

개인정보 개념에 대한 사용자의 인식 연구*

Users' Understanding of the Concept of Personal Information

최 한 별 (Hanbyul Choi)**
정 윤 혁 (Yoonhyuk Jung)***
남 진 영 (Jin Young Nam)****

국문초록

최근 지능정보기술을 이용한 제품 및 서비스가 현실화되면서 개인의 편리함이 증가하고 있지만, 개인정보에 대한 문제 또한 심화되고 있다. 이는 지능정보사회의 도래와 함께 수집 및 활용되는 개인정보 범위가 전례없이 확대되면서 개인정보 침해 혹은 재식별화 위험성이 또한 높아졌기 때문이다. 이러한 개인정보에 대한 위협에 대처하고 동시에 효율적인 데이터 활용을 위해 정부와 기업이 제도 마련에 나서고 있다. 최근 국내에서도 데이터 3법 개정과 함께 데이터 이용 활성화를 통한 신산업 육성이 국가적 과제로 대두되고 있는 만큼, 올바른 데이터 활용 및 보호를 위한 사회적 합의에 대한 관심이 높아지고 있다. 본 연구는 이러한 사회적 요구를 반영하여 개인정보 개념에 대한 사용자의 인식을 탐색하였다. 본 연구의 결과는 다음과 같이 요약된다. 첫째, 사용자는 특정 개인을 정확하게 식별할 수 있거나, 유출 시 금전적 피해를 유발할 수 있는 정보일수록 더 강하게 개인정보로 인식하는 경향을 보였다. 둘째, 개인정보 범위에 대한 사용자의 인식은 성별 및 디지털 세대와 같은 개인적 특성에 따라 차이가 있었다. 셋째, 사용자가 인식하는 개인정보에 대한 유형은 현 법률체계가 제공하는 유형과 차이를 보였다. 이와 같은 결과는 개인정보 개념에 대한 사회적 인식의 역동성이 있어, 정보통신기술의 진화에 따라 그러한 인식이 재탐색될 필요성을 시사한다. 또한 본 연구의 결과는 개인정보 활용에 관한 적절한 정책 및 전략을 수립하기 위해서는 사용자 관점을 포괄하는 접근방식이 필요함을 시사한다.

주제어: 개인정보, 개인정보 보호법, 지능정보기술, 정보 프라이버시

* 논문접수일: 2020. 4. 10, 수정일: 2020. 5. 18, 게재확정일: 2020. 6. 11

* 이 논문은 2017년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2017S1A5A2A01027403).

** 울산과학기술원 경영공학과 석박사통합과정, 제1저자, E-mail: choihanbyul@unist.ac.kr

*** 고려대학교 미디어학부 부교수, 교신저자, E-mail: beyond@korea.ac.kr

**** 고려대학교 미디어학과 석사과정, 공동저자, E-mail: skalara@korea.ac.kr

ABSTRACT

While individuals can enjoy products and services that use intelligent information technology, in which a large amount of data is stored, analyzed and used to create useful knowledge, they face the threats of personal information misuse. With the advent of the intelligent information era, more data are being employed to provide users with value-added services, but the risk of information misuse also grows. If social and legal norms are not established to enforce privacy rights in a timely manner, social issues related to privacy management may escalate. In South Korea, data privacy laws were recently revised. A social consensus on information privacy norms is now called for.

The primary objective of this study is to explore user awareness of the concept of personal information as reflecting the social needs for a consensus on information privacy issues. The study finds that: first, users recognize that one's identification and financial information are highly personal. Second, the range of information perceived as personal varies across users according to their characteristics, such as gender and digital generation cohort. Third, substantial differences exist between the information viewed as personal by users, and that protected by the legal system. The concept of personal information thus needs to be re-examined following the advancement of information communication technology. This requires a more user-centric approach to formulate appropriate policies and strategies regarding private information.

Key words: Personal information, Privacy act, Intelligent information technology, Information privacy

I. 서론

최근 빅데이터(Big Data), 인공지능(AI: Artificial Intelligence), 사물인터넷(IoT: Internet of Things) 등으로 대표되는 지능정보기술의 발전은 기존 산업 구조를 근본적으로 변화시키고 있다. 지능정보기술이란 인간의 고차원적 정보처리를 정보통신기술(ICT: Information Communication Technology)을 통해 구현하는 기술로, 제4차 산업혁명의 핵심 동력으로 인식되고 있다 (Schwab, 2016). 이와 같은 데이터 기반 기술은 개인, 산업, 공공 등 사회 전체 영역 모두를 아우르고 있다는 점에서 더 큰 의의를 갖는다. 다수의 IT기업들은 비슷한 성향을 가진 소비자들을 한데 묶은 시장 세분화(market segmentation) 전략을 뛰어넘어, 개인별 취향 및 상황에 따른 맞춤 추천을 실시간으로 제공하는 등 해당 기술을 통해 효율적인 지식정보 체계를 구현하고 있다. 예를 들어 현대 소비자들은 자신의 기존 소비 패턴은 물론 현재 위치에 따른 맞춤형 혜택을 쉽게 접할 수 있게 되었다. 이와 같은 첨단 데이터 처리 기술은 비단 상업적인 영역에만 국한되지 않으며, 공공정책 수립에 활용되는 등 공익적인 차원으로도 쓰이고 있다 (신동희·김용문, 2015).

하지만 이러한 산업 성장과 변화의 이면에는 새로운 문제 또한 존재한다. 빅데이터 분석을 위해 수집되는 대부분의 정보가 사용자의 일상 활동과 관련된 민감한 개인정보일 가능성이 높다는 점이 바로 그것이다 (Janssen & Helbig, 2018). 최근 연구에서는 사물인터넷 환경에서 데이터 융합 및 통합을 거치는 중간 처리 과정이 사용자의 개인정보 침해 위협을 야기할 수 있는 것으로 알려졌다 (Madaan et al., 2018). 즉, 지능정보사회에서 수집 및 활용되는 개인정보의 범위가 확대되면서 개인정보 재식별화 위험성이 증가하고 있는 것이다. 이처럼 지능정보기술을 이용한 제품 및 서비스가 현실화되면서 개인의 편리함이 증가하고 있지만, 개인정보 침해에 대한 문제 또한 심화되고 있다. 개인정보에 대한 증가하는 사회적 위험과 염려를 포괄적으로 대처하기 위해서 개인정보에 대한 사회적 합의를 도출하고 이에 따른 대책을 마련할 필요가 있다. 유럽 연합(EU: European Union)은 앞서 언급한 개인정보 활용의 순기능과 역기능을 모두 고려하여 일반 개인정보 보호법(GDPR: General Data Protection Regulation)을 제정한 바 있다. 특히 일반 개인정보 보호법은 제4차 산업혁명 시대의 정보통신기술 발전을 수용하면서도, 정보 주체

의 개인정보 보호 권리를 세분화하였다는 점에서 정책적 시사점을 제공한다 (조수영, 2018). 최근 국내에서도 데이터 3법 개정을 통해 효과적인 데이터 활용 및 보호를 위한 정책적 움직임을 보이고 있는 만큼, 개인정보에 대한 사회적 규범을 정립하기 위하여 지속적인 논의가 필요한 시점이라고 할 수 있다. 실제로 개인정보에 대한 법적 정의의 포괄성으로 인해 개인정보 범위 및 유형에 대한 사회적 동의가 충분히 이루어지지 않고 있다는 지적이 꾸준히 제기되어 왔다 (이성엽, 2018).

이와 같은 사회적 요구를 반영하여 본 연구는 개인정보 개념에 대한 사용자의 인식을 심층적으로 탐색하고자 한다. 특히 본 논문은 정보 주체가 인식하는 개인정보에 대한 개념을 인구통계학적 특성에 따라 구분하는 동시에, 이를 현 법률체계와 비교하고자 한다. 개인정보 보호의 근본적인 의미가 개인정보 자기결정권을 보장하는 것이라고 볼 때 개인정보에 관한 사용자 인식을 탐색하는 것은 해당 권리를 실현하기 위한 기초적인 작업이다. 또한, 이는 기업 및 조직이 개인정보 활용을 위한 전략을 수립하는데 초석이 될 수 있다는 점에서 의의를 갖는다. 더불어, 본 연구는 개인정보에 대한 사용자의 인식을 살펴봄으로써 개인과 기업 간의 개인정보 활용을 둘러싼 갈등을 완화하는데 기여할 수 있을 것이라 사료된다.

II. 이론적 배경

1. 개인정보 개념 및 연구 동향

개인정보란 ‘살아 있는 개인에 관한 정보’로, 성명, 주민등록번호, 영상 등을 통하여 개인을 식별할 수 있는 정보를 의미한다.¹⁾ 이는 개인을 특정할 수 있는 모든

1) 개인정보 보호법, 제1장 제2조 제1항: "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

나. 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.

다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

정보를 의미하며, 다른 정보와 용이하게 결합하여 개인식별이 가능한 상황도 포함한다. 이에 따라 개인정보 유형은 기본인적사항부터 종교, 사회활동 등 다양한 영역을 포괄하고 있다(<표 1> 참고). 개인정보 개념에 대한 연구는 학문 분야에 따라 다르게 진행되어왔지만, 많은 학자들이 프라이버시(privacy) 개념을 전제로 연구를 수행하였다. 본래 ‘개인 사생활에 대한 권리’로 정의되었던 프라이버시는, 정보통신기술의 발전과 함께 대량의 개인정보가 수집 및 활용됨에 따라 ‘개인의 정보를 통제할 수 있는 권리’로 확장되었다 (Pavlou, 2011). 이는 ‘개인정보에 대한 자기결정권’을 내포하는 보다 적극적인 권리를 뜻하며, 오늘날 프라이버시에 대한 정보적 측면이 강조된 정보 프라이버시(information privacy) 개념으로 재조명되었다 (Smith et al., 2011). 정보 프라이버시의 화두는 수집된 개인정보의 활용 문제라고 볼 수 있다 (Bélanger & Crossler, 2011). 온라인 환경에서 사용자는 서비스 이용을 위해 자발적으로 정보를 제공하기도 하지만, 이러한 과정에서 개인이 제공한 정보가 정보 주체의 동의 없이 제3자에 의해 이용될 수도 있으며 이는 곧 정보 프라이버시 침해로 이어진다 (Bansal & Gefen, 2010; Junglas et al., 2008). 이와 같은 정보 프라이버시 침해는 현대의 지능정보기술 맥락에서 더 많은 시사점을 제시한다. 오늘날 빅데이터와 인공지능 등으로 대표되는 데이터 처리 및 분석 기술의 발전은 고객 개개인별로 상황에 따른 맞춤 혜택을 실시간으로 제공하는 개인화 서비스를 발전시켰다. 이는 이전보다 많은 양의 데이터로부터 보다 가치 있는 정보를 추출해낼 수 있는 기술이 가능해진 결과다. 여기서 중요한 것은 정보통신 기술 발전이 제시하는 청사진도 프라이버시에 대한 우려를 피해갈 수 없다는 점이다. 개인정보 활용 범위가 확장될수록 그것이 유출 혹은 오용되었을 때의 위험도가 더 커질 수 있다. 실제로 최근 연구들은 지능정보기술을 활용한 제품 및 서비스의 개인정보 보호 문제에 대한 윤리적 의문을 활발히 제기하고 있다 (남형두, 2019; 윤혜선, 2019; Jones, 2018; Madaan et al., 2018). 예를 들어 최근 연구에서는 다양한 데이터의 연결 및 공유를 가능케하는 지능정보기술의 활용이 개인 의료 정보를 이용한 보험사기, 자율주행 차량 운행정보 유출로 인한 사생활 침해 등 개인의 민감 정보 침해 사례로 이어질 수 있음을 경고하였다 (김중세, 2020).

<표 1> 개인정보 유형 및 항목

유형 구분	항 목
일반정보	• 이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	• 가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	• 학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항
병역정보	• 군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	• 소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
소득정보	• 현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타 수익정보	• 보험 (건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	• 대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	• 현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과 직무태도
법적정보	• 전과기록, 자동차 교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	• 가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	• 노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	• 전자우편(e-mail), 전화통화내용, 로그파일(log file)
위치정보	• GPS나 휴대폰에 의한 개인의 위치정보
신체정보	• 지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	• 흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

출처: 개인정보보호위원회(<http://pipc.go.kr>)

이처럼 지능정보기술의 발전과 함께 수집 및 활용되는 개인정보의 범위가 확대됨에 따라 개인정보 보호에 대한 지속적인 연구의 필요성이 강조되고 있다. 개인정보에 관한 연구 동향은 개인정보 개념 정립에 집중한 연구부터 사용자 인식까지 그 범위가 넓으며, 특히 최근에는 새로운 정보통신기술 환경 내에서 개인정보 관리 체계나 법적 규범 등을 탐색한 논문이 주를 이루고 있다(<표 2> 참고). 먼저 개인정보 개념 및 범위에 대한 연구는 공통적으로 올바른 개인정보 보호 및 활용에 대한 접근법에 초점을 맞추고 있다. 기존 연구는 개인정보 개념이 프라이버시 보호와 경제적 유통 사이의 균형을 유지할 수 있는 범위에서 정립되어야 한다고 주장하고 있으며 (이대희, 2015), 현대 정보통신기술의 발전을 고려하여야 한다고 역설하고 있다 (문재완, 2014; 임규철, 2012). 또한, 개인정보 법적 규범에 대한 연구는 개인정보 보호를 위한 정책적 과제를 모색하는데 주안점을 두고 있다 (김재광, 2012; 정대경, 2012). 이와 관련하여 최근 연구에서는 빅데이터 시대의 개인정보 처리 방식에 대한 법적 쟁점을 살펴본 바 있다 (김정현, 2020). 개인정보에 대한 연구는 정보 주체인 소비자 관점에서도 구체적으로 전개되어왔다. 예를 들어 사업자가 소비자에게 개인정보 제공에 대한 동의를 요구할 시 소비자가 느끼는 인지적 부담감과 해당 상황에 대한 문제점을 명확화한 연구가 있다 (구혜경·나종연, 2014). 특히, 최근 개인정보에 대한 연구는 지능정보기술 맥락에서 활발히 진행중에 있다. 이는 사물인터넷 환경 내 개인정보 관리 기술 (전수지 외, 2018), 빅데이터 시대에 소비자가 인지하는 개인정보 과잉과 저항 (이환수 외, 2013) 등 지능정보사회에서 새롭게 제기되고 있는 문제들을 포괄한다. 이러한 연구 동향에서 주목해야할 점은 사용자 관점의 연구의 경우 실제 이용자의 개인정보 개념에 대한 이해보다는 현행 제도 및 기술 환경에 대한 소비자의 태도를 조사하는 연구가 주로 진행되고 있다는 점이다. 앞서 언급하였듯이 개인정보 개념에 대한 사용자 인식을 탐색하는 것은 개인정보 보호의 근본적인 의미인 개인정보 자기결정권을 보장하는데 있어 근간이 되는 기초적인 작업이다. 따라서 본 연구에서는 정보 주체인 사용자의 입장에서 개인정보 개념을 탐색하고, 이를 국내 개인정보 보호 환경과 비교하고자 한다. 이는 현대 정보 사회에서 개인정보 보호 개념이 기존의 식별성 중심에서 개인정보에 대한 통제력까지 포괄하는 프라이버시 보호 개념으로 확장되어야 할 뿐만 아니라, 인격의 자율성 관점으로 해석되어야 할 필요성이 대두되고 있다는 점에서 (권건보, 2017) 더욱 의의가 있다. 특히 본 연구는 개인정보에 대한 개념을 인구통계학적 특성에 따라 분석하고자 한다. 기존 연구들은 개

인정보에 대한 인식과 이와 관련된 변수들을 분석하는데 있어 인구통계학적 요소를 주로 통제 변수로 사용해왔다. 하지만 개인정보에 대한 인식은 개인의 평가와 더불어 개인적 특성에 의해서도 영향을 받는다 (Dinev & Hart, 2006). 실제로 과거 연구에서는 개인정보에 대한 인식이 동일한 조건에서도 개인의 주관적인 판단과 인구통계학적 요소에 따라 유의한 차이를 보임을 확인하였다 (Bergström, 2015; Lee et al., 2019). 따라서 인구통계학적 요소는 개인정보 인식에 직접적인 영향을 미치는 주요 요소로 논의 되어야할 필요성이 있다. 더불어 정보 프라이버시와 인구통계학적 요소 간의 관계를 분석한 연구가 아직 부족한 실정에서, 이러한 접근은 개인적 특성을 고려한 프라이버시 보호 정책을 확립하는데 있어서 중요한 역할을 할 수 있다 (Kim et al., 2018; Lee et al., 2019). 본 분석에 들어가기 앞서 이 연구는 국내의 개인정보 보호 환경을 살펴보고자 한다.

<표 2> 개인정보 연구 동향

주제	저자(연도)	제목	주요 내용
개인정보 개념 및 범위	문재완 (2014)	개인정보의 개념에 관한 연구	개인정보 개념 정립은 헌법상 권리인 개인정보 자기결정권의 내용을 담고 있어야 하며, 동시에 현대 정보통신기술의 발전을 수용할 수 있어야 함
	이대희 (2015)	개인정보 개념의 해석 및 범위에 관한 연구	한국은 개인을 식별할 수 있는 정보를 광범위하게 인정하고 있으며, 프라이버시 보호와 정보의 경제적 유통 사이의 균형을 유지하기 위한 대책이 필요함
	임규철 (2012)	개인정보의 보호범위	개인에 관한 특정 가능성으로 규정되는 개인정보 개념은 보호범위의 포괄적인 인정의 타당성과 정보통신기술의 발전을 고려하여 정립되어야 함

개인정보 법적 규범	김재광 (2012)	개인정보보호법에 관한 새로운 법적 문제	개인정보 보호법은 (1)민간부문 법실효성; (2)추진체계의 모호성; (3)개인정보 보호위원회의 공정성 및 전문성 확보; (4)다른 법령과의 체계적합성; (5)개인정보 영향평가제도 시행 등의 사항들을 고려하여 개선되어야 함
	정대경 (2012)	국내외 개인정보보호정책 비교 분석: 개인정보보호 법률과 전담조직을 중심으로	국내외 개인정보 보호정책에 대한 비교연구를 통하여 국가별 정책 현황을 분석하고 개인정보 보호를 강화하기 위해 필요한 정책적 과제를 탐색함
개인정보 관리 기술	최대선 외 (2013)	빅데이터 개인정보 위험 분석 기술	온라인에 공개된 다양한 개인정보의 위험도를 분석하는 기술을 제안함
	Feng & Agosto (2019)	Revisiting personal information management through information practices with activity tracking technology	인터뷰를 통해 개인 활동 추적 기술(ATT, Activity Tracking Technology) 사용자의 개인정보관리에 대한 인식을 탐색함
개인정보에 대한 소비자 태도	구혜경·나종연 (2014)	소비자의 개인정보 제공 동의 인식에 대한 탐색적 연구	현행 법률상에서 사업자가 개인정보를 수집하고 이용하기 위해 소비자에게 고지해야 하는 주요 내용을 확인하고, 이에 관한 소비자 인식을 확인함
	윤수영·여정성 (2018)	개인정보 이용내역 통지제도에 대한 소비자 인식에 관한 연구	2012년 방송통신위원회가 발표한 개인정보 이용내역 통지제도에 대한 소비자 인식을 조사하여 실효성 있는 개인정보 보호 제도 개선 방안 탐구함

	Kim & Yeo (2010)	Valuation of consumers' personal information: A south korean example	설문을 통해 소비자 입장에서 개인 정보의 금전적 가치를 도출함
	Hargittai & Marwick (2016)	“What can I really do?” Explaining the privacy paradox with online apathy	인터뷰를 통해 젊은 세대들의 정보 프라이버시에 대한 냉담한 태도를 탐색함
개인정보와 지능정보기술	김정현 (2020)	빅데이터 시대의 개인정보 보호법제 개선방안	빅데이터 시대의 올바른 개인정보의 보호와 활용을 위해서는 개인정보 범위의 조정이 필요하며, 특히 가명처리의 한계점과 대안에 대한 지속적인 논의가 필요함
	이환수 외 (2013)	빅데이터 시대의 개인정보 과잉이 사용자 저항에 미치는 영향	빅데이터 시대에 사용자가 인지할 수 있는 개인정보의 과잉이 프라이버시 위험과 염려에 어떠한 영향을 주는지를 살펴보고, 이것이 사용자 저항과 어떠한 관계가 있는지 분석함
	윤승욱 (2018)	빅데이터 환경에서 개인정보 제공 의도 결정요인에 관한 연구	빅데이터 환경에서 개인정보 제공 의도를 결정하는 요인을 살펴보고, 프라이버시에 대한 염려와 서비스 제공자에 대한 신뢰가 큰 영향을 미치는 것으로 나타남
	조재영 (2019)	온라인 맞춤형 광고 활성화를 위한 개인정보 보호에 대한 법적 고찰: 개인정보의 개념을 중심으로	빅데이터 시대에 주목받고 있는 온라인 맞춤형 광고를 활성화시킬 목적으로 기존 연구에서 분명하게 규명되지 않았던 개인정보와 행태정보의 의미를 명확히 하고, 개인정보에 대한 법적 개념을 분석함

전수지 외 (2018)	IoT 환경에서 일반개인정보 보호규정에 부합하는 개인정보 관리 기술에 관한 연구	사물인터넷 환경에서 개인정보 활용 시 일반 개인정보 보호법을 만족하기 위한 개인정보 관리 체계에 대해 연구함
황태희 외 (2019)	빅데이터와 경쟁정책: 국내 온라인 비즈니스 분야 시장 현황 분석을 중심으로	국내의 개인정보 법제 내 빅데이터 관련 쟁점을 파악하고, 기업 입장에서 시장 상황을 분석함
Kim et al. (2018)	Willingness to provide personal information: Perspective of privacy calculus in IoT services	사물인터넷 서비스 이용 시 정보를 제공하고자 하는 의도에 영향을 미치는 요인을 프라이버시 계산 이론을 기반으로 설명하였고, 그 결과 사람들이 개인화된 서비스보다 개인정보 침해 위험이 높은 의료 서비스에서 개인정보 제공 용의가 낮아지는 것으로 나타남
Madaan et al. (2018)	Data integration in IoT ecosystem: Information linkage as a privacy threat	사물인터넷 생태계에서 프라이버시 위협을 기술 및 법적 맥락에서 논의하였으며, 그 결과 데이터의 수집 및 통합을 포함한 중간 데이터 처리 단계에서 프라이버시 위협이 발생한다는 것을 밝힘

2. 개인정보 보호 환경: 개인정보 보호법과 데이터 3법

현재 개인정보 보호를 둘러싼 국내 규제 환경은 관련 법제가 다양하게 연계되어 있으며, 그 중 개인정보 보호법은 민간, 공공 부문을 포괄적으로 규율한다. 개인정보 보호법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유

와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.²⁾ 개인정보 보호법은 사회 전반의 개인정보 보호를 규율하는 일반법으로, 개인정보 보호와 관련하여 타 법률(예: 신용정보법, 의료법, 정보통신망법 등)에 특별한 규정이 있는 경우를 제외하고는 해당 법률을 적용함을 원칙으로 하고 있다. 동 법령은 개인정보 해당 여부에 대한 판단 기준 및 정의를³⁾ 제시하고 있는데 이는 아래 <표 3>과 같다 (행정안전부·한국인터넷진흥원, 2019). 먼저 개인정보는 살아있는 개인에 대한 정보로 사망한 자, 단체, 혹은 사물에 관한 정보는 이에 해당하지 않는다. 개인정보는 단체 및 사물에 관한 정보가 아닌 순수 개인에 관한 정보로 구분하고 있는데, 단체에 대한 정보이면서 동시에 개인에 관한 정보는 개인정보에 해당한다(예: SNS 단체 사진). 개인정보는 개인 식별성을 지닌 정보로, 개인정보 식별의 주체인 정보처리자가 개인을 알아볼 수 있는 정보가 이에 해당한다. 또한 개인 식별성과 더불어 개인정보 해당 여부를 판단하는 기준은 다른 정보와의 결합 가능성을 포함하고 있다. 이는 결합 대상이 될 다른 정보의 입수 가능성과 결합 가능성 모두를 고려한다. 개인정보의 종류 및 형식에 대한 제한은 없으며, 이는 정보의 형태와 처리 방식에 대한 부문도 포함하고 있다. 이처럼 개인정보 보호법은 개인정보에 관한 개별법 체계에 해당하지 않는 모든 민간, 공공 부문을 대상으로 정보의 형태나 처리방식에 관계없이 적용되고 있지만, 구체적인 개인정보의 범위를 설정하는데 있어 모호함을 야기한다는 지적도 존재한다 (이성엽, 2018). 또한 이와 더불어 지능정보기술을 통해 새롭게 생성되는 개인정보를 보호 및 활용하는데 있어서도 법적 정비의 필요하다는 점이 꾸준히 제기되어 왔다 (이애리 외, 2016; 차상욱, 2014).

2) 개인정보 보호법, 제1장 제1조: 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

3) 개인정보 보호법, 제1장 제2조 참고.

<표 3> 개인정보 해당 여부 판단 기준

기 준	내 용
살아있는 개인에 대한 정보	<ul style="list-style-type: none"> 사망한 자, 단체, 또는 사물에 관한 정보는 해당하지 않음 유족과의 관계를 알 수 있는 정보는 유족과 관련된 개인정보에 해당함
개인에 관한 정보	<ul style="list-style-type: none"> 단체 및 사물에 관한 정보는 해당하지 않음 단체에 대한 정보이면서 동시에 개인에 관한 정보는 개인정보에 해당함
개인을 알아볼 수 있는 정보	<ul style="list-style-type: none"> 특정 개인을 알아보기 어려운 정보는 해당하지 않음 개인정보 식별의 주체는 정보를 제공받은 자를 포함한 정보처리자이며, 정보처리자의 입장에서 개인을 알아볼 수 없다면 개인정보에 해당하지 않음
다른 정보와 쉽게 결합하여 알아볼 수 있는 정보	<ul style="list-style-type: none"> 결합 대상이 될 다른 정보의 입수 가능성이 존재하여야 하며, 결합 가능성 또한 높아야 개인정보에 해당함 입수 가능성에는 해킹 등과 같은 불법적인 방법이 고려되지 않으며, 결합 가능성에는 현재 기술 수준이 고려됨
정보의 종류 및 형식에 구애받지 않는 개인 정보	<ul style="list-style-type: none"> 정보의 형태(예: 디지털 혹은 수기)나 처리 방식(예: 자동 혹은 수동)에 관계없이 개인정보 판단 기준에 따름

출처: 행정안전부·한국인터넷진흥원 (2019). 2019년 개인정보 보호법 주요 내용. 재구성.

이와 같이 개인정보 판단 기준을 명확히 할 필요성은 4차 산업혁명 시대 국가 과제인 데이터 이용 활성화를 통한 신산업 육성 정책과 맞물려 개인정보 관련 법령 개정으로 이어졌다. 2020년 1월 9일부로 국회 본회의를 통과한 데이터 3법 개정안은 개인정보 보호 및 활용을 위한 사회적 규범을 정립함과 동시에 협치 체계를 구축하는 것을 그 목적으로 ①개인정보 보호법, ②정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법), ③신용정보의 이용 및 보호에 관한 법률(약칭: 신용정보법) 세 가지를 포괄하여 수립되었다(<표 4> 참고).

먼저 개인정보 보호법 개정안은 개인정보 개념을 정립하고, 보다 안전한 데이터 활용을 위해 가명정보 개념을 도입하였다. 가명정보는 개인을 식별할 수 없도록 안전하게 처리된 정보로, 동 법률 개정안은 해당 정보를 시장 조사를 위한 통

계 처리, 과학적 연구, 공익적 목적으로 정보 주체의 동의 없이 활용할 수 있도록 허용하였다. 또한 개인정보 보호법 개정안은 개인정보의 식별 및 결합 가능성을 판단하는 기준을 신설하였으며, 개인정보보호위원회를 국무총리 소속 중앙행정기관으로 격상하여 감독 및 법 집행을 포함한 개인정보 보호 체계를 일원화하였다는 점에서 의의가 있다 (정희수, 2020). 둘째로, 정보통신망법 개정안은 개인정보 관련 다른 법령과의 중복 조항을 정비하는데 초점을 맞췄다. 동 법률 개정안의 주요 내용은 개인정보 보호 관련 사항을 개인정보 보호법으로 이관한다는 것이며, 이를 통해 동 법상의 개인정보 처리 조항을 크게 축소하였다. 셋째로, 신용정보법 개정안은 데이터 활용의 법적 근거를 분명히 하고 안전장치를 강화하는데 목적을 두었다. 이를 위해 동 법률 개정안은 개인정보(특정 개인에 대한 정보), 가명정보(추가정보 없이는 개인을 식별할 수 없도록 조치한 정보), 익명정보(더 이상 개인을 식별할 수 없도록 조치한 정보) 개념을 명확히 정의하고 이에 따른 활용 가능 범위를 명시하였다. 또한 신용정보법 개정안은 개인신용정보의 전송요구권을 포함한 새로운 개인정보 자기결정권을 도입하고 신용정보 유출에 대한 징벌적 손해 배상금을 강화(기존 손해액의 3배에서 5배로 상향)하는 등 금융 분야 내 개인정보 보호를 위한 체계를 새롭게 구축하였다. 본 연구는 이처럼 데이터 활용에 대한 법, 제도적 혁신이 이루어지고 있는 가운데 사용자가 인식하는 개인정보 개념에 대해 면밀히 살펴보았다.

<표 4> 데이터 3법 개정안 주요 내용

개정안	내 용
개인정보 보호법	<ul style="list-style-type: none"> • 가명정보 개념 도입 및 활용: 가명정보를 시장 조사, 연구, 공익적인 기록 보존을 위한 목적 외에도 데이터를 기반으로 한 새로운 제품 및 서비스를 개발하는데 있어서도 이용할 수 있게 함 • 개인정보보호위원회를 국무총리 소속 중앙행정기관으로 격상하여 기존 3개 법률(개인정보 보호법, 정보통신망법, 신용정보법)에 나뉘어 있던 개인정보 처리 및 보호에 대한 사항을 일원화 • 다른 정보를 사용하여도 개인을 식별할 수 없는 익명정보의 법 적용 배제 명확화

정보통신망법	<ul style="list-style-type: none"> • 기존의 개인정보 관련 규정을 개인정보 보호법으로 이관: 정보통신망 법상의 개인정보 처리 조항을 개인정보 보호법으로 이관하여 축소 • 온라인상의 개인정보 보호 관련 규제 및 감독 주체를 개인정보 보호위원회로 변경
신용정보법	<ul style="list-style-type: none"> • 금융 분야 데이터 활용의 법적 근거 확립 • 금융 분야 개인정보 보호 장치 강화: 사용자가 개인정보 활용 동의 시 이에 따른 사생활 침해위험, 혜택을 고루 평가하여 정보 활용 동의 등급을 산정하여 제공, 금융권의 정보 활용 실태 상시 평가, 신용 정보 유출에 대한 징벌적 손해배상금 강화 • 신용정보 관련 산업의 규제체계 선진화: 신용조사업의 구분 및 진입규제 요건 완화

출처: 대한민국 정책포털 ‘정책위키’ - 데이터 3법. 재구성(<http://www.korea.kr>).

Ⅲ. 연구 방법

1. 자료 수집

본 연구는 개인정보에 대한 사용자 인식을 탐색하기 위해 온라인 설문조사를 시행하였다. 온라인 설문조사는 국내 연구 업체인 엠브레인을 통해 2019년 5월 8일부터 16일까지 약 일주일 동안 진행되었다. 조사 대상자는 전국 만 20세에서 59세까지의 일반인으로 성별(남녀 비율 각각 50%) 및 연령별(연령 20~50대 각각 25%씩) 할당 표집하였다. 설문 문항은 성별 및 나이를 포함한 인구통계학적 요소부터 개인정보 항목에 따른 사용자의 인식을 조사하는 질문들로 구성하였다. 특히 개인정보의 경우 정보통신정책연구원(KISDI)의 연구 결과를 참조하여 크게 기본 정보, 제공 정보, 구성 및 조합정보, 소셜 미디어 정보, 위치 정보로 구분되는 총 18개의 항목(<표 5> 참고)으로 구성하였으며 (조성은·이시직, 2015), 이후 본 분석에서는 각 항목을 간략하게 줄여서 표기하였다. 해당 문항은 리커트(Likert) 7점 척도(1점: 전혀 그렇지 않다, 7점: 매우 그렇다)를 통해 평가되었다.

<표 5> 개인정보 설문 항목

분류	항 목	표 기
“귀하는 다음 정보를 개인정보라고 생각하십니까?”		
기본 정보	1) 이름	1) 이름
	2) 우편주소	2) 우편주소
	3) 주민등록번호	3) 주민등록번호
	4) 핸드폰 번호	4) 핸드폰 번호
	5) 핸드폰 뒷번호 네 자리	5) 핸드폰 뒷 네 자리
	6) 금융정보(은행계좌, 신용카드 등)	6) 금융정보
	7) 이메일주소	7) 이메일주소
제공 정보	8) 주로 사용하는 온라인 서비스 아이디	8) 온라인 서비스 아이디
	13) 회원가입 때 온라인 서비스에 제공한 정보	13) 회원가입 제공 정보
구성 및 조합 정보	12) 웹 브라우저에 기록된 나의 웹 활동정보(쿠키 정보)	12) 쿠키 정보
	14) 온라인서비스사가 회원정보와 회원의 활동 정보를 결합해 재구성한 정보	14) 재구성 정보(회원정보, 활동정보)
	15) 내가 지난 3개월동안 주로 검색한 단어를 분석해 새로 만든 개인 취향 정보	15) 검색 기반 개인 취향 정보
	17) 구글, 네이버 등으로 검색해 확인할 수 있는 개인관련정보	17) 검색 가능한 개인관련 정보
소셜 미디어 정보	9) 소셜 미디어(블로그, 페이스북, 트위터, 인스타그램 등)에 전체 공개로 올린 글	9) 소셜 미디어 전체 공개 글
	10) 소셜 미디어 친구 목록	10) 소셜 미디어 친구 목록
	11) 소셜 미디어에 특정인만 보도록 설정해 올린 글	11) 소셜 미디어 공개 제한 글
	16) 페이스북에서 주로 메시지를 주고받는 친구 목록과 메시지 내용을 분석해 새로 생성한 개인 성향 정보	16) 개인 성향 정보(메시지, 친구목록)
위치 정보	18) 위치 정보(스마트폰 등 기기를 통해 개인이 어디에 있는지 확인할 수 있는 정보)	18) 위치 정보

총 표본 수는 498명으로 설문 응답자의 특성은 아래 <표 6>과 같다. 설문 응답자의 성비는 남성이 49.6%(247명), 여성이 51.4%(251명)를 기록했다. 설문 응답자의 평균 연령은 40.4세였으며, 학력별 분포는 대학 졸업의 비율이 66.7%(332명)로 가장 높게 나타났다.

<표 6> 설문 응답자 특성

항목	척도	빈도	비율(%)
성별	남성	247	49.6
	여성	251	51.4
연령	20대	122	24.5
	30대	123	24.7
	40대	127	25.5
	50대 이상	126	25.3
학력	고졸 이하	65	13.1
	대학 재학	42	8.4
	대학 졸업	332	66.7
	대학원 졸업	59	11.8
소득	100만원 미만	58	11.6
	100 - 200만원	64	12.9
	200 - 300만원	114	22.9
	300 - 400만원	107	21.5
	400 - 500만원	70	14.1
	500만원 이상	85	17.1

2. 자료 분석

본 연구는 개인정보 항목에 대한 사용자의 점수를 계산하고 이를 인구통계학적 요소에 따라 구분하여 그 차이를 분석하였다. 본 연구는 자료 분석을 위해 SPSS 21.0 통계 프로그램을 이용하였다. 인구통계 집단별 평균차이 검증은 독립표본 t-검정과 일원배치 분산분석(ANOVA)을 통해 실시하였다. t-검정의 경우 등분산 가정이 충족되지 못하였을 때 이분산을 가정한 분석방법(Behrens-Fisher approach)을

활용하였다 (Snedecor & Cochran, 1989). 일원배치 분산분석의 경우 등분산 가정이 충족되었을 때 F-검정과 함께 집단별 다중비교를 위한 사후분석으로 Bonferroni 방식을 활용하였으며, 등분산 가정이 충족되지 못하였을 때에는 Welch 검정과 함께 (Welch, 1947) 집단별 다중비교를 위한 사후분석으로 Games-Howell 방식을 채택하였다. 또한 자료 분석 과정에서 개인정보 항목에 대해 사용자가 매긴 점수를 기반으로 탐색적 요인 분석(exploratory factor analysis)을 시행하였다. 탐색적 요인 분석은 다수의 측정 변인들이 어떤 구조로 서로 관련성이 있는지를 탐색하는 방법으로 해당 변인들의 내재된 요인구조에 대한 결과를 도출할 수 있다. 요인 추출은 주성분분석(principle component analysis) 기법을 사용하였고, 회전방법으로는 직각회전(varimax) 방식을 사용하였다. 본 연구는 이와 같은 요인 분석 방법을 이용하여 추출된 요인의 고유 값(eigen value)이 1 이상인 것을 최종적으로 채택하였다.

IV. 연구 결과

1. 개인정보에 대한 사용자 인식과 실제

앞서 밝혔듯이, 개인정보에 대한 법적 정의의 포괄성으로 인해 개인정보 범위 및 유형에 대한 사회적 동의가 충분히 이루어지지 않고 있다. 정보통신기술의 발전에 따라 수집 및 처리되는 정보의 범위와 양이 급증하는 상황에서 이러한 정의의 포괄성은 향후 개인정보에 대한 쟁점을 논하는데 많은 제한을 가져올 수 있다. 따라서 본 논문은 이러한 문제인식 하에서 개인정보 범위에 대한 사용자의 인식을 조사하였고, 이를 성별을 포함한 인구통계학적 요소에 따라 구분하여 비교하였다. 본 연구에서 조사한 개인정보의 범위에 대한 인식은 <표 7>과 같다. 먼저 18개 개인정보 항목에 대한 인식을 7점 척도로 평가하였을 때, 주민등록번호(3)가 가장 높은 값(6.66)을 보였다. 이는 주민등록번호가 모든 개개인을 식별할 수 있는 기능적 특성을 가지고 있기 때문이라고 볼 수 있다. 반면 소셜 미디어 전체 공개 글(9)은 가장 낮은 값(5.04)을 나타냈으며, 최대값(주민등록번호, 6.66)과 최소값(소셜 미디어 전체 공개 글, 5.04)의 차이는 약 2.62를 기록하였다. 설문 응답자가 개인정보로 인식하는 상위 세 가지 항목은 주민등록번호(3), 금융정보(6), 핸드폰 번호(4)였으며, 하위 세 가지 항목은 소셜 미디어 친구 목록(10), 핸드폰 뒷 네

자리(5), 소셜 미디어 전체 공개 글(9)이 차지했다. 이와 같은 사용자의 인식은 현재의 법률적 해석과 간극이 존재한다. 먼저 핸드폰 뒷 네 자리의(5)의 경우 오로지 뒤 네 자리만 있을 경우 개인정보에 해당하지 않으나, 다른 정보(생일, 집 전화번호 등)와의 결합 가능성을 고려하여 개인정보에 해당된다고 판시한 바 있다.⁴ 또한 소셜 미디어 전체 공개 글(9)의 경우 공개된 정보에 해당하나, 정보주체의 동의가 있다고 인정되는 범위 내에서만 수집 및 이용이 가능하다 (방송통신위원회·한국인터넷진흥원, 2015). 다만 이와 관련하여 정보처리자의 행태로 인해 정보주체의 공개의도, 목적, 대상 범위가 달라졌는지 객관적으로 판단하여야 한다는 판례가 있다.⁵ 또한 사용자의 개인정보 범위에 대한 인식은 이분법적(예/아니오) 구조에서 큰 차이를 보이지는 않았다(<표 8> 참고). 설문 응답자의 약 95%가량이 핸드폰 번호(4), 주민등록번호(3), 금융정보(6)가 개인정보에 해당한다고 판단하였다. 반면 소셜 미디어 전체 공개 글(9)의 경우 전체 응답자의 64.5%만이 개인정보라고 답했다. 이전 결과와 마찬가지로 사용자가 판단하는 개인정보 해당 여부는 소셜 미디어 친구 목록(10), 핸드폰 뒷 네 자리(5), 소셜 미디어 전체 공개 글(9)이 최하위에 위치하였다.

<표 7> 사용자의 개인정보에 대한 인식(전체)

항 목	평균	표준편차
3) 주민등록번호	6.66	1.02
6) 금융정보	6.64	1.03
4) 핸드폰 번호	6.52	1.00
18) 위치 정보	6.17	1.11
13) 회원가입 제공 정보	6.08	1.14
14) 재구성 정보(회원정보, 활동정보)	5.95	1.15
8) 온라인 서비스 아이디	5.85	1.24
16) 개인 성향 정보(메시지, 친구목록)	5.85	1.19
7) 이메일주소	5.83	1.23
12) 쿠키 정보	5.79	1.13

4) 대전지방법원 논산지원2013고단17판결 참고

5) 대법원 2014다235080판결 참고

17) 검색 가능한 개인관련정보	5.73	1.22
2) 우편주소	5.71	1.33
15) 검색 기반 개인 취향 정보	5.60	1.19
1) 이름	5.59	1.35
11) 소셜 미디어 공개 제한 글	5.40	1.25
10) 소셜 미디어 친구 목록	5.35	1.30
5) 핸드폰 뒷 네 자리	5.34	1.28
9) 소셜 미디어 전체 공개 글	5.04	1.48

<표 8> 사용자가 판단하는 개인정보 해당 여부(전체)

항 목	비율(%)
4) 핸드폰 번호	95.0
3) 주민등록번호	94.8
6) 금융정보	94.4
18) 위치 정보	91.0
13) 회원가입 제공 정보	89.8
14) 재구성 정보(회원정보, 활동정보)	89.0
12) 쿠키 정보	86.1
16) 개인 성향 정보(메시지, 친구목록)	86.1
8) 온라인 서비스 아이디	85.9
17) 검색 가능한 개인관련정보	84.9
7) 이메일주소	84.1
15) 검색 기반 개인 취향 정보	82.1
2) 우편주소	80.7
11) 소셜 미디어 공개 제한 글	76.9
1) 이름	75.5
10) 소셜 미디어 친구 목록	75.5
5) 핸드폰 뒷 네 자리	74.3
9) 소셜 미디어 전체 공개 글	64.5

개인정보 범위에 대한 사용자의 인식은 인구통계학적 요소에 따라서도 차이를 보였다. 먼저 18개의 항목 중 12개의 항목에서 성별에 따라 통계적으로 유의한 차이를 보였으며, 모두 여성이 더 높은 수치를 기록했다(<표 9> 참고). 이는 상대적으로 여성이 개인정보에 대한 민감도가 더 높은 것으로 해석된다. 특히 개인 온라인 활동 정보, 소셜 미디어 정보와 같은 대부분의 디지털 정보 유형에서 여성이 더 높은 수치를 보였는데, 이는 여성이 남성에 비해 상대적으로 정보통신기술에 대한 염려가 더 높다는 과거 연구결과와 유사하다 (Broos, 2005). 과거 문헌에서는 여성이 남성에 비해 온라인 공간에서 수집 및 활용되는 개인정보에 대해 염려가 더 크다는 것이 밝혀진 바 있다 (Graeff & Harmon, 2002). 가장 큰 차이를 보인 항목은 소셜 미디어에 전체 공개로 올린 글(9)이었으며, 남성이 여성에 비해 비교적 더 낮은 수치를 기록했다(-0.590, $p<0.001$).

<표 9> 인구통계학적 요소에 따른 개인정보에 대한 인식 차이(성별)

항 목	남성	여성	차이	p -value
1) 이름	5.445	5.741	-0.296	0.014*
2) 우편주소	5.587	5.837	-0.250	0.036*
3) 주민등록번호	6.648	6.681	-0.034	0.715
4) 핸드폰 번호	6.437	6.602	-0.164	0.067
5) 핸드폰 뒷 네 자리	5.073	5.610	-0.537	0.000***
6) 금융정보	6.595	6.677	-0.082	0.376
7) 이메일주소	5.676	5.988	-0.312	0.005**
8) 온라인 서비스 아이디	5.721	5.984	-0.264	0.017*
9) 소셜 미디어 전체 공개 글	4.745	5.335	-0.590	0.000***
10) 소셜 미디어 친구 목록	5.166	5.538	-0.372	0.001**
11) 소셜 미디어 공개 제한 글	5.340	5.458	-0.118	0.291
12) 쿠키 정보	5.721	5.849	-0.128	0.209
13) 회원가입 제공 정보	5.931	6.227	-0.296	0.004**
14) 재구성 정보(회원정보, 활동정보)	5.838	6.068	-0.230	0.026*
15) 검색 기반 개인 취향 정보	5.486	5.713	-0.227	0.034*
16) 개인 성향 정보(메시지, 친구목록)	5.737	5.964	-0.227	0.034*
17) 검색 가능한 개인관련정보	5.534	5.932	-0.398	0.000***
18) 위치 정보	5.996	6.339	-0.343	0.001**

* $p<0.05$; ** $p<0.01$; *** $p<0.001$

개인정보 범위에 대한 사용자의 인식은 다른 인구통계학적 요소에 따라서도 차이를 보였다(<표 10> 참고). 먼저 18개의 항목 중 우편주소(2), 이메일주소(7), 쿠키 정보(12)를 포함한 3가지 항목에서 연령에 따라 통계적으로 유의한 차이를 보였다. 이에 반해 교육 및 소득의 경우 그 수준에 따른 차이가 거의 없었으며, 단 1개의 항목인 우편주소(2)에서 통계적으로 유의한 차이를 보였다. 집단별 다중비교를 위한 사후분석을 실시한 결과는 다음과 같다(<표 11> 참고). 연령의 경우 앞서 언급한 3가지 항목에서 20대와 30대 간의 차이는 보이지 않았다. 가장 큰 차이를 보인 것은 20대와 40대 간의 우편주소(2)에 대한 인식으로 확인되었고, 20대가 40대에 비해 더 높은 수치를 기록했다. 반면 이메일 주소(7)의 경우 20대가 40대와 50대에 비해 더 낮은 수치를 기록했다. 쿠키 정보(12)는 비교적 더 젊은 연령대인 20대와 30대가 50대보다 더 높은 수치를 기록했다. 종합하자면 개인정보 범위에 대한 사용자 인식은 연령대에 따라 유의한 차이를 보였으며, 그 차이는 젊은 세대(20대, 30대)와 기성 세대(40대, 50대) 간에서 두드러졌다. 앞서 밝혔듯이 소득 수준에 따른 개인정보 범위에 대한 사용자 인식은 우편주소(2)에서만 차이를 보였으며, 이는 소득이 100만원 미만인 집단과 500만원 이상인 집단에서 가장 큰 차이를 보였다.

<표 10> 인구통계학적 요소에 따른 개인정보에 대한 인식 차이(연령, 교육 수준, 소득 수준)

항 목	연령		교육 수준		소득 수준	
	F 통계량	p-value	F 통계량	p-value	F 통계량	p-value
1) 이름	0.981	0.401	0.820	0.483	0.942	0.453
2) 우편주소	6.818	0.000***	0.225	0.879	2.746	0.018*
3) 주민등록번호	0.630	0.596	0.331	0.803	0.191	0.966
4) 핸드폰 번호	1.384	0.247	0.776	0.508	0.572	0.721
5) 핸드폰 뒷 네 자리	0.890	0.446	0.547	0.650	0.984	0.427
6) 금융정보	0.941	0.420	1.055	0.368	0.399	0.850
7) 이메일주소	5.589	0.001**	1.892	0.130	0.439	0.821
8) 온라인 서비스 아이디	1.913	0.126	0.788	0.501	0.750	0.586
9) 소셜 미디어전체 공개 글	0.617	0.604	0.744	0.526	0.662	0.653

10) 소셜 미디어 친구 목록	0.368	0.776	0.452	0.716	0.242	0.944
11) 소셜 미디어에 특정 공개 글	0.339	0.797	1.138	0.333	0.712	0.615
12) 쿠키 정보	5.376	0.001**	2.293	0.077	0.619	0.685
13) 회원가입 정보	0.514	0.673	1.098	0.349	0.565	0.727
14) 회원정보 및 활동정보 결합 재구성 정보	0.462	0.709	0.828	0.479	0.752	0.585
15) 검색 기반 개인 취향 정보	1.256	0.289	0.853	0.465	0.284	0.922
16) 페이스북 친구 목록 및 메시지 내용 결합 개인 성향 정보	1.412	0.238	1.623	0.183	0.438	0.822
17) 검색 가능한 개인관련정보	1.635	0.180	0.698	0.554	2.057	0.070
18) 위치 정보	2.570	0.054	0.747	0.524	1.615	0.154

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

<표 11> 인구통계학적 요소에 따른 개인정보에 대한 인식 차이(사후분석)

항 목	연 령					
	(1)-(2)	(1)-(3)	(1)-(4)	(2)-(3)	(2)-(4)	(3)-(4)
2) 우편주소	0.163	0.624**	0.573**	0.461*	0.410	-0.051
7) 이메일주소	-0.297	-0.532**	-0.556**	-0.235	-0.259	-0.024
12) 쿠키 정보	0.097	0.157	0.531**	0.059	0.434*	0.374*

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; (1): 20대, (2): 30대, (3), 40대, (4) 50대

항 목	소득 수준				
	(1)-(2)	(1)-(3)	(1)-(4)	(1)-(5)	(1)-(6)
2) 우편주소	0.316	0.514	0.562*	0.593	0.771**
	(2)-(3)	(2)-(4)	(2)-(5)	(2)-(6)	(3)-(4)
	0.198	0.246	0.276	0.455	0.048
	(3)-(5)	(3)-(6)	(4)-(5)	(4)-(6)	(5)-(6)
	0.079	0.258	0.031	0.210	0.179

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; (1): 100 만원 미만, (2): 100 - 200 만원, (3): 200 - 300 만원, (4): 300 - 400 만원, (5): 400 - 500 만원, (6): 500 만원 이상

앞서 분석한 결과에 따르면 인구통계학적 요소에 따른 개인정보 범위에 대한 인식은 젊은 세대와 기성세대 간에서 그 차이가 두드러졌다. 이에 본 연구는 보다 종합적인 해석을 위해서 설문 응답자를 디지털 원주민(digital native)과 디지털 이민자(digital immigrant) 세대로 구분하여 추가적으로 분석을 진행하였다(<표 12> 참고). 이는 미국의 교육학자 마크 프렌스키(Marc Prensky)가 처음 사용한 용어로, 디지털 원주민은 태어날 때부터 디지털 기기와 기술을 일상적으로 접한 세대를 일컬으며 디지털 이민자는 해당 문물에 익숙해지기 위해 노력한 세대를 뜻한다 (Prensky, 2001). 과거 문헌에서는 1980년대 이후에 출생한 세대를 디지털 원주민으로 구분하고 있으며, 해당 세대는 정보통신기술을 매개로 한 소통과 정보 접근에 익숙한 것으로 나타났다 (Palfrey & Gasser, 2011). 이러한 디지털 세대 개념은 최근까지도 정보통신기술과 관련된 인식 및 행동을 분석하는데 있어 국내외로 널리 활용되고 있으며 (최인호·정세훈, 2019; Kesharwani, 2020), 다국가 분석을 통해 검증된 바 있다 (Evjemo et al., 2019). 또한 각 세대는 디지털 현상에 대해 서로 다른 이해를 가지고 있는 것으로 밝혀져, 인터넷 환경에서 세대 간의 인식 격차를 이해하는데 유용한 개념으로 판단된다 (Ahn & Jung, 2016). 이에 본 연구에서는 1980년대 이후 출생한 20~30대를 디지털 원주민으로 구분하였다. 디지털 원주민은 상대적으로 기본신상정보인 우편주소(2)를 더 개인정보라고 인식하는 반면, 디지털 이민자는 웹 상의 공개 정보인 이메일주소(7)와 온라인 서비스 아이디(8)를 더 개인정보라고 생각하는 경향이 있었다. 이는 디지털 원주민을 표방하는 젊은 세대는 온라인상으로 공개한 정보를 그들이 제대로 통제 및 관리할 수 없는 개인정보로 인식한다는 연구결과와 일치한다 (Hargittai & Marwick, 2016). 쿠키 정보(12)와 위치 정보(18)의 경우 디지털 원주민이 디지털 이민자에 비해 상대적으로 더 높은 수치를 기록하였다. 이 결과는 과거 연구에서 기술에 대한 개인적인 판단이 해당 기술에 대해 충분한 지식을 습득한 후 이루어진다고 밝혀진 바와 같이 (Straub, 2009), 해당 정보들의 활용처에 대해 이해도가 높은 디지털 원주민이 더 민감하게 응답했을 것으로 추정된다. 가장 큰 차이를 보인 항목은 우편주소(2)였으며, 디지털 원주민이 디지털 이민자에 비해 상대적으로 더 높은 수치를 기록했다(0.517, $p<0.001$).

<표 12> 인구통계학적 요소에 따른 개인정보에 대한 인식 차이(디지털 세대)

항 목	디지털 원주민	디지털 이민자	차이	p-value
1) 이름	5.580	5.609	-0.029	0.810
2) 우편주소	5.976	5.459	0.517	0.000***
3) 주민등록번호	6.661	6.668	-0.007	0.941
4) 핸드폰 번호	6.502	6.538	-0.035	0.693
5) 핸드폰 뒷 네 자리	5.425	5.265	0.160	0.164
6) 금융정보	6.633	6.640	-0.008	0.934
7) 이메일주소	5.633	6.028	-0.395	0.000***
8) 온라인 서비스 아이디	5.735	5.968	-0.234	0.035*
9) 소셜 미디어 전체 공개 글	4.988	5.095	-0.107	0.419
10) 소셜 미디어 친구 목록	5.318	5.387	-0.069	0.554
11) 소셜 미디어 공개 제한 글	5.343	5.455	-0.112	0.318
12) 쿠키 정보	5.935	5.640	0.294	0.004***
13) 회원가입 제공 정보	6.041	6.119	-0.078	0.447
14) 재구성 정보(회원정보, 활동정보)	5.988	5.921	0.067	0.519
15) 검색 기반 개인 취향 정보	5.682	5.522	0.160	0.136
16) 개인 성향 정보(메시지, 친구목록)	5.931	5.775	0.156	0.145
17) 검색 가능한 개인관련정보	5.816	5.656	0.160	0.144
18) 위치 정보	6.269	6.071	0.198	0.047*

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

2. 사용자 인식에 기반한 요인분석

본 연구는 설문 응답자가 매긴 점수를 바탕으로 요인 분석을 실시하였다(<표 13> 참고). 요인 분석 과정에서 요인 계수 값이 0.6 미만이거나 교차 적재(cross-loading) 기준치(0.4 이상)를 상회하는 문항들은 제거하였고(Hair et al., 1998), 총 14개의 항목을 가지고 분석을 수행하였다. 요인 분석 시 전체 자료의 적합성을 보여주는 KMO(Kaiser-Meyer-Olkin measure) 값은 0.910을 기록하며 기준치(0.8 이상)를 만족하였다(Fraenkel & Wallen, 2000). 또한 Bartlett의 구형성 검정치 또한

유의수준(p -value<0.05)보다 낮게 산정되어(0.000), 요인 분석을 실시하기에 적합한 것으로 나타났다 (Davidshofer & Murphy, 2005). 탐색적 요인 분석 결과 1 이상의 고유 값을 가진 4개의 요인이 추출되었고, 총 분산 중 69.9%가 이들 요인에 의해서 설명되는 것으로 나타났다. 이후 내적 신뢰도를 측정하기 위해 각 요인의 크론바흐 알파(Cronbach's alpha) 값을 산출하였으며, 요인 4를 제외한 모든 요인이 0.7 이상으로 나타나 항목 간의 내적 일관성이 확보되었다. 요인 4의 크론바흐 알파 값 또한 0.6 이상을 기록하며, 탐색적인 연구에서 수용 가능한 수준으로 평가되었다 (Hair et al., 1998). 본 연구는 추출된 4개의 요인을 구성하는 항목에 근거하여 다음과 같이 명명하였다: ①재구성(2차 활용) 정보, ②민감한 개인정보, ③자발적 공개 정보, ④기본신상정보. 먼저 첫 번째 요인인 재구성 정보의 경우 총 6개의 개인정보 항목들로 구성되었으며 주로 온라인 공간 내 개인의 디지털 활동과 관련된 정보이다. 해당 요인에는 개인이 제공한 정보, 활동 정보, 여러 정보가 결합된 디지털 정보 등이 포함되었다. 두 번째 요인인 민감한 개인정보는 금융정보(6), 주민등록번호(3), 핸드폰 번호(4)를 포함한 세 가지 항목으로 구성되었다. 두 번째 요인을 구성하는 항목들은 유출 시 개인에게 실질적인 금전적 피해 혹은 사생활 침해가 발생할 가능성이 높은 정보들이다. 세 번째 요인인 자발적 공개 정보는 소셜 미디어에 전체 공개로 올린 글(9), 소셜 미디어 친구 목록(10), 온라인 서비스 아이디(8)로 구성되었으며, 이는 주로 사용자가 자발적으로 공개하는 항목들이다. 네 번째 요인인 기본신상정보의 경우 두 가지 항목인 이름(1)과 우편주소(2)로 구성되었다.

<표 13> 개인정보 항목에 대한 탐색적 요인 분석 결과

항 목	성 분			
	1	2	3	4
15) 검색 기반 개인 취향 정보	0.837			
16) 개인 성향 정보(메시지, 친구목록)	0.827			
14) 재구성 정보(회원정보, 활동정보)	0.707			
12) 쿠키 정보	0.685			
17) 검색 가능한 개인관련정보	0.657			
13) 회원가입 제공 정보	0.604			

6) 금융정보		0.896		
3) 주민등록번호		0.895		
4) 핸드폰 번호		0.810		
9) 소셜 미디어 전체 공개 글			0.857	
10) 소셜 미디어 친구 목록			0.742	
8) 온라인 서비스 아이디			0.636	
1) 이름				0.780
2) 우편주소				0.776
고유 값(eigen value)	8.417	1.693	1.353	1.123
분산(variance) %	46.763	9.405	7.515	6.239
크론바흐 알파(Cronbach's alpha)	0.904	0.942	0.777	0.665
적합성(Kaiser-Meyer-Olkin)	0.910			

본 연구는 사용자 인식에 기반한 요인 분석 결과를 실제 법률적 유형과 비교하였다(<표 14> 참고). 먼저 응답자들은 기존에 디지털 정보로 묶이는 정보들도 ① 재구성(2차 활용)정보와 ③자발적 공개 정보로 나뉘어 인식하는 것으로 나타났다. 또한 그들은 기존 유형 구분에서 기본인적사항 정보로 묶이는 정보들도 ②민감한 개인정보와 ④기본신상정보로 구분하고 있었다. 금융정보(6)의 경우 기본인적사항 정보 유형에 해당하는 주민등록번호(3), 핸드폰 번호(4)와 같은 요인으로 묶이며 개인정보 기본 유형과 차이점을 보였다.

<표 14> 사용자 인식과 개인정보 기본 유형과의 차이

사용자 인식	개인정보 기본 유형
요인 1: 재구성 정보	
15) 검색 기반 개인 취향 정보	통신(디지털)정보
16) 개인 성향 정보(메시지, 친구목록)	통신(디지털)정보
14) 재구성 정보(회원정보, 활동정보)	통신(디지털)정보
12) 쿠키 정보	통신(디지털)정보
17) 검색 가능한 개인관련정보	통신(디지털)정보
13) 회원가입 제공 정보	통신(디지털)정보

요인 2: 민감한 개인정보	
6) 금융정보	신용(금융)정보
3) 주민등록번호	일반(인적사항)정보
4) 핸드폰 번호	일반(인적사항)정보
요인 3: 자발적 공개 정보	
9) 소셜 미디어 전체 공개 글	통신(디지털)정보
10) 소셜 미디어 친구 목록	통신(디지털)정보
8) 온라인 서비스 아이디	통신(디지털)정보
요인 4: 기본신상정보	
1) 이름	일반(인적사항)정보
2) 우편주소	일반(인적사항)정보

본 연구는 사용자 인식에 기반한 요인분석을 성별에 따라 추가적으로 실시하였다(<표 15> 참고). 해당 분석에서는 앞서 진행한 방식과 동일하게 요인 계수 값이 0.6 미만이거나 교차 적재(cross-loading) 기준치(0.4 이상)를 상회하는 항목들은 제거하였다 (Hair et al., 1998). 요인 분석 시 전체 자료의 적합성을 보여주는 KMO(Kaiser-Meyer-Olkin measure) 값은 두 성별 모두 기준치(0.8 이상)를 만족하였으며 (Fraenkel & Wallen, 2000), Bartlett의 구형성 검정치 또한 유의수준(p -value<0.05) 보다 낮게 산정되어(0.000) 요인 분석을 실시하기에 적합한 것으로 나타났다 (Davidshofer & Murphy, 2005). 탐색적 요인 분석 결과 두 성별 모두에서 1 이상의 고유 값을 가진 4개의 요인이 추출되었으며, 각 요인의 구성 요소는 성별에 따라 차이를 보였다. 먼저 ②민감한 개인정보와 ④기본신상정보 요인의 경우 성별에 관계없이 같은 항목들을 포함하는 것으로 나타났다. 하지만 ③자발적 공개 정보 요인을 구성하는 항목들의 경우 남성은 소셜 미디어 전체 공개 글(9), 소셜 미디어 친구 목록(10), 이메일주소(7), 온라인 서비스 아이디(8)를 포함한 반면, 여성은 소셜 미디어 전체 공개 글(9)과 소셜 미디어 친구 목록(10)만을 구성 항목들로 인식하였다. 성별에 따른 차이는 ①재구성(2차 활용) 정보 요인을 구성하는 항목들에서도 차이를 보였다. 남성의 경우 개인 성향 정보(메시지, 친구목록)(16), 검색 기반 개인 취향 정보(15), 검색 가능한 개인관련정보(17)만을 해당 요인을 구성하는 항목들로 포함한 반면, 여성의 경우 재구성 정보(회원정보, 활동정보)(14)와 쿠키 정보(12) 또한 해당 요인을 구성하는 항목들로 인식하였다.

<표 15> 개인정보 항목에 대한 탐색적 요인 분석 결과(성별)

항 목	성분(남성)			
	1	2	3	4
6) 금융정보	0.905			
3) 주민등록번호	0.894			
4) 핸드폰 번호	0.789			
16) 개인 성향 정보(메시지, 친구목록)		0.805		
15) 검색 기반 개인 취향 정보		0.798		
17) 검색 가능한 개인관련정보		0.633		
9) 소셜 미디어 전체 공개 글			0.819	
10) 소셜 미디어 친구 목록			0.733	
7) 이메일주소			0.702	
8) 온라인 서비스 아이디			0.662	
1) 이름				0.831
2) 우편주소				0.774
고유 값(eigen value)	7.647	1.914	1.389	1.211
분산(variance) %	42.485	10.635	7.717	6.730
크론바흐 알파(Cronbach's alpha)	0.926	0.832	0.793	0.617
적합성(Kaiser-Meyer-Olkin)	0.871			
항 목	성분(여성)			
	1	2	3	4
15) 검색 기반 개인 취향 정보	0.879			
16) 개인 성향 정보(메시지, 친구목록)	0.856			
14) 재구성 정보(회원정보, 활동정보)	0.722			
17) 검색 가능한 개인관련정보	0.716			
12) 쿠키 정보	0.713			
3) 주민등록번호		0.889		
6) 금융정보		0.876		
4) 핸드폰 번호		0.849		
1) 이름			0.831	

2) 우편주소			0.774	
9) 소셜 미디어 전체 공개 글				0.876
10) 소셜 미디어 친구 목록				0.765
고유 값(eigen value)	9.101	1.614	1.416	1.034
분산(variance) %	50.561	9.024	7.867	5.747
크론바흐 알파(Cronbach's alpha)	0.909	0.958	0.705	0.804
적합성(Kaiser-Meyer-Olkin)	0.918			

V. 결론 및 시사점

본 연구는 사용자의 입장에서 개인정보 개념을 탐색하고, 이를 실제 개인정보 보호 환경과 비교 분석하기 위해 수행되었다. 이를 위해 본 연구는 개인정보 개념부터 연구 동향, 규제 현황을 소략하게 살펴보고, 이후 사용자들을 대상으로 그들이 인식하는 개인정보 범위에 대한 설문을 실시하였다. 본 연구의 주요 결과는 다음과 같다. 먼저 사용자가 생각하는 개인정보 항목 상위 세 가지는 주민등록번호(3), 금융정보(6), 핸드폰 번호(4)로 나타났다. 이는 사용자가 평가하였을 때 특정 개인을 정확하게 식별할 수 있는 정보이거나, 혹은 유출 시 실질적인 피해를 야기할 수 있는 항목들로 이해할 수 있다. 본 연구의 결과를 정보통신정책연구원에서 실시한 연구의 결과 (조성은·이시직, 2015)와 비교할 시, 시간의 흐름에 따른 사용자의 개인정보에 대한 인식 변화를 알아볼 수 있다. 먼저, 2015년도와 비교하여 개인정보 범위에 대한 인식은 총 세 가지 항목에서 10%이상 차이를 보였다. 해당 연도와 비교하여 가장 큰 폭의 차이를 보인 것은 소셜 미디어 전체 공개로 올린 글(9)이었으며, 해당 항목이 개인정보에 해당한다고 답변한 사용자는 2015년도의 조사 결과(44.3%)에 비해 본 연구가 수행된 2019년도에 약 20%가량 증가하였다(64.5%). 이는 불특정 다수를 대상으로 온라인상에 공개한 정보로도 개인 식별이 가능하다고 인식하는 경향이 늘어났다고 해석이 가능하다. 그 외로 우편주소(2)와 핸드폰 뒷 네 자리(5)가 2015년도의 결과와 비교하여 10% 이상의 상승세를 보였다. 또한 재구성 정보의 경우 한 가지 항목(14)을 제외하고 모두 상승 추세를 보였는데, 이는 데이터 처리 기술의 발전과 함께 재구성 정보에 대한 인식

이 변화한 것으로 추정된다. 가장 큰 하락세를 보인 항목은 이름(1)이었으며, 2015 년도에 비해 약 9%가량 하락한 것으로 나타났다(75.5%).

본 연구에 따르면 개인정보 범위에 대한 사용자의 인식은 인구통계학적 특성에 따라 차이를 보였다. 특히 여성의 경우 18개의 개인정보 항목 중 12개 항목에서 남성보다 더 높은 수치를 기록하였다. 이와 같은 결과는 과거 문헌에서 증명되었 듯이 여성이 남성보다 온라인 공간에서 수집 및 활용되는 개인정보에 대한 염려가 더 크기 때문으로 판단된다 (Graeff & Harmon, 2002). 또한 이러한 결과는 개인정보에 대한 인식이 다양한 심리적, 행동적 결과에 영향을 미친다는 것을 고려할 때 더 큰 의미가 있다 (Smith et al., 2011; Westin, 2003). 즉 정보 프라이버시의 핵심 요소가 개인정보에 대한 통제라고 볼 때 (Westin, 2003) 위와 같은 차이는 성별에 따라 개인정보 자기결정권에 대한 인식 수준이 다를 수 있음을 보여주며, 이에 따른 보호 행동 또한 달라질 수 있다는 점에서 시사점을 제시한다. 예를 들어 본 분석에서는 여성이 남성에 비해 위치 정보(18)에 대한 민감도가 더 높은 것으로 나타났는데, 실제로 기존 연구에서 여성은 위치 정보에 대한 위험도를 느낄수록 해당 정보를 공개하고자 하는 용의가 남성에 비해 현저히 떨어지는 것으로 밝혀졌다 (Sun et al., 2015). 따라서 본 연구의 결과는 개인정보에 대한 인식의 차이가 프라이버시와 관련된 주요 행동 차이를 야기할 수 있다는 전제 하에, 개인적 특성을 고려한 체계적인 프라이버시 보호 접근법에 대한 근거를 제공한다는 점에서 그 의미가 있다. 개인정보 범위에 대한 인식은 디지털 세대에 따라서도 차이를 보였다. 디지털 기술을 일상의 일부로 인식하며 자라온 디지털 원주민의 경우 디지털 이민자에 비해 온라인상의 기본신상정보인 이메일주소(7)와 온라인 서비스 아이디(8)를 비교적 낮은 수준의 개인정보로 평가하였다. 이는 디지털 원주민을 표방하는 젊은 세대의 경우 온라인상으로 공개한 신상정보를 그들이 제대로 관리할 수 없는 개인정보로 인식한다는 기존 연구 결과와 더불어 (Hargittai & Marwick, 2016), 해당 세대에서 개인정보 관리에 대한 냉소주의 현상이 존재함을 보여준다. 또한 디지털 원주민은 디지털 이민자에 비해 쿠키 정보(12)와 위치 정보(18)를 더 높은 수준의 개인정보로 인식하였다. 앞서 언급하였듯이 기존 문헌에서 진보된 기술에 대한 개인적인 판단은 해당 기술에 대해 충분한 지식을 습득한 후 이루어지는 것으로 밝혀졌다 (Straub, 2009). 이에 본 연구는 쿠키 정보(12)와 위치 정보(18)의 활용처에 대한 이해도가 높은 디지털 원주민이 해당 정보에 대해 더 민감하게 반응하였을 것으로 추정한다. 이와 같은 점을 통해서 본 연구의 결과는 정

보 프라이버시에 대한 논의를 진전시키기 위해서는 디지털 세대에 따른 관점의 차이와 기술적 이해도를 고려해야함을 시사한다.

사용자 인식에 기반한 요인분석 결과 총 4개의 요인이 추출되었고, 이는 ①재구성(2차 활용) 정보, ②민감한 개인정보, ③자발적 공개 정보, ④기본신상정보로 구분되었다. 더 나아가, 본 연구의 요인분석 결과에 따르면 사용자가 본래 신용정보와 일반정보로 나누는 개인정보들(금융정보, 주민등록번호, 핸드폰 번호)을 하나로 요인으로 인식하는 등 현 법률체계가 제공하는 개인정보 유형과 사용자가 인식하는 유형 간 차이가 존재함을 보여주었다. 좀 더 구체적으로 본 연구는 사용자가 인식하는 개인정보 항목 상위 세 가지인 주민등록번호(3), 금융정보(6), 핸드폰 번호(4)가 ②민감한 개인정보 요인으로 묶인 것을 확인하였다. 이는 비교적 낮은 민감도를 기록했던 이름(1)과 우편주소(2)가 ④기본신상정보 요인으로 묶인 것과 분명한 차이가 있다. 즉 사용자는 개인정보 유형을 구분할 시 실질적인 금전적 피해 혹은 심각한 사생활 침해가 발생할 가능성에 집중하는 것을 알 수 있다. 따라서 본 연구의 결과는 개인정보의 범위가 해당 정보의 유출 시 초래할 수 있는 부정적인 결과에 기반하여 정교화될 필요가 있다는 것을 시사한다. 또한 사용자는 법률상 디지털 정보로 묶이는 항목들도 ①재구성(2차 활용)정보와 ③자발적 공개 정보 요인으로 구분하였다. 이는 최근 연구에서 사용자의 정보 공개 용의를 자발적과 비자발적인 맥락으로 구분하여 분석한 것과 같이 (Li et al., 2020), 같은 유형의 개인정보에 대한 인식을 탐색하는데 있어서도 명확한 영역 구분이 필요하다는 것을 보여준다. 또한 본 연구의 결과는 성별에 따라 해당 요인을 구성하는 항목들이 다르다는 것을 확인하였다. 본 분석에 따르면 성별에 따라 ①재구성(2차 활용) 정보 요인과 ③자발적 공개 정보 요인을 구성하는 항목들이 다른 것으로 나타났다. 특히 여성의 경우 ①재구성(2차 활용) 정보 요인을 구성하는 항목들이 남성에 비해 많은 반면, 남성의 경우 ③자발적 공개 정보 요인을 구성하는 항목들이 여성에 비해 많았다. 이는 정보통신기술에 대한 염려가 높은 여성의 특성과 해당 기술에 대한 남성의 자기 과신 성향이 반영된 것으로 추정된다 (Broos, 2005). 즉 여성은 활용도가 높은 재구성 디지털 정보에 관하여 더 많은 경우를 고려하는 반면, 남성은 자기 확신 성향으로 인해 자발적으로 공개할 수 있는 정보를 보다 많이 인식하는 것으로 해석된다.

본 연구의 분석 결과는 다음과 같은 시사점을 제시한다. 첫 째로, 본 논문은 사용자 입장에서 개인정보에 대한 동적(dynamic) 개념 정립이 필요함을 보여주었다.

이는 개인정보 개념에 대한 사회적 인식의 변화가 필요함과 동시에 해당 개념을 정보통신기술의 진화에 따라 재탐색해야 함을 시사한다. 사용자 인식을 탐색하는 것은 실질적인 개인정보 보호 권리를 실현하기 위한 기초적인 작업이며, 기업 및 조직이 정보 주체의 거부감을 최소화한 개인정보 활용 체계를 수립하는데 초석이 될 수 있다는 점에서 의의를 갖는다. 또한 이는 개인과 기업 간의 개인정보 활용을 둘러싼 첨예한 갈등을 완화하는데 기여할 수 있다. 둘째로, 본 연구의 결과는 개인적 특성에 따라 개인정보에 대한 이해가 상이함을 나타냈다. 이는 개인정보에 관하여 사회적 갈등을 최소화할 수 있는 접근법이 필요함을 시사한다. 다시 말해, 개인정보 수집 및 활용에 관한 정책 및 전략을 수립할 시 인구통계학적 특성에 따른 차이를 인지하여야 하며, 이를 기반으로 의사결정이 이루어져야 함을 시사한다. 최근 연구에서도 개인적 특성에 따라 개인정보 수집 및 활용 행태에 대한 태도가 다르다는 것이 증명된 바 있으며 (Lee et al., 2019), 본 연구의 결과는 향후 개인정보에 대한 연구가 인구통계학적 특성에 따라 세부적인 분석이 필요함을 제시한다. 마지막으로, 본 연구는 개인정보 관련 규제를 사회적 인식과 정보기술 환경을 포함하여 사용자 관점에 초점을 두고 지속적으로 논의할 필요성을 제시한다. 본 연구에 따르면 현 법률체계상의 개인정보 유형과 사용자가 실제로 인식하는 개인정보 유형 간에 분명한 차이가 존재하였다. 이는 개인정보 체계와 관련하여 실질적인 사용자 입장에서의 검토가 필요함을 시사하며, 이를 위해 추가적인 정책적 과제 탐색이 이루어져야 함을 의미한다.

본 연구의 가장 큰 한계점은 사용자가 이해하는 개인정보 개념을 탐색하는데 있어 다소 제한적인 정보를 제공한다는 점이다. 본 논문은 실제 사용자가 인식하는 개인정보 개념에 대한 연구가 부족한 실정에서 사용자의 관점을 심층적으로 파악하는데 그 목적을 두었다. 이에 본 연구는 기존 문헌을 참고하여 실제 사용자가 충분히 구분할 수 있는 개인정보 항목을 설문에 포함하였다. 추후 연구에서는 본 연구의 결과를 바탕으로 사용자의 개인정보 인식에 대한 보다 다양한 접근을 할 수 있을 것으로 예상된다. 예를 들어 설문 응답자의 특성 외로 미디어 이용행태, 개인정보에 대한 민감도 등을 측정하여 이에 따른 개인정보 범위에 대한 인식 차이를 탐색할 수도 있다. 이와 관련하여 추후 연구에서는 개인정보에 대한 인식 차이를 보다 다양한 개인적 특성을 고려하여 연구할 수 있을 것으로 기대한다. 예를 들어 기존 연구에서 살펴보았듯이 (예: Kim et al., 2018) 개인의 성격적 특성이 개인정보 개념 평가에 미치는 영향을 향후 추가적으로 조사할 수 있을 것이

라 판단된다. 또한 향후 연구에서는 정형화된 항목뿐만 아니라, 개인정보 개념 자체에 대한 사용자의 인식을 개방적이고 유연한 질문을 통해 탐구할 수 있을 것으로 기대한다.

참고문헌

- 구혜경·나종연 (2014). 소비자의 개인정보 제공 동의 인식에 대한 탐색적 연구. 『소비문화연구』, 17(2), 151-181.
- 권건보 (2017). 개인정보자기결정권의 보호범위에 대한 분석: 개인정보의 개념을 중심으로. 『공법학연구』, 18(3), 199-224.
- 김재광 (2012). 개인정보보호법에 관한 새로운 법적 문제. 『강원법학』, 36, 95-120.
- 김정현 (2020). 빅데이터 시대의 개인정보 보호법제 개선방안. 『법학논총』, 46, 111-134.
- 김종세 (2020). 인공지능의 안전성과 인간윤리에 대한 법정정책적 고찰. 『법학연구』, 20(1), 1-35.
- 남형두 (2019). 건강정보 빅데이터와 프라이버시 침해 문제. 『정보법학』, 23(3), 1-33.
- 문재완 (2014). 개인정보의 개념에 관한 연구. 『공법연구』, 42, 53-77.
- 방송통신위원회·한국인터넷진흥원 (2015). 『빅데이터 개인정보보호 가이드라인』 해설서, 1-42.
- 신동희·김용문 (2015). 국내 재난관리 분야의 빅 데이터 활용 정책방안. 『한국콘텐츠학회논문지』, 15(2), 377-392.
- 윤수영·여정성 (2018). 개인정보 이용내역 통지제도에 대한 소비자 인식에 관한 연구. 『소비자학연구』, 29(3), 17-38.
- 윤혜선 (2019). 인공지능 규제 정책에 관한 연구: 주요국의 규제 정책 사례를 중심으로. 『정보통신정책연구』, 26(4), 135-176.
- 이대희 (2015). 개인정보 개념의 해석 및 범위에 관한 연구. 『고려법학』, 79, 165-207.
- 이성엽 (2018). 한국의 데이터주도 혁신에 대한 법의 대응과 진화. 『경제규제와 법』, 11(2), 147-167.

- 이애리·손수민·김현진·김범수 (2016). 사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도 개선 방안. 『정보보호학회논문지』, 26(4), 995-1012.
- 이환수·임동원·조항정 (2013). 빅데이터 시대의 개인정보 과잉이 사용자 저항에 미치는 영향. 『지능정보연구』, 19(1), 125-139.
- 임규철 (2012). 개인정보의 보호범위. 『한독법학』, 17, 223-248.
- 윤승욱 (2018). 빅데이터 환경에서 개인정보 제공 의도 결정요인에 관한 연구. 『언론과학연구』, 18(1), 52-78.
- 전수지·양진홍·정성관·김철수 (2018). IoT 환경에서 일반개인정보보호규정에 부합하는 개인정보 관리 기술에 관한 연구. 『한국통신학회 학술대회논문집』, 1152-1153.
- 정대경 (2012). 국내외 개인정보보호정책 비교 분석: 개인정보보호 법률과 전담조직을 중심으로. 『정보보호학회논문지』, 22(4), 923-939.
- 정희수 (2020). 데이터 3법 개정의 의미와 시사점. KEB 하나은행 하나금융경영연구소. Retrieved March 5, 2020, <http://www.hanaif.re.kr/kor/jsp/board/board.jsp?sa=ci&bid=177&pg=1&no=34273>.
- 조성은·이시직 (2015). 『빅데이터 시대 개인 행태 정보 수집 및 활용에 대한 정책 연구』 (기본연구 15-03). 정보통신정책연구원.
- 조수영 (2018). 개인정보보호법과 EU의 GDPR 에서의 프라이버시 보호에 관한 연구. 『법학논고』, 61, 117-148.
- 조재영 (2019). 온라인 맞춤형 광고 활성화를 위한 개인 정보 보호에 대한 법적 고찰: ‘개인 정보’의 개념을 중심으로. 『한국산학기술학회 논문지』, 20(2), 492-497.
- 차상욱 (2014). 빅데이터(Big Data) 환경과 프라이버시의 보호. 『IT와 법 연구』, 8, 193-259.
- 최대선·김석현·조진만·진승현 (2013). 빅데이터 개인정보 위협 분석 기술. 『정보보호학회지』, 23(3), 56-60.
- 최인호·정세훈 (2019). 연령, 소득 및 디지털 리터러시가 온라인 개인정보 노출 및 보호 행동에 미치는 영향. 『한국언론학보』, 63(5), 233-266.
- 행정안전부·한국인터넷진흥원 (2019). 2019년 개인정보 보호법 주요 내용. Retrieved February 15, 2020, https://www.privacy.go.kr/edu/ttb/selectBoardArticle.do?nttId=9922&bbsId=BBSMSTR_00000000032&bbsTyCode=BBST01&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1&searchCnd=&searchWrd=&replyLc=0.

- 황태희·김민기·조혜신·윤성훈 (2019). 빅데이터와 경쟁정책: 국내 온라인 비즈니스 분야 시장 현황 분석을 중심으로. 『정보통신정책연구』, 26(3), 101-124.
- Ahn, J., & Jung, Y. (2016). The common sense of dependence on smartphone: A comparison between digital natives and digital immigrants. *New Media & Society*, 18(7), 1236-1256.
- Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138-150.
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1042.
- Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419-426.
- Broos, A. (2005). Gender and information and communication technologies (ICT) anxiety: Male self-assurance and female hesitation. *CyberPsychology & Behavior*, 8(1), 21-31.
- Davidshofer, K. R., & Murphy, C. O. (2005). Psychological testing: Principles and applications. Pearson/Prentice-Upper Saddle River, New Jersey.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Evjemo, B., Castejón-Martínez, H., & Akselsen, S. (2019). Trust trumps concern: Findings from a seven-country study on consumer consent to ‘digital native’ vs. ‘digital immigrant’ service providers. *Behaviour & Information Technology*, 38(5), 503-518.
- Feng, Y., & Agosto, D. E. (2019). Revisiting personal information management through information practices with activity tracking technology. *Journal of the Association for Information Science and Technology*, 70(12), 1352-1367.
- Fraenkel, J. R., & Wallen, N. E. (2000). *How to design and evaluate research in education*. McGraw-Hill, New York.
- Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers’ awareness and concerns. *Journal of Consumer Marketing*, 19(4), 302-318.
- Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis*. Upper Saddle River, New Jersey.
- Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10, 3737-3757.

- Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle: Policy-makers be prepared!. *Government Information Quarterly*, 35(4), S99-S105.
- Jones, V. K. (2018). Voice-activated change: Marketing in the age of artificial intelligence and virtual assistants. *Journal of Brand Strategy*, 7(3), 233-245.
- Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387-402.
- Kesharwani, A. (2020). Do (how) digital natives adopt a new technology differently than digital immigrants? A longitudinal study. *Information & Management*, 57(2), 103170.
- Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273-281.
- Kim, J. E., & Yeo, J. (2010). Valuation of consumers' personal information: A South Korean example. *Journal of Family and Economic Issues*, 31(3), 297-306.
- Kim, Y., Choi, B., & Jung, Y. (2018). Individual Differences in Online Privacy Concern. *Asia Pacific Journal of Information Systems*, 28(4), 274-289.
- Lee, H., Wong, S. F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly*, 36(2), 294-303.
- Li, K., Cheng, L., & Teng, C. I. (2020). Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Information Processing & Management*, 57(1), 102128.
- Madaan, N., Ahad, M. A., & Sastry, S. M. (2018). Data integration in IoT ecosystem: Information linkage as a privacy threat. *Computer Law & Security Review*, 34(1), 125-133.
- Palfrey, J. G., & Gasser, U. (2011). *Born digital: Understanding the first generation of digital natives*. Basic, New York.
- Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. *MIS Quarterly*, 35(4), 977-988.
- Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon*, 9(5), 1-15.
- Schwab, K. (2016). The fourth industrial revolution. In: World Economic Forum, 51-59.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1016.

- Snedecor, G. W., & Cochran, W. G. (1989). *Statistical Methods*. Iowa State University Press, Ames.
- Straub, E. T. (2009). Understanding technology adoption: Theory and future directions for informal learning. *Review of Educational Research*, 79(2), 625-649.
- Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52, 278-292.
- Welch, B. L. (1947). The generalization of student's' problem when several different population variances are involved. *Biometrika*, 34(1/2), 28-35.
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453.