하는 것이므로 데이터가 삭제되거나 변경 될 수 없는 것이 기술적 본질이다. 이에 기초하여, 블록체인의 핵심 기능 원리를 정보통제자/개인정보처리자의 ‘합법적 이익’에서 발생하는 ‘지속적인 필요성’로 간주할 수 있다. Recital 69에서도 개인정보통제자는 정보주체의 기본적 권리와 자유를 침해하지 않는 한 상응하는 합법적 이익을 주장할 수 있어야 한다고 기술하고 있으며,[71] GDPR의 제17조(1)은 개인정보통제자는 수집 또는 처리 목적과 관련하여 더 이상 필요하지 않게 되었을 때 개인정보를 삭제할 의무가 있다고 규정하고 있다.[72] 블록체인은 기록의 불변성/지속성을 본질로 하는바, 수집처리 목적과 관련하여 개인정보의 보유가 지속적으로 필요하므로 ‘더 이상 필요하지 않게 되었을 경우’에 정당화되는 정보주체의 삭제권이 인용될 수 없다고 보여 진다.

이 부분과 관련하여 사법부에서 본격적으로 다루어 진 바는 없으나, 이미 블록체인에 기반 한 서비스가 확산되고 있는 만큼 서비스/기술의 안정적 발전을 위해서는 정책당국의 구체적 가이드라인이라도 주어지는 것이 타당하다.

한편 블록으로부터 정보를 삭제하는 것은 불가능하지만 접근금지 시키는 것은 가능하다. 즉 블록에 있는 데이터를 읽고 기록하지(read and write) 못하도록 하는 것은 가능하다. 문제는 이와 같은 다른 사람에 대한 접근금지가 법률상 삭제권과 동일하게 취급될 수 있는가 하는 점이다. 기능적 형평성측면에서 이러한 접근금지를 삭제권 보장에 준하는 것으로 인정하는 것도 가능하다고 본다.[73] 삭제권은 궁극적으로 개인정보에 어떠한 접근이나 수정 등을 못하게 함으로서 프라이버시를 보호하고자 하는 것이다. 정보주체 외에 누구도 접근할 수 없도록 기술적 조치가 가능하다면 동등한 기능을 수행하는 것이

---

70) Recital 65 of the GDPR: “(...) the further retention of the personal data should be lawful where it is necessary, (...) for compliance with a legal obligation”.

71) Recital 69: “(...) It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject (in order to trump the right of objection of a data subject for processing of his/her data)”.

72) Article 17(1):“(...) the controller shall have the obligation to erase the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed”.

73) Salmensuu, C., 앞의 논문(주 12), 24면.

라고 볼 수 있다. 특히 ENISA[74]는 보안 및 책임 통제와 관련된 기능에 세분화 된 접근 통제가 포함된다고 한다.[75] GDPR의 개인정보 삭제권은 정보주체의 개인정보에 대한 지배권을 보장하려는데 기초하므로[76] 이러한 접근통제 장치가 자기 정보에 대한 타인의 접근을 통제할 수 있는 수단이라면 삭제권과 등가의 가치를 지닐 수 있다고 본다.

오히려 블록체인은 개인정보의 보안을 강화하는 방법으로 사용되도록 고안될 수 있다.[77] 블록체인 설계시 두개의 블록체인의 조합으로 구성해서 하나는 접근통제를 위한, 또 하나는 데이터를 위한 오프체인저장소(off-chain storage)로 구성한다. 오프체인저장소는 '퍼미션(permissioned) 블록체인'에 의해 유지되며 이용자만이 그의 데이터를 통제하도록 설계한다. 체인 위의 정보는 단지 GDPR하에서 가명화된 상태로 존재하게 되고 이러한 정보는 권원 없이 정보주체의 신원을 밝히고자 하는 적대자에게는 아무 의미 없는 정보이므로 정보주체의 신원은 보장될 수 있다.

한편 거래당사자가 블록체인 참여시 개인정보의 삭제·정정권을 포기한다는 포괄적 의사표시를 내포한 것이라고 볼 수 있는가에 대한 검토도 필요하다. 그러나 그러한 이러한 의사표시를 하였다 할지라도 이러한 포기가 정보주체의 권리 보장 차원에서 유효한지는 또다시 의견이 분분할 수밖에 없다.

3. 개인정보 국외이전

(1) 개인정보 국외이전 규정현황

개인정보의 국외 이전과 관련하여「개인정보보호법」제17조 제3항에서는 "개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외이전에 관한 계약을 체결하여서는 아니 된다"고 규정하고 있다. 「정보통신망 이용촉진 및 정보보호등에관한 법률」제63조 제2항에서는 "정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전

74) European Union Agency for Network and Information Security.

75) GDPR의 Recital 7은 명백히 다음과 같이 기술하고 있다. "the GDPR framework is based on the ideal of giving natural persons the control of their own personal data".

76) Recital 7 explicitly states that the GDPR framework is based on the ideal of giving natural persons the control of their own personal data; also see "A New Consumer Empowering Agenda 2012" and the WP 2016 Opinion 242.

77) Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE CS Security and Privacy Workshop*. 181·183.

“이라 한다)하려면 이용자의 동의를 받아야 한다”고 명시하고 있어 국외이전의 범위를 개인정보를 국외의 제3자에게 제공하는 경우와 함께 처리위탁 및 보관하는 경우까지 포함하고 있다.

개인정보의 국외 이전은 정보주체가 외국의 글로벌 기업등에 해당되는 개인정보처리자에게 직접 제공하는 경우와, 국내에 있는 개인정보처리자가 외국의 개인정보처리자에게 개인정보를 제공하는 경우로 나누어 볼 수 있다. 예를 들어 전자는 정보주체가 구글과 페이스북등의 서비스를 이용하기 위해 직접 외국법인인 이들에게 개인정보를 제공하는 경우이며. 후자는 글로벌 기업의 국내법인(구글코리아)이 내국인으로부터 개인정보를 수집한 후 이를 본국의 법인(미국 구글본사)에게 제공하는 경우이다.

현재 국내법상 국외이전 규정은 후자에 대하여만 규정하고 있다. 전자의 경우법률의 문헌적 해석상 외국의 개인정보처리자의 경우에도 내국인인 개인정보처리자와 동일한 의무가 부과되며 개인정보 국외이전에 대한 특별한 규정은 없는 것으로 보인다.[78]

(2) 블록체인과 개인정보 국외이전

블록체인의 참여자들은 불가피하게 다른 관할권을 가진 여러 나라에 거주하고 있을 수밖에 없다. 각 참여자들이 거주하는 장소가 불확실하고 국경의 제약을 받지 않으므로 외국 관할 구역에 개인 정보를 저장하기 위해 모든 정보 주체로부터 의미 있는 동의를 얻는 것은 실질적으로 실행곤란하다.

앞서 언급한 개인정보를 블록이 아닌 외부 데이터베이스에 별도로 저장하도록 하여 융통성을 제공할 수 있다는 견해도 있다.[79] 그러나 블록체인에 저장된 해시를 개인정보라고 보는 한 이러한 방안은 개인정보 국외이전 규정과의 갈등을 해결할 수 있는 방안은 아닌 듯하다. 개인정보 국외이전 문제는 국경 없이 이루어지는 플랫폼서비스의 공통된 문제이나, 블록체인의 경우 대부분 원장을 가지고 있는 참여자가 누구인지 알 수 없는 경우이므로 정보주체로서는 국외 이전에 대한 인식자체가 곤란할 수 있다. 또한 현행법상 정보주체의 사전 동의를 전제로 개인정보의 국외이전을 허용하고 있는바 앞서 전

78) 전자에 해당하는 직접적 개인정보 국외이전에 해당하는 경우 국제적 규율동향에 대하여는 첫째, 분리된 네트워크를 원칙으로 하는 유형이다. 이러한 경우 언제든 정부에 의한 데이터 통제가 가능하므로 가장 강력한 데이터 국지화 유형이라고 할 수 있다. 둘째, 모든 데이터에 대한 국지화를 원칙으로 하되, 예외적으로 국외이전을 허용하는 경우이다. 세 번째는 개인정보 등 특정 데이터에 대한 국지화를 원칙으로 하는 유형이다. 이에 대한 자세한 내용은 ‘김현경, “데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰”, 『토지공법연구』(한국토지공법학회, 2017), 제78집, 213-260면 참조.’

79) Chang, H., 앞의 논문(주 2).

개한 ‘동의’의 문제점이 그대로 국외이전의 경우에도 적용될 수밖에 없다.

Ⅵ. 결 론

개인정보는 절대적 권리가 아니다.[80] GDPR의 Recital 4 역시 “개인정보 보호에 대한 권리는 절대적 권리가 아니다. 이는 사회를 구성하는 기능과 관련하여 고려되어져야 하며, 비례성 원칙에 부합하도록 다른 기본권들과도 조화되어야 한다”고 기술하고 있다.[81] 개인정보 규제는 국민/시민의 프라이버시를 지키기 위함이지, 혁신이나 비즈니스를 수행함에 있어서 장애가 되고자 고안된 제도는 아니다. 현존하는 규제구조를 이탈할까봐 두려워서 유용한 기술을 배척하는 것은 바람직하지 않다.

개인정보규제와 블록체인의 문제를 검토한 본 연구의 결과를 요약하면 다음과 같다.

첫째, 블록체인의 거래정보 등은 개인정보를 포함하고 있을 수 있으며, 거래정보 자체가 식별가능성이 인정되는 한 개인정보에 해당된다. 해시 역시 ‘식별가능성’에 비추어 볼 때 개인정보에 해당된다. 다만 일정부분 개인을 식별하지 못하도록 기술적 조치를 한 경우 일종의 ‘가명정보’가 될 수 있다. 다만 우리나라는 GDPR이나 일본과는 달리 ‘가명정보’ 역시 ‘개인정보’와 동일하게 취급하므로 이에 대한 개선이 시급하다. ‘가명정보’의 이용근거, 이에 상응하는 ‘재식별 금지’ 등의 입법적 개선이 필요하다.

다음으로 ‘개인정보처리자’ 문제는 좀 더 신중한 검토가 필요하다. ‘퍼미션리스(permissionless) 블록체인’에서 블록체인 시스템 운영자는 엄격히 개인정보처리자라고 볼 수 없다. 블록체인 참여자가 개인정보처리자이다. 이러한 ‘퍼미션리스(permissionless) 블록체인’의 경우 거래의 참여자가 무제한이므로 실질적으로 개인정보처리자에게 규범준수를 강제하도록 설계하는 것이 곤란하다. 결국 개인정보처리자가 아님에도 불구하고 블록체인 시스템 운영자(사업자)에게 일정한 책임을 부여하는 입법의 가능성이 있다. 유

80) 개인정보의 보호는 규제합리화라는 이유로 타협되어서는 안 된다는 견해가 있을 수 있다. 그러나 필자는 개인정보 보호의 본질과 관련하여 “개인정보는 사회적 가치와 경제적 가치, 그리고 개인적 가치를 동시에 지니고 있으며, 이 세 가지 가치가 개인정보 사용자의 관점에 따라 서로 경합하므로 그 가치들 사이의 균형을 이루기 위한 방향을 탐색하는 것이 중요함”을 밝힌바 있다. 즉 개인정보제도는 공익적 가치와 사익적 가치의 접점에 위치하며 이들 간 적절한 균형을 추구하는 방향으로 설계되어야 한다. 이렇게 볼 때, 개인정보 보호를 불가침의 절대적 권리로 간주하는 것은 타당하지 않다고 생각한다. 이와 관련된 자세한 내용은 ‘김현경, 앞의 논문(주 58), 267-297면’에서 구체적으로 논증하였는바 참조하길 바란다.

81) Recital 4 and Art. 2 GDPR.

사하게 저작권법상 온라인서비스제공자는 실질적으로 불법저작물을 게재하는 저작권침해의 협의의 공동정범이 아님에도 불구하고 그러한 행위의 방조책임을 인정한 바 있다. 다만 저작권법은 이러한 사업자의 안정적 서비스를 위해 면책 요건을 법률에 규정하였으므로, 이러한 입법례를 참조해 볼 만 하다.

셋째, 블록체인의 기술적 특성에 비추어 볼 때 현행법상 '적법한 동의'의 요건을 충족하는 것은 상당히 곤란하다. i)사전 고지사항의 명확화, ii)포괄적 동의 금지, iii)동의의 대상과 동의내용을 표시하는 방법의 구체화 등을 통해 동의의 형식을 엄격히 법정화하고 있다. 그러나 스마트계약을 포함한 블록체인상에서 이러한 '동의'의 법정요건이 충족될 수 있을지 의문이다. 스마트 계약의 실행과정에서 개인정보의 수집이 발생하는 경우 위의 동의요건들을 모두 스마트계약 내에 프로그램코드로 구현할 수 있는지, 구현한다 할지라도 정보주체가 이해할 수 있는 명확한 고지 요건을 충족할 수 있는지는 의문이다. 적법한 동의가 없으면, 실제 개인정보를 포함하는 블록체인 서비스 구현은 불가능하다. 사실 이러한 '동의'가 과연 정보주체의 개인정보자기결정권을 보장하는가에 대한 근본적 질문부터 다시 제기되어야 한다.

넷째, 정보주체의 권리와 관련하여 블록체인의 기록의 불변성에 의할 때 정보주체의 정정·삭제권 보장은 블록체인의 본질에 어긋난다. 블록의 개인정보를 읽고 기록할 수 없도록 접근금지조치를 취하는 한 정보주체의 정정·삭제권을 보장하는 것으로 볼 필요가 있다. 즉 개인정보에 대한 접근금지를 통해 정보주체의 정정·삭제권 보장으로 추구하고자 했던 법익을 지킬 수 있다면 양자의 기능은 등가로 취급하여야 한다.

'블록체인'은 더 많은 '자유'와 '중립성' 그리고 '투명성'을 필요로 하는 영역에 가치를 제공할 수 있고 이로부터 많은 혜택을 얻을 수 있다. 이러한 혜택에 개인정보 규제가 걸림돌이 되어서는 안 될 것이다.

원고 접수일 : 2018년 8월 24일
게재 심사일 : 2018년 9월 14일
게재 확정일 : 2018년 9월 19일

참 고 문 헌

1. 국내문헌

김민호, “공공부문 개인정보보호법제의 현황과 과제”, 『토지공법연구』(한국토지공법학회, 2007), 제37집 제1호.

김민호, “개인정보처리자에 관한 연구”, 『성균관법학』(성균관대학교 법학연구소, 2014), 제26권 제4호.

김일환·김민호, “개인정보보호기구 법제정비의 원칙과 방향에 관한 공법체계적 고찰”, 『토지공법연구』(한국토지공법학회, 2007), 제36집.

김제완, “블록체인 기술의 계약법 적용상의 쟁점- ‘스마트계약(Smart Contract)’을 중심으로-”, 『法曹』(법조협회, 2018), 제67권 제1호.

김현경, “개인정보보호제도의 본질과 보호법익의 재검토”, 『성균관법학』(성균관대학교 법학연구소, 2014).

김현경, “기술혁신환경에서 프라이버시와 공권력의 충돌과 조화”, 『가천법학』(가천대학교 법학연구소, 2016), 제9권 제3호.

성승제, “블록체인 활성화의 법적 과제”『기업법연구』(한국기업법학회, 2017), 제31권 제2호.

유승언·이병준·김경태·윤희용, “블록체인에 기반한 합의 알고리즘”『한국컴퓨터정보학회 학술발표논문집』(한국컴퓨터정보학회, 2018), 제26권 제1호.

이병준·최경진·김건호, “개인정보 국외이전 관련 국내 현황 분석 및 대응 방안”, 『한국인터넷진흥원』(2016).

2. 외국문헌

Amuial, S., Dewey, J. N., & Seul, J. (2016). The Blockchain: A Guide for Legal & Business Professionals. Legal Works.

ENISA. (2016). Distributed Ledger Technology & Cybersecurity- improving information security in the financial sector. Greece:ENISA(European Union Agency for Network and Information Security). 15. 21.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. New York: Springer Link.

Borgesius, F. J. Z. (2016). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer law & Security review*. 9.

De Filippi, P. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production*. 7:Alternative Internets.

El Khourya, A. (2017). Dynamic IP Addresses Can Be Personal Data, Sometimes. A Story of Binary Relations and Schrodinger's Cat. *European Journal of Risk Regulation (EJRR)*. 8(1).

Esayas, S. Y. (2015). The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Technology*. 6(2).

Levy, K. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*. 2017(3).

Matthias, B., & Malgorzata, S. (2016). Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers. *European Data Protection Law Review*. 2.

Narayanan, A., Bonneau, J., Felten, E. W., Miller, A., Goldfeder, S., & Clark, J. (2016). Bitcoin and Cryptocurrency Technologies, A Comprehensive Introduction. Princeton University Press.

Salmensuu, C. (2018). The General Data Protection Regulation and the Blockchains. *Liikejuridiikka*. 2018(1). 10.

Savelyev, A. (2016). Contract Law 2.0: «Smart» Contracts As the Beginning of te End of Classic Contract Law. *Higher School of Economics Research Paper. No. WP BRP71/LAW/ 2016*. 15.

Spindler, G., & Schmechel, P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. *JIPITEC*. 2016(7). 14.

Stalla-Bourdillon, S., & Knight, A. (2017). Anonymous Data v. Personal Data- A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. *Wisconsin International Law Journal*. 34(2).

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal. 21.

Zetzsche, D., Buckley, R. & Arner, D. (2017). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review*.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE CS Security and Privacy Workshop*.

General Data Protection Regulation (EU) 2016/ 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Article 29 Working Party 2007 on the concept of personal data, WP 136.

Article 29 Working Party 2014 on the Anonymisation Techniques, WP 216.

Article 29 Working Party, 'Opinion 05/2012 on Cloud Computing' WP 196.

Article 29 Working Party, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' WP 215.

Article 29 Working Party, 'Opinion 01/2010 on the concepts of "controller" and "processor"'

Article 29 Working Party 'Opinion 2016 on Guidelines on the right to data portability".

Enisa Report 2016 Distributed Ledger Technology, Distributed Ledger Technology & Cybersecurity- improving information security in the financial sector.

Enisa Report 2015 on Privacy by design in big data, An overview of privacy enhancing technologies in the era of big data analytics.

3. 전자자료

https://bitcoin.org/bitcoin.pdf (최종방문일 2018. 8. 21.).

http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (최종방문일 2018. 8. 21.).

https://hal.archives-ouvertes.fr/hal-01382006/document (최종방문일 2018. 9. 27.).

https://namu.wiki/w/salt (최종방문일 2018. 5. 17.).

https://ssrn.com/abstract=3018214 (최종방문일 2018. 8. 21.).

https://ssrn.com/abstract=3137606. (최종방문일 2018. 8. 21.).

https://www.enisa.europa.eu/publications/blockchain-security (최종방문일 2018. 9. 27.).

https://www.jipitec.eu/issues/jipitec-7-2-2016/4440/spindler_schmechel_gdpr_encryption_jipitec_7_2_2016_163.pdf (최종방문일 2018. 8. 21.).

http://www.sedaily.com/NewsView/1ONIHGZBQ7 (최종방문일 2018. 6. 6.).

Abstract

A Study on Rationalization of Personal Information Regulation in Block Chain Technology and Services

Hyun-Kyung KIM*

The right to personal information is not an absolute right, and it must be harmonized with other fundamental rights to conform to the principle of proportionality. Especially, personal information protection system is not designed to be a hindrance to innovative technology. From this point of view, this study examined the issue of regulation of personal information about the block chain technology and service which is becoming a recent issue and searched for improvement plan. The transaction information of the block chain can be regarded as personal information in the light of the judgment of the identifiability in the current law even if it is difficult to identify the individual by itself. Therefore, it is necessary to establish the basis of the use of 'pseudonymized information' in order to prevent the processing of 'transaction information' in the block chain service from violating the law, and to adopt the corresponding prohibition of re-identification. Also, in the case of 'permissionless block chain', the participant of the transaction may correspond to the personal information processor, but since the number is unlimited, it is difficult to actually design the personal information processor to comply with the norm. In the end, there is a possibility of legislation that gives the block chain system operator a certain responsibility. In such a case, it is necessary to alleviate the burden on the block chain system operator by stipulating the requirements for exemption of liability. On the other hand, in view of the technical characteristics of the block chain, it is very difficult to meet the requirements of "legitimate agreement" under the current law. In order to provide stable service of the block chain, it is necessary to improve the 'agreement' regulation in the current law.

'Block Chain' can provide new value and service in many areas, and our society, including users, can benefit from it. These benefits should not hinder the regulation of personal information.

[Key Words] Block Chain, Personal Information, Personal Information Processor, Block Chain System Operator, Information Subject's Right

* Professor, Seoul National University of Science and Technology