

연구보고서

2024

08

금융의 디지털화와 소비자 보호

오병국·변혜원·이소양

본 보고서에 수록된 내용은 집필자 개인의 의견이며 우리원의 공식 의견이 아님을
밝혀 둔다.



목 차

• 요약	1
I. 서론	2
1. 연구배경 및 목적	2
2. 주요 선행연구 및 연구구성	3
II. 금융의 디지털화와 위험요소	7
1. 금융의 디지털화	7
2. 금융의 디지털화에 따른 위험요소	9
3. 소결	31
III. 금융의 디지털화 관련 해외 소비자정책	34
1. OECD/G20 금융소비자보호 상위원칙	34
2. 데이터 수집 및 활용 관련 논의	38
3. AI 관련 논의 및 조치	40
4. 디지털 취약계층 보호 관련 논의	45
IV. 금융소비자 보호를 위한 과제	48
1. 데이터 관련 위험 대응	50
2. 기술발전과 소비자보호 법·규제 간 격차	55
3. 취약계층	57
V. 결론	58
• 참고문헌	60

표 차례

〈표 I-1〉 주요 선행연구 정리	4
〈표 II-1〉 코로나19 발생 이후 국내의 사이버리스크 발생 사례	10
〈표 II-2〉 우리나라 금융권별 전산장애 사고 현황	12
〈표 II-3〉 보험회사 보유데이터	16
〈표 II-4〉 보이스피싱 범죄의 발생 및 검거 현황	20
〈표 II-5〉 우리나라 연령별 보이스피싱 피해금액 현황	21
〈표 II-6〉 Eurobarometer 설문조사: 보험구매 중 다크패턴 경험	26
〈표 II-7〉 국내 취약계층의 디지털 정보화 수준	27
〈표 II-8〉 우리나라 4대 취약계층의 디지털 정보화 접근, 역량 및 활용 수준	28
〈표 II-9〉 우리나라 4대 취약계층의 스마트폰 보유율, 인터넷 이용률, 모바일 기기 이용 능력	29
〈표 II-10〉 우리나라 4대 취약계층의 디지털 금융거래 서비스 이용률(2022년 기준)	31
〈표 II-11〉 국내 보험시장에서의 디지털화 관련 소비자보호 이슈	33
〈표 III-1〉 G20/OECD 금융소비자보호 상위원칙	34
〈표 III-2〉 디지털 시대에 맞춘 G20/OECD 금융소비자보호 상위원칙의 재해석	35
〈표 IV-1〉 국제기구의 디지털 금융소비자 보호 관련 원칙과 국내 디지털 금융소비자 보호 관련 법규 및 조치	49
〈표 IV-2〉 개인정보 수집 및 활용 동의방식 개선방안	51
〈표 V-1〉 금융의 디지털화 관련 대응과제	59

그림 차례

〈그림 II-1〉 금융산업의 디지털 전환 동인	8
〈그림 II-2〉 금융권 눈속임 설계 예시	24
〈그림 II-3〉 보험시장에서 나타나는 다크패턴 사례	26
〈그림 II-4〉 우리나라 인구 특성별 디지털 금융 사용 현황	30
〈그림 III-1〉 NAIC AI 모델 가이드라인 채택 주	44
〈그림 IV-1〉 정보활용 동의서양식안	53

Digitalization of Finance and Consumer Protection

As the digitalization of the financial industry accelerates, new and diverse forms of financial services are being offered to financial consumers, improving convenience and accessibility and enhancing value through market innovation. However, consumer protection issues related to data storage and the provision of data-driven financial services, gaps in consumer protection regulation, and consumer harm to financially vulnerable groups are being discussed.

Consumer risks associated with the digitization of finance include cyber risks, data breaches, misuse of data analytics algorithms, and errors; in terms of consumer protection regulations and gaps between laws due to technological advances, issues such as lack of consumer protection laws, digital financial crime, and dark patterns may arise; and in terms of financially vulnerable consumers, there are concerns about the digital divide and digital marginalization of older consumers.

Financial institutions are expected to strengthen cyber risk management, comply with guidelines and policy measures on AI and personal information security, establish guidelines for responding to complex and diverse security threats and guidelines for consumer transfers between companies, establish measures to improve the way financial institutions collect and use personal information, and establish guidelines for online appropriateness and self-management of dark patterns, Strengthening the process of financial firms' response to consumer losses and providing incentives to policymakers, formulating guidelines and conducting surveys on digital financial transactions for the four financially vulnerable groups, expanding the Financial Love Bus

program, and addressing the problem of financial exclusion of the elderly in preparation for bank branch closures should strengthen the ability of policymakers and the financial industry to respond to consumer risks.

요약

금융산업의 디지털화가 가속화되면서 금융소비자에게 새롭고 다양한 형태의 금융서비스가 제공됨에 따라 편의성 및 접근성이 개선되고, 시장혁신을 통한 효율 증진이 기대되고 있다. 하지만 데이터 저장 및 데이터 기반 금융서비스 제공, 법 및 규제 공백, 금융 취약계층 측면에서 소비자 피해가 우려되며, 이와 관련된 소비자 보호 이슈가 논의되고 있다.

금융의 디지털화 관련 소비자 위험요소는 우선 데이터 측면에서 사이버리스크, 데이터 유출, 데이터분석 알고리즘 부당 사용 및 오류 등이 있고, 기술발전예 따른 소비자보호 규제 및 법간 격차 관점에서는 소비자보호법의 미비, 디지털 금융범죄, 다크패턴 등의 문제가 발생할 수 있으며, 금융 취약계층 관련해서는 디지털 격차 발생, 고령 소비자의 디지털소외 문제 등이 우려된다.

이에 대한 대응과제로서 금융회사의 사이버리스크 관리 강화, 금융회사의 AI 및 개인정보 보안 관련 가이드라인 및 정책방안의 준수, 정책당국의 복잡하고 다양한 보안위협에 대응할 수 있는 가이드라인 및 회사 간 소비자 이동 관련 지침 마련, 정책당국의 금융회사 개인정보 수집 및 활용방식 개선 방안 마련, 정책당국의 온라인 적정성 가이드라인 및 다크패턴 자율관리 가이드라인 마련, 금융회사의 소비자피해 대응 프로세스 강화 및 정책당국의 유인 제공, 4대 금융취약계층 디지털금융거래 관련 지침 마련 및 실태조사 실시, 금융사랑방버스 프로그램 확대, 은행 점포폐쇄에 대비한 고령층 금융소외 문제 해소 등을 통해 소비자 위험요소에 대한 정책당국과 금융산업의 대응 역량을 강화할 필요가 있다.

1. 연구배경 및 목적

인공지능(Artificial Intelligence; AI), 클라우드컴퓨팅, 사물인터넷, 블록체인, API(Application Programming Interface) 등 정보통신기술(Information and Communication Technology; ICT)의 발전과 머신러닝 및 빅데이터 활용이 확대되면서 디지털화(digitalization)가 전 산업에 확대되고 있다. 특히, 최근 금융과 산업의 결합, 금융상품의 제조와 판매 분리, 디지털 기반의 금융확장이 이뤄지면서 금융산업의 디지털화가 가속화되고 있다.¹⁾ 예를 들면, 은행의 경우 대다수 은행이 온라인 및 모바일 뱅킹을 통해 각종 금융서비스를 제공하며, 오픈뱅킹 및 마이데이터 서비스 제공을 통해 소비자가 실시간 거래를 실행하거나 모니터링하는 것이 가능하다. 게다가 전자 서명 기술 등을 도입해 서류 작성 및 인증 절차를 전자화하고 있고, AI 기술을 활용해 업무 자동화를 시도하고 있으며, 블록체인 기술을 통해 금융거래의 투명성과 보안성 제고에 활용하고 있다. 보험회사의 경우 빅데이터와 AI 등을 활용해 고객맞춤형 상품개발, 자동화를 통한 업무효율화, 사물인터넷 기기 연계를 통한 실시간 자산 모니터링, 클라우드 기반 업무확장 등을 시도 중에 있다. 또한, 손해보험회사의 경우 이미징인식 기술, 머신러닝 기반 보험사기 감지시스템 구축 등을 통해 고객센터 혁신을 위한 디지털화를 진행 중에 있다.

한편, 금융소비자 입장에서 금융산업의 디지털화는 금융서비스에 디지털 기술이 접목된 형태인 디지털 금융서비스(digital financial services)를 제공받는 것을 의미할 것이다. 국제기구인 OECD는 디지털 금융서비스를 전자화폐, 모바일 금융서비스, 온라인 금융서비스, 무점포은행 등과 같은 디지털 기술을 사용하는 금융업으로 정의하고 있다.²⁾ 소비자에게 미치는 순기능 측면에서는 디지털 금융서비스가 제공되면서 소비자의 금융 포용성, 편

1) 금융과 타산업 간의 결합의 예로서 자회사 투자부수 업무위탁 범위 규제 완화, 디지털 유니버설 금융허용, 빅테크의 금융서비스 제공 등이 있음. 또한, 온라인 플랫폼 서비스 확대, 온라인 금융상품중개기관의 예금, 대출 및 보험상품 판매중개 허용을 제판분리로 간주될 수 있으며, 금융회사의 클라우드, 대안신용평가, 가치평가, AI 활용 이용확대, 마이데이터 도입 등을 디지털 기반의 금융확장으로 해석할 수 있음

2) OECD(2018)

의성 및 접근성이 개선되고, 시장혁신을 통해 금융소비자의 효용이 제고될 것으로 기대되고 있다. 구체적으로 기존 금융시장에서 활용하던 전통적 데이터에 더해 소비자 데이터를 사용해 금융 포용성이 증진될 것으로 예상되고 있으며, 디지털 형식의 신분 확인을 통해 편의성이 제공되고, 모바일 기기 및 온라인 채널 등을 이용해 금융서비스 접근에 대한 시공제약이 낮춰지고 있다. 또한, 핀테크, 온라인 플랫폼 기반 사업자 등의 진입으로 인해 시장경쟁이 촉진되고, 서비스의 혁신과 가격 인하가 유도될 수 있을 것으로 보인다.

하지만 이러한 순기능 이외에도 데이터 저장 및 데이터 기반 금융서비스 제공, 규제 사각지대 및 법규 미비, 소외계층의 새로운 발생 등으로 인해 금융소비자 보호 이슈가 논의되고 있으며, 관련 조치의 필요성이 대두되고 있다. 데이터 활용 측면에서는 개인정보 대규모 유출 등의 사이버 리스크 발생 가능성, 무분별한 개인정보 수집 및 동의, 알고리즘 오류 및 남용이 우려되고 있으며, 규제 및 법규 측면에서는 비대면 모집 채널 및 영업행위 규제 공백, 행태편향을 이용한 무분별한 대출 및 투자, 금융 범죄로 인한 소비자 피해 등이 우려되고 있다. 또한, 디지털 격차 발생, 비대면 채널 활용 증가로 인한 고령 소비자의 디지털 금융 소외 문제 등 신 소외계층 발생 측면에서도 우려점이 존재한다.

이에 본 연구는 금융의 디지털화에 따른 금융소비자 보호의 개선을 위해 금융의 디지털화와 관련된 금융소비자 위험요인들을 파악하고, 이를 바탕으로 정책당국과 금융산업이 이러한 위험요인들에 어떻게 대응해야 할지 논의하고자 한다.

2. 주요 선행연구 및 연구구성

현재까지 금융의 디지털화에 따른 금융소비자 보호 이슈 및 과제 제시를 시도하거나, 금융산업의 디지털 혁신이 소비자에 미치는 영향을 분석한 다수의 국내외 연구가 존재한다. 먼저 국내 선행문헌의 경우 핀테크, 빅테크, 마이데이터, 디지털 지급결제 등을 중심으로 특정 디지털 금융서비스가 소비자에게 제공되면서 발생 되는 소비자 보호 이슈 및 영향을 분석하고, 정책과제를 제시한 연구들이 존재한다(김두진, 2019; 김재영, 2021; 구본성, 2021; 이효섭, 2023; 황순주, 2022). 다음으로 디지털 금융거래 증가에 따른 금융소비자 문제 및 대응 사례를 제시하거나, 비대면 채널 활용, 금융소비자 보호 관련 법적 보완 및 개선사항을 논의하는 등 디지털 금융거래 및 금융상품 판매채널 관련 금융소비자

보호 이슈 및 과제를 제시한 연구들이 있다(강동수·오윤해, 2022; 서병호, 2023; 이성복, 2021; 정영훈·송민수, 2022). 또한, 고연령, 정보격차, 낮은 보안능력, 충동성, 중독성 등에 따라 발생되고 있는 디지털 취약계층의 접근성, 착취 및 남용 문제 등을 중심으로 동계층의 금융소비자 보호 이슈 및 과제를 제시한 연구들도 존재한다(박소정, 2023; 변혜원, 2023; 신경희, 2021; 황남희 외 5인, 2020).

해외 선행연구도 국내 선행연구와 마찬가지로 핀테크, 빅테크, 오픈뱅킹, 플랫폼 등 특정 디지털 금융서비스가 소비자에게 미치는 영향을 이론적 혹은 실증분석을 시도했으며, 이와 더불어 소비자보호 관련 위험 요소를 논의한 연구가 다수 존재한다(Acemoglu, Makhdomi, Malekian, and Ozdaglar, 2022; Croxson, Frost, Gambacorta, and Valletti, 2022; World Bank Group, 2022). 또한, 디지털 혁신이 금융소비자 보호에 미치는 긍정적 혹은 부정적 영향을 분석하거나, 디지털 전환이 소비자 편익에 미치는 영향을 분석한 연구도 존재한다(Dinh, Le, Duong, and Pham, 2023; Feyen, Frost, Gambacorta, Natarajan, and Saal, 2021).

〈표 I-1〉 주요 선행연구 정리

구분	주요내용	선행연구
국내	특정 디지털 금융서비스의 금융소비자 보호 이슈 및 과제 제시	김두진(2019), 김재영(2021), 구분성(2021), 이효섭(2023), 황순주(2022)
	디지털 금융거래 및 금융상품 판매 채널 관련 금융소비자 보호 이슈 및 과제 제시	강동수·오윤해(2022), 서병호(2023), 이성복(2021), 정영훈·송민수(2023)
	디지털 취약계층의 금융소비자 보호 이슈 및 과제 제시	박소정(2023), 변혜원(2023), 신경희(2021), 황남희 외 5인(2020)
해외	특정 디지털 금융서비스의 영향 분석 및 소비자보호 관련 이슈 제기	Acemoglu, Makhdomi, Malekian, and Ozdaglar(2022), Croxson, Frost, Gambacorta, and Valletti(2022), World Bank Group(2022)
	디지털 혁신 및 디지털 전환에 따른 이슈 제기 및 영향 분석	Dinh, Le, Duong, and Pham(2023), Feyen, Frost, Gambacorta, Natarajan, and Saal(2021), Yang, Wu, and Huang(2020)

본 연구는 금융의 디지털화에 따른 소비자 보호 관련 위험 요소를 종합적으로 식별하여 제시한다는 점에서 일부 선행연구(서병호 2023; 정영훈·송민수 2022)의 연장선상에 위치

하고 있다.

이들의 연구를 보다 구체적으로 살펴보면 우선 서병호(2023)는 금융의 디지털화 진전에 따라 온라인 채널을 이용하는 금융소비자 비중이 급격히 확대된 상황에 초점을 두어 이와 관련된 금융소비자 보호 이슈와 과제를 제시하였다. 동 연구에서는 국내 디지털 금융소비자 보호 차원에서 금융상품 판매원칙의 실질적 미이행, 금융소비자의 행태편향을 이용한 마케팅, 핀테크 사업자의 폐업에 따른 손실위험 노출, 디지털 금융범죄 노출, 디지털 격차, 특정 금융플랫폼의 집중에 따른 불공정 경쟁 이상 등을 디지털 금융서비스 도입에 따른 금융소비자 보호 이슈로 제시했다. 이를 극복하기 위한 과제로는 챗봇이나 채팅을 통한 적정성 심사 및 설명의무 이행, 행태편향을 이용한 금융권 마케팅 사례연구, 핀테크 사업자의 폐업 리스크 관리, 중장년층 대상의 디지털 금융교육 강화, 디지털 채널의 접근성 강화를 통한 차별 완화, 빅테크 감독을 위한 정부 부처 간 공조를 제시하였다.

다음으로 정영훈·송민수(2023)는 디지털 경제 확산 및 코로나19에 따른 거래방식의 변화 등으로 금융산업의 디지털화가 적극적으로 이뤄지고 있는 점에 주목해 디지털 금융거래의 소비자 문제를 검토하고, 소비자 인식조사를 통해 시사점을 제시하였다. 디지털 금융거래 서비스에서의 소비자 문제로서 개인정보 수집, 보관, 관리, 활용에서의 문제점과 디지털 취약계층의 발생, 유사한 디지털 금융서비스를 제공하는 사업자의 역할과 책임 범위가 달라짐에 따라 발생하는 소비자 피해를 지적하였다. 그리고 디지털 금융거래 소비자 인식조사를 통해 개인정보 취급방식 변경, 소비자 참여형 개인정보 활용 플랫폼 활성화, 디지털 금융거래 웹 및 앱 개선, 오프라인 금융거래 접근성 확보를 소비자 권익 증진을 위한 대응방안으로 제시하였다.

이상의 관련 연구를 정리해 보면, 먼저, 대부분의 연구가 디지털 금융거래와 관련된 위험 요소에 집중되어 있음을 알 수 있다. 다음으로 금융소비자 보호 체계, 판매규제, 디지털 이해력 등에 대해서는 심도 있는 논의가 이루어졌으나(강동수·오윤해 2022; 이성복 2021; 박소정 2024), 금융소비자 데이터 관련 위험요소에 대해 종합적으로 다룬 연구는 상대적으로 부족한 것으로 판단된다. 아울러 보험의 디지털 전환과 관련된 소비자 위험 요소에 대해 논의한 연구도 부족한 것으로 보인다. 따라서 본 연구는 기존 연구들에서 상대적으로 부족하게 다루어진 내용을 보완해 선행연구와 차별성을 두고자 한다. 이와 함께 본 연구에서도 금융의 디지털화와 관련된 소비자 보호 위험 요소에 대응하기 위한 과제를 검토하고 제시하고자 한다.

본 연구는 다음과 같이 구성되어 있다. 서론에 이어 제2장에서 금융산업의 디지털화 의미 및 양상, 금융의 디지털화에 따른 소비자 보호 관점에서의 위험 요소와 보험산업의 디지털화가 야기할 수 있는 소비자 관련 위험 요소를 제시한다. 제3장에서는 소비자 보호를 위한 대응과제 도출에 참고할 만한 금융의 디지털화와 관련된 해외의 소비자 관련 정책을 정리하여 제시한다. 제4장에서는 소비자 보호를 위한 대응과제를 제2장에서 제시한 위험 요소별로 제안한다.

1. 금융의 디지털화

금융산업은 전통적으로 기술과 밀접한 관련을 맺으면서 발전해 왔으며, 최근 들어 핀테크의 발전, 빅데이터 기반 분석, ICT 기술 접목, 비대면 업무환경 확대, 행동경제학 적용 등으로 인해 금융산업의 디지털 전환이 가속화되고 있다.

우선 핀테크(fintech)는 금융기술(financial technology)의 줄임말로써 일반적으로 기술과 금융의 결합을 의미한다. 2008년 글로벌 금융위기 이후 핀테크라는 용어가 일상적으로 사용되고 있으며, 은행, 자본시장, 보험, 지급결제, 여신(신용카드) 등 금융의 모든 분야에 영향을 미치고 있다. 핀테크의 발전은 금융산업 내 디지털 혁명을 가속화 하는데 큰 기여를 하고 있으며, 금융산업이 실용적 디지털 기술과 빅데이터 분석을 기초로 한 디지털 전환으로 이어지는데 증추적인 역할을 하고 있다.³⁾ 다만, 핀테크에 의한 금융혁신은 비대면 금융거래 확대, 소비자에게 제공되는 정보의 양적·질적 격차 해소, 금융서비스의 결합과 융합, 금융산업의 금융시장의 구조 재편이라는 긍정적 영향을 가져오는 한편, 소비자 권익 침해 및 불건전 영업행위 노출, 고령자의 금융 소외와 같은 부정적 영향에 대한 우려도 함께 제기되고 있다.⁴⁾

이러한 핀테크의 발전과 더불어 빅데이터 기술의 발달로 대용량의 새로운 정보를 효과적 그리고 효율적으로 추출 및 활용하는 것이 가능해지고, ICT 기술과 금융이 융합되면서 금융의 거래비용이 획기적으로 감축되고, 금융서비스를 구성하는 공정이 단계별로 분리(unbundling)되거나 재결합(rebundling)되는 등 세분화되는 모습도 나타나고 있다.⁵⁾ 또한, 비대면 업무환경이 늘어나고, 비대면 서비스 발전에 따른 긍정적 고객 경험이 증가하면서 금융회사 간 경쟁적인 디지털 전환을 촉진하는 시장환경도 만들어지고 있으며, 금융회사가 고객 경험의 변화를 분석하거나 고객이 비대면 금융상품 또는 서비스를 경험할

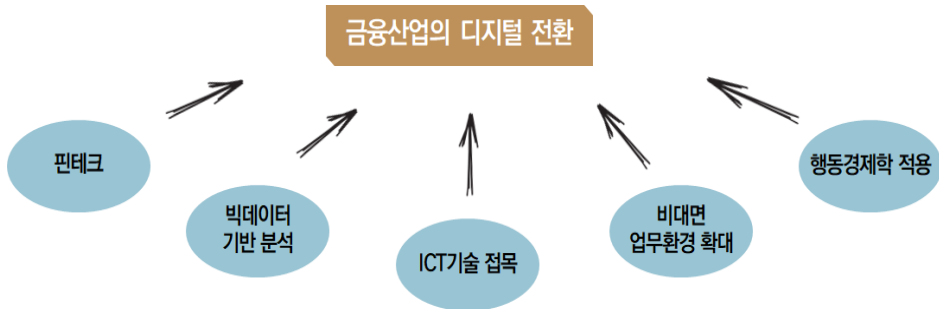
3) 정광민(2021)

4) 이성복(2021)

5) 한국개발연구원(2022)

때 행동경제학이 적극적으로 사용되고 있다. 궁극적으로 금융산업의 디지털 전환으로 인해 인적, 정보, 시설, 기술, 자산에 전반적인 변화가 생겨나고, 이에 따라 금융회사 전체의 경영환경 및 절차의 디지털화가 유도되고 있으며, 결국 금융서비스의 디지털화로 이어지고 있다.⁶⁾

〈그림 II-1〉 금융산업의 디지털 전환 동인



자료: 정광민(2021); 한국개발연구원(2022)

앞서 언급한 바와 같이 금융산업의 디지털화는 소비자 측면에서 금융서비스에 디지털 기술이 접목된 형태인 디지털 금융서비스(digital financial services)를 제공하는 것으로 정의될 수 있다. 보다 구체적으로 은행, 금융투자업, 보험업 등에서 제공하는 전통적 금융서비스에 프로세스 자동화, 데이터 분석, 고객경험 개선 등을 위한 빅데이터, 오픈 API, AI/머신러닝, 플랫폼, 클라우드, 분산컴퓨팅 등의 다양한 디지털 기술이 적용되어 인터넷 및 모바일 금융거래가 확대되고, 소비자에게 새롭고 다양한 형태의 혁신적인 금융서비스가 제공되는 것이다.⁷⁾

한편, 소비자에게 디지털 금융서비스는 크게 전통 금융회사, 핀테크, 빅테크 이상 삼각구도 양상으로 제공되고 있다.⁸⁾ 이 중 빅테크는 플랫폼 기반, 핀테크는 주로 틈새시장을 통

6) 정광민(2021)

7) 빅데이터는 대량의 데이터로부터 가치를 추출하고 결과를 분석하는 기술, 오픈 API는 누구나 온라인상에서 응용프로그램을 작성할 수 있게 하는 인터페이스, AI/머신러닝은 기계가 데이터를 학습하여 인간의 의사결정을 대신하는 기술, 플랫폼은 공급자가 제공하는 가상 플랫폼 안에서 생산자와 소비자가 상품 및 서비스를 거래하는 기술, 클라우드는 ICT 자원을 포함하는 데이터 센터로부터 정보통신망을 통해 유료로 서비스를 이용하는 방식, 분산컴퓨팅은 컴퓨터 처리 능력을 분산시킴으로써 고성능 컴퓨팅 파워를 가능하게 하는 기술로 요약될 수 있음(정광민, 2021). 특히 API 기술은 핀테크 기업들의 혁신을 주도하는 대표적 기술로 평가받고 있음(장성연 외 3인, 2024)

8) 권지은(2023)

한 디지털 금융서비스를 제공이며, 전통 금융회사는 디지털 혁신을 통한 대응을 강화 중이다.⁹⁾

디지털 금융서비스 유형 측면에서 우선 전통 금융회사는 오픈뱅킹, 마이데이터, 토큰증권발행(Security Token Offering; STO), 디지털 헬스케어 등의 서비스 제공으로 고객 편리성 및 편익을 제고하는 방향으로 디지털 금융서비스 혁신 경쟁에 대응하고 있다. 다음으로 핀테크의 경우 높은 디지털 기술력을 기반으로 고객자문, 간편결제 등 영역에 집중해 서비스를 제공하는 한편, 이러한 서비스 제공을 넘어 금융솔루션, 디지털 자산관리 등 새로운 서비스의 제공으로 업무영역을 확대하고 있다. 마지막으로 빅테크의 경우 자사 플랫폼과 기존 ICT 사업으로 축적한 두터운 고객층을 바탕으로 대안신용평가, 디지털지급결제, 비교추천서비스, 디지털 손해보험 등으로 다양한 서비스를 제공하여 금융분야에 진출을 확대하고 있으며, 디지털 서비스 시장장악력과 방대한 고객데이터를 기반으로 개인화·고도화된 디지털 금융서비스를 제공해 점점 영향력이 커질 것으로 예상되고 있다.

이처럼 각기 다른 주체가 제공하는 다양한 형태의 디지털 금융서비스가 등장하면서 소비자는 비대면채널, 디지털 기기 및 디지털 플랫폼에 기반한 수요자 중심의 신속하고 편리한 금융서비스 제공을 접할 수 있는 환경을 가지게 될 것으로 기대되고 있다.

2. 금융의 디지털화에 따른 위험요소

한편으로 금융산업의 디지털화가 진행되면서 기존 소비자 위험요소가 심화되거나, 새로운 위험요소가 등장할 가능성이 우려되고 있다. OECD, G20, IAIS 등 국제기구는 데이터, 소비자 자산, 취약계층 보호 관점에서 금융의 디지털화와 관련된 소비자 위험을 줄이거나 방지하기 위한 규제 및 정책 방안을 논의하거나 제시한 바 있다.¹⁰⁾ 이러한 점을 참조해 본 절에서는 금융의 디지털화에 따른 소비자 위험 요소를 크게 데이터, 기술발전과 소비자 보호 법·규제 간 격차, 취약계층으로 나누어 논의하고자 한다. 또한, 보험의 디지털화가 진행되면서 발생하는 소비자 위험요소도 같은 범주 하에 식별하여 제시하고자 한다.

9) 권지은(2023)

10) OECD(2018), OECD(2020)

가. 데이터 관련 위험

1) 사이버리스크

코로나19 확산에 따른 비대면 거래 선호, 재택근무 시행 확대 등으로 이전부터 진행되어 온 금융의 디지털화 추세가 2020년부터 가속화되고 있다. 온라인 거래가 증가함에 따라 인터넷뱅킹을 통한 자금이체, 전자결제, 대출 신청 등의 디지털 기반 금융서비스 이용이 많이 증가하였다. 또한, 금융부문에 대한 사이버공격이 지속적으로 증가하고 있으며, 특히 코로나19 발생과 맞물려 더욱 확산되고 있다(〈표 II-1〉 참조).

전 세계적으로 살펴보면 코로나19 확산 기간에 코로나19를 키워드로 한 악성의심 이메일 등 사이버공격이 많이 증가한 것으로 나타났다. 우리나라 금융산업의 경우에도 WTO 사칭 기부 요청, 마스크 판매 위장 등의 형태로 악성코드가 전파되었고, 코로나19 관련 악성 의심 이메일 형태로 피싱사이트가 유포되는 사례가 많이 발견되었다. 이러한 금융산업에 대한 사이버공격은 금융회사 시스템 정보 및 소비자 개인정보 유출을 초래할 수 있을 뿐만 아니라 자금 편취 등의 피해로 이어지기도 하였다.¹¹⁾

〈표 II-1〉 코로나19 발생 이후 국내외 사이버리스크 발생 사례

국내	해외
<ul style="list-style-type: none">• 2020년 4월: 소상공인 대상 코로나19 관련 정부 지원 대출을 빙자한 자가 원격 프로그램이 휴대폰에 설치되도록 유도한 후 피해자의 자금을 편취• 2020년 6~9월: 카카오페이, 토스 등 국내 일부 핀테크 기업에서 1,000만 원 상당 규모의 부정 결제 발생• 2020년 11월: 가짜 증권회사 홈트레이딩시스템(HTS)을 통해 해당 이용자에게 조작된 주가를 제시하고 추가 투자금액을 입금하도록 유도해 자금을 편취	<ul style="list-style-type: none">• 2020년 6월: 미국에서 코로나19 관련 지원금 지급 관련 내용으로 국세청을 사칭한 가짜 문자를 통해 개인정보 유출 후 자금을 편취• 2020년 7월: 미국 인터넷은행 Dave의 제3자 서비스 제공자를 대상으로 하는 사이버사기가 발생하면서 고객정보 일부 유출• 2020년 10월: American Bank System(ABS)에 대한 랜섬웨어 공격으로 인해 금융기관 및 이용고객 정보 일부 유출

자료: 한국은행(2020)을 재구성함

11) 한국은행(2020)

게다가 인프라 문제, 인적 오류 문제 등 내부 요인으로 인한 IT 시스템 장애가 대형 금융 사고로 이어지고 소비자의 잠재적 피해 위험도 커지고 있다. 특히 전자금융사고 발생 요인 측면에서는 외부 요인(사이버공격 등)보다는 주로 내부 요인(프로그램 오류 등)에서 비롯되는 장애 사고가 다수를 차지하고 있다.¹²⁾ 금융감독원(2023)¹³⁾에 따르면 2023년 상반기에 발생한 전자금융사고(197건) 중 프로그램 오류 등으로 인한 장애 사고가 194건, 침해 사고가 3건이었다. 2022년 10월 데이터센터 화재로 발생한 대규모 '카카오 먹통' 사건은 대표적인 인프라 문제로 인한 서비스 장애 사고다. 당시 카카오 분당 데이터센터 화재로 카카오톡, 카카오페이 등의 주요 서비스들이 중단되며 전국에서 혼란이 빚어졌다. 카카오페이는 전체 기능이 마비되면서 카카오페이를 이용해 제품을 판매하는 소상공인의 피해와 배달의민족 등 유통 서비스를 이용하는 소비자들의 불편이 매우 컸다. 또한, 카카오 서비스 장애 사태를 틈타 해킹 이메일과 스미싱 문자 유포 등 사이버공격이 기승을 부리기도 하였다. 그리고 카카오 서비스 장애로 인해 이용자 계정 정보나 프로필 등 개인정보가 노출되거나 유출되는 피해를 본 이용자도 있었다. 이에 대해서 금융감독원은 카카오의 일부 금융서비스가 작동하지 않는 등 국민 피해가 발생한 것에 대해 심각한 문제로 인식하며 카카오의 금융계열사인 카카오페이, 카카오페이증권의 비상 대응 상황을 점검하고 카카오페이에 대해 개선 명령을 내렸다.

한편, 강민국 의원실이 공개한 금융감독원 자료¹⁴⁾(〈표 III-2〉 참조)에 따르면 2019년부터 2022년 8월까지의 3년여간 금융권에서 발생한 전산장애 사고가 781건에 달하였으며 피해추정액은 346억 4,241만 원으로 집계되었다. 전산장애 사고 건수를 연도별 보면 2019년 196건, 2020년 198건, 2021년 228건으로 매년 증가하고 있다. 회사별로 보면 케이뱅크가 34건으로 가장 많았고, 다음으로 신한은행 32건, 카카오페이 27건, 한국산업은행 25건, 한국스탠다드차타드은행 23건 순으로 나타났다. 보험업권은 교보생명이 18건으로 가장 많았으며, ABL생명(15건), 비엔피파리바카디프생명(10건), 미래에셋생명(9건), 현대해상화재(9건) 등도 전산장애 사고가 발생하였다. 금융회사 전산장애로 인한 피해 규모를 정확히 산출하기 어려워 소비자가 적절한 보상을 받기가 어렵다는 문제가 있다. 이러한 이유로 인해 전산장애와 같은 금융사고가 발생하더라도 금융소비자는 불편만 당하고 있고 제대로 된 보상을 받지 못해 불만이 높을 가능성이 있다.

12) 주성철(2024)

13) 금융감독원 보도자료(2023. 9. 6), "2023년 상반기 전자금융사고 발생 현황 및 대응방안"

14) 조세일보(2022. 10. 12), "최근 3년간 금융권 전산장애 781건...피해추정액 346억 원"

〈표 II-2〉 우리나라 금융권별 전산장애 사고 현황

(단위: 건)

금융권	2019	2020	2021	2020.8	합계
은행	63	71	81	60	275
저축은행	14	19	23	10	66
보험	42	34	36	25	137
증권	59	55	76	56	246
카드	18	19	12	8	57
합계	196	198	228	159	781

자료: 조세일보(2022. 10. 12), “최근 3년간 금융권 전산장애 781건...피해추정액 346억 원”

한편, 보험산업의 디지털화는 보험회사가 이전보다 더 많은 양의 데이터를 보유하고 이용하게 함으로써, 보험회사의 사이버리스크에 대한 노출도 증가시켰다고 할 수 있다. 금융회사는 비금융회사에 비해 사이버공격의 대상으로 주목받기 쉬운데, 특히 보험회사는 많은 양의 데이터를 보유하고 있고 건강 관련 정보 등 민감정보를 다루므로 사이버 공격의 목표 대상이 되기 쉽다.

EIOPA는 2019년 스트레스 테스트 개선 절차를 시작하였으며, 보험산업 스트레스 테스트 방법에 대한 원칙들을 설명하는 보고서들을 발간하였다. 2023년에 발간된 네 번째 보고서는 사이버리스크에 초점을 맞추었는데, 동 보고서는 보험회사가 직면하는 사이버리스크를 크게 보험회사가 사이버공격의 직접적 대상이 되는 경우와 사이버리스크 인수를 통해 노출되는 경우로 나누어 설명하였다(EIOPA, 2023).

EIOPA는 유럽에서의 사이버공격 동향(ENISA Threat Landscape 2021)¹⁵⁾과 MITRE ATT&CK의¹⁶⁾ 자료를 바탕으로 유럽 내 보험회사가 받을 수 있는 사이버공격 방법은 랜섬웨어, DoS(Denial of Service), 크립토재킹(Cryptojacking)¹⁷⁾, 데이터 탈취 등일 것으로 예상하였다. 사이버 공격자들은 피싱 이메일과 같은 사회공학적 기술을 사용하지만, 웹대면(Web-Facing) 응용 프로그램이나¹⁸⁾ 제3자를 대상으로 공격할 수도 있다.

15) ENISA, “ENISA Threat Landscape 2021”

16) MITRE 홈페이지(<https://attack.mitre.org/>)

17) 암호화폐(cryptocurrency)와 강탈(hijacking)의 합성어로서 일반 사용자의 PC에 악성코드를 설치해 암호화폐를 채굴 후 수취하는 범죄임

18) 웹 대면 응용 프로그램(Web-Facing Application)이란 인터넷을 통해 사용할 수 있고, 웹 기술과 브라우저를 사용하여 작업을 수행하는 모든 프로그램을 의미함

실제로 보험회사들이 클라우드 컴퓨팅이나 빅데이터분석 분야에서 제3자 아웃소싱을 하는 경우가 많아지면서 제3자 관련 사이버리스크 노출도 증가할 것으로 예상된다. 유럽 보험회사들은 혁신적인 기술이나 영업모형을 신속하게 도입하기 위해 아웃소싱이나 제3자 서비스제공자를 이용하는 것으로 조사되었다(EIOPA, 2024). 회사 내에 혁신랩을 만들거나 인슈어테크 스타트업에 투자를 하거나, 인슈어테크 스타트업에 아웃소싱을 하고 있었다. 그러나 클라우드 컴퓨팅 서비스나 AI 분석 등 데이터분석 서비스의 경우에는 빅테크에게 아웃소싱하는 경우가 대부분이었다. 한편 미국 생명보험회사를 대상으로 한 AI 및 머신러닝 관련 설문조사(NAIC, 2023) 결과에 의하면, 마케팅 분야 AI/머신러닝 모형 중 56%가 제3자가 개발한 모형이었다. 보험료 책정 및 언더라이팅 분야 AI/머신러닝 모형의 46%는 내부 개발, 54%는 제3자가 개발한 것으로 응답하였으나, 비자동화 승인 및 거절에 활용되는 모형 중 68%는 제3자가 개발한 모형이었다.¹⁹⁾

2) 데이터 수집 및 활용

소비자들의 일상생활과 재정에 큰 영향을 미치는 저축·결제·투자과 같은 금융거래는 코로나19 확산으로 인해 급속하게 디지털화되면서 소비자의 편의성을 높인 반면, 이 과정에서 생성된 다량의 데이터의 집적과 활용 과정에서 새로운 소비자 문제를 발생시켰다. 디지털 경제에 참여하는 소비자들은 수많은 디지털 거래기록을 남기게 된다. 온라인상에서 인터넷 이용자의 행동, 선호도, 사용 패턴 등이 기록되고 저장되고 있으며, 금융소비자들의 이용 행태, 대출 등을 위한 개인정보(성별, 연령, 직장, 소득, 주거 형태 등), 은행 계좌 잔액 등 금융정보까지 모두 포함하는 금융거래 관련 데이터가 생성된다. 또한, 인터넷 접속기록, 게시물 등의 온라인 행태정보뿐만 아니라 오프라인 거래에서 소비 패턴을 파악하여 소비자를 정의하는 다양한 정보들도 금융소비자 데이터에 포함된다. 이러한 개인정보를 포함한 데이터의 유출은 소비자에게 큰 피해를 야기할 수 있다. 예를 들어 소비자의 동의 없이 소비자 정보가 무단으로 사용되거나 해킹 등으로 인해 외부인에게 유출되거나 활용됨으로 인해 소비자 문제가 발생할 수 있다.

한편, 정영훈·송민수(2023)는 디지털 금융거래에서의 개인정보 관련 소비자 문제는 데이터 수집, 보관·관리, 그리고 활용 단계별로 발생할 수 있다고 밝히고 있으며, 이를 정리하면 다음과 같다.

19) 미국 14개 주 161개 생명보험회사가 동 설문에 응답함

첫째, 데이터의 수집 단계에서 디지털 금융거래 제공 사업자는 이용자의 회원가입 시 실명인증을 위한 성명, 전화번호, 주소, 계좌, 카드 정보 등의 각종 개인정보를 수집할 수 있다. 이는 금융거래의 특성상 보안 확보가 중요하여 본인 여부가 필수적인 요소이며, 조회·송금 등의 거래를 위해 각종 개인정보가 등록될 수밖에 없기 때문이다. 다만, 수집 과정에서 개인정보 제공 및 활용 등에 관한 동의 범위, 방식 등에서 소비자 문제가 발생하거나 소비자 피해 발생이 우려되는 상황이 존재한다. 즉, 개인정보 보호를 위해서는 ‘최소한’의 항목만 수집되어야 하지만, 서비스 제공을 위해 필수적이라는 사업자의 판단에 따라 과도하게 개인정보가 수집되는 경우가 존재한다. 예를 들어, AI를 통해 디지털 자산관리 서비스에 가입하기 위해서는 다양한 항목에 걸쳐 개인정보를 제공하는 것이 필수로 요구되며 소비자가 개별 항목을 선택할 수 없도록 설계된 사례가 있다. 소비자의 선택권을 강화하고 개인정보 수집을 최소화하기 위해서는 이용약관 동의 절차에서 소비자가 필수 항목만 선택할 수 있는 옵트인(opt-in) 방식이 바람직하다. 하지만 현재 해당 서비스에서는 모든 항목이 미리 선택되어 있고, 소비자가 직접 선택을 취소해야 하는 옵트아웃(opt-out) 방식을 사용하고 있어, 소비자가 원하지 않는 항목에 동의하게 될 가능성이 있다. 게다가 필수 항목으로 설정된 ‘개인정보 수집·이용 동의’에 대해서도 문제가 존재한다. 여기에는 소비자가 직접 입력하거나 금융회사가 제공한 정보를 통해 수집될 수 있는 대부분의 항목이 포함되어 있어, 각각의 항목에 대해 동의를 거부하기가 어려움에 따라 사업자가 과도하게 많은 개인정보를 제공받게 될 가능성이 있다.

둘째, 데이터의 보관·관리 단계에서 디지털 금융거래 제공 사업자가 수집하거나 소비자로부터 제공받은 다양한 정보는 사업자에 의해 데이터화 되어 보관 및 관리되며, 이때 가장 문제가 되는 부분은 개인정보 유출 문제이다. 대부분 디지털 서비스에서 가장 빈번하게 논의되는 소비자 문제 역시 개인정보 관련 사항이지만, 디지털 금융서비스에서는 일반적인 서비스에 비해 사업자가 보유한 개인정보의 항목이 다양하며 계좌 정보 등이 포함되어 금전적 피해가 직접 발생할 수 있다. 앞서 언급한 사이버 리스크와 더불어 사업자에 의한 개인정보 유출 문제로 인해 소비자 피해가 크게 발생할 수 있는데, 예를 들어 최근 국내 대형 핀테크 사업자가 보험설계사에게 고객정보를 건당 6만 9천 원 정도에 판매한 것이 적발된 경우가 있었으며,²⁰⁾ 소비자들에게 개인정보 판매 관련 사항을 명확히 전달하지 않았다는 점, 개인정보 판매를 통한 혜택이 소비자에게 전달될 수 있도록 조치하는 방안이 부족했다는 비판이 가능한 사례이다.

20) 증권경제신문(2022. 6. 10), “토스, 개인정보 판매 논란에 “고객동의 과정 보완하겠다”

셋째, 소비자로부터 수집된 다양한 정보를 보관 및 관리하는 사업자가 활용하는 단계에서 소비자가 동의를 철회하거나 선택적으로 정보를 제공할 수 있는지 여부에 대해 논의가 필요하다. 우선 최초 동의 시점에서는 정보제공 및 활용에 어렵지 않게 동의할 수 있지만 많은 경우 동의 후 이를 번복하거나 취소할 방법에 대한 안내가 상대적으로 부족한 것으로 보인다. 예를 들어 다양한 정보 항목들이 과도하게 일괄적으로 묶여 필수 수집 및 제공 항목으로 간주되거나 선택항목으로 포함되면서 개별 항목별로 선택적으로 정보 동의를 할 수 있는 등의 조치가 이뤄지지 않는 것으로 평가되고 있다.

보험산업과 관련해서도 보험회사는 무분별한 정보수집과 활용으로 인해 소비자의 권익을 침해할 가능성에 유의해야 한다. 과거에는 보험회사가 가입정보, 보험금 청구 정보 등 계약 관련 내부 관리 데이터, 흡연 여부나 건강 상태, 차량 종류 등 고객 수집 데이터 등 전통적인 데이터를 활용했다면, 최근에는 웨어러블 기기, 텔레매틱스 등을 통해 수집하는 소비자의 행동 데이터, 해외 보험회사의 경우에는 온라인 구매, 소셜미디어 활동 등 온라인 미디어 데이터, 소비자의 구매 습관, 소득 및 자산 데이터 등 새로운 고객 수집 데이터를 활용하는 사례가 늘고 있다. 보험회사가 새로운 종류의 데이터들은 사용함으로써 소비자에게 보험료 할인이나(특히 텔레매틱스나 웨어러블 기기 수집 정보 공유의 경우), 리스크 경감이나 사고방지를 위한 맞춤형 알림이나 리스크 관리 자문을 제공하는 등 혜택을 제공할 수 있고, 리스크 집단을 세분화함으로써 새로운 종류의 보험상품을 제공할 수도 있을 것이다. 그러나 소비자가 개인정보 수집 및 이용 동의 시에 약관을 제대로 읽지 않거나 이해하지 못한 채 동의하는 행동을 이용하여 금융회사가 무분별하게 정보수집이나 활용을 시도할 가능성도 존재한다. 필수항목과 선택항목을 구분하지 않고 동의를 요구하여 서비스 이용을 위해서는 선택항목을 포함한 모든 정보 수집 및 활용에 동의하도록 하거나, 수집 및 활용 동의를 기본 설정으로 하고 비동의하는 경우 적극적으로 비동의를 선택해야 하도록 설계하는 방법 등을 해당 사례로 들 수 있다. 이러한 문제를 방지하기 위해서는 유럽 GDPR(General Data Protection Regulation)을 참고할 수 있는데, 동법은 개인정보처리 관련 동의를 통해 개인정보처리 관련 동의는 자유의지로 제공되어야 하고, 구체적이어야 하고, 정보를 바탕으로 해야 하며, 모호하지 않아야 한다고 규정하고 있다.²¹⁾ 아울러 데이터 주체(소비자)가 언제든지 쉽게 동의를 취소할 수 있어야 한다.

21) GDPR.EU, "What are the GDPR consent requirements?"

〈표 II-3〉 보험회사 보유데이터

구분	사례
계약 관련 내부 관리 데이터	<ul style="list-style-type: none"> 경험통계: 나이, 성별, 사망률, 질병률, 사고율 등 계약철회, 해지, 청구, 가입 정보 등
(전통적) 고객 수집 데이터	<ul style="list-style-type: none"> 의료 관련: 흡연 여부, 음주 여부, 건강 상태, 병력, 가족 병력 등 차량 관련: 차량 종류, 차량 탑재 부품 등
(새로운) 고객 수집 데이터	<ul style="list-style-type: none"> 웨어러블 수집 데이터: 걸음 수, 소모 칼로리, 심박수 등 텔레매틱스 수집 데이터: 주행데이터(주행거리, 주행시간), 운전 습관 데이터(차로 이탈, 과속, 급제동) 등 신용정보
자체 수집 데이터	<ul style="list-style-type: none"> 날씨, 자연재해, 공공데이터, 웹 크롤링 데이터 등

자료: 박희우·강윤지(2024); EIOPA(2019)

3) 데이터분석 알고리즘

금융서비스의 디지털 전환이 가져온 가장 두드러진 변화는 새로운 사업자인 플랫폼 기업이 금융시장에 진입한 것이라고 할 수 있다. 비교적 보수적인 기존 금융회사들과는 달리 빠르게 발전하고 변화해야 살아남을 수 있는 기술 기반의 플랫폼 사업자들이 금융 혹은 유사 금융 영역에 진출함에 따라 소비자들이 더욱 편하게 이용할 수 있는 서비스 제공이 많아졌다.

플랫폼 시장은 네트워크 효과 때문에 후발 사업자들이 진입하기 어려운 특성이 있는 시장이라고 할 수 있다. 데이터분석 알고리즘을 개발하고 학습하는 데 있어, 많은 데이터, 비용, 시간이 필요하기 때문에 실제로 이런 기술을 활용할 수 있는 사업자는 한정적인 것으로 보인다. 특히 기존의 대형 플랫폼 사업자들은 많은 이용자와 자본을 가지고 있어 유리한 위치를 점하고 시장에서의 영향력을 유지하거나 심화시킬 가능성이 있다. 예를 들어 데이터분석 알고리즘 기술을 적극적으로 활용하는 플랫폼 사업자들의 시장지배력이 기존의 플랫폼 사업자들을 능가할 경우에 시장독점 현상이 나타나거나 소비자 후생을 저해할 가능성이 있다. 또한, 플랫폼 사업자가 알고리즘을 통해 얻은 소비자 정보를 이용해 동일한 상품과 서비스에 개인마다 다른 가격을 책정하는 경우가 발생할 수 있다. 이른바 ‘가변가격제(variable pricing)’라는 전략에 따라 상황에 따라 충성도가 높은 ‘단골’ 고객에 더 높은 가격을 책정하기도 하며, 이는 불공정한 기만행위라는 소비자 불만을 야기할 수 있다.

또한, 금융거래에서 AI 기술을 활용할 경우 AI가 인간의 감정, 편견 등을 배제하고 데이터에만 기반한 판단, 결정을 내림으로써 소비자에게 보다 적합한 상품 추천, 정보제공·분석 등 서비스를 제공할 수 있다. 그러나 AI에 활용된 데이터의 편향성이나 상관관계를 인과관계로 잘못 해석하여 야기된 알고리즘의 오류는 특정 고객들의 금융서비스 접근을 거절하는 등 부적절한 결과를 초래할 수 있다.²²⁾ 예를 들어 금융권 사례는 아니지만 AI 챗봇 '이루다'가 사회적 소수자에 대한 혐오 발언을 여과 없이 하다가 챗봇 서비스를 개시한 지 1개월도 못 된 2021년 1월에 이용이 잠정 중단된 사례가 있다. 금융소비자 피해가 발생할 경우, AI 활용 업체가 사용된 알고리즘과 데이터 등의 정보를 제공하더라도 소비자가 이를 충분히 이해하기 어려워 업체에 손해배상책임이 있음을 입증하기가 곤란할 수 있다. 더욱이 AI 개발업체와 AI를 활용하는 금융회사가 서로 다른 법적 주체일 경우에 양자 간 책임소재 문제로 금융소비자의 손해배상책임 입증은 더 힘들어질 수 있다.²³⁾

한편, 금융회사의 의사결정에 사용하는 모형이 가지는 모형리스크(Model Risk)는 과거에도 존재했으나, AI 활용 이후 AI 시스템의 운영 속도와 AI 모형의 복잡성, 데이터 리스크, 복수의 모형이 네트워크 내에서 상호작용을 하면서 나타날 수 있는 리스크 등으로 인해 금융회사가 직면한 모형리스크는 더 심각해졌다고 할 수 있다.²⁴⁾ 보험회사도 다양한 분야에서 빅데이터 분석을 활용하고 있으므로, 학습 데이터의 문제에 기인하는 오류나 AI 모형리스크에 노출되어 있는데, 특히 마케팅이나 고객 관리 분야보다는 보험료 책정이나 언더라이팅 과정에서의 AI 분석 오류가 소비자에게 큰 피해를 줄 가능성이 높다. 예를 들어, AI가 편향된 데이터나 위험평가 요소(Rating Factor)를 사용할 경우 불법적 가격차별 행위를 초래할 수 있으며, 상관관계를 인과관계로 오인할 경우 편향된 의사결정을 할 수 있고, 이러한 의사결정은 특정 소비자집단에 대한 보험인수 거절이나 부적절한 보험료 책정으로 이어질 수 있다.

22) 금융산업에서 머신러닝 기반 AI 활용에 대한 논의가 점점 증가하고 있는 가운데, 이러한 머신러닝 기반 AI의 주된 특징은 주어진 데이터에 기반해 기계가 규칙을 스스로 학습하고 그 결과에 따라 행동하도록 하는 것임. 이때 학습 알고리즘에 따라 이를 반복적으로 수행하면서 보상을 최대화하는 행동 규칙을 생성해 AI 활용 관련 목표가 이뤄지게 됨(노성호, 2023).

23) 금융·보험산업 인적자원개발위원회(2021)

24) BIS(2024); AIPPF(2022)

나. 기술 발전과 소비자보호 법·규제 간 격차

1) 금융소비자 보호 규제 적용의 한계

2021년 3월부터 시행된 금융소비자보호법에서는 금융소비자 보호 차원에서 금융상품 판매 시 판매업자나 자문업자(이하 ‘금융회사’라 함)의 준수사항을 열거하고 분쟁조정 절차 등을 규정하고 있으나, 온라인 환경을 충분히 반영하지 못하는 한계가 존재한다. 이에 디지털 금융소비자 보호와 관련하여 가장 큰 이슈는 금융소비자보호법에 명시된 금융상품 판매 시 금융회사가 준수해야 하는 6대 판매원칙이 온라인 환경에서 구현되기 어렵다는 점이다. 금융소비자보호법에 담겨 있는 금융회사가 지켜야 하는 6대 판매원칙은 적합성 원칙, 적정성원칙, 설명의무, 불공정 영업행위 금지, 부당권유 금지, 광고규제로 구성된다. 이들 가운데 설명의무는 금융회사가 소비자의 이해를 돕기 위해 상품설명서를 제공하고, 상품설명서의 중요한 사항에 대해 알아듣도록 충분히 설명하고, 소비자가 설명을 이해했음을 확인하는 3단계 절차를 요구하고 있다. 이에 더해 금융위원회는 2021년 7월에 판매 현장에서 금융회사의 금융상품 설명이 합리적으로 이루어질 수 있도록 「금융상품 설명의무의 합리적 이행을 위한 가이드라인」²⁵⁾을 발표하였다.

그러나 오프라인 채널과 달리 편리성을 강조하는 온라인 채널에서는 금융소비자의 클릭이나 터치로 신속한 금융상품 가입이 가능하여 금융회사의 실질적 설명의무 이행이 어렵다. 또한 금융소비자와 금융회사 간 소통이 원활하지 않으며, 금융상품이 금융소비자에 적합한지, 적정한지 등을 판단하기 쉽지 않다. 이는 온라인 채널에서의 설명의무 이행이 금융상품 가입 전 상품설명서를 읽었음을 확인하는 버튼 클릭이나 터치 방식을 통해 이루어지고 있지만, 실제로 소비자가 상품설명서를 읽고 이해했는지 확인하기는 어려워 형식적인 상품설명서 교부 수준에서 그칠 가능성이 크기 때문이다.

이러한 문제를 해결하기 위해 금융위원회는 2022년 8월에 온라인 판매과정에 효과적인 금융상품 설명방안 마련을 위해 「온라인 설명의무 가이드라인」²⁶⁾을 마련하였으며, 동 가이드라인은 금융상품 설명화면 구성, 금융소비자의 이해 지원, 이해 여부 확인 등 3개 분야에 대한 7대 원칙으로 구성되어 있다. 동 가이드라인에 따르면 금융회사는 기본적으로

25) 금융위원회 보도자료(2021. 7. 14), “판매현장에서 금융상품 설명이 합리적으로 이루어질 수 있도록 지속적으로 지원해나가겠습니다”

26) 금융위원회 보도자료(2022. 8. 11), “온라인 판매에 효과적인 금융상품 설명방안 마련”

설명서를 알기 쉽게 구성하고 가입하기 전에 시간의 공백을 두고 질의응답이 가능한 채널을 확보해야 한다. 만약 모든 디지털 금융소비자가 금융상품의 내용을 자세히 알아보고 궁금증을 해소한다면, 온라인 설명의무 가이드라인으로도 충분할 수 있다. 그러나 현실에서는 상품 내용에 대해 표면적인 이해만 하고 구체적인 정보를 찾아보려 하지 않는 금융소비자가 매우 많다. 한편, 2022년 2월에 금융위원회는 고령자가 온라인 화면을 잘 읽지 못하는 점에 착안하여 은행권과 함께 고령자 친화적 모바일 금융앱 구성지침을 마련하였다. 그러나 고령자 친화적 모바일 금융앱 구성지침이 은행업권에만 해당하는 지침이기 때문에 참여하지 않는 금융권이나 전자금융업자의 경우 해당 사항이 없다. 한편 온라인 채널 설명의무 등의 관련 사항을 감독규정이나 시행령에 답아야 한다는 주장이 있었으나, 실현되지는 못하고 가이드라인 혹은 지침으로 운영되고 있다. 이에 따라 해당 가이드라인 및 지침은 아직까지 모두 법적 효력이 없으며 위반 시 처벌 근거가 없고 법적 강제성이 없는 상황이다.²⁷⁾

2) 디지털 금융범죄

최근 디지털 기술의 발달과 디지털 기기의 대중화로 인해, 모든 업종에서 금융거래가 점점 더 디지털화되고 있다. 금융거래의 디지털화로 인해 금융회사 직원에 의한 디지털 금융범죄 예방이 어려워진 측면이 있으며, 이로 인해 보이스피싱 등 금융사기와 금융착취 등 디지털 금융범죄의 비중이 높아지는 문제가 발생하고 있다. 이는 금융회사 직원이 확인하는 절차가 있는 오프라인 채널과 달리 온라인 채널에서 고객이 직원의 확인 없이 즉각적으로 송금하여 의심되는 거래를 인지하기 어렵기 때문이다.

대표적인 디지털 금융범죄인 보이스피싱은 정부를 비롯한 다수의 유관기관이 다양한 방법으로 방지하기 위한 노력을 기울이고 있으나, 피해 규모는 오히려 증가하고 있다. 정부는 보이스피싱 범죄의 수법에 따라 크게 대출사기형²⁸⁾ 및 기관사칭형²⁹⁾으로 구분해 통계를 직접하여 제공하고 있다. 보이스피싱 범죄의 발생건수는 2016년 17,040건에서 2022년 21,832건으로 늘어났으며, 피해금액도 같은 기간 1,468억 원에서 5,438억 원으

27) 서병호(2023)

28) 대출사기형은 전화 SMS 등을 통해 대출 상담 알선을 가장해 대출수수료 입금 명목으로 금전을 요구해 가로채는 수법임

29) 기관사칭형은 정부기관을 사칭해 사건연루조사를 한다고 기망하는 수법과 메시지를 통한 지인사칭형 금원편취 및 납치협박 등 범죄를 사칭하여 편취하는 수법을 사용함

로 큰 폭으로 증가하였다. 다만, 정부의 단속 및 수사, 그리고 통신·금융분야의 특별대책 등으로 인해 2022년 보이스피싱 발생건수 및 피해금액이 전년 대비 30% 가량 감소하였다.

〈표 II-4〉 보이스피싱 범죄의 발생 및 검거 현황

(단위: 건, 억 원, 명)

구분	발생건수	피해금액	검거건수	검거인원
2016	17,040	1,468	11,386	15,566
2017	24,259	2,470	19,618	25,473
2018	34,132	4,040	29,952	37,624
2019	37,667	6,398	39,278	48,713
2020	31,684	7,000	34,051	39,324
2021	30,982	7,744	27,647	26,397
2022	21,832	5,438	24,552	25,030

자료: 시사뉴스(2018. 9. 27), “김병관 “보이스피싱 등 서민대상 범죄, 경찰 금융당국 적극 대응해야””;
 JS메거진(2023. 2. 3), “경찰청, '22년 보이스피싱 피해 발생, 16년 만에 큰 폭으로 감소”

한편, 금융감독원(2021)³⁰⁾에 따르면 2020년 모바일과 인터넷 등 온라인 채널에 의한 금융사기 피해금 비중은 75.2%를 차지하고 있는 것으로 나타났다. 또한, 최근에는 가상자산 연계 투자사기 등 디지털 금융범죄의 종류도 늘어나고 있다. 금융감독원(2023)에 따르면 2022년 가상자산 연계 유사수신 투자 피해 신고 건수는 199건으로 2021년 대비 67.2% 급증하였으며, 이들은 주로 카카오톡 대화방 등 SNS를 통하여 발생하였다. 이에 가상자산이용자보호법이 2023년 6월에 국회 본회의에서 통과되었고, 현재 시행 중이다. 그리고 금융감독원은 2023년 6월에 가상자산 연계 투자사기 신고센터를 개설하고 다양한 가상자산 연계 투자사기 사례 및 대응책을 공유하고 있다. 또한 우리나라 금융당국 등에서 디지털 금융범죄 예방을 위한 금융교육은 청소년과 고령층 위주로 실시되고 있으나, 60대 이상 고령층 금융사기 피해 규모가 전 연령층에서 가장 심각하고 갈수록 심해지고 있다. 금융감독원(2023)³¹⁾에 따르면 2022년 60대 이상 고령층의 보이스피싱 피해금액 비중은 46.7%로 2020년 대비 17.3%p 늘어났다.

30) 금융감독원 보도자료(2021. 4. 16), “2020년 중 보이스피싱 현황 분석”

31) 금융감독원 보도자료(2023. 4. 21), “2022년 보이스피싱 피해현황 및 주요 특징”

〈표 II-5〉 우리나라 연령별 보이스피싱 피해금액 현황

(단위: 억 원, %, %p)

구분	2020		2021		2022	
	금액	비중	금액	비중	금액	비중
20대 이하	66	2.8	52	3.1	92	6.4
30대	243	10.5	121	7.3	53	3.7
40대	485	20.9	219	13.2	145	10.1
50대	843	36.3	650	39.3	477	33.1
60대 이상	683	29.4	612	37.0	673	46.7
합계	2,320	100.0	1,654	100.0	1,440	100.0

주: 보이스피싱 피해금액은 피해구제신청접수(1차 계좌) 기준(법인 피해자 제외)으로 집계됨
 자료: 금융감독원 보도자료(2023. 4. 21), “2022년 보이스피싱 피해현황 및 주요 특징”

3) 다크패턴

코로나19 이후 온라인 거래가 급속하게 확산되면서 온라인 플랫폼 시장 규모가 더욱 커지고 있으며, 온라인 채널에서 비합리적 소비를 유도하는 기업의 ‘다크패턴(Dark patterns, 눈속임 설계)’은 소비자보호 문제에 있어 위험요인으로 작용할 수 있다.

OECD(2022)에서는 다크패턴을 ‘일반적으로 온라인 사용자 인터페이스에서 보이는, 소비자가 자신들의 최선의 이익으로 이어지지 않는 선택을 하도록 하는 넓은 범위의 행위를 이르는 말’로 정의하고 있다. 또한, 이러한 다크패턴의 유형으로 행동강제(Forced Action), 화면조작(Interfere Inference), 반복간섭(Nagging), 경로방해(Obstruction), 숨겨진규정(Sneaking), 사회적 증거(Social Proof), 시급성(Urgency)을 제시하였다.

먼저 행동강제는 소비자가 특정 기능에 접근하려면 어떤 행동을 하도록 강요하는 것을 의미하며, 여기엔 소비자의 동의 없이 연락처 정보를 이용하거나 추출하는 것이 포함된다. 화면조작은 온라인 사업자가 소비자에게 유리한 특정 행동을 하도록 유도하는 것을 의미하며, 이 경우에 행동경제학에서 제시된 프레이밍 효과, 앵커링 효과, 디폴트 편향 등이 이용되기도 한다. 반복간섭은 사업자에게 유리한 특정 행위를 지속적으로 요구하는 것을 뜻하며, 예를 들어 지속적으로 알림을 보내거나 위치 추적 기능을 켜도록 요구하는 것이 포함된다. 경로방해는 작업 흐름이나 상호작용을 복잡하게 만들어 특정 행동을 방해하는 것을 의미한다. 예를 들어, 서비스 가입이나 사생활 침해적인 설정에 동의하는 것

은 쉽게 만들어 놓고, 이를 취소하는 것은 어렵게 만들어 놓거나, 특정 옵션을 선택할 때 클릭을 더 복잡하게 하거나 간단하게 하는 것이 포함된다. 숨겨진 규정은 소비자의 결정 및 가격과 관련된 정보를 숨기거나 위장하거나 공개를 늦추는 것을 의미한다. 예를 들어, 소비자가 구매를 완료하려고 할 때 예상치 못한 추가 요금을 더하는 것이 포함된다. 사회적 증거는 다른 소비자들의 행동을 보여주어 결정을 유도하려는 시도를 의미한다. 예를 들어, 다른 소비자의 선택이나 후기를 알림으로 보내는 것이 이에 해당된다. 마지막으로, 긴급성은 소비자에게 구매를 압박하기 위해 실제이거나 조작된 시간적 또는 수량적 제한을 부과하는 것을 의미한다. 예를 들어, “재고가 부족하다”는 메시지나, 할인 또는 판매 종료까지 카운트다운하는 시스템 등이 포함될 수 있다.

한편, 한국소비자원(2021)의 실태조사³²⁾에 따르면, 우리나라 전자상거래 모바일 앱 100개 중 97개 모바일 앱에서 최소 1개 이상의 다크패턴 문제가 발견된 것으로 나타났다. 소비자 자신도 모르는 사이에 계약이 자동으로 갱신·결제되는 ‘숨은 갱신’ 유형을 92.6%가 경험하였고, 사업자에게 유리한 옵션을 미리 선택해 놓고 소비자가 이를 무심코 지나치도록 유도하게 하는 ‘특정 옵션 사전 선택’ 유형을 88.4%가 경험하였다.³³⁾

공정거래위원회는 2023년 7월에 눈속임 설계를 방지하기 위한 자율관리 가이드라인을 발표하였는데, 이는 전자상거래, 통신판매 또는 통신판매중개 사업자가 소비자에게 제공하는 온라인 인터페이스를 설계하고 운용할 때 고려할 사항을 제시하고 있다. 동 가이드라인은 사업자가 소비자의 착각이나 부주의를 유발하여 불필요한 지출을 유도하는 것을 다크패턴이라고 정의하고 이를 자율적으로 방지하려는 목적을 가지고 있다. 공정거래위원회에 따르면 다크패턴은 편취형, 오도형, 방해형, 압박형 등 4가지로 분류될 수 있으며, 각 유형은 다시 19개 세부 유형으로 재분류될 수 있다.³⁴⁾ 다만 동 가이드라인의 적용 대상은 전자상거래업자, 전자상거래업자, 표시광고법상 광고업자이기 때문에 전자금융업자나 금융회사에는 해당되지 않는다.

32) 국은숙(2021)

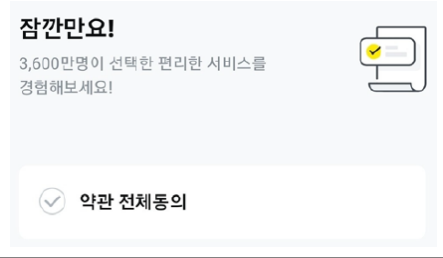



33) 서병호(2023)

34) 공정거래위원회(2023)는 다크패턴 유형으로서 편취형에 숨은갱신, 순차공개 가격책정, 몰래 장바구니 추가, 오도형에 거짓할인, 거짓추천, 유인판매, 위장광고, 속임수 질문, 잘못된 계층 구조, 특정옵션 사전선택, 방해형에 취소·탈퇴방해, 숨겨진 정보, 가격비교 방해, 클릭피로감 유발, 압박형에 반복간섭, 감정적 언어사용, 시간제한 알림, 재고 없음·높은수수료 알림, 다른소비자의 활용알림을 포함해 제시하고 있음(공정거래위원회(2023. 4. 21), “온라인 다크패턴으로부터 소비자 보호를 위한 정책방향 발표”)

다만, 최근 들어 이러한 규제 공백을 해소하기 위한 정책적 움직임이 있는데, 우선 온라인 채널에서 ‘다크패턴’ 행위를 통해 소비자를 기만하는 것을 금지하는 내용이 담긴 ‘전자상거래 등에서의 소비자보호법’ 개정안이 2024년 1월에 국회 본회의를 통과했고, 2024년 2월에 개정되어 2025년 2월부터 시행될 예정이다. 전자상거래법 개정안이 금지한 다크패턴 행위를 구체적으로 살펴보면, 총비용이 아닌 일부 금액만 고지, 특정 상품 구매 과정에서 영뚱하게 다른 상품 구매 여부를 물은 뒤 거래 유인, 선택 항목의 크기·모양·색깔 등에 크게 차이를 두고 특정 항목 선택을 유인, 취소·탈퇴·해지 방해, 선택 내용 변경을 팝업창으로 반복 요구 등 5가지이다. 다만 전자상거래법의 적용 대상은 전자상거래 및 통신판매 사업자이기 때문에 금융권 사업자에는 해당되지 않는다.

눈속임 설계 등 소비자의 행태 편향을 이용한 마케팅은 소비자의 판단을 왜곡시켜 원하지 않거나 필요하지 않은 금융상품 구매를 유도할 수 있는데, 금융상품은 일반 상품에 비해 계약 금액이 많고 대출이나 보험상품처럼 계약 기간이 긴 경우가 많아 디지털 금융소비자에게 장기간 큰 피해를 줄 우려가 있다. 그러나 금융소비자보호법에는 디지털 금융소비자의 행태 편향을 이용한 눈속임 설계 등을 금지하는 내용이 담겨 있지 않으며, 이와 관련한 금융권을 대상으로 적용한 가이드라인도 아직 없는 상황이다. 이에 금융위원회는 2024년 3월에 ‘비대면(온라인) 금융상품 판매과정에서 다크패턴 사용제한 가이드라인’을 마련할 계획이라고 밝혔으며, 가이드라인 마련을 위한 정책연구용역이 진행 중이다. 또한, 2024년 내에 전 금융권의 비대면(온라인) 금융상품 판매과정에서 다크패턴 사용 실태를 점검한 후 다크패턴 사용 제한을 위한 가이드라인을 마련할 것이라고 밝혔다. 동 가이드라인의 적용 대상은 예금, 대출, 보장성 보험, 투자성 증권 등 4개 금융상품 분야가 선정될 예정이다.

〈그림 II-2〉 금융권 눈속임 설계 예시

유형	사례	예시
<p>(압박형-다른 소비자의 활동 알림) 해당 제품을 다른 고객의 숫자를 알려줌으로써 신속한 구매를 하도록 압박</p>	<p>(카카오페이) '3,600만 명이 선택한 편리한 서비스' 등 서비스 이용 소비자 수를 표시하여 선택 유도</p>	
<p>(압박형-반복간섭) 팝업 등을 통해 특정 행위를 반복적으로 요구하여 원하는 행위를 하도록 압박</p>	<p>(토스뱅크) 토스 앱 접속 시 금융 팁을 제공하는 것처럼 보이는 팝업창이 반복적으로 뜨며, 클릭 시 토스 계좌 연결</p>	
<p>(방해형-숨겨진 정보) 구매를 결정하기 위해 필요한 정보를 은폐하거나, 누락시키거나 축소시키는 행위</p>	<p>(카카오페이) 사용자가 알아야 하는 주요 정보에 관한 여러 과정을 놓치게 하여, 결과적으로 해당 내용을 발견하기 어렵게 함</p>	
<p>(오도형-특정 옵션 사전선택) 사업자에게 유리한 옵션을 기본으로 설정하고 고객이 본의 아니게 수용하도록 유도</p>	<p>(카카오페이) 사용자가 선택하기 전, 기업에게 유리한 정보 (후불교통카드 내역 등의 청구정보) 제공에 동의하도록 미리 선택해 둠</p>	

주: 온라인 시장에서 사업자의 이익을 위해 소비자의 착각, 실수, 비합리적인 지출 등 인지·행동 편향을 유도하는 상술을 의미함
 자료: 서병호(2023) 재인용함

2023년 EIOPA EuroBarometer 설문조사 결과에 따르면, 보험시장에서도 소비자들이 다크패턴을 경험하는 것으로 조사되었다. 보험시장 맥락에서 다크패턴은 소비자가 개인정보를 제공하도록 설득하거나, 할인가격의 시간 제약 등을 이용하여 중요한 계약조건, 보장내용, 면책조항 등을 제대로 확인하지 않은 채로 보험상품을 구매하도록 유도함으로써 소비자에게 잠재적 피해를 줄 수 있다.

EIOPA³⁵⁾는 보험분야에서 발견할 수 있는 사회적 증거(Social Proof), 소비자의 감정 이용, 행동 강제, 긴박감 조성, 미리 선택된 조건, 허위 위계구조, 정보 감추기, 경품 활용 등 다크패턴의 사례를 제시하였다. 사회적 증거(Social Proof)는 주어진 상황에 어떠한 행동이 적절한지 불확실한 경우, 다른 사람들의 행동을 모방하는 심리적 현상을 이르는데, 예를 들어 “92%의 소비자들이 OO 보장에 가입했습니다.” 등의 문장이 사회적 증거 현상을 이용하여 소비자의 결정에 영향을 주고자 하는 사례이다. 소비자의 감정을 이용해서 편향된 결정을 유도하는 경우도 있는데, 손실회피 감정을 자극하는 안내문을 이용하여 가입을 유도하는 사례를 들 수 있다. 행동 강제를 이용한 다크패턴의 사례로서는 소비자가 보험료 전적을 얻거나 상품비교를 위해서는 회원가입이나 정보수집 및 활용에 동의해야만 하는 것으로 믿도록 하는 관행을 제시하였다. 긴박감 조성을 통한 다크패턴은 전적 가격의 시간제한을 두어 해당 상품을 사지 못할 것을 두려워하거나 모든 정보를 충분히 읽지 않고 구매결정을 하도록 유도하기도 한다. 한편 보험 웹사이트 등에서 미리 특정 조건을 선택하여 소비자가 해당 선택이 자신들에게 최선의 선택이라고 믿도록 하는 방법을 이용하기도 하는데, 특히 개인정보 입력이나 개인정보 수집 동의에 이용하는 사례가 발견되었다. 사용자가 특정 선택을 유도하거나, 특정 선택을 숨기기 위해 글자 색이나 글자 크기를 이용하기도 한다. 아울러 경품을 통해 이메일 주소를 공유하도록 하고, 해당 정보를 향후 마케팅 통로로 이용하는 사례도 다크패턴의 사례로 제시하였다.

35) EIOPA, “Dark patterns in insurance: practices that exploit consumer biases”

〈그림 II-3〉 보험시장에서 나타나는 다크패턴 사례

구분	사례						
감정 이용	<p>Select Yes or No to continue booking:</p> <p>O Yes, I want Hotel booking Insurance for my trip. 71 € Per person</p> <p>O No, I am willing to risk my 2585€ trip. ← 감정: 리스크에 대한 관념과 여행비용 손실희피를 이용</p> <p>"Things happened outside of my control which caused the trip to be cancelled. The travel insurance was valuable in reducing the loses when I had to cancel my trip." – Mr. Rodman ← 추천</p>						
긴박감 조성	<table border="1"> <tr> <td data-bbox="336 634 470 822">Insurance Company</td> <td data-bbox="470 634 604 822"> 1338 EUR Per year Expires in 6 days </td> <td data-bbox="604 634 739 822"> Voluntary 250 EUR Compulsory 350 EUR Total 600 EUR </td> <td data-bbox="739 634 873 822"> √ </td> <td data-bbox="873 634 1008 822"> √ </td> <td data-bbox="1008 634 1130 822"> More Info </td> </tr> </table> <p>← 제한된 기간 동안만 적용되는 가격</p>	Insurance Company	1338 EUR Per year Expires in 6 days	Voluntary 250 EUR Compulsory 350 EUR Total 600 EUR	√	√	More Info
Insurance Company	1338 EUR Per year Expires in 6 days	Voluntary 250 EUR Compulsory 350 EUR Total 600 EUR	√	√	More Info		

자료: EIOPA, "Dark patterns in insurance: practices that exploit consumer biases"

〈표 II-6〉 Eurobarometer 설문조사: 보험구매 중 다크패턴 경험

(단위: %)

구분	모든 응답자	2년 내 온라인 보험 구매 경험 소비자
많은 사람들이 이미 해당 보험상품을 구매했다는 문장	13	20
견적 보험료는 제한된 시간 내에 유효하다는 문장	18	28
보험상품 비교를 위해 필요하지 않을 것으로 판단되는 개인정보를 제공하도록 요청함	17	26
위 사례 중 아무것도 경험하지 않음	58	43
잘 모르겠음/대답하고 싶지 않음	7	3

자료: EIOPA(2024)

다. 취약계층

1) 디지털 격차

디지털 금융거래는 기본적으로 디지털 기기를 기반으로 제공되는 만큼 디지털 격차 취약 계층들의 서비스 제공 기회가 박탈되는 등 소비자 문제가 발생할 수 있다. 또한 금융서비스의 디지털화로 인한 혜택을 모두 소비자가 보고 있는 것은 아니며, 디지털 거래에 익숙하지 않은 계층들은 사라지는 오프라인 채널로 인해 금융서비스를 받는 것이 더 불편해지고 소외되는 현상이 생길 수 있다. 즉, 정보접근성 관점에서는 크게 디지털 서비스 자체에 대한 접근성 관련 문제와 디지털 전환에 따른 오프라인 접근성 배제와 같은 두 가지 방향의 소비자 문제가 발생할 수 있다.

과학기술정보통신부·한국지능정보사회진흥원(2024)의 실태조사 결과(〈표 II-7〉 참조)에 따르면 장애인, 고령층, 저소득층, 농어민의 평균 디지털 정보화 수준은 2019년 69.9%에서 2023년 76.9%로 꾸준히 상승하고 있는 추세이긴 하나, 100%로 가정한 일반 국민의 디지털 정보화 수준에 비해 전반적으로 크게 미치지 못한 수준인 것으로 파악된다. 이에 따라 장애인, 고령층, 저소득층, 농어민은 디지털 정보화에 있어서 일반 국민과 비교해 디지털 격차가 발생하고 있는 디지털 취약계층으로 분류될 수 있다. 즉, 장애인, 고령층, 저소득층, 농어민(이하 '4대 취약계층'이라 함)의 정보화 수준이 낮아서 디지털 금융거래에 익숙하지 않고 이용상 문제가 발생할 가능성이 있다.

〈표 II-7〉 국내 취약계층의 디지털 정보화 수준

(단위: %)

구분		2019	2020	2021	2022	2023
계층별 수준 ¹⁾	장애인	75.2	81.3	81.7	82.2	82.8
	고령층	64.3	68.6	69.1	69.9	70.7
	저소득층	87.8	95.1	95.4	95.6	96.1
	농어민	70.5	77.3	78.1	78.9	79.5
	취약계층 평균 ²⁾	69.9	72.7	75.4	76.2	76.9

주: 1) 수준을 나타내는 지표는 일반 국민의 디지털 정보화 수준을 100%로 간주할 때 일반 국민 대비 4대 취약계층의 디지털 정보화 수준을 의미함

2) 취약계층 평균은 계층별 인구 규모를 고려한 가중 평균임

자료: 과학기술정보통신부·한국지능정보사회진흥원(2024)

4대 취약계층의 디지털 정보화 접근, 역량 및 활용 수준을 세부적으로 살펴보면(표 <II-8> 참조), 이들 계층의 디지털 정보화 접근 수준은 일반 국민과 큰 차이가 없지만, 역량 및 활용 수준에서는 저소득층을 제외한 나머지 계층이 일반 국민보다 매우 부족한 것으로 나타났다. 특히, 디지털 정보화 활용보다는 역량 수준에서 이러한 경향이 더욱 두드러졌다. 보다 구체적으로 살펴보면 2023년 기준 4대 취약계층의 디지털 정보화 평균 접근 수준은 일반 국민(100.0%)에 근접한 96.5%인 반면, 평균 역량 및 활용 수준은 일반 국민보다 각각 34.9%p 및 21.0%p 더 낮은 65.1%와 79.0%이었다. 또한, 디지털 정보화 역량 및 활용 수준의 경우 전반적으로 4대 취약계층의 역량 및 활용 수준이 상승 추세에 있으나, 고령층의 경우 다른 취약계층보다 현저히 낮은 것으로 나타났다. 2023년 기준 고령층의 디지털 정보화 역량 및 활용 수준은 4대 취약계층의 디지털 정보화 평균 역량 및 접근 수준(65.1%, 79.0%)보다 각각 9.8%p, 5.2%p 더 낮은 55.3%, 73.8%이었다.

〈표 II-8〉 우리나라 4대 취약계층의 디지털 정보화 접근, 역량 및 활용 수준¹⁾

(단위: %)

구분		2019	2020	2021	2022	2023
접근 수준	장애인	92.6	95.4	95.6	96.7	98.0
	고령층	90.6	92.8	93.1	95.1	95.3
	저소득층	95.2	98.3	98.7	99.5	99.6
	농어민	91.3	94.8	94.9	95.7	97.0
	평균 ²⁾	91.7	93.7	94.4	96.0	96.5
역량 수준	장애인	67.8	74.2	74.9	75.2	75.6
	고령층	51.6	53.7	53.9	54.5	55.3
	저소득층	86.5	92.5	92.9	92.9	93.0
	농어민	63.6	69.0	69.6	70.6	71.0
	평균 ²⁾	60.2	60.3	63.8	64.5	65.1
활용 수준	장애인	74.0	81.4	81.5	82.0	82.5
	고령층	63.9	71.4	72.3	72.6	73.8
	저소득층	85.4	96.1	96.3	96.4	97.4
	농어민	67.2	76.9	78.1	78.8	79.2
	평균 ²⁾	68.8	74.8	77.6	78.0	79.0

주: 1) 대비 수준은 일반 국민의 디지털 정보화 수준을 100%로 할 때 일반 국민 대비 4대 취약계층의 디지털 정보화 수준을 의미함

2) 취약계층 평균은 계층별 인구 규모를 고려한 가중 평균임

자료: 과학기술정보통신부·한국지능정보사회진흥원(2024)

또한, 스마트폰 보유율, 인터넷 이용률, 모바일 기기 이용 능력 <표 II-9>을 살펴보면, 2023년 우리나라 국민의 스마트폰 보유율 및 인터넷 이용률은 각각 96.1%, 94.0%에 달하며 대체로 국민 전원의 인터넷 접속은 무리 없이 가능한 것으로 나타났다. 다만, 4대 취약계층의 스마트폰 보유율 및 인터넷 이용률은 각각 90.8%, 85.5%를 기록하여 일반 국민과 비교해 인터넷 접속에 다소 어려움이 있는 것으로 나타났다. 또한, 우리나라 일반 국민의 모바일 기기 이용 능력은 72.0%로 나타난 반면, 4대 취약계층의 모바일 기기 이용 능력은 이보다 더욱 낮은 53.6%로 조사되어 일반 국민과 비교해 매우 낮은 것으로 확인되었다. 즉, 우리나라 4대 취약계층은 일반 국민과 비교해 인터넷 접속에 어려움이 있고 모바일 기기 이용 능력이 역시 일반 국민 대비 뒤처져 있어 디지털 금융거래 이용상 문제가 발생할 가능성이 있는 것으로 파악된다.

<표 II-9> 우리나라 4대 취약계층의 스마트폰 보유율, 인터넷 이용률, 모바일 기기 이용 능력
(단위: %)

구분	스마트폰 보유율	인터넷 이용률	모바일 기기 이용 능력 ¹⁾
일반 국민	96.1	94.0	72.0
4대 취약 계층	장애인	89.2	58.1
	고령층	91.0	48.6
	저소득층	94.0	68.2
	농어민	86.8	57.0
	평균 ²⁾	90.8	53.6

주: 1) 모바일 기기 이용 능력은 기본적인 환경설정, 무선 네트워크 설정, 파일을 컴퓨터에 이동, 다른 사람에게 파일 전송, 필요한 앱 설치 및 이용, 약성코드 검사 및 치료, 문서 및 자료 작성의 7개 항목에 대한 조사 결과를 기준으로 산출됨

2) 취약계층 평균은 계층별 인구 규모를 고려한 가중 평균임

자료: 과학기술정보통신부·한국지능정보사회진흥원(2024)

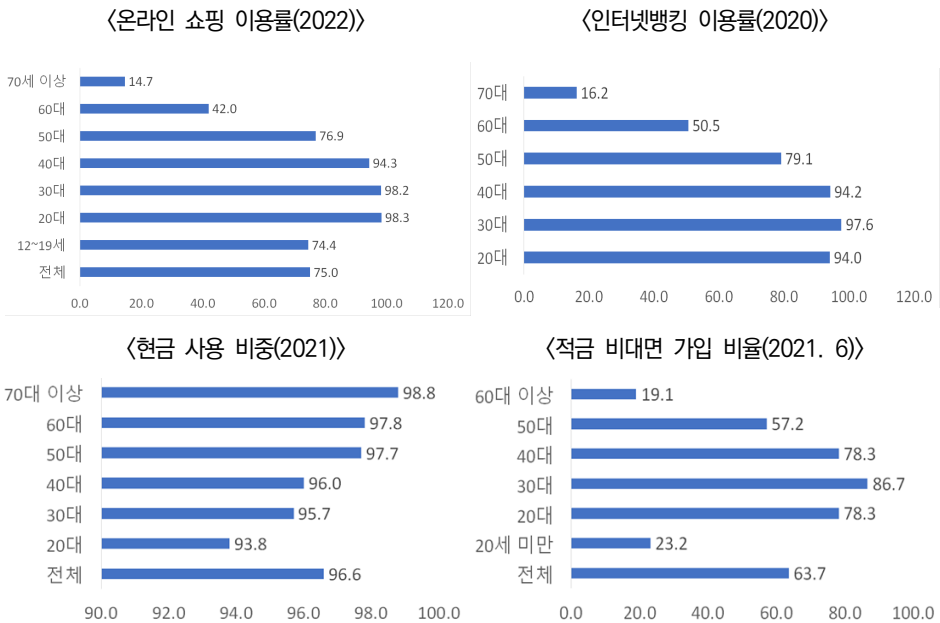
2) 고령 소비자의 디지털소외

금융거래의 디지털화로 인해 은행 창구에서 일어나던 거래가 인터넷 뱅킹이나 모바일 뱅킹으로 옮겨가면서 비용 절감을 위해 영업점 폐쇄가 증가하고 있으며, 인터넷 뱅킹이나 모바일뱅킹을 사용하지 않는 금융계좌 보유자들은 새로운 형태의 금융소외를 경험하고 있다. 또한 온라인 채널을 통한 디지털 금융서비스에서만 추가적인 혜택이 주어지는 현상은 반대로 이를 이용하지 못하는 소비자 집단의 역차별이 발생할 수 있다.³⁶⁾

과학기술정보통신부·한국지능정보사회진흥원이 발표한 실태조사에 따르면, 우리나라 60대 이상의 온라인 쇼핑이용률은 다른 연령대에 비해 매우 낮았다. 구체적으로는 전체 연령대의 온라인 쇼핑 이용률이 75.0%였던 것에 반해, 60대와 70대의 이용률은 각각 42.0% 및 14.7%에 불과했다. 또한, 대표적인 디지털 금융서비스인 인터넷뱅킹 이용률에 있어서도 다른 연령대보다 60대 및 70대의 이용률이 매우 낮은 것으로 조사되었다. 20~40대는 거의 100%에 가깝게 사용하고 있으며, 50대가 79.1% 사용하고 있어 인터넷뱅킹의 활용 수준이 매우 높은 것으로 나타난 반면, 60대 및 70대는 각각 50.5% 및 16.2%로 매우 낮게 나타났다. 적금 비대면 가입 비율의 경우에도 전체 연령대의 가입률이 63.7%인데 반해, 60대 이상의 경우 19.1%로 매우 낮은 것으로 조사되었다. 이는 60대 이상 고령 금융 소비자가 상대적으로 디지털 기기 및 비대면 채널을 이용한 금융거래에 있어 상대적으로 익숙하지 못하고 취약할 가능성이 있음을 보여준다고 하겠다.

〈그림 II-4〉 우리나라 인구 특성별 디지털 금융 사용 현황

(단위: %)



자료: 과학기술정보통신부·한국지능정보사회진흥원(2023); 과학기술정보통신부·한국지능정보사회진흥원(2021); 한국은행 보도자료(2022. 5. 18), “한국은행, 「2021년 지급수단 및 모바일금융서비스 이용행태 조사결과」 발간”; 윤관석 의원실 보도자료(2021. 9. 21), “우대금리 못 받는 적금가입자 60대 이상 81%, 2030세대 17%로 4배 이상 격차”

36) 박소정(2024)

또한, 과학기술정보통신부·한국지능정보사회진흥원(2023)이 발표한 ‘디지털정보격차 실태조사’ 결과에 따르면, 우리나라 고령층의 디지털 금융거래 서비스 이용률도 매우 낮은 것으로 나타났다. 특히, 2022년 기준 고령층의 금융서비스 이용률은 49.2로 4대 취약계층 중에서도 가장 낮은 수준인 것으로 나타났다. ‘디지털정보격차 실태조사’와 ‘인터넷이용 실태조사’의 조사 내용 차이는 있으나, 과학기술정보통신부·한국지능정보사회진흥원은 2가지 실태조사를 통해 우리나라 고령 소비자가 디지털 금융의 소외계층임을 공통적으로 보여줬다.

〈표 II-10〉 우리나라 4대 취약계층의 디지털 금융거래 서비스 이용률(2022년 기준)

(단위: %)

구분	생활정보 서비스	전자상거래 서비스	금융거래 서비스	공공 서비스	이용률	
일반국민	80.8	69.4	68.2	37.5	89.3	
취약 계층	장애인	79.8	51.5	53.4	31.2	84.4
	고령층	70.7	42.1	49.2	21.2	76.7
	저소득층	80.7	61.7	57.4	39.9	86.6
	농어민	73.2	50.7	54.2	30.0	79.7
	평균	73.6	47.1	51.5	26.2	79.5

주: 인터넷 이용자(최근 1개월 이내 인터넷 이용자) 기준. 이용률은 4개 항목 중 1개라도 이용하는 비율임
 자료: 과학기술정보통신부·한국지능정보사회진흥원(2023)

3. 소결

개발도상국과는 달리 우리나라에서는 이미 대부분 성인이 제도권 금융계좌를 보유하고 있으며, 신용카드 등의 결제 수단도 사용하고 있으므로 금융소비자들이 디지털 금융으로 인해 새로운 제도권 금융시스템으로 들어오는 것이 아니라, 기존의 금융서비스가 디지털 서비스로 전환되는 방식으로 진행되었다. 금융의 디지털화는 혁신적인 기술을 통해 맞춤형 서비스를 편리하고 신속하게 제공하기도 하고, 기존에는 서비스를 제공하지 못했던 대상들에게 금융서비스를 제공하는 등 소비자에게 혜택을 줄 수 있는 반면, 사이버리스크 증가, 개인정보의 무분별한 수집 및 활용 위험, 데이터 분석 알고리즘 문제 등 데이터 보

유 및 분석으로 인한 문제, 빠르게 변화하는 기술 발전과 법·규제 간 격차로 인한 소비자 보호 부족 현상, 새로운 계층의 소외 발생 등의 새로운 문제들을 야기할 수 있음을 살펴 보았다. 이러한 소비자 문제를 요약하면 다음과 같다.

첫째, 디지털 금융서비스의 발전으로 금융회사는 더 많은 데이터를 보유하게 되고, 다량의 데이터를 활용하게 되면서 사이버공격 등 외부 요인으로 인한 개인정보 노출뿐만 아니라, 인프라 문제나 인적 오류 문제 등 내부 요인으로 인한 IT 시스템 장애가 대형 금융사고로 인한 소비자 피해 발생 위험이 더욱 커지고 있다. 또한 금융거래 관련 데이터에는 개인정보, 금융정보, 그리고 행태정보까지 포함되어 있어 데이터의 유출로 인한 소비자 피해는 비금융거래 관련 데이터에 비해 더 클 수 있다. 한편 빅데이터 분석 알고리즘의 부적절한 사용이나 오류로 인해 특정 소비자에게 높은 금융서비스 비용을 부과하거나 특정 소비자에게 해당 금융서비스 제공을 거절하는 결과를 초래할 수도 있다. 전통적으로 보험회사는 데이터 분석을 기반으로 리스크를 평가하고, 보험료를 책정하는 등 주요 의사결정에 데이터를 활용해 왔으나, 다량의 새로운 데이터와 빅데이터 분석 기술의 활용, 클라우드 컴퓨팅이나 외부 제3자 아웃소싱 이용으로 인해 데이터 보유와 분석 관련 소비자 리스크를 야기할 가능성이 커졌으므로 보험회사는 동 분야의 리스크 대응의 중요성이 가장 클 것으로 예상된다.

둘째, 2021년 3월부터 시행된 금융소비자보호법 등 일련의 금융소비자 보호 규제는 온라인 환경을 충분히 반영하지 못했다는 평가가 있었으나, 이를 보완하기 위해 금융당국과 금융산업은 「온라인 설명의무 가이드라인」을 마련하는 등 디지털 금융소비자에 대한 보호의 사각지대를 줄이기 위해 노력하고 있다. 온라인 채널을 이용한 보이스피싱이나 투자사기 등 신종범죄도 새롭게 나타난 소비자 관련 리스크라고 할 수 있는데, 주로 대출이나 투자 분야에서 많이 발생하고 있어서 보험 분야에 있어서 관련성은 다른 금융권역과 비교하여 상대적으로 적은 것으로 판단된다. 다만 현재까지는 보험시장에서 온라인 판매채널 비중은 적은 편이지만, 향후 온라인 판매채널의 확대를 고려할 때, 소비자의 인지편향이나 행동과학적 특성을 이용하여 소비자에게 바람직하지 않은 결정을 하도록 유도하는 다크패턴 이용을 방지할 필요가 있으며, 판매 과정뿐만 아니라 광고나 소셜미디어를 이용한 마케팅에서 나타날 수 있는 다크패턴을 이용한 불공정 영업 관행을 점검하고 개선할 필요가 있다. 한편 최근 빅테크 플랫폼이나 라이브커머스 플랫폼에서 보험판매자들이 광고를 하고 댓글이나 연락처 공유를 통해 보험상품을 판매하는 행태가 늘어나고 있는데, 이 과정에도 소비자의 행동편향이나 부주의, 착각 등을 유도하여 불필요한 상품구매를

유도하거나 소비자의 합리적인 의사결정을 방해하는 현상이 종종 발생하고 있다. 새로운 매체를 통해 이루어지는 광고에 대한 심의 절차나 점검 절차가 마련되어 있지 않아 이에 대한 대응이 필요하다.

마지막으로, 금융의 디지털화로 인해 나타난 새로운 취약계층과 관련된 문제이다. 금융시장 전반적으로 볼 때, 디지털 금융거래가 디지털 기기를 기반으로 이루어지다 보니 디지털 취약계층의 서비스 접근성이 저하될 수 있는데, 최근 은행 점포 수 감소로 인해 디지털 거래에 익숙하지 않은 고령소비자가 불편함을 겪는 사례가 이에 해당한다.

그러나 보험시장의 경우, 예·적금, 투자 등에 비해 금융의 디지털화로 인한 고령 소비자의 소외문제는 크지 않은 것으로 보인다. 대면 판매채널이 중요한 역할을 하고 있고, 보험금청구의 경우에도 모바일이나 온라인 청구 이외에 다른 방법을 사용할 수 있고, 대부분의 경우 담당 설계사의 도움으로 보험금을 청구하는 사례가 많기 때문이다. 다만 빅데이터 분석 기술의 발전이 위험집단을 더 자세히 세분화할 수 있도록 할 것이며, 위험에 기초한 보험료 책정 기술도 더 향상시킬 것으로 예상된다. 이 과정에서 높은 보험료나 인수거절로 인해 기존에 보험에 가입하지 못했다가 보험에 가입할 수 있게 되는 소비자가 생기는 반면, 위험집단이 세분화 되면서 높은 보험료로 인해 보험에 가입하지 않게 되는 고위험 소비자도 생길 가능성은 존재한다(EIOPA, 2019).

〈표 II-11〉 국내 보험시장에서의 디지털화 관련 소비자보호 이슈

구분	내용
데이터 보유 및 분석	<ul style="list-style-type: none"> • 사이버리스크 증가 • 클라우드 컴퓨팅, AI 분석 관련 제3자 아웃소싱 • 데이터 수집 및 활용 • 데이터 분석 알고리즘
기술 발전과 법·규제 간 격차	<ul style="list-style-type: none"> • 온라인 상에서의 6대 판매원칙 준수 • 디지털 금융범죄 • 다크패턴
취약계층	<ul style="list-style-type: none"> • 고령 소비자 디지털 소외 • 위험집단 세분화로 인한 고위험자의 보험료 상승

III

금융의 디지털화 관련 해외 소비자정책

본장에서는 최근 금융의 디지털화를 반영하여 최신화된 금융소비자보호 원칙과 비교적 활발한 논의가 진행되고 있는 소비자 데이터 수집 및 활용, AI 분석 및 이용, 디지털 취약 계층 보호 등과 관련된 국제적 논의와 제도를 검토하도록 한다.

1. OECD/G20 금융소비자보호 상위원칙

OECD는 G20 정상회의를 통해 “금융소비자보호에 대한 상위원칙(G20/OECD High-Level Principles on Financial Consumer Protection)”을 2011년 10월에 제안했으며, 이후 상위원칙을 꾸준히 업데이트한 결과, 현재 해당원칙은 12대 상위원칙으로 구성되어 있다(<표 III-1> 참조).

<표 III-1> G20/OECD 금융소비자보호 상위원칙

원칙	내용
1	법적, 규제적, 감독적 체계(Legal, Regulatory, and Supervisory Framework) 마련
2	감독 기관의 역할(Role of Oversight Bodies) 강화
3	접근 및 포용(Access and Inclusion)
4	금융 이해력 및 인식(Financial Literacy and Awareness)
5	경쟁(Competition)
6	소비자에 대한 공평하고 공정한 대우(Equitable and Fair Treatment of Consumer)
7	공시와 투명성(Disclosure and Transparency) 강화
8	양질의 금융상품(Quality Financial Products)
9	금융서비스 제공자 및 중개업체의 책임 있는 사업 운영(Responsible Business Conduct of Financial Services Providers and Intermediaries) 강화
10	소비자 자산의 사기 및 오용으로부터의 보호(Protection of Consumer Assets against Fraud and Misuse) 강화
11	소비자 데이터 및 개인정보 보호(Protection of Consumer Data and Privacy) 강화
12	불만 처리 및 구제(Complaints Handling and Redress) 절차 접근성 제고

자료: OECD(2024)

또한, OECD는 디지털 금융거래가 점차 활성화되면서 디지털 금융환경에 적합한 금융소비자 보호체계 구축을 주요한 주제로 삼아 앞서 언급한 기존 상위원칙을 디지털 금융환경에 적용할 수 있도록 수정 및 보완한 새로운 원칙을 제시하였다. 새로운 원칙은 기존 원칙 중 2번인 감독기구의 역할 강화, 7번인 공시와 투명성 강화, 10번 사기 및 오남용으로 부터 금융소비자 자산보호, 11번 금융소비자 데이터 및 프라이버시 보호 강화를 디지털 금융거래 환경에 맞춰 재해석함에 초점이 맞춰져 있다.

〈표 Ⅲ-2〉 디지털 시대에 맞춘 G20/OECD 금융소비자보호 상위원칙의 재해석

원칙	내용
2	<ul style="list-style-type: none"> • 감독기구는 새로운 상품, 채널, 사업자에 관한 시장검토 및 연구를 통해 금융시장에 대한 적절한 지식을 갖췄는지 확인할 것 • 감독기구는 디지털 금융 환경에 적합한 감독수단 및 도구를 갖추고 있는지 확인할 것 • 감독기구는 디지털 금융 환경에서 효율적 그리고 유연적으로 작동하는 자원 및 능력을 갖출 것 • 감독기구는 기술혁신 및 발전을 다룰 수 있을 것 • 감독기구는 데이터보호 및 경쟁을 점검할 수 있는 내부조직을 갖출 것 • 감독기구는 소비자권익을 위한 혁신적 접근 및 사업모형을 추구하는 새로운 사업자에게 적용될 규제체계에 대한 지침을 제공할 것 • 감독기구는 기존 규제를 재평가할 것 • 감독기구는 특정 리스크를 수반하는 국경 간 거래를 가능케 하는 디지털 채널을 통한 금융서비스에 대해 적절한 소비자보호 조치가 이뤄지는지 확인할 것
7	<ul style="list-style-type: none"> • 공시 및 투명성 조건이 디지털 금융서비스에 관한 정보 전달에 적용 가능하고 적절한지 확인할 것 • 소비자 소통이 소통채널과 관계없이 투명하고 간결할 것 • 디지털 금융서비스 관련 기존 공시 요건에 대해 평가할 것 • 소비자 의사결정 및 행동 편향성에 대한 이해 • 디지털 금융서비스가 다양한 화면크기, 소통포맷 등을 고려해 해당 공시가 효과적으로 이뤄질 수 있도록 함 • 비례적이며 고객 중심적인 관점에서 소비자에게 효과적으로 전달될 수 있는 공시 방법을 평가하고 연구할 것 • 디지털 금융서비스 제공자의 공시 실행을 모니터링할 것 • 고객 프로파일, 목적, 금융이해력에 근거해 자문이 실행되고 있는지 확인할 것 • 기술발전, 데이터 이용가능성 및 접근이 기존 공시 체계를 평가하고 대안적인 체계를 생성하는지 고려할 것 • 데이터 수집, 저장, 활용과 관련된 공시정책과 관련해 소비자 동의에 대한 요청방식이 명확하고 가능한 이해가 되는 방식일 것
10	<ul style="list-style-type: none"> • 정책 입안자와 감독 당국은 금융서비스 제공자가 시행하는 조치를 감독하는 데 필요한 기술 역량, 자원 및 감독 도구를 확보할 것 • 정책 입안자와 감독 당국은 업계, 기타 규제 및 감독 당국, 법 집행 기관(디지털 보안 정책 수립, 이행, 정보 공유 및 동향 모니터링을 담당하는 기관 포함)과 협력하여 정보를 공유하고 새로운 유형의 디지털 금융 사기 및 사기와 관련된 새로운 동향을 파악할 것

〈표 Ⅲ-2〉 계속

원칙	내용
10	<ul style="list-style-type: none"> • 정책 입안자와 감독 당국은 국경을 넘나드는 디지털 금융 사기 및 사기에 대한 정보와 첩보를 공유하기 위해 해외 대응 기관 및 관련 국제기구 및 네트워크와 협력할 것 • 정책 입안자와 감독 당국은 업계, 디지털 보안 및 법 집행 기관과 협력하여 보이스피싱에 사용된 전화번호를 식별 및 차단하거나 잠재적인 유해 이메일을 식별하기 위해 인공지능을 사용하는 등 금융소비자를 대상으로 하는 사기행위를 탐지하고 대처하기 위한 기술 혁신의 역할을 모색할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체와 협력하여 사기 또는 무단 거래에 대한 금융 소비자의 책임 제한 규정이 새로운 유형의 모바일 또는 온라인 거래(예: '푸시 결제')로 확대 적용될 수 있도록 할 것 • 정책 입안자와 감독 당국은 다른 정부 및 규제 기관, 디지털 보안 기관, 법 집행 기관, 금융서비스 업계, 유틸리티 회사 등 관련 이해관계자와 협력하여 디지털 보안 위험에 대한 대중의 인식을 높이고 안전한 온라인 및 디지털 거래를 장려하기 위한 캠페인을 운영하거나 참여할 것 • 정책 입안자와 감독 당국은 위험, 취약성, 사고 및 완화 조치를 포함한 디지털 보안 위험에 대한 경험 공유를 촉진하기 위해 기관 및 업계 간의 네트워크 또는 실무 커뮤니티 구축에 참여하거나 이를 고려해야 할 것 • 감독 당국은 불만 처리 데이터와 분석을 통해 잠재적인 보안 침해/사고, 위험 및 금융서비스 제공업체가 채택한 모범 사례를 파악할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체가 적어도 매년 정기적으로 결제 서비스 관련 사기 활동에 대한 통계 데이터를 감독 당국에 보고하도록 요청할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체가 제공하는 서비스에 대한 디지털 보안 위험을 지속적으로 평가하고, 위험을 줄이기 위해 적절한 보안 조치를 채택하며, 온라인 사기 위험을 최소화하기 위해 채택해야 하는 보안 절차를 금융소비자에게 알릴 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체가 보안 목표, 역할 및 책임 등을 정의하는 디지털 보안 위험 관리 프레임워크를 갖추고 있는지 확인할 것. 이 프레임워크는 문서화, 승인 및 주기적인 검토를 거쳐야 할 것. 보안 위험 프레임워크에는 금융서비스 제공자가 제3자 제공자에게 디지털 서비스 제공 또는 활동을 아웃소싱하는 경우, 제3자 제공자의 사이버 복원력에 대한 적절한 평가가 포함되어야 할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체가 위험과 취약성을 모니터링하고 정의된 위험 시나리오를 정기적으로 검토(즉, 주기적인 위험 관리 프로세스)하도록 할 것. 보안 관련 고객 불만을 포함한 보안 사고를 일관되고 통합적으로 모니터링, 처리 및 후속 조치를 취해야 할 것 • 금융서비스 제공업체는 디지털 금융 상품이나 서비스를 계약할 때 충분히 강력한 고객 인증 메커니즘을 구현할 것. 여기에는 고객 인증 및 보안 조치를 강화하기 위한 기술 혁신 탐색(예: 이중 인증 방법 사용)이 포함될 수 있음 • 정책 입안자와 감독 당국은 금융서비스 제공자가 금융소비자를 위해 무단 또는 사기 거래, 비밀번호와 같은 인증 메커니즘 위반, 액세스 장치 또는 토큰 분실 등을 신고할 수 있는 효과적인 이고 편리한 절차를 마련하도록 할 것 • 정책 입안자, 감독 당국 및 금융서비스 제공업체는 확인된 위협이나 사기에 대해 고객에게 경고를 보내는 SMS 메시지와 같은 기술 사용을 고려할 것

〈표 Ⅲ-2〉 계속

원칙	내용
11	<ul style="list-style-type: none"> • 정책 입안자와 감독 당국은 금융소비자 보호를 위한 법적, 규제 및 감독 프레임워크에 금융서비스 제공업체와의 거래와 관련된 소비자 데이터 및 개인정보 보호, '개인 데이터'의 정의 포함. 일부 관할권에서는 이 프레임워크의 관리가 금융 또는 기타 국가 소비자 보호 또는 기타 당국의 책임일 수 있으며, 다른 관할권에서는 전담 개인 데이터 보호 당국의 책임이거나 둘 다의 책임일 것 등이 포함되어 있는지 확인할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체와 협력하여 (1) 정보 수집 및 사용 관행을 투명하게 하고, (2) 소비자가 적절한 시기와 상황에서 자신의 데이터에 대한 의사 결정을 내릴 수 있도록 장려할 것 • 금융소비자 보호를 담당하는 정책 입안자 및 감독 당국은 데이터보호 당국이 존재하는 경우 해당 당국과 연락하여 금융서비스 제공업체에 대한 데이터보호 법률 및 규정을 이해하고 적용하도록 할 것. 여기서 금융서비스 제공자는 금융상품 또는 서비스와 관련하여 개인 데이터의 수집, 저장 및 사용에 대한 동의 요청이 관련 시기와 맥락에서 정보에 입각한 동의를 보장하기 위해 명확하고 이해하기 쉽도록 해야 할 것. 동의 요청은 지나치게 법률적, 기술적 또는 전문적 성격의 언어나 용어를 사용하지 않아야 할 것 • 정책 입안자 및 감독 당국은 다른 정부 및 규제 기관, 법 집행 기관, 금융서비스 제공업체 등 관련 이해관계자와 협력하여 데이터 프라이버시 보호를 포함한 안전한 온라인 거래를 장려해야 할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체와 함께 소비자가 핀테크 기업을 포함한 공인된 제3자와 금융거래 데이터를 공유할 수 있도록 하는 방안을 모색해야 할 것. 다만, 개인정보 보호 및 데이터 보안 문제가 이러한 혁신에 장애가 되어서는 안 되며, 이는 혁신적인 금융관리 서비스(예: 오픈뱅킹 또는 기타 금융 도구)의 개발을 촉진하고 이를 통해 더 큰 금융포용을 지원할 수 있을 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체가 개인화된 금융 상품과 서비스를 개발하기 위해 금융소비자 데이터를 사용하는 것을 모니터링할 것. 이러한 개인화는 개인의 필요에 따라 금융상품과 서비스를 더욱 맞춤화할 수 있지만, 정책 입안자와 감독 당국은 이러한 개발이 불법적인 차별이나 배제의 위험을 초래하지 않도록 모니터링할 것 • 정책 입안자와 감독 당국은 금융서비스 제공업체가 디지털 기능(예: AI, 알고리즘, 머신러닝 기술)의 사용과 관련하여 강력하고 투명한 거버넌스, 책임, 리스크 관리 및 통제 시스템을 갖추도록 할 것 • 감독 당국은 금융서비스 제공업체가 배포하는 디지털 기능을 감독하고 이해할 수 있는 기술 역량, 리소스 및 도구를 확보할 것. 금융서비스 제공자. 이러한 역량은 자체적으로 개발하거나 필요한 전문 지식을 제공할 수 있는 관할 구역 내의 다른 공공기관에 아웃소싱할 수 있을 것 • 정책 입안자와 감독 당국은 신용 평가와 같은 자동화된 의사 결정 모델을 사용하는 금융서비스 제공업체가 자동 거절과 같은 무책임하거나 부적절한 결과를 방지할 수 있는 조치를 취하도록 해야 할 것 • 금융서비스 제공업체는 개인정보 보호 친화적인 기본 설정을 사용하거나 최소한의 개인정보만 최소한의 기간 동안 수집 및 저장하는 등(즉, "개인정보 보호 설계") 금융 상품 또는 시스템을 설계할 때부터 개인정보 보호 기능을 포함시키는 것을 고려할 것(즉, "데이터 최소화")

자료: OECD(2018); OECD(2020)

2. 데이터 수집 및 활용 관련 논의

가. 국제적 논의

G20은 2018년 개인 및 기업의 디지털금융 포용력을 촉진하기 위한 주요 정책적 제안을 제시하였는데, 이중에서도 소비자 데이터 보호와 관련해서는 ① 안전하고 효과적인 동의 모델을 개선할 것, ② 접근·정정·취소 및 의의 제기권(이하 'ARCO 권리'라 함) 강화, ③ 데이터 보안 강화를 강조하였다.³⁷⁾

구체적으로 내용을 살펴보면, 우선 안전하고 효과적인 동의 모델을 개선하기 위해서 1) 규제 당국은 업계 참여자들이 '설계에 의한 개인정보 보호' 접근 방식을 채택하도록 장려해야 하며, 데이터 수집의 최소화를 고려해야 한다. 2) 특정 유형의 데이터 처리 또는 특정 목적에 따라 소비자에게 다양한 유형의 동의를 요구하는 계층형 동의 개념을 도입하는 것이 적절할 수 있다. 3) 또 다른 대안으로는 동의의 유효기간을 설정할 수 있다. 4) 옵트아웃(opt-out) 동의가 아닌 옵트인(opt-in) 동의는 규제 기관이 선호하는 옵션이 될 수 있다. 5) 업계 참여자(및 데이터 소스)는 소비자로부터 수집한 동의의 증거를 기록해야 할 책임이 있다. 6) 정책 입안자와 업계 참여자는 대체 데이터의 예측 능력을 테스트하고 검증하며, 데이터가 공정하게 사용되고, 대체 데이터를 사용하여 개발된 채점 모델이 소수자나 보호 대상 그룹에 중립적인지 확인하기 위한 조치를 채택할 수 있다 등을 제시하였다.

또한, ARCO 권리 강화와 관련해서는 1) ARCO 권한은 디지털 금융서비스의 맥락에서 특히 중요하다. 2) 최소한 소비자가 자신의 데이터에 액세스할 수 있도록 허용하는 것은 데이터 보호법이 시행되고 있는 국가에서 널리 받아들여지고 있는 원칙이다. 3) 소비자에게는 자신의 데이터를 수정할 수 있는 옵션이 제공되어야 한다. 4) 소비자에게는 특정 목적을 위해 자신의 정보를 사용하는 것과 관련하여 결정할 수 있는 권리가 주어져야 한다 등을 제시하였다.

데이터 보안 강화와 관련해서는 1) 데이터는 핵심 자산이 되고 있으며 개인 데이터와 신원 도용은 소비자들에게 큰 위협이 되고 있다. 2) 규제 당국은 금융서비스 제공업체가 데이터 손실, 손상, 파괴, 무단 액세스, 조작 또는 오용을 방지하기 위한 보안 조치를 채택하도록 장려할 수 있다. 3) 사이버 보안 평가는 모든 서비스 제공업체 또는 데이터 제공업

37) G20(2018)

체의 전반적인 위험 관리 정책 및 절차의 일부가 되어야 한다. 4) 규제 당국은 국경을 넘나드는 데이터의 이점을 활용하기 위해 지속적으로 노력해야 한다 등을 제시하였다.

나. EU 일반정보보호규정(General Data Protection Regulation; GDPR)

우리나라에서는 데이터의 사회적 및 경제적 가치가 커짐에 따라, 개인의 권리 강화와 데이터 경제 활성화를 위해 2020년에 금융 분야를 중심으로 ‘마이데이터’가 도입되었다. 이와 관련하여 해외 정책 동향 중 가장 많이 언급되는 것은 2018년 유럽연합(EU)의 GDPR(일반 데이터 보호 규정) 시행이다. EU는 GDPR에 개인정보 이동권을 신설함으로써 정보를 제공하는 주체가 개인정보 자기결정권을 행사할 수 있는 법적 근거를 마련했다.

EU GDPR의 정식 명칭은 “개인정보의 처리와 관련된 자연인의 보호 및 그 정보의 자유로운 이전과 지침 95/46/EC를 폐지하는 2016.4.27. 유럽의회 및 유럽이사회의 2016/679 규정”이며 이를 줄여서 일반정보보호규정(GDPR)로 불리운다. GDPR은 개인정보의 처리와 관련된 개인 보호 및 개인정보의 자유로운 이동을 규율하는 것을 목표로 하며(제1조 제1항), 자연인의 기본권과 자유, 특히 개인정보 보호에 대한 권리를 보장하고 있다(제1조 제2항).

GDPR은 개인정보 삭제권, 이동권, 거부권, 처리 제한권 등과 같은 개인의 정보관리 권한을 새롭게 규정하여 이전보다 정보주체의 권리를 강화했다. 또한, 개인정보를 처리하는 기업에게는 이러한 처리활동의 기록과 DPO(Data Protection Officer: 개인정보보호 책임자)의 지정, 개인정보 영향평가 등을 하도록 규정하여 기업의 책임을 강화시켰다. 개인정보이동과 관련해서는 GDPR 제20조 개인정보보호권(The Right to the protection of personal data)에 개인정보이동권(Right to data portability)을 포함시켜 이를 정보주체가 ① 정보관리자(Controller)에게 제공한 본인 개인정보를 구조화하고, 통상적으로 사용되며, 기계 판독이 가능한 형식으로 수령하며, ② 원하는 경우 정보관리자의 방해 없이 다른 정보관리자에게 전송할 수 있는 권리와, ③ 기술적으로 실현 가능한 경우에 한해서 해당 정보를 한 정보관리자에게서 다른 정보 관리자에게 직접 전송되도록 요구할 수 있는 권리를 규정하고 있다. 동 규정에 적용 대상이 되는 개인정보는 본인이 제공한 정보로 동의했거나 계약이행을 위한 것이며, 자동화된 수단에 의해 처리가 이뤄지는 정보에 한해 정의된다. EU GDPR의 개인정보 이동권은 온라인 서비스에 대한 정보주체의 선택권 강화, 서비스 제공자 간 공정한 경쟁환경 조성, 개인정보보호 법제의 단일화를 통해 EU 역

내 디지털 경제를 보다 활성화하고자 하는 목적으로 도입된 것이다. 또한, 정보주체인 개인이 기존 기업들이 보유하고 있는 개인정보 통제에 대한 주도권을 돌려받고, 이를 기반으로 여러 곳에 산재해 있던 자신의 데이터를 통합적으로 관리하고, 개인에게 유리한 서비스를 찾을 수 있게 되면서 개인정보 활용 방식의 패러다임을 변화시킬 수 있게 되었다.³⁸⁾

3. AI 관련 논의 및 조치

가. 국제적 논의³⁹⁾

AI와 관련하여 국제적 합의가 시작된 것은 2019년 5월에 OECD에 의해 채택된 OECD AI 권고안이 제시한 AI 원칙(OECD AI Principles)이라고 할 수 있다. 신뢰할 수 있는 AI의 책임감 있는 관리를 위한 원칙으로서 포용적 성장 및 지속가능개발, 인간 중심 가치 및 공정성, 투명성 및 설명 가능성, 견고성 및 안전성, 책임성을 제시하였는데, 2019년 6월 G20 정상 선언 부속서에 G20 AI 원칙(G20 AI Principles)으로 통합되었다.

한편 UNESCO의 AI 윤리에 대한 권고안(Recommendation on the Ethics of Artificial Intelligence)은 최초의 AI 윤리 관련 국제 기준으로서 2021년 11월 기준으로 193개국에서 채택하였다. 동 권고안은 필요한 정책적 행동을 윤리적 효과 평가, 윤리적 지배구조 및 관리, 데이터 정책, 개발 및 국제적 협력, 환경 및 생태계, 젠더(Gender), 문화, 교육 및 연구, 소통 및 정보, 경제 및 노동, 건강 및 사회 후생 등 11개 분야로 나누어 제시하였다.⁴⁰⁾

이후 2023년, 히로시마에서 있었던 G7 정상회의에서 포용적 AI 지배구조(Governance)와 AI 지배구조 체계 간 상호운용성(Interoperability)에 대한 국제적 논의를 진행시키는 ‘히로시마 AI 프로세스’를 수립하기로 합의하였다. 의장국인 일본은 G7 국가들을 대상으로 생성형 AI의 기회와 위험, 정책 우선순위, 기존 정책 계획 및 예정되어 있는 정책 계획 등에 대한 설문조사를 실시하고 결과를 분석하였다.⁴¹⁾

38) 노현주(2021)

39) Kobayshi, Shinya(2023)

40) UNESCO(2021)

41) OECD(2023)

나. EU AI법

AI 규제 체계구축에 있어서는 EU가 선두에 있다고 할 수 있는데, 개발자(Developer 또는 Provider)나 배포자 또는 사용자(Deployer 또는 User)에게 AI의 특정 사용에 대한 명확한 요건과 의무를 규정하는 AI법안을 마련했고, 최종안을 올해 3월 13일 유럽의회 본회의에서 가결하였다.⁴²⁾ 유럽 이사회의 최종 점검 후 유럽연합 관보에 게재되면 20일 후에 발효되고, 기간을 두고 단계적으로 적용될 예정이다. EU는 동법을 'AI 혁신 패키지'와 'AI에 대한 조직화된 계획'과 함께 신뢰할 수 있는 AI 개발을 지원하는 일련의 정책 조치들 중 일부라고 설명한다. AI법은 최초의 AI에 대한 종합적인 법체계라고 할 수 있다.

EU AI법의 주요 내용은 첫째, AI법은 AI가 야기하는 위험을 허용할 수 없는 위험, 고위험, 제한적 위험, 최소한의 위험으로 나누어 접근한다.⁴³⁾ 허용할 수 없는 위험을 야기하는 AI는 금지되며, 대부분의 내용은 고위험 AI를 다루고 있다. 둘째, 대부분의 의무는 고위험 AI 체계 개발자에게 해당되는데, EU에서 고위험 AI 체계를 출시하거나 서비스를 제공하려는 기업은 동 법이 규정하는 의무를 이행해야 한다. 셋째, 동법에서는 사용자(Developer)는 영향을 받는 최종 사용자가 아닌 전문가로서 AI 체계를 배포하는 자연인이나 법인이다. 고위험 AI 체계의 사용자는 개발자보다는 약하지만 일정 정도의 의무를 진다. 넷째, 범용 AI(General Purpose AI; GPAI)과 관련해서는 모든 범용 AI 모형 개발자는 기술 문서, 사용 설명서를 제공하고, 저작권 지침을 준수하며 교육에 사용할 내용에 대한 요약을 제시해야 한다. 또한 시스템 리스크를 야기하는 모든 범용 AI 개발자들은 모형 평가, 대립적 테스트(Adversarial Testing) 수행, 심각한 사고의 추적 및 보고, 사이버 보안 보호의 의무를 진다.⁴⁴⁾

특기할 만한 점은 AI법이 고위험 AI로 분류한 사례에는 금지되지 않은 생체인식, 주요 인프라, 교육 및 직업 훈련, 고용, 근로자 관리 및 자영업에 대한 접근, 필수적인 사적 서비스 및 공공 서비스에 대한 접근 및 이용, 법 집행, 이민, 국경 통제 관리, 사법행정 및 민주적 절차가 포함되는데, 필수적인 사적 서비스와 관련해서 건강보험과 생명보험의 위험 평가 및 보험료 책정도 이에 해당된다.

42) 여기서 개발자는 AI 체계와 모델을 만드는 사람과 조직을, 배포자는 AI 도구를 사용하는 사람 및 조직을 의미함. 예를 들어, AI 챗봇을 구매하고 사용하여 고객 서비스 문의를 처리하는 조직은 배포자가 됨(IBM, "유럽연합 인공지능법(EU AI Act)이란 무엇인가요?")

43) European Commission, "AI Act"

44) EU Artificial Intelligence Act(2024. 2. 27), "High-level summary of the AI Act"

다. 영국 AI 규제 이행 및 AI 규제방안

영국 정부는 2023년 3월 AI 규제 백서를 통해 AI 규제에 있어 혁신 친화적인 접근을 제시하였다. 동 접근은 규제당국들이 해석하고 적용할 수 있는 규제방향을 i) 안정, 보안, 견고성, ii) 적절한 투명성 및 설명가능성, iii) 공정성, iv) 책임감과 지배구조, v) 경합성 및 보상 등 다섯 가지 원칙으로 제시하였다. 영국 과학혁신기술부(Department for Science, Innovation and Technology; DSIT)는 AI 규제 이행에 대한 최근 보고서를 통해 규제 당국이 상기 원칙들을 고려하고 그에 대한 도구와 지침 마련을 시작할 수 있도록 규제당국들을 지원하고자 하였다.⁴⁵⁾ DSIT는 4 단계로 나누어 지침을 제공할 예정인데, 동 보고서가 1단계 지침에 해당한다. 2단계에서는 규제당국들과 이해당사자들로부터 받은 피드백을 바탕으로 더 자세한 내용을 제공함으로써 1단계 지침을 반복하고 확장할 계획이며 2024년 여름에 발표할 예정이라고 밝혔다. 3단계에서는 감독당국들과 협력하여 잠재적인 공동 수단 및 지침이 필요한 분야를 식별하고, 추가 정보나 자원이 필요한 곳을 찾고, 공동의 해결책을 찾을 수 있는 분야를 식별할 계획이다.

또한, 영국 중앙은행(Bank of England)과 건전성 규제당국(Prudential Regulation Authority; PRA)은 2024년 4월, 그들의 규제 권한 내에서 안전하고 책임감 있는 AI 및 머신러닝을 제공하기 위한 작업을 발표하였는데, AI 및 머신러닝 관련 규제 체계에 대한 추가적인 명확화가 필요할 수 있는 네 가지 잠재적 영역(데이터 관리, 모형 리스크 관리, 지배구조, 운영 회복력과 제3자 리스크)을 검토 중이라고 밝혔다. 중앙은행과 PRA는 FCA와 함께 포괄적인 3차 '영국 금융서비스 분야에서의 머신러닝' 설문조사를 실시할 계획이며, 올해 AI 및 머신러닝이 금융 안정성에 미칠 잠재적 영향에 대해 심층 분석을 진행 중이다.

그동안 영국 중앙은행과 PRA는 2019년과 2022년에 금융서비스 분야의 머신러닝 도입과 사용에 대한 보고서를 발표하였으며, 2020년부터 2022년까지 FCA와 함께 AI 공공-민간 포럼(AI Public-Private Forum; AIPPF)을 운영하여 금융서비스 내에서 AI 및 머신러닝 사용 관련 과제를 검토하고 이 주제에 대한 공공 부문과 민간 부문 간의 소통을 시작하였다.

한편 FCA는 올해 4월 AI Update라는 보고서를 통해 AI 규제에 있어서 기술에 구애받지 않는(Technology-Agnostic), 원칙 중심, 결과에 초점을 둔(Outcomes-Focused) 접근을 취한다고 밝혔으며, 현존하는 FCA의 규제들을 영국 정부의 AI 백서의 5개 원칙에 적용하

45) Department for Science, Innovation, and Technology(2024)

여 제시하였다.⁴⁶⁾ 같은 보고서에서 FCA는 향후 규제가 리스크에 비례하도록 하는 동시에 유익한 혁신을 위한 체계를 만들고자 한다고 밝히고, 향후 1년 동안의 계획을 다음과 같이 밝혔다. 먼저 영국 금융시장에서의 AI 활용을 검토 분석하여 AI의 혜택과 위험을 균형 있게 고려함으로써 AI의 금융서비스 활용에 대해 비례적이고 효과적인 접근을 취하고자 한다. 중앙은행과 지급결제서비스 규제당국(Payment Services Regulator; PSR)와 함께 머신러닝 설문조사를 통해 회사들이 현재 AI 관련 전략을 어떻게 전개하고 있는지 이해하고 관련 위험은 무엇인지 식별하고자 할 계획이다. 또한 AI 모형 검증, 유효성, 설명가능성에 초점을 맞추고, 개방성과 투명성으로 운영하는 기업문화에 의해 강화된 강력한 책임원칙을 요구할 예정이라고 밝혔다. 더 넓은 기술 맥락, 아웃소싱된 위험, 사이버 보안 및 회복력(빅테크에 대한 정책 작업 및 중요 제3자(CTP)에 대한 규제 체계 포함)의 맥락에서 AI 규제를 고려할 계획이다. 특히, FCA는 운영 회복력, 아웃소싱 및 중요한 제3자 관련 규제 제도가 기업의 안전하고 책임감 있는 AI 사용과 관련성이 높아질 것이라고 설명했다. 국내외 협력과 관련해서는 디지털 규제 협력 포럼(DRCF) 회원 규제 기관과의 협력을 통해 파일럿 AI 및 디지털 허브, 합성 데이터를 통해 기술을 검증할 수 있는 FCA 디지털 샌드박스, 그리고 FCA가 인증하는 규제 샌드박스를 제공할 예정이고, 영국 은행, PSR, DRCF 및 IOSCO 및 FSB와 같은 국제 및 글로벌 동료들과 계속 협력할 계획이라고 밝혔다.

라. 미국 NAIC의 AI 원칙 채택

미국보험감독자협의회(National Association of Insurance Commissioners; NAIC)는 2020년에 AI 체계를 개발하거나 활용하는 보험회사와 관련 이해당사자에 대한 가이드의 기초가 되는 AI 원칙(the Principles of Artificial Intelligence)을 채택하였는데, 동 원칙은 AI의 공정하고 윤리적 활용의 중요성, 책임, 주 법률 및 규정 준수, 투명성, 안전하고 공정하며 강건한 체계를 강조한다.⁴⁷⁾ NAIC는 2023년 12월 AI 체계 사용 관련 모델 가이드라인(NAIC Model Bulletin: Use of Artificial intelligence Systems by Insurers)⁴⁸⁾을 발표하였는데, 동 가이드라인은 보험회사들이 특정 AI 기술의 개발, 구입, 활용을 어떻게 통제, 관리할 것인지에 대한 보험감독당국의 기대와 고려사항을 제시하고, AI 기술

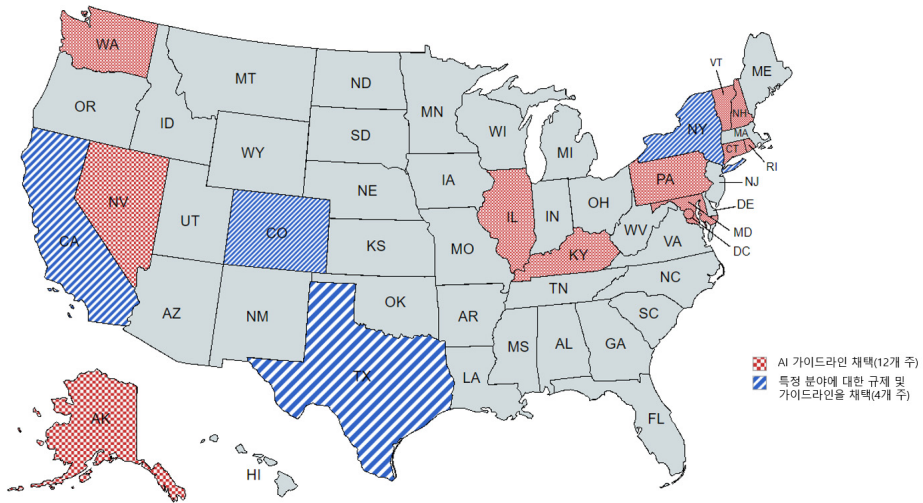
46) FCA(2024)

47) NAIC(2020. 8. 14), "National Association of Insurance Commissioners(NAIC) Principles on Artificial Intelligence (AI)"

48) NAIC(2023. 12. 4), "NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers"

이나 체계 사용과 관련하여 보험회사를 조사하거나 검사하는 동안 보험감독당국이 요구할 수 있는 정보와 문서에 대해 설명한다.⁴⁹⁾ 동 가이드라인에 따르면, 보험회사는 AI 체계 활용이 불공정한 거래 행태나 불공정한 보험금 지급 행태를 야기하지 않도록 보장하는 지배구조 체계와 리스크관리 규약(Protocol) 등의 관행을 채택해야 하며, 모든 손해보험(P&C) 상품에 있어서 AI 기술이나 예측모형을 사용하여 개발한 보험요율, 보험요율 책정 규칙 등이 지나치거나 불충분하거나 불공정하게 차별적인 보험요율을 만들어내지 않도록 할 책임을 진다. 특히 동 가이드라인은 보험회사가 AI 체계 활용으로 인해 소비자에게 부정적인 영향을 줄 수 있는 리스크를 경감시키기 위해 설계된 문서화된 프로그램(AI System Program: AIS Program)을 마련, 시행, 유지하게 하는데, AIS 프로그램은 지배구조, 리스크관리 통제, 내부감사 기능 등에 대한 내용을 포함해야 한다. 2024년 6월 기준으로 12개 주가 동 모델 가이드라인을 채택했으며, 이 중 4개 주는 모델 가이드라인 내용 중 특정 분야에 대해 채택하였다.

〈그림 III-1〉 NAIC AI 모델 가이드라인 채택 주



자료: <https://content.naic.org/sites/default/files/cmte-h-big-data-artificial-intelligence-wg-ai-model-bulletin.pdf>

49) NAIC(2023. 12. 4), “NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers”; 김가현 (2024)

4. 디지털 취약계층 보호 관련 논의

가. 국제적 논의

G20는 포용적 금융⁵⁰⁾ 실천의 일환으로 금융소외계층 포용을 위한 글로벌 파트너십(Global Partnership for Financial Inclusion: GPFI)를 중심으로 고령 금융소비자 보호 이슈를 다루고 있으며, 2019년 2월에 고령화와 포용적 금융을 위한 ‘G20 후쿠오카 Policy Priority’를 발표하였다.⁵¹⁾

‘G20 후쿠오카 Policy Priority’는 고령화 대응을 위한 8개 정책과제를 포함하고 있으며, 이 중 고령자의 디지털 금융 거래와 관련해서는 금융환경 변화에 대응하기 위해 고령자에게 필요한 기술과 지식을 제공할 필요성을 강조하고 있다. 연령별 비교에서 고령자의 금융 이해도가 낮다는 점을 지적하고 있으며, 고령자의 특성과 디지털 및 모바일 금융 환경의 변화를 고려하여 맞춤형 지원이 필요하다는 점을 강조하고 있다. 이를 위해 온라인 교육, 민간기업의 연수, SNS, 지역 내 금융교육 네트워크 등과 같은 금융지식 전달 수단을 다양화할 필요가 있으며, 고령자의 안전한 디지털 금융서비스 이용을 위한 교육을 실시해 디지털 활용역량을 강화할 필요가 있음도 언급하고 있다.

또한, 금융교육, 금융상품 개발, 소비자보호 등 실시에 있어 기술을 최대한 활용해 고령자의 금융접근성 확대에 기여할 것을 언급하고 있다. 휴대전화와 인터넷을 통해 디지털 금융서비스가 이용되고 있는 가운데, 고령자의 디지털 금융 접근성이 다른 연령층에 비해 낮는데, 특히, 고령자는 종이 명세서와 현금·대면 거래 등 기존의 거래 형태를 선호함에 따라 디지털 금융서비스 이용에 어려움을 겪고 있음을 지적하고 있다. 따라서 정책당국은 신체·본인인증 관련 최신 기술을 도입해 신체장애 고객 등의 자립을 지원하거나, 알고리즘 기술을 통해 고객의 실수·오해로 발생하는 전형적인 행동 패턴을 파악하거나 잠재적 부정거래를 특정해 사고 발생을 사전에 방지할 필요가 있으며, 고령자가 활용하기 쉬운 디지털 수단을 활용해 금융상품 선택과 재무목표 달성을 지원할 필요가 있음을 강조했다.

50) G20는 포용적 금융을 “모든 경제주체가 제도권 금융회사가 제공하는 다양한 금융서비스(저축, 지급결제, 신용, 보험 등)에 접근이 가능한 상태”로 정의함

51) 예금보험공사(2020)

나. 개별 국가의 정책적 대응

개별 국가 차원에서 디지털 취약계층 보호를 위한 정책적 대응이 있다. 우선 미국은 고령층 보호를 위해 경제성장, 규제완화 및 소비자보호법(Economic Growth, Regulatory Relief, and Consumer Protection Act)에서 고령자의 금융자산 착취를 엄격하게 규제하고 있다. 또한, 금융 착취로부터 고령 소비자를 보호하기 위한 모델법(NASAA Model Act to Protect Vulnerable Adults from Financial Exploitation)에서는 금융 자문업자, 중개인, 투자 자문업자 등을 포함한 금융 회사가 65세 이상의 고령 금융 소비자를 상대할 때, 금융 자산 착취가 이루어졌다는 합리적인 확신이 있을 경우, 이를 금융 당국과 성인 보호 서비스(Adult Protective Services)에 보고할 의무를 부여하고 있다. FINRA Rule 2165는 금융 자문업자 및 중개인이 고객의 금융 자산에 착취가 있었다는 합리적인 확신이 있을 경우, 고객 계좌에서 자금인출을 일시적으로 유보할 수 있도록 허용하고 있다. 게다가 CFPB(Consumer Financial Protection Bureau)의 노인 재정보호국(Office of Financial Protection for Older Americans)은 고령자를 대상으로 금융 사기를 예방하고 인식할 수 있는 금융 교육을 설계하며, 간병인이나 이해관계자에 의한 재정 착취를 방지하기 위한 네트워크 개발을 강화하는 등 다양한 정책과 연구 및 교육 이니셔티브를 제공하고 있다.⁵²⁾

일본에서는 일본 증권업협회가 ‘고령 투자자에 대한 권유 및 판매에 대한 지침’을 통해 신체적 쇠약이나 이해력 저하 등 취약한 특성을 가진 고령층을 보호할 필요성을 인식하고, 고령 금융소비자를 위한 가이드라인을 제공하고 있다. 또한, 금융청은 ‘금융상품거래업자 등을 위한 종합적인 감독 지침’을 통해 고령 금융 소비자에 대한 보호 모니터링 규정을 제시하고 있다. 이 지침에 따르면, 금융회사는 고령 고객에 대한 권유 및 판매와 관련된 사내 규칙을 정비하고, 상품 판매 후에도 고령 고객의 입장에서 상담과 투자 판단을 지원하거나 지속적으로 모니터링하는 등 후속 조치를 실시하도록 요구하고 있다.⁵³⁾

영국 FCA에서는 취약 금융소비자에 대한 공정한 대우를 위한 지침을 마련하고 있다. 취약금융소비자(Vulnerable Customer) 보호를 강화하기 위한 지침의 주요 내용은 금융회사가 취약 고객의 필요를 이해하고 적절히 대응하며, 고객의 취약 상태를 파악해 지원과 상품 설계의 적절성을 판단해야 한다는 것이다. 또한, 금융상품 및 서비스를 제공할 때는

52) 신경희(2021)

53) 신경희(2021)

고객에게 필요한 상품인지 여부를 고려하고, 금융 피해를 방지하기 위해 고객의 배우자나 가족 구성원의 연락처를 작성하도록 권장하고 있다. 게다가 취약 고객과의 의사소통은 명확하고 이해하기 쉽게 하며, 제공된 정보와 이해 여부를 확인하도록 요구하고 있다.⁵⁴⁾

54) 신경희(2021)

IV

금융소비자 보호를 위한 과제

앞서 살펴본 것처럼 금융의 디지털화에 따른 소비자 권익 강화를 위한 국제적 논의가 상당히 진행되었고, 개별 국가 차원에서도 관련 정책을 마련하거나 추진 중에 있는 것으로 보인다. 따라서 정책당국은 OECD/G20 금융소비자 상위원칙 및 재해석의 큰 틀 안에서 우리나라 금융산업의 디지털화 관련 소비자 보호체계가 국제적 정합성에 부합하는 방향으로 가는지 지속적으로 점검할 필요가 있다. 또한, 우리나라와 타국가 간의 디지털화의 정도와 소비자관련 정책기조 및 특성의 차이가 있어 모든 해외사례를 벤치마킹 할 필요는 없겠으나, 보다 촘촘한 디지털금융 소비자 정책으로 나아가기 위해서 데이터 수집 및 활용, AI 활용, 디지털 취약계층 해소 관련 국제적 논의 및 개별 국가의 정책적 움직임을 꾸준히 모니터링할 필요가 있다.

한편, OECD, G20, IAIS, EU 등 국제기구에서 마련한 디지털 금융소비자 보호 관련 정책 지침 및 핵심원칙을 요약하면, 우선 데이터 및 개인정보 보호와 관련해서는 금융회사의 소비자 데이터 수집 및 사용 관행의 투명성 확보, 금융당국과 정보보호 당국 간의 협력, 금융회사의 데이터 사용 모니터링 체계구축, AI 사용 관련 내부통제시스템 구축을 G20/OECD에서 주요 정책지침으로 제시하였다.⁵⁵⁾ 또한, 비대면 보험상품 판매와 관련해서는 IAIS에서 보험핵심원칙을 개정해 보험계약의 모든 과정에서 고객을 공정하게 대우해야 한다는 영업행위 원칙을 보험회사는 물론 모집중사자에게도 적용하도록 했다.⁵⁶⁾ 다음으로 소비자 자산보호 측면에서는 기술적 능력, 자원, 감독 도구 보유, 사기행위 감시 및 퇴치를 위한 기술 보유, 사기성 거래에 대한 금융소비자의 책임제한 제도의 온라인 거래 적용을 주요 정책지침으로 제시했으며, 취약계층 포용과 관련해서는 금융교육의 중요성을 강조했다.⁵⁷⁾

국제기구에서 마련한 정책 관련 주요 권고사항은 국내 감독 당국에서 대부분 반영한 것으로 평가되고 있다.⁵⁸⁾ 게다가 현재 우리나라는 데이터 및 개인정보보호, 기술발전과 소

55) OECD(2018)

56) 서병호(2023)

57) OECD(2018)

비자보호 법·규제 간 격차, 취약계층에 걸쳐 법, 시행령, 감독규정, 가이드라인, 정책 및 방안 등이 거의 빠짐없이 구성된 디지털 금융소비자 보호체계를 갖춘 것으로 보인다 (<표 IV-1> 참조). 따라서 일차적인 정책과제로는 이러한 소비자 보호체계가 원활하고 빈틈없이 작동하도록 관련 부처의 책임 강화, 관련 부처 간 정책공조, 금융회사 애로 사항 및 금융소비자 실태조사에 근거한 정책 개선 등이 필요할 것이다.

<표 IV-1> 국제기구의 디지털 금융소비자 보호 관련 원칙과 국내 디지털 금융소비자 보호 관련 법규 및 조치

구분	국제기구의 핵심원칙	국내 디지털 금융소비자 보호 관련 법규 및 조치
데이터 관련 위험	<ul style="list-style-type: none"> • G20/OECD 제11원칙 • IAIS ICP19 영업행위 	<ul style="list-style-type: none"> • 개인정보보호법 • 전자금융거래법 • 신용정보법 • 금융분야 개인정보보호 가이드라인 • 금융분야 AI 가이드라인 • 금융분야 AI 보안 가이드라인
기술발전과 소비자보호 법·규제 간 격차	<ul style="list-style-type: none"> • G20/OECD 제7원칙 • IAIS ICP19 영업행위 	<ul style="list-style-type: none"> • 금융소비자보호법 시행령 • 금융소비자보호법 감독규정 • 온라인 설명의무 가이드라인
	<ul style="list-style-type: none"> • G20/OECD 제10원칙 	<ul style="list-style-type: none"> • 본인계좌 일괄 지급정지 서비스 • 통신사기피해환급법 개정안 • 금융거래 안심차단 서비스
취약계층	<ul style="list-style-type: none"> • G20/OECD 제3원칙 및 제4원칙 	<ul style="list-style-type: none"> • 고령자 친화적 모바일 금융앱 구성지침 • 은행 점포폐쇄 내실화 방안

주: G20/OECD 금융소비자보호 상위원칙

제3원칙: Access and Inclusion

제4원칙: Financial Literacy and Awareness

제7원칙: Disclosure and Transparency

제10원칙: Protection of Consumer Assets against Fraud, Scams and Misuse

제11원칙: Protection of Consumer Data and Privacy

자료: OECD(2018); IAIS(2019); OECD(2020); OECD(2024)

1. 데이터 관련 위험 대응

데이터 관련 위험 대응과 관련해 세부적인 정책과제는 다음과 같다. 먼저 금융회사는 데이터 보유량이 증가함에 따라 사이버공격에 의한 개인정보 유출, 기술사고 등으로 인한 피해 가능성이 커질 가능성에 대비해 사이버 리스크 관리에 보다 만전을 기울일 필요가 있다. 이에 따라 데이터보안 사고 후 처리절차 등 데이터 보안정책이 제대로 작동하고 있는지 지속적으로 점검할 필요가 있고, 보안기술의 도입 및 직원 교육 등으로 자체적인 보안 역량을 강화해야 하며, 리스크관리의 요소로 포함되는 사이버보안 평가도 보다 철저히 이뤄지도록 해야 한다. 또한, 정책당국도 디도스(DDos), 랜섬웨어, 피싱, 음성분석, 딥페이크 등 더욱 정교하고 복잡한 기술로 다양하게 이뤄지고 있는 사이버보안 위협에 대응할 수 있는 가이드라인을 마련한 후 권고함으로써 금융회사의 해당 리스크 관리 및 예방 역량 강화에 기여할 필요가 있다.

한편, 2020년 8월 개인정보의 활용을 촉진하기 위해 「개인정보보호법」, 「신용정보법」, 「정보통신망법」 등 데이터 3법이 개정되었다. 가명정보 개념 도입 및 비동의 방식의 정보 처리 허용, 개인정보의 추가적인 이용 허용, 데이터결합 근거 조항 마련, 마이데이터 산업 도입 및 개인 신용정보 이동권 도입 등으로 금융회사의 디지털금융서비스 개발 및 제공을 위한 데이터 활용의 폭이 보다 커질 수 있게 되었다. 다만, 금융회사가 다른 금융회사 및 비금융회사의 소비자 정보 활용 시 개인정보 이동권이 주요 쟁점이 될 수 있다. 여기서 개인정보 이동권은 EU GDPR에서 제시하고 있는 개인정보이동권에 해당하는 개인신용정보의 전송 요구권을 의미한다.⁵⁹⁾ 앞서 3장 3절에서 언급한 것처럼, 개인정보 이동권은 정보 주체가 제공한 개인정보를 구조화된 형식으로, 통상적으로 사용되며 기계 판독이 가능한 형태로 받을 권리와, 원하는 경우 정보 관리자의 방해 없이 다른 정보 관리자에게 전송할 수 있는 권리를 의미한다. 또한, 기술적으로 가능한 경우에는 해당 정보를 한 정보 관리자에서 다른 정보 관리자에게 직접 전송되도록 요구할 수 있는 권리도 포함된다. GDPR의 정보이동권과 우리나라의 정보이동권과의 큰 차이는 전자는 개인정보 전체를

59) 신용정보법 제33조의2에 명시된 개인신용정보의 전송요구권은 신용 정보주체인 개인이 금융회사, 공공기관 등에 제공한 본인의 개인신용정보를 본인이나 본인신용정보관리회사, 개인신용평가회사 등에게 전송하여 줄 것을 요구할 수 있는 권리를 규정한 것임. 적용 대상이 되는 정보는 컴퓨터 등 정보처리장치로 처리된 개인신용정보를 의미하며, 기업은 컴퓨터 등 정보처리장치로 처리가 가능한 형태로 제공해야 함. 기존 제공동의 기반의 정보제공 방식은 사업자(기업)가 제3자에게 정보제공할 의사를 가지고 요청하면, 고객(개인)은 단지 동의 여부만 결정할 수 있었던 데 반해 전송요구권은 개인이 의지를 가지고 사업자에게 실행하도록 요구하는 것으로, 전송 정보, 제공받는 대상 등을 스스로 결정할 수 있음

대상으로 하는 반면에 후자는 개인신용정보에 관해 이동권을 적용한다는 것이다(노현주, 2021). 비록 개인신용정보는 개인의 신용도와 신용거래 능력을 파악하기 위한 정보로 예를 들어 성명, 주민등록번호 등을 통해 개인을 식별할 수 있는 정보만을 의미하고 있지만, 정책당국은 회사 간 소비자정보 이동에 있어 명확하지 않거나, 논쟁의 여지가 있는 부분이 있다면 관련 지침을 마련하여 소비자 정보보호를 강화할 필요가 있다.

다음으로 금융회사가 소비자의 개인정보 수집과 활용에 대해 동의를 구할 때, 소비자가 내용을 알고 동의(Informed Consent)할 수 있도록 돕는 방안을 논의하는 과정에서 표준화된 동의 형식, 순차적 동의, 유효기간 설정이나 선택적 동의방식 등이 소비자의 주의집중과 동의 내용에 대한 이해도를 높이는 방법으로 제시된 바 있다.⁶⁰⁾ 개인정보 수집 및 활용 관련 정보를 제공하더라도 소비자가 알고 동의하는 것이 실질적으로 어렵다는 현실을 감안하여, 개인정보를 수집하는 기관이 관련 서비스나 상품을 설계할 때 개인정보 보호를 고려해야 한다는 견해나 데이터집적을 최소화하기 위해 반드시 필요한 데이터만을 수집하도록 하는 제도를 마련해야 한다는 견해도 있다. 금융당국도 향후 금융회사의 개인정보 수집 및 활용 방식 개선 방안을 마련할 때 이러한 방안 및 견해를 참고할 필요가 있다.

〈표 IV-2〉 개인정보 수집 및 활용 동의방식 개선방안

구분	금융소비자 보호체계
순차적 동의 (Tiered Consent)	<ul style="list-style-type: none"> • 특정 목적이나 특정 종류의 데이터 이용에 따라 소비자의 동의도 구별함으로써 소비자가 공유 데이터의 종류와 자신의 정보 접근을 허락하는 서비스 제공자를 선택할 수 있도록 하는 방법 • 예를 들어 서비스 사용을 위해 필수적인 항목과 부차적인 항목을 구별하여 제시하고 선택적으로 동의하도록 함
동의 유효기간 설정	<ul style="list-style-type: none"> • 동의의 효과에 유효기간을 정하여 해당 정보의 수집 및 이용에 제한을 두는 방법
선택적 동의 (Opt-in Consent)	<ul style="list-style-type: none"> • 동의를 기본 설정으로 하고 선택적으로 비동의하는 형식을 취하는 대신, 선택적으로 동의하는 형식을 사용 • 참고: EU GDPR Recitals 32
개인정보 보호를 고려한 설계 (Privacy by Design)	<ul style="list-style-type: none"> • 개인정보 보호를 위한 기술, 절차, 실행방안들을 처음부터 시스템 설계의 일부로 포함

60) 변혜원(2023)

〈표 IV-2〉 계속

구분	금융소비자 보호체계
데이터집적 최소화 (Data Minimization)	<ul style="list-style-type: none"> • 데이터 이용 목적에 반드시 필요한 데이터만을 수집하도록 하는 방법 • 예를 들어 감독당국이 리스크평가를 위한 개인정보 수집의 경우 리스크평가와 관련 있는 주요 데이터 항목을 식별하고 해당 데이터들이 특정 상황에서만 집적되고 사용되는지 확인하거나, 금융회사가 해당 데이터 항목이 리스크평가 목적에 관련이 있다고 감독당국에게 입증하도록 하는 방법을 사용할 수 있음 • 참고: EU GDPR 5.(1)(C)

주: Privacy by Design란 1990년대에 Ann Cavoukian에 의해 처음 소개된 개념으로서, EU GDPR에 'Privacy by Design'이라는 개념으로 적용됨

자료: OECD(2020); GPF(2018)

또한, 우리나라 금융당국은 「금융분야 개인정보보호 가이드라인(2017)」이나 「정보보호 내실화 방안(2018)」 등을 통해 개인정보 수집 및 활용 동의방식 개선을 위한 방안을 제시하였다. 「금융분야 개인정보보호 가이드라인(2017)」에는 개인신용정보 처리시 수집 최소화 원칙, 개인정보 활용 동의 시 필수, 선택 정보를 구분, 정보주체의 본인 정보 삭제 요구권, 마케팅 용도 신용정보 활용 시 별도 사전동의 의무화 등의 내용이 반영되었다. 또한, 금융당국은 2018년 「금융분야 데이터활용 및 정보보호 종합방안」을 발표하였고, 금융분야 빅데이터 활성화, 금융분야 데이터 산업 경쟁력 제고, 정보보호 내실화를 3대 추진전략으로 제시하였다. 이 중 2018년 5월에 발표한 「정보보호 내실화 방안」은 정보활용 동의제도 실질화, 다양한 개인정보 자기결정권 보장 강화, 금융권 정보보호 및 보안 강화 방안을 제시하고 있는데, 내용 단순화, 수집정보 민감도 등을 반영한 정보 수집항목 별 등급 부여, 정보활용기관 설명 등을 보여주는 정보활동 동의서 양식 사례를 제공하였다(〈그림 IV-1〉 참조). 따라서 금융회사는 금융당국이 발표한 이러한 가이드라인 및 정책방안의 세부 사항을 적극적으로 준수해 개인정보 수집 및 활용 과정 관련 소비자 보호를 강화할 필요가 있다.

〈그림 IV-1〉 정보활용 동의서양식안

필수	<p style="text-align: center;">개인(신용)정보 수집·이용에 관해 동의하시겠습니까?</p> <p style="text-align: center;"><input type="checkbox"/> 동의 <input type="checkbox"/> 동의안함</p> <hr/> <p> 개인식별번호(성명, 주민등록번호 등)를 제공해야 해요 상세보기</p> <p> 보험금 지급, 심사 등 민원처리 및 금융거래 시 필요해요</p> <p> 계약 정보, 사고 정보, 질병 관련 정보를 조회해요</p> <p> 청구서류접수대행서비스 및 사고조사 시 필요해요</p>
선택1	<p style="text-align: center;">결제내역 PUSH 알림 서비스를 제공 받으시겠습니까?</p> <p style="text-align: center;"><input type="checkbox"/> 동의 <input type="checkbox"/> 동의안함</p> <hr/> <p> 적정</p> <p> 전화번호 제공해야 해요 상세보기</p> <p> PUSH서비스를 제공받을 수 있어요</p>
선택2	<p style="text-align: center;">상품개발 및 연구에 개인정보 활용 동의를 하시겠습니까?</p> <p style="text-align: center;"><input type="checkbox"/> 동의 <input type="checkbox"/> 동의안함</p> <hr/> <p> 비교적 적정</p> <p> 개인정보(8건)와 민감한 정보(6건)를 제공해야 해요 <small>(연락처, 주거형태, 소득 정보 등)</small> 상세보기</p> <p> 금리0.3% 를 우대받을 수 있어요</p>
선택3	<p style="text-align: center;">고객만족도 조사를 위해 제3자 제공에 동의하시겠습니까?</p> <p style="text-align: center;"><input type="checkbox"/> 동의 <input type="checkbox"/> 동의안함</p> <hr/> <p> 신중</p> <p> 개인정보(4건)와 민감한 정보(4건)를 AA리서치회사로 전달되요 <small>(연락처, 주거형태, 소득 정보 등)</small> 상세보기</p> <p> 부가 서비스를 이용할 수 있어요</p> <p> 타 업체로부터 상담전화가 올 수 있어요</p>
선택4	<p style="text-align: center;">상품개발 및 연구에 개인정보 활용 동의를 하시겠습니까?</p> <p style="text-align: center;"><input type="checkbox"/> 동의 <input type="checkbox"/> 동의안함</p> <hr/> <p> 매우 신중</p> <p> 개인정보(4건)와 민감한 정보(4건)를 2개 업체에 제공해야 해요 <small>(연락처, 주거형태, 소득 정보 등)</small> 상세보기</p> <p> 경품 이벤트에 지원자격이 생겨요</p> <p> 타 업체로부터 홍보메일 및 가입전화가 올 수 있어요</p>

자료: 금융위원회 보도자료(2018. 5. 10), “금융분야 개인정보보호 내실화 방안”

아울러 금융회사의 AI 활용과 관련해서도 「금융분야 AI 가이드라인」 및 「금융분야 AI 보안 가이드라인」 준수 관련 금융회사 내부 원칙, 준수 모니터링을 위한 내부 통제시스템 등을 갖춰 가이드라인 준수를 통해 소비자 보호가 효과적으로 이루어질 수 있도록 조치할 필요가 있다. 특히, 동 가이드라인에 따라 AI 시스템이 데이터 학습을 통해 운영되는 점을 고려해 금융회사는 AI 학습데이터의 품질 검증·개선 및 최신성이 잘 유지 되는지 주기적

으로 점검해야 하며, AI가 사생활 정보, 민감정보 등을 활용하는 경우 비식별 조치 등 충분한 안전조치 후 개인정보가 활용되는지 혹은 AI모델이 잠재적 공격 또는 개인정보 유출 등으로부터 안전한지 평가해 보안성을 지속적으로 검증할 필요가 있다.

한편, II장에서 살펴본 바와 같이 금융의 디지털화가 소비자에게 심화시키거나 새롭게 초래할 수 있는 리스크 중 보험회사는 데이터 보유 및 분석과 관련된 리스크에 대한 대응이 가장 시급하고 중요하다고 판단된다.

먼저 보험회사는 전통적으로 민감정보를 포함한 고객데이터를 보유하므로 과거부터 외부 공격에 의한 고객 정보 유출이나 시스템 오류로 인한 전산장애 등 사이버리스크를 점검하고 대비해 왔다. 그러나 보험의 디지털화로 인해 데이터량 자체가 많아졌을 뿐 아니라, 빅테크나 다른 기술기업 등 제3자 아웃소싱이나 클라우드 컴퓨팅 활용 확대로 인해 보험회사의 시스템과 외부 회사와의 접촉점이 많아지면서 사이버 공격이 진입할 수 있는 기회도 늘어날 것으로 예상된다. 또한 API나 클라우드 컴퓨팅 등에 대한 의존도가 높아질수록 금융권역내 또는 비금융권역과의 상호연결성(Interconnectivity)이 증가하면서 사이버 위협에 대한 노출도 확대될 수 있다. 따라서 보험회사는 이러한 변화에 유의할 필요가 있으며, 특히 아웃소싱이나 클라우드 컴퓨팅 등 제3자 리스크관리를 강화해야 할 것이다.

다음으로 앞서 언급한 금융회사의 개인정보 수집 및 활용 관련 대응과제와 같은 맥락에서 보험회사도 「금융분야 개인정보보호 가이드라인」, 「정보보호 내실화 방안」 등에서 권고하는 사항들을 준수할 필요가 있으며, 특히 소비자의 알고 하는 동의(Informed Consent)를 도울 수 있도록 현존하는 개인정보 수집 및 활용 동의 형식을 개선할 필요가 있는데, 「정보보호 내실화 방안」에서 제시한 개선안을 참고할 수 있다. 아울러 앞서 언급한 사이버리스크 확대나 정보보안을 위한 규제가 강화되는 추세를 고려할 때, 반드시 필요한 데이터에 집중하고 데이터집적을 최소화할 필요가 있다.

보험회사의 AI나 머신러닝 등 빅데이터분석 활용으로 인해 발생할 수 있는 소비자보호 관련 리스크를 최소화하기 위해서는 빅데이터분석과 관련된 회사 내 AI 정책을 수립하고, 인간의 감독을 통해 분석모형 결과를 인간이 검토하고 수정·보완하는 절차를 마련해야 할 것이다. AI 거버넌스나 AI 위험관리정책 등과 관련해서는 「금융분야 AI 가이드라인」을 참고할 수 있을 것이며, 보험료 책정 및 언더라이팅 등을 위한 AI 분석 모형 리스크관리에 대해서는 「AI 신용평가모형 검증체계」를 참고할 수 있다. 특히 AI 거버넌스 수립에 있어서 외부 개발 모형을 사용하거나 아웃소싱을 하는 경우가 늘어나는 만큼 AI 모형의 개발

자, 소유자, 사용자 간의 책임과 역할을 확실히 할 필요가 있다. 아울러 회사 내 구성원들이 분석모형의 한계와 리스크를 이해하고, 분석결과에서 잠재적 오류를 식별할 수 있도록 관련 교육과 훈련도 필요하다. 또한 「금융분야 AI 가이드라인」은 AI를 통해 금융계약체결 여부 결정될 경우 소비자가 이에 대한 설명요구권과 정정요구권(프로파일링 대응권)이 있음을 안내하도록 하고 있는데, 이러한 권리행사가 불편함 없이 제대로 이루어질 수 있도록 해야 할 것이다.

2. 기술발전과 소비자보호 법·규제 간 격차

비대면 금융상품 판매 관련해서는 기존 금융소비자보호법 시행에 있어서 디지털 금융거래와 관련된 소비자 보호 의무의 보완을 위해 온라인 적정성 가이드라인을 마련할 필요가 있다. 서병호(2023)의 제안처럼 온라인 설명의무 가이드라인과 유사한 민관합동 방식으로 온라인 적정성 가이드라인을 마련하는 방안이 있으며, 적정성 의무의 온라인 환경에서 적절한 이행을 위해 챗봇이나 채팅을 통해 기본적인 정보(고객 동의 시 마이데이터 정보 포함)을 수집한 이후, 금융소비자가 필요한 정보를 제공했는지, 상품 구매 의도가 무엇인지 등을 확인하는 절차를 통해 적정성을 평가한 이후 적정하지 않을 경우 동 사실을 알리는 시스템 도입을 검토할 필요가 있다. 다만, 시스템 도입에 따른 금융회사의 비용 부담 문제, 동의된 개인정보의 오남용 문제 발생 등이 걸림돌이 될 수 있어 이에 대해 충분히 논의할 필요가 있다.

또한, 금융상품 설명이나 광고에 소비자에게 불리한 판단을 유도할 수 있는 요소가 있어서 이를 점검하고 개선할 수 있는 조치 내지는 가이드라인을 추가적으로 마련할 필요가 있다. 다크패턴 문제와 관련해서는 정책당국이 밝힌 것처럼 금융회사에 적용되는 자율관리 가이드라인을 조속히 마련해 규제공백 해소로 인한 소비자 피해를 최소화할 필요가 있다.

금융회사는 디지털 금융거래에 있어서 전자금융사기, 금융 범죄 등에 소비자가 노출되어 피해를 입을 경우 이에 대한 대응을 신속히 할 필요가 있으며, 이를 예방하기 위한 노력도 적극적으로 수행할 필요가 있다. 현행 전자금융거래법에 따르면 접근 매체의 위·변조나 거래수행 과정에서 발생한 사고에 대하여 소비자의 고의·과실과 상관없이 금융회사에 손해를 배상할 책임을 지우고 있다.⁶¹⁾ 또한, 보이스피싱 등 비대면 금융사고가 발생하여

소비자에게 금전적 손해가 발생할 경우 '비대면 금융사고 책임분담 기준'에 따라 금융회사는 소비자에게 손해를 배상할 수 있다.⁶²⁾ 이러한 사용자책임 부담 강화에 대응하기 위해서 전자금융사기 및 금융범죄 관련 손해배상업무를 전문적으로 담당할 상시적인 부서 설치를 검토할 필요가 있고, 업무상황을 꾸준히 모니터링할 필요가 있으며, 이상거래 모니터링 등 금융사고 예방활동도 적극적으로 수행해 실제 혹은 잠재적 소비자 피해를 최소화할 필요가 있다. 이러한 노력은 금융소비자보호 실태평가 및 금융소비자 중심 경영 인증을 통해 금융회사에 직접적으로 긍정적인 영향을 미칠 수 있을 것이며, 해당 노력을 적극적으로 수행하는 금융회사에 정부 포상 수여를 검토한다면, 금융회사의 보다 적극적인 소비자 피해대응 프로세스가 유도될 수 있을 것이다.

한편, 보험회사는 최근 빅테크 플랫폼이나 라이브커머스 플랫폼을 통해 광고를 하고, 보험상품을 판매하는 사례가 늘고 있는데, 이러한 광고들은 방송심의나 보험협회의 금융광고 심의를 받지 않으므로 금융광고 요건을 준수하지 않을 가능성이 높아 소비자피해를 야기할 가능성이 있다. 현재 금융소비자법은 금융광고 필수기재사항과 금지사항을 규정하고 있고, 금융상품판매업자 등은 금융광고를 하기 위해서는 준법감시인의 사전심의를 받도록 하고 있다(시행령). 또한, 협회 등 자율규제기관은 금융소비자법에 근거하여 금융상품판매업자 등이 금융광고 관련 규제를 준수하고 있는지 사전심의, 사후점검 등을 실시하고 있다. 그러나 빅테크 플랫폼이나 라이브커머스 플랫폼을 이용하는 광고에 대한 심의 절차나 점검에 대한 절차가 마련되어 있지 않아 이에 대한 대응이 필요한데, 상품광고에 대해서는 사전심의 및 사후점검, 업무광고는 영상 녹화본과 스크립트를 사후심의하는 방안을 검토해 볼 수 있겠다(변혜원 외, 2023).⁶³⁾

61) 전자금융거래법 제9조

62) 금융감독원 보도자료(2023. 10. 5), "비대면 금융사고 예방 추진을 위한 협약 체결"

63) 「금융광고규제 가이드라인」에 따르면 판매광고는 금융상품의 내용, 거래조건, 그 밖의 거래에 관한 사항을 소비자에게 널리 알리거나 제시한 행위를, 업무광고는 자문 서비스에 관한 광고와 금융거래 유인 관련 업무에 관한 광고라고 설명함. 보험협회에서는 상품광고, 판매방송(홍소핑), 상품이미지광고, 대출광고 등을 판매광고로, 금융상품에 관한 계약 체결을 유인할 목적으로 소비자에게 제공하는 서비스에 관한 광고를 업무광고라고 정의함

3. 취약계층

앞서 2장에서 식별한 4대 금융취약 계층의 포용과 관련해서는 영국 및 일본 사례를 참조해 정책당국 주도하에 장애인, 고령층, 저소득층, 농어민 등에 대한 디지털 금융거래 관련 지침을 마련해 보다 실제적이며, 예측 가능한 정책을 모색할 필요가 있다. 또한, 이들 계층에 대한 실태조사를 통해 디지털 채널에 대한 접근성 강화를 위한 개선방안도 함께 마련할 필요가 있다. 금융교육과 관련해서도 현재 금융감독원이 운영 중인 금융피해 고위험계층 대상으로 찾아가는 금융교육서비스인 ‘금융사랑방버스’ 프로그램을 더욱 확대해 취약계층에 대한 교육을 강화할 필요가 있다.

한편, 은행 점포폐쇄에 따른 은행서비스 접근성 문제에 대응하여 금융위는 작년 4월 은행권 경영·영업 관행·제도 개선 실무작업반을 통해 「은행 점포폐쇄 내실화 방안」을 발표하였는데, 동 방안은 점포 폐쇄 전에 사전영향 평가를 하고, 점포를 폐쇄할 경우에는 공동점포, 소규모점포, 이동점포, 창구제휴 등 대체점포를 마련하도록 했다.⁶⁴⁾ 또한, 최근에는 국민통합위원회 포용금융으로 다가서기 특별위원회는 전국에 점포를 보유한 우체국에서 현재 수행하고 있는 단순 은행업무 범위를 확대하여 다양한 은행서비스를 제공할 수 있도록 은행대리업 도입 추진을 제안하기도 하였다. 다만, 이러한 노력에도 불구하고 은행 점포 감소세는 지속될 것으로 예상되는 바 고령층 금융거래 불편이나 금융소외 경감을 위한 노력을 금융회사 차원에서 지속할 필요가 있다. 특히, 인구고령화가 심화되면서 고령층 디지털 소외현상이 더욱 가중될 것으로 예상됨에 따라 ‘G20 후쿠오카 Policy Priority’에서 논의된 내용을 참조해 소외 해소를 위한 민관 합동 방식의 정책방안을 추가로 마련할 필요가 있다. 이를 위해 정책당국은 민간 금융회사 및 지역사회와의 협력을 통해 고령자의 디지털 금융이해력을 높일 수 있는 교육 프로그램을 개발해 제공하는 것을 검토할 필요가 있으며, 고령자의 디지털 금융서비스 이용 장벽을 해소할 수 있는 기술을 적극적으로 개발하는 금융회사에는 정부 차원의 포상 검토 등을 통해 해당 금융회사의 적극적인 노력을 이끌어낼 필요가 있다.

64) 국민통합위 보도자료(2024. 7. 18), “국민통합위, 서민을 위협하는 불법사금융 엄정 대응 추진한다”

금융산업의 디지털화로 인해 전통적 금융서비스와 기술이 결합해 소비자에게 새롭고 다양한 형태의 금융서비스가 제공되고 있으며, 그 결과 소비자의 편의성 및 접근성 개선, 시장혁신을 통한 금융소비자 효용 증진 등이 예상되고 있다. 반면, 데이터 저장 및 데이터 기반 금융서비스 제공, 규제 사각지대 및 법규 미비, 소외계층 측면에서 소비자 피해가 우려되거나 금융소비자 보호 이슈가 논의되고 있는 상황이다.

디지털 금융과 관련해 소비자 보호에 대한 위험요소는 우선 데이터 측면에서 사이버리스크, 데이터 유출, 데이터분석 알고리즘 부당 사용 및 오류 등이 있고, 기술발전에 따른 소비자보호 규제 및 법간 격차 측면에서는 금융소비자보호법의 미비, 디지털 금융범죄, 다크패턴 등의 문제가 발생할 수 있으며, 취약계층 측면에서는 소비자 간의 디지털 격차 발생, 고령 소비자의 디지털 소외 문제 등이 주요 위험요소로 식별되었다.

이와 같은 소비자보호 위험요소에 대응하기 위한 과제는 우선 데이터 및 개인정보 보호, 비대면 금융상품 판매, 소비자 자산 보호, 취약계층 포용 영역에서 구축된 기존 소비자 보호체계가 원활하고 빈틈없이 작동할 수 있도록 관련부처의 책임강화, 관련부처 간 정책공조, 금융회사 애로 사항 및 금융소비자 실태조사에 근거한 정책 개선 등이 필요할 것이다.

보다 세부적인 과제로는 금융회사의 사이버리스크 관리 강화, AI 및 개인정보 보안 관련 가이드라인 및 정책방안의 준수, 정책당국의 복잡하고 다양한 보안위협에 대응할 수 있는 가이드라인 및 회사 간 소비자 이동 관련 지침 마련, 정책당국의 금융회사 개인정보 수집 및 활용방식 개선 방안 마련, 정책당국의 온라인 적정성 가이드라인, 다크패턴 자율 관리 가이드라인 마련, 금융회사의 소비자피해 대응 프로세스 강화 및 정책당국의 유인 제공, 4대 금융취약계층 디지털금융거래 관련 지침 마련 및 실태조사 실시, 금융사랑방버스 프로그램 확대, 은행 점포폐쇄에 대비한 고령층 금융소외 문제 해소 등을 통해 소비자 위험요소에 대한 정책당국과 금융산업의 대응 역량을 강화할 필요가 있다.

〈표 V-1〉 금융의 디지털화 관련 대응과제

구분	대응과제	보험산업 대응과제
데이터 보유 및 분석	<ul style="list-style-type: none"> • 금융회사의 사이버리스크 관리 강화, AI 및 개인정보 보안 관련 가이드라인 및 정책방안의 준수 • 정책당국의 복잡하고 다양한 보안위협에 대응할 수 있는 가이드라인 및 회사 간 소비자 이동 관련 지침 마련 • 정책당국의 금융회사 개인정보 수집 및 활용방식 개선 방안 마련 	<ul style="list-style-type: none"> • 정보보안 및 제3자 리스크관리 강화 • 개인정보 수집·활용 동의형식 개선, 데이터집적 최소화 • AI 정책(거버넌스, 위험관리 등) 수립, 구성원 교육, 소비자의 프로파일링 대응권 행사 체계 점검
기술 발전과 법·규제 간 격차	<ul style="list-style-type: none"> • 정책당국의 온라인 적정성 가이드라인, 다크패턴 자율관리 가이드라인 마련 • 금융회사의 소비자피해 대응 프로세스 강화 및 정책당국의 유인 제공 	<ul style="list-style-type: none"> • 디지털 채널 인터페이스 점검 • 신매체 광고심의 및 점검체계 점검
취약계층	<ul style="list-style-type: none"> • 4대 금융취약계층 디지털금융거래 관련 지침 마련 및 실태조사 실시 • ‘금융사랑방버스’ 프로그램 확대 • 은행 점포폐쇄에 대비한 고령층 금융소외 해소 	-

본 연구는 점차 빠르게 진행되고 있는 금융의 디지털화와 관련해 소비자 관점에서 위험요소와 대응과제를 모두 제시하였다는데 의의가 있다. 다만, 보험의 디지털화에 따른 위험요소에 대한 대응과제 도출을 보다 충분하게 담지 못했다는 한계점이 있다. 이를 향후 우리나라 보험산업의 디지털화가 가속화되는 정도에 따라 위험요소가 보다 다양해지고, 구체화되면 진행할 수 있는 후속 연구로 남긴다. 마지막으로 금융산업의 디지털화는 현재완료형이 아닌 진행형이므로 그 진행되는 정도에 따라 새롭게 등장할 위험요소를 식별하고 평가하며, 이에 대한 대응책을 마련하는데 본 연구가 주요하게 참조될 수 있기를 바란다.

참고문헌

- 강동수·오윤해(2022), 「금융혁신과 원칙중심 소비자보호체계」, 『연구보고서』, 한국개발연구원
- 과학기술정보통신부·한국지능정보사회진흥원(2021), 『2020년 인터넷이용 실태조사』
_____ (2023), 『2022년 디지털정보격차 실태조사』
_____ (2024), 『2023년 디지털정보격차 실태조사』
_____ (2024), 『2023년 인터넷이용 실태조사』
- 구본성(2021), 「BigTech 금융서비스 확대에 따른 주요이슈와 정책적 논의」, 『KIF 금융분석리포트』, 한국금융연구원
- 국은숙(2021), 「다크 패턴(눈속임 설계) 실태조사」, 『KCA보고서』, 한국소비자원
- 권지은(2023), 「디지털의 거대한 흐름, 디지털금융」, 『ICT 산업동향』, 정보통신기획평가원
- 금융·보험산업 인적자원개발위원회(2021), 「포스트 코로나 시대의 금융소비자 보호」, 『이슈리포트(ISSUE REPORT)』
- 김가현(2024), 「미국, 보험회사 인공지능 시스템에 대한 NAIC의 가이드라인」, 『KIRI 리포트』, 보험연구원
- 김두진(2019), 「디지털 경제와 핀테크: 소비자보호를 중심으로」, 『비교사법』, 제26권 제3호, 한국사법학회
- 김재영(2021), 「마이데이터서비스 소비자보호방안 연구」, 『정책연구보고서』, 한국소비자원
- 노성호(2023), 「금융산업에서의 인공지능(AI) 활용 방안에 따른 리스크 요인 분석」, 『이슈보고서』, 자본시장연구원
- 노현주(2021), 「금융 마이데이터 도입 현황과 시사점」, 『연구보고서』, 보험연구원
- 박소정(2024), 「디지털 금융이해력(Digital Financial Literacy)에 관한 연구」, 『연구보고서』, 보험연구원
- 박희우·강윤지(2024), 「보험회사 데이터 거래 현황과 과제」, 『연구보고서』, 보험연구원
- 변혜원(2023), 「디지털 금융서비스의 위험요소와 소비자보호」, 『KIRI 리포트』, 보험연구원
- 변혜원·송민규·윤민섭·이성복(2023), 『금융광고 규제의 실효성 제고방안』, 금융협회합동

- (은행연합회, 금융투자협회, 생명보험협회, 손해보험협회, 저축은행중앙회, 여신금융협회, 신협중앙회) 연구용역 보고서
- 서병호(2023), 「디지털 금융소비자 보호 이슈 및 과제」, 『KIF 분석보고서』, 한국금융연구원
- 신경희(2021), 「금융소비자의 디지털소외 현황 및 각국의 대응」, 『자본시장포커스』, 자본시장연구원
- 예금보험공사(2020), 「고령 금융소비자 보호 국제기준 및 일본 사례」, 『KDIC 조사분석정보』
- 이성복(2021), 「비대면 금융상품 수요 증가에 따른 금융상품시장 변화와 금융소비자 보호 강화 방향」, 『이슈보고서』, 자본시장연구원
- 이효섭(2023), 「빅테크 금융진출과 금융안정」, 『연구보고서』, 자본시장연구원
- 장성연·장호규·박재성·빈기범(2024), 「금융 디지털화와 금융산업 고용」, 『금융정보연구』, 13권 1호, 한국금융정보학회
- 정광민(2021), 「금융산업의 디지털 전환과 운영리스크 - 은행과 보험산업을 중심으로」, 『연구보고서』, 보험연구원
- 정영훈·송민수(2023), 「디지털 금융거래에서의 소비자권의 증진방안 연구」, 『KCA보고서』, 한국소비자원
- 주성철(2024), 「디지털금융의 이면, Tech Risk에 대비하라 - 글로벌 금융회사의 Tech Risk 사례와 시사점」, 『연구보고서』, 우리금융그룹
- 한국개발연구원(2022), 「디지털 전환에 따른 금융의 혁신과 개혁방안」, 『연구보고서』, 한국개발연구원
- 한국은행(2020), 『금융안정보고서』(2020년 12월)
- 황남희·김혜수·김경래·주보혜(2020), 「노년기 정보 활용 현황 및 디지털 소외 해소 방안 모색」, 『연구보고서』, 2020-46, 한국보건사회연구원
- 황순주(2022), 「디지털 지급결제 시장의 개방이 금융소비자에게 미치는 영향과 정책과제」, 『연구보고서』, 한국개발연구원
- Acemoglu, Makhdomi, Malekian, and Ozdaglar(2022), "Learning from reviews: The selection effect and the speed of learning," *Econometrica*

AIPPF(2022), “Artificial Intelligence Public-Private Forum: Final Report”

BIS(2024), “Digitalisation of Finance”

Croxson, Frost, Gambacorta, and Valletti(2022), “Platform-based business models and financial inclusion. Bank for International Settlements,” *Journal of Competition Law & Economics*

Department for Science, Innovation, and Technology(2024), “Implementing the UK’s AI Regulatory Principles: Initial Guidance for Regulators”

Dinh, Le, Duong, and Pham(2023), “Determinants affecting digital financial consumer protection: Evidence from 135 countries,” *The Journal of Economic Asymmetries*

EIOPA(2019), “Big Data Analytics in Motor and Health Insurance: A Thematic Review”

_____ (2023), “Methodological Principles of Insurance Stress Testing: Cyber Component”

_____ (2024a), “Dark patterns in insurance: practices that exploit consumer biases”

_____ (2024b), “Report on the Digitalisation of the European Insurance Sector”

FCA(2024), “AI Update”

Feyen, Frost, Gambacorta, Natarajan, and Saal(2021), “Fintech and the digital transformation of financial services: implications for market structure and public policy,” BIS Papers

G20(2018), “Digitisation and Informality: harnessing digital financial inclusion for individuals and MSMEs in the formal economy,” G20 Policy Guide

GPII(2018), G20 Policy Guide - Digitisation and Informality: Harnessing Digital Financial Inclusion for Individuals and MSMEs in the Informal Economy

IAIS(2019), Insurance Core Principles and Common Framework for the Supervision of Internationally Active Insurance Groups

Kobayshi, Shinya(2023), “AI Regulation in the Financial Sector: How to Ensure Financial Institutions’ Accountability”, Deloitte

- OECD(2018), “Financial Consumer Protection Policy Approaches in the Digital Age”
- _____(2020), “Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers’ assets, data and privacy”
- _____(2022), “DARK COMMERCIAL PATTERNS”, OECD DIGITAL ECONOMY PAPERS, p366
- _____(2023), “G7 Hiroshima Process on Generative AI: Towards a G7 Common Understanding on Generative AI”
- _____(2024), “Recommendation of the Council on High-Level Principles on Financial Consumer Protection”, OECD/LEGAL/0394
- UNESCO(2021), “Recommendation on the Ethics of Artificial Intelligence”
- World Bank Group(2022), “Financial consumer protection and fintech: an overview of new manifestations of consumer risks and emerging regulatory approaches”
- Yang, J., Wu, Y., & Huang, B. (2020). “Digital finance and financial literacy: An empirical investigation of Chinese households.”, *working paper*

도서회원 가입안내

회원	연회비	제공자료	
법인 회원	₩300,000원	- 연구보고서 - 기타보고서 - 연속간행물 · 보험금융연구	영문 연차보고서 추가 제공
특별 회원	₩150,000원		
개인 회원	₩150,000원		

* 특별회원 가입대상 : 도서관 및 독서진흥법에 의하여 설립된 공공도서관 및 대학도서관



가입 문의

보험연구원 도서회원 담당

전화 : (02)3775-9113 | 팩스 : (02)3775-9102



회비 납입 방법

무통장입금

- 계좌번호 : 국민은행 (400401-01-125198) | 예금주: 보험연구원



자료 구입처

서울 : 보험연구원 자료실(02-3775-9113 | lsy@kiri.or.kr)

| 저자약력

오 병 국 Texas A&M University 경제학 박사 / 연구위원
E-mail : bkoh@kiri.or.kr

변 혜 원 The Pennsylvania State University 경제학 박사 / 연구위원
E-mail : hw.byun@kiri.or.kr

이 소 양 중앙대학교 경영학 석사 / 연구원
E-mail : lishaoyang@kiri.or.kr

연구보고서 2024-08

금융의 디지털화와 소비자 보호

발 행 일 2024년 9월
발 행 인 안 철 경
발 행 처 보험연구원
주 소 서울특별시 영등포구 국제금융로 6길 38 화재보험협회빌딩
인 쇄 소 고려씨엔피

ISBN 979-11-93021-49-1
979-11-85691-50-3(세트)

(정가 10,000원)