API와 개인정보 이동권

구본효
서울대학교 법학대학원
박사과정

김병필
KAIST 기술경영학부

Ⅰ. 논의 배경

최근 API(Application Programming Interface; 애플리케이션 프로그래밍 인터페이스)가 주목받고 있다. 일반적으로 API란 애플리케이션들이 상호 작용하는 규약을 말한다. 인간이 애플리케이션과 상호 작용하는 규약을 유저 인터페이스(User Interface)라고 하듯이, 애플리케이션이 다른 애플리케이션과 상호 작용하는 규약을 API라 하는 것이다. API, 특히 웹 서비스 기반 API는 일반적으로 잘 정의된 메소드(methods)와 함수(functions), 프로토콜(protocols), 루틴(routines) 또는 명령(commands)으로 구성되어 있다.[1] 이를 통해 여러 시스템을 네트워크상에서 상호 연결할 수 있게 된다.

국내에서 API에 대한 관심이 높아지고 있지만, 이를 새로운 현상이라 보기는 어렵다. 기술 비즈니스에서 API의 가능성은 최소 2000년대 후반부터 주목받아 왔고, 폭발적인 성장세를 보여 왔다.[2] 2019년 통계에 의하면, 22,000개 이상의 API가 존재할 뿐 아니라, 매년 2,000개 정도 증가하고 있다.[3] 개발자가 아닌 일반 사용자도 누구든지 구글(Google), 페이스북(Facebook) 등의 주요 IT 기업들과 정부, 공공기관에서 Open API를 제공하고 있는 것을 쉽게 사용할 수 있다.

이 글은 특히 API와 개인정보 이동권의 관계에 주목한다. 국내에서는 금융 분야 마이데이터 사업이나 의료 분야 마이 헬스웨이(My Healthway) 사업과 같이 개인정보 이동권을 API를 통해 보장하고자 하는 시도가 이루어지고 있다. 이는 세계적으로도 마찬가지이다. EU에서 API의 아키텍쳐 및 디자인은 이른바 "유럽 공통 데이터 공간(Common European Data Spaces)"의 핵심적 요소로 인식되고 있다. EU 집행위원회는 잘 문서화되어 있고, 표준화된 개방형 API의 중요성을 강조한다.[4] 이미 EU의 개정 지급결제 서비스 지침(Payment Services Directive 2, 이하 "PSD2")으로 API를 통한 지급결제, 거래정보 전송 등이 의무화되었다. 영국, 일본 또한 금융 분야에서 Open API를 도입하는 등의 정책들을 추진하고 있다.

이와 같은 배경 하에 이 글에서는 우선 API가 무엇인지 논의한 후, 개인정보 이동권과 마이데이터를 중심으로 API의 사용례를 소개한다.

Ⅱ. API의 개념

1. 소프트웨어 라이브러리와 API

API는 소프트웨어 개발 산업에서 오랫동안 활용되어 왔다. 전통적인 API는 운영체제나 프로그래밍 언어가 제공하는 기능을 활용할 수 있도록 만든 인터페이스이다. 컴퓨터 프로그램을 개발하기 위해서는 다른 사람이 미리 작성해 놓은 프로그램을 호출하여 활용할 수 있어야 한다. 파일을 읽고 쓰거나, 인터넷으로 통신을 하거나, 수학 계산 작업을

1) ISO/TS 23029:2020 Web-service-based application programming interface (WAPI) in financial services
2) Daniel Jacobson/Dan Woods/Gregory Brail, APIs: A Strategy Guide, O'Reilly, 2012, 12-13.
3) Wendell Santos, "APIs show Faster Growth Rate in 2019 than Previous Years", ProgrammableWeb, https://www.programmableweb.com/news/apis-show-faster-growth-rate-2019-previous-years/research/2019/07/17 (2021. 4. 30. 확인).
4) Oscar Borgogno/Giuseppe Colangelo, "Data sharing and interoperability: Fostering innovation and competition through APIs", 35 Computer Law & Security Review 2-4 (2019).

하기 위해 프로그래머가 일일이 처음부터 모든 기능을 구현한다는 것은 현실적으로는 상상할 수 없다. 이처럼 프로그램이 이미 개발되어 있는 기능을 호출할 수 있도록 미리 정해 놓은 인터페이스가 API이다.

보통 프로그램이 API를 통해 정해진 기능을 실행시키기 위해서는 API를 구동시키는 SDK(Software Development Kit; 소프트웨어 개발 도구)가 해당 컴퓨터에 미리 설치되어 있어야 한다. 개발자는 공개된 SDK를 다운로드 받거나, 이를 유상으로 구입하여 활용한다. 프로그램이 API에 정해진 기능을 호출하면 SDK에 구현된 코드가 실행된다. 프로그램 개발이 완료되면, SDK를 함께 포함하여 배포한다. 이처럼 API와 SDK를 이용하면 프로그래머는 레고 블록을 조립하는 것처럼 기존의 프로그램을 조합해서 새로운 프로그램을 손쉽게 작성할 수 있다.

간단한 예로 증권거래 API를 생각해 보자. 일반적으로 증권사 고객들은 증권사 웹사이트나, HTS, MTS를 통해 주식을 거래한다. 하지만 전문 투자자들이 스스로 거래 프로그램을 개발하여 주식 정보를 얻고, 정해진 알고리즘에 따라 자동으로 거래를 하는 시스템을 구축하고자 할 수 있다. 이러한 고객을 위해 여러 증권사는 API를 제공하고 있다. 거래 시스템 개발자들은 증권사로부터 SDK를 내려 받아 증권거래 API를 호출함으로써, 증권사 서버에 접속하여 실시간 주가 정보를 가져오거나 거래 주문을 할 수 있다.

구체적으로 API에는 프로그래머가 호출하는 ① 함수의 명칭과 ② 그 함수가 받아들일 입력 값, ③ 그 함수의 처리 결과 반환되는 반환 값 등이 정의되어 있다. 예컨대 주식 종목 가격을 가져오는 함수, 주문을 내는 함수 등이 있고, 각 함수를 호출할 때에는 미리 정해져 있는 형태로 입력값을 제공해야 한다. 예컨대 거래 주문을 위해 사용하는 함수의 경우, 계좌번호, 주문유형, 주식종목코드, 주문수량, 주문단가 등을 입력값으로 넣어야 한다. 애플리케이션이 API에 정해진 대로 거래 주문 함수를 호출하면, 증권사가 제공한 SDK가 증권사 서버에 접속하여 주문을 하고, 주문 성공 여부를 결괏값으로 반환한다.[5)]

이러한 API와 관련하여 가장 잘 알려진 법적 분쟁은 Google LLC v. Oracle America, Inc. 사건이다.[6)] 이 사건에서 문제 된 API는 자바(Java) 프로그래밍 언어에 미리 구현된 라이브러리(library)를 사용하기 위한 인터페이스였다. 자바 언어는 전 세계적으로 많은 개발자들이 사용하고 있는 인기 프로그래밍 언어이다. 따라서 구글은 안드로이드의 확산을 위해 안드로이드 운영체계에서 자바 API를 사용할 수 있도록 제공하였다. 하지만 구글은 오라클로부터 자바 API에 대한 이용 허락을 얻지 않았다. 이에 오라클은 구글이 자바 API의 선언 코드(declaration line) 및 SSO(Structure, Sequence & Organization)의 저작권을 침해하였다고 주장하였다.[7)]

10년 넘게 이어진 소송 결과, 미국 연방대법원은 Java API의 저작물로서의 성격에도 불구하고, 저작권법상 공정이용의 4가지 요건[8)]에 부합한다는 이유로, 구글의 손해배상책임을 부정하였다. 이 사건에서 연방대법원은 이러한 API의 특징에 관하여 "컴퓨터

5) 키움증권, "키움 Open API+", https://www.kiwoom.com/h/customer/download/VOpenApiInfoView (2021. 8. 1. 확인).
6) Google LLC v. Oracle America, Inc, 593 U.S. ___ (2021).
7) 권사현/박성필/김용길, "API의 저작권 보호에 관한 고찰-자바 API의 저작물성을 중심으로", 지식재산연구 12 (2017), 144-146면.
8) 17 U.S.C. §107.

는 프로그래머가 사용하고 싶어 하는 수천, 수백만의 서로 다른 작업들을 수행할 수 있다. … API는 컴퓨팅 작업의 세계를 특정한 방식으로써 분할하고 조직한다. 프로그래머는 API를 사용함으로써 프로그램을 위하여 필요한 특정한 작업을 선택할 수 있다."라고 설명하였다. 이 판결은 저작물성과 공정이용에 관한 여러 중요한 쟁점을 다루고 있으나, 이 글의 목적에서 벗어나므로 논의를 줄인다.

2. 웹 API

소프트웨어 라이브러리 기반의 API는 현재까지도 널리 활용되고 있다. 하지만 이러한 API를 활용하기 위해서는 보통 프로그램을 실행하는 컴퓨터에 SDK를 설치하여야 하는 불편함이 따른다. 한편 SDK 배포 과정에서 소스코드 역분석(decompile)을 통해 프로그램의 소스코드가 공개될 위험성도 있다. 이와 달리 웹 API는 인터넷을 통해 상대방 시스템에 어떠한 기능을 수행할 것을 요청하고, 그 기능을 수행한 결과를 다시 인터넷을 통해 반환받는 방식이다. 따라서 SDK를 별도로 설치하지 않더라도 다른 시스템의 기능을 호출할 수 있게 된다. 또한, 웹 API를 통해 자료의 교환도 용이하게 된다. 이로써 웹 API는 여러 시스템을 손쉽게 상호 연결할 수 있게 되고, 그 결과 웹 API가 사회적으로 주목받고 널리 활용되고 있다.

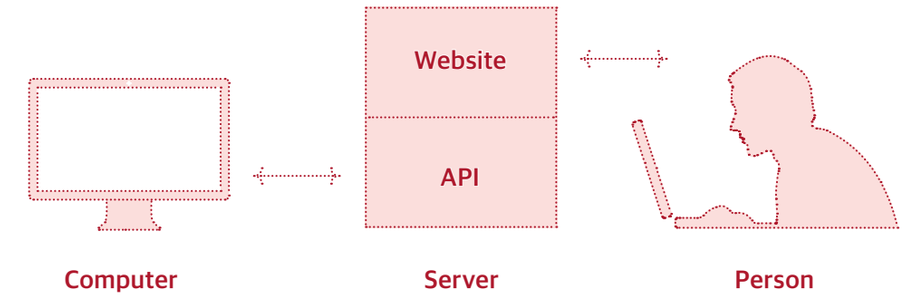

그림 1 웹사이트와 API[9)]

웹 API를 사용하는 것은 여러모로 인터넷을 통해 웹사이트를 읽는 것과 유사하다. 우리가 웹 브라우저를 사용하여 인터넷을 이용하는 것은 곧 서버에 저장된 웹 문서를 내려받아서 보는 것이라고 설명할 수 있다. 이때 웹 문서는 인간 이용자가 가장 보기 편한 방식으로 표현되어 있다. 하지만 만약 이용자가 인간이 아닌 컴퓨터라면 어떨까? 컴퓨터로 처리될 수 있는 정보의 형식은 인간 이용자가 쉽게 인식할 수 있는 것과는 다르다. 이처럼 인터넷을 통해 컴퓨터가 서버에 기능을 호출하거나 자료를 요청하는 방법과 그 결과를 내려받는 규약을 정해 놓은 것이 웹 API이다.[10)]

9) Brian Cooksey, An Introduction to APIs (Bryan Landers & Danny Schreiber eds., 2014), 7면.
10) Brian Cooksey, 앞의 책, 6-8면.

국가법령정보센터의 "국가법령정보 공동활용" 사이트를 예로 들어 보자. 국가법령정보센터는 웹사이트를 통해 법령과 판례 정보를 제공한다.[11] 그런데 이 사이트는 Open API를 통해서도 접속할 수 있다. 인간 이용자를 위한 웹사이트는 HTML(Hyper-Text Markup Language) 형식으로 작성되어 있다. HTML 형식에는 실제 정보 이외에도 웹 브라우저에 어떠한 내용을 어떻게 표시할 것인지 등 디자인 요소가 다수 포함되어 있다. 하지만 리걸테크 소프트웨어가 법령 정보를 다운로드할 때에는 이러한 디자인 요소가 필요하지 않다. 그저 법령이나 판례에 대한 세부 정보가 구조화되어 저장되어 있으면 족하다. 그래서 오픈 API를 이용하여 원하는 법령이나 판례를 요청하면 기계 판독이 가능한(machine-readable) 형태로 데이터가 전송된다.

```
{
    "crust": "original",
    "toppings": ["cheese", "pepperoni", "garlic"],
    "status": "cooking"
}
```

그림 2 JSON 예시[12]

이때 웹 API에서 자료를 교환하기 위해 일반적으로 사용되는 형식으로는 JSON(JavaScript Object Notification), XML(Extensible Markup Language) 등이 있다. 보다 널리 사용되고 있는 JSON은 키(key), 값(value) 구조로 되어 있으며, 수(number), 문자열(string), 배열(array), 객체(object) 등 자료형을 표현한다.

요컨대 웹 상의 자료 교환은 (1) 우리가 흔히 생각하는 인간이 볼 수 있도록 정보를 제공하는 방식과 (2) API를 이용하여 애플리케이션 간에 정보를 주고 받는 방식으로 구분해 볼 수 있다. 이 점에서 마이데이터 사업과 관련하여 논란이 되었던 스크레이핑(scraping) 방식과 API 방식은 서로 차이가 있다. 스크레이핑 방식은 API를 활용하지 않고 컴퓨터 프로그램이 인간을 위한 HTML 형식 웹 문서를 읽고 분석하여 데이터를 수집하는 방식이다. 이는 규약에 따른 API 방식의 데이터 전송과 다르다(금융 분야 마이데이터와 관련한 스크레이핑 방식에 관하여는 후술한다).

3. API의 사용 목적 - 콘텐츠 중심 API와 기능형 API

API는 그 사용 목적에 따라 '콘텐츠 중심(content-focused) API'와 '기능형(feature) API' 등으로 구분해 볼 수 있다. 앞서 예로 든 국가법령정보센터 사례는 법령과 판례 자

11) 국가법령정보센터, "Open API 활용가이드", https://www.law.go.kr/LSO/openApi/guideList.do (2021. 6. 2. 확인).
12) Brian Cooksey, 앞의 책, 22면.
13) 공공데이터포털, "공공데이터 활용방법", https://www.data.go.kr/ugs/selectPublicDataUseGuideView.do (2021. 6. 2. 확인)
14) N. Cameron Russell et al., APIs and Your Privacy, Fordham CLIP(Center on Law and Information Policy) (2019), 4-6면.
15) 네이버 개발자 센터, "API 소개", https://developers.naver.com/products/intro/plan/plan.md (2021. 6. 2. 확인)
16) ETRI, "공공 인공지능 오픈 API·DATA 서비스 포털", http://aiopen.etri.re.kr/ (2021. 6. 2. 확인).
17) Daniel Jacobson, Dan Woods & Gregory Brail, APIs: A Strategy Guide, O'Reilly, 2012, 6-8면.

료를 기계 판독이 가능한 형태로 제공하기 위한 것이다. 마찬가지로 우리 정부의 공공데이터 포탈(data.go.kr)은 오픈 API를 통해 공공데이터를 개방하고 있다.[13] 이처럼 데이터를 공유하기 위한 목적으로 활용되는 경우를 '콘텐츠 중심 API'라 할 수 있다. 페이스북, 트위터 등의 주요 사회관계망 서비스는 API를 통해 게시물을 가져오는 기능을 제공하고 있다. CNN, ESPN 등의 언론사는 자신의 기사를 API를 통해 제공하고 있기도 하다. 특히, CNN News-Graph API를 이용하면 개발자들이 최신 뉴스 데이터에 대해 손쉽게 접근할 수 있다.[14]

이와 달리 API를 통해 특정 작업을 수행하는 경우도 있다. 이를 '기능형 API'라 부를 수 있다. 예컨대 네이버는 검색, 로그인, Papago 번역, 얼굴 인식, 트렌드 조회 등의 기능을 API를 통해 제공하고 있다.[15] 네이버의 "CLOVA Face Recognition API"는 입력받은 이미지로부터 얼굴을 감지한 다음 (1) 감지한 얼굴이 어떤 유명인과 닮았는지 분석하여 그 결과를 반환하거나 (2) 입력된 이미지에서 얼마나 많은 얼굴이 감지되었고 각 얼굴이 어디에 어떤 크기로 위치하며 어떤 모습을 하고 있는지 반환하는 기능을 제공한다. 이러한 정보는 기계 판독이 가능한 형태로 구조화되어 있어서, 컴퓨터 프로그램을 통해 용이하게 분석할 수 있다. 기능형 API의 또 다른 사례로는 한국전자통신연구원(ETRI)의 오픈 API 서비스가 있다.[16] 이는 한국전자통신연구원이 과학기술정보통신부 R&D 과제를 통해 개발된 인공지능 기술을 연구목적으로 활용할 수 있도록 제공하는 것이다. 이 서비스를 통해 언어 분석, 어휘관계 분석, 질의 응답 등의 언어처리, 음성인식과 발음평가, 이미지 및 동영상 인식, 대화모델 등의 인공지능 기술을 활용할 수 있다.

우리에게 친숙한 기능형 API로는 웹사이트에 별도 계정을 생성하지 않고 SNS 계정을 통해 웹사이트에 로그인할 수 있도록 제공하는 '소셜 로그인(social login)' API가 있다. 이러한 기능을 제공하기 위해 구글, 페이스북, 네이버, 카카오 등의 소셜 플랫폼 사업자는 '로그인 API'를 제공하고 있다. 한편 이러한 API는 소셜 플랫폼 사업자가 제3자가 운영하는 웹사이트나 앱으로부터 데이터를 수집하는 경로가 되기도 한다. 누군가가 소셜 로그인이 사용되는 쇼핑몰을 방문하였다면 해당 플랫폼으로 방문 데이터가 전송되기 때문이다. 구글, 페이스북 등은 이러한 소셜 로그인 API로부터 전송받은 데이터를 근거로 한 분석 결과를 해당 쇼핑몰에 제공하기도 한다. 이러한 경우를 '분석(analytics) API'라 부르기도 한다.

4. 개방형(Open) API와 폐쇄형(Closed) API

개방형(Open) API는 별도의 계약 없이 약관에 동의하면 누구든지 이를 사용할 수 있는 API를 말한다. 물론, API 제공자가 이용자로부터 수수료를 받거나, 무료 이용자에게는 호출 횟수와 이용 용량을 제한하고, 유료 이용자에게는 제한을 완화하는 방식으로 수익화할 수도 있다. 이에 비해 폐쇄형(Closed) API는 주로 기업 내부에서 사용하는 API를 의미한다. 국내에서는 대부분의 관심이 개방형 API를 향하고 있는 것으로 보인다. 하지만 그 활용 빈도에 있어 폐쇄형 API가 높기도 하고, API로부터 창출되는 혁신의 적지 않은 부분을 차지하고 있기도 하다. 예를 들어, 뉴욕타임스는 자원을 효율적으로 관리하기 위한 내부 필요성에 따라 우선 폐쇄형 API를 개발하였고, 이후 이를 개방형 API로 전환하였다.[17]

기술적으로 보면 개방형 API와 폐쇄형 API는 다르지 않다. API는 개방형으로도, 폐쇄형으로도 운영될 수 있고, 기술적으로 어느 것이 더욱 우월하다고 볼 수는 없다. 서로 차이가 있는 점은 결국 가치 창출 사슬(value chain)이다. 다시 말해, 이는 누가 누구에게 어떤 비즈니스 자산을 제공하는가의 문제이다. 기업의 이해관계에 따라서는 개방형 API를 폐쇄형 API로 전환할 수도 있다. 예를 들어, 넷플릭스(Netflix) 사는 2014년 개방형 API를 중단하였으며, 현재 일부 파트너에 대하여만 API를 제공하고 있다.[18)]

일반적으로 폐쇄형 API는 모듈화된 소프트웨어 개발을 위한 기반구조로써 기능한다. 특히 기업 내부에서 사용되는 폐쇄형 API는 부서 간의 데이터를 교환하고, 기존(legacy) 시스템을 통합하는 수단으로 활용될 수 있다. 기업의 내부 전산 시스템 개발이 오랫동안 진행되어 오면서 기존 시스템과 신규 시스템을 연동하거나 통합하여 운영할 필요성이 있는 경우가 많다. 이때 API를 활용하면 조직 내부 상호 연결성과 협업성이 증가하여 궁극적으로 생산성을 증가시킬 수 있다.[19)]

개방형 API를 통해 얻을 수 있는 이점은 폐쇄형 API와는 차이가 있다. 정부나 공공기관이 개방형 API를 통해 공공데이터를 개방하고 여러 기술을 공개하는 목적은 쉽게 이해할 수 있다. 하지만, 여러 IT 기업들이 개방형 API를 이용하여 자신의 데이터를 공개하고, 자신이 개발한 (인공지능 서비스 등) 기능을 제공하고 있는 이유는 무엇일까? 특히 해당 데이터를 수집, 가공하거나 해당 기능을 개발하기 위해 상당한 비용과 시간이 투입된 경우에도 개방형 API를 통해 이를 공개하는 경우가 적지 않다.

이는 주로 데이터에 기반을 둔 서비스 플랫폼의 성장과 관련되어 있다. 개방형 API를 제공하는 기업들은 제3자가 자신의 서비스와 데이터를 이용하여 혁신을 가져올 수 있는 환경을 마련하고자 한다. 이를 통해 디지털 혁신의 생태계가 구축될 수 있다. 예를 들어, iOS 앱 개발자는 애플이 제공하는 API를 사용하여 아이폰의 여러 기능들을 실행하는 앱을 개발할 수 있다. 그에 따라, 애플은 자신의 노력만으로 개발할 수 없었던 수많은 다양한 앱들을 아이폰 이용자에게 신속히 제공할 수 있게 된다. 한편, 웹사이트 운영자는 구글이나 페이스북의 API를 사용하여 이용자 맞춤형 광고와 이용자 분석 서비스를 활용할 수 있다. 또한, 개방형 API에 대해 사용 수수료를 부과함으로써 부수입을 발생시키기도 한다. 요컨대 개방형 API를 통해 비즈니스 플랫폼을 형성함으로써 네트워크 효과를 통한 성장을 기대하고 있는 것이다.[20)] 최근의 한 연구에 따르면, 개방형 API를 제공하는 기업들을 120개 이상 조사한 결과, 이들 기업들의 매출액, 당기순이익, 시가총액, 무형자산 등이 모두 상승하였다고 한다.[21)]

이처럼 개방형 API는 제공자의 혁신성과 인지도를 높여 주는 만큼, 법적, 기술적인 위험성도 가져온다. 예를 들어, 시스템과 리소스에 대한 공격들이 이루어질 수도 있고, 리소스가 경쟁자들에게 과다하게 노출되는 한편, 경쟁 제품에 의해 자사 제품이 잠식되는 상황 또한 발생할 수도 있다.[22)]

18) Daniel Jacobson/Dan Woods/Gregory Brail, 앞의 책, 32-34면.
19) Markos Zachariadis/Pinar Ozcan, "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking", SWIFT Institute (2017), 5-7면.
20) Markos Zachariadis/Pinar Ozcan, 앞의 논문, 5-7면.

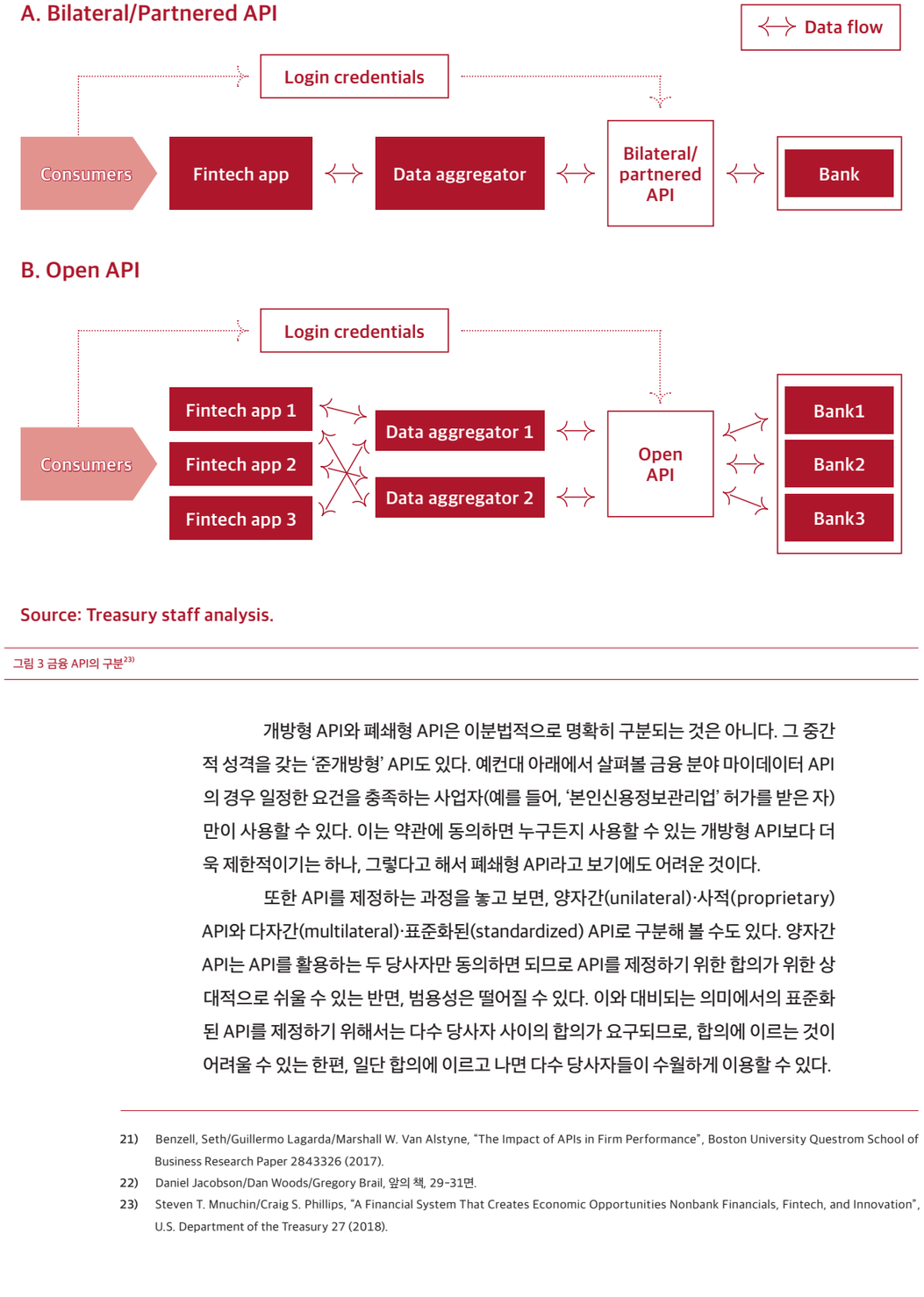

그림 3 금융 API의 구분[23)]

개방형 API와 폐쇄형 API은 이분법적으로 명확히 구분되는 것은 아니다. 그 중간적 성격을 갖는 '준개방형' API도 있다. 예컨대 아래에서 살펴볼 금융 분야 마이데이터 API의 경우 일정한 요건을 충족하는 사업자(예를 들어, '본인신용정보관리업' 허가를 받은 자)만이 사용할 수 있다. 이는 약관에 동의하면 누구든지 사용할 수 있는 개방형 API보다 더욱 제한적이기는 하나, 그렇다고 해서 폐쇄형 API라고 보기에도 어려운 것이다.

또한 API를 제정하는 과정을 놓고 보면, 양자간(unilateral)·사적(proprietary) API와 다자간(multilateral)·표준화된(standardized) API로 구분해 볼 수도 있다. 양자간 API는 API를 활용하는 두 당사자만 동의하면 되므로 API를 제정하기 위한 합의가 위한 상대적으로 쉬울 수 있는 반면, 범용성은 떨어질 수 있다. 이와 대비되는 의미에서의 표준화된 API를 제정하기 위해서는 다수 당사자 사이의 합의가 요구되므로, 합의에 이르는 것이 어려울 수 있는 한편, 일단 합의에 이르고 나면 다수 당사자들이 수월하게 이용할 수 있다.

21) Benzell, Seth/Guillermo Lagarda/Marshall W. Van Alstyne, "The Impact of APIs in Firm Performance", Boston University Questrom School of Business Research Paper 2843326 (2017).
22) Daniel Jacobson/Dan Woods/Gregory Brail, 앞의 책, 29-31면.
23) Steven T. Mnuchin/Craig S. Phillips, "A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation", U.S. Department of the Treasury 27 (2018).

Ⅲ. 개인정보 이동권과 API

API는 개인정보 이동권을 보장하기 위한 주요한 수단이 된다. 대표적으로 국내 금융 분야 마이데이터 제도는 신용정보주체가 신용정보를 다른 사업자에 전송할 수 있는 기술적 수단으로 API를 활용하고 있다. 현재 개인정보 보호법 개정안도 유사한 취지에서 개인정보 이동권을 보장하는 조항을 포함하고 있다. 이를 현실에서 구현하기 위하여서는 표준화된 API를 활용하는 방안이 주로 고려된다.

이하에서는 개인정보 이동권의 개념을 간략히 살펴본 다음 개인정보 이동권을 보장하기 위해 API를 활용하는 이유 및 그 활용 방식을 살펴본다. 본 장에서는 그 구체적인 활용 사례로 의료 분야 마이데이터 사업인 '마이 헬스웨이(My Healthway)'에 관해 살펴본다.[24] 금융 분야 마이데이터 제도는 다음 장에서 별도로 다룬다.

1. 개인정보 이동권

EU GDPR상의 개인정보 이동권은 정보주체가 본인과 관련된 개인정보를 체계적으로 작성된, 일반적으로 쓰이는 기계적으로 판독이 가능한 형식에 의하여(structured, commonly used and machine-readable format) 전송해 달라고 요구할 수 있는 권리를 뜻한다.[25] [26] 개인정보 이동권은 정보주체에게 효과적인 통제권을 부여하는 한편, 개인정보처리자가 더욱 투명하고 균형적인 방식으로 개인정보를 처리하도록 만들기 위하여 도입된 것이다.

개인정보 이동권은 개인정보의 보호뿐만 아니라 경쟁의 촉진과 소비자 보호의 측면에서도 기여하는 바가 있다. 개인정보의 이동을 법적으로 보장하여 개인정보의 효용에 기반을 둔 시장의 진입장벽을 낮춤으로써 시장을 더 경쟁적이고 덜 독점적으로 만들 수 있다는 것이다. 예컨대 EU의 PSD2에서 API를 통한 지급결제, 거래 정보 전송 등을 의무화한 것은 소매 금융 산업에 있어서의 경쟁을 촉진하기 위한 것이다.[27]

이에 따라 개인정보 이동권은 고객들이 특정 사업자에 고착(lock-in)되는 것을 막고, 다른 사업자로부터 서비스를 제공받는 길을 열어 준다. 이러한 점에서 GDPR이 개인정보 이동권을 규정한 것은 구글, 페이스북, 애플 등의 미국 IT 기업들이 유럽 내의 데이터 시장에서 지배적인 지위를 점해 가는 현상에 대응하기 위한 취지로서 이를 규정하게 되었다는 것이 일반적인 평가라 한다.[28]

24) 4차산업혁명위원회, "국민 건강증진 및 의료서비스 혁신을 위한 마이 헬스웨이(의료분야 마이데이터) 도입 방안" (2021).

25) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1-88.

26) 참고로, 데이터 컨트롤러는 정보주체가 개인정보의 전송을 요구할 때 비용을 청구할 수 없다고 규정하였다. 그러나, 데이터 주체의 요구가 명백히 근거가 없거나 과도한 경우에 한하여, 특히나 요청이 반복적으로 이루어지는 경우에, 예외적으로 합리적 비용을 부과하거나 거부할 수 있다고 규정하였다(제12조 제5항). 이와 관련하여, A29WP는 API 등 자동화된 시스템에 의해 데이터 전송의 비용이 감소하므로, 데이터 주체가 다수의 청구를 한다고 하여도, "요구가 명백히 근거가 없거나 과도한 경우에" 해당한다고 보기는 어려울 수 있다는 취지로 설명하기도 하였다. Article 29 Working Party, Guidelines on the right to data portability 14-15면 (2017).

27) 이진규, "개인정보 이동권의 취지를 다시 살펴보다-개인정보 이동권은 과연 무엇을, 누구를 위한 것인가?", 9 KISA Report (2020), 2-3면.

28) 고환경/손경민/주성환, "정보이동권과 마이데이터산업", BFL 93 (2019), 27-28면.

2. API 활용의 필요성 - 상호운용성의 확보

개인정보 이동권 보장을 위해 API를 활용하는 이유는 무엇일까? 이는 주로 API, 특히 웹 기반의 개방형 API를 통해 상호운용성(interoperability)을 확보할 수 있기 때문이다. 예컨대 정보주체가 A 개인정보처리자에게서 B 개인정보처리자에게로 개인정보를 전송할 것을 요구했다고 생각해 보자. 이때 A의 시스템과 B의 시스템을 서로 연동할 수 있는 방법이 필요하다. A의 개발자는 B의 시스템이 어떻게 작동하는지 알 수 없고, B의 개발자도 A의 시스템이 어떻게 작동하는지 알 수 없다. 경쟁 사업자 간에 내부 시스템을 상호 공개할 것을 요구할 수도 없다. 이때 웹 API는 여러 시스템을 상호 연결함으로써 데이터를 공유할 수 있는 한 수단으로 활용될 수 있다. 개인정보처리자가 API에 정한 규약에 맞추어 데이터를 전송하기만 하면 상대방 시스템의 구성 요소나 작동 방식을 알지 못하다고 하더라도 서로 연결될 수 있다. 이처럼 상호운용성을 확보하기 위한 방안으로, 개인정보 보호법 개정안은 "정보주체가 전송을 요구하는 경우에 개인정보처리자는 시간, 비용, 기술적으로 허용되는 합리적 범위 내에서 컴퓨터 등 정보처리장치로 처리 가능하고 통상적으로 이용되는 구조화된 형식으로 전송하여야 한다." 라는 조항을 포함하고 있다.

한편 상호운용성은 상호호환성(compatibility)과 구별할 필요가 있다. A의 시스템에서 전송된 데이터 형식이 B의 시스템에서도 곧바로 처리될 수 있다면 이는 상호호환되는 것이다. 하지만 여러 개인정보처리자들이 제각기 다른 데이터 형식을 사용하고 있다면 다른 모든 사업자의 시스템과 호환될 것을 요구하는 것은 매우 부담스러울 것이다. 이에 비해 서로 다른 데이터 형식이 적절한 중간 변환 과정을 거쳐 전송될 수 있다면 상호운용성은 충족될 수 있다. 이에 GDPR 전문(Recital) 제68조는 컨트롤러가 개인정보 이동성을 가능하도록 '상호운용성'을 갖는 포맷을 개발하도록 권장하지만, 데이터 컨트롤러가 기술적으로 '상호호환' 가능한 시스템을 채택·유지할 의무를 부과하는 것은 아니라고 설명하고 있다. 즉, 개인정보처리자 간에 상호호환성이 구현되어 있지 않더라도, 상호운용성은 체계성, 상용성, 기계적 판독성을 구현함으로써 달성될 수 있다.[29] 이를 위해서 여러 시장참여자들이 상호운용이 가능한 표준과 형식에 대해 합의하기 위해 협력할 필요가 있다.

흥미롭게도, 개인정보 이동권이 '겨냥' 하는 주요 빅테크 기업들(애플, 페이스북, 구글, 마이크로소프트, 트위터 등)은 2018년 데이터의 상호운용성과 이동성을 확보하기 위한 오픈소스 플랫폼을 수립하는 것을 목적으로 'Data Transfer Project'를 시작하였다.[30] 이는 주요 시장참여자들 사이에서 데이터의 이동성이 주요 관심사가 되었다는 것을 보여준다.[31] 특히 GDPR은 상호운용성을 확보하기 위한 구체적인 규정, 지침 등을 제공하지 않고 있는 반면, 이와 같은 자율적인 이니셔티브가 등장한 데 의의가 있다고 할 수 있다.

'Data Transfer Project'는 표준화된 API를 제정하는 것이 아니라 데이터 모형(data models)과 변환기(adapters)의 개념을 통하여 상호운용성을 확보하고 있다는 점이 주목할 만하다. 여기서 변환기는 데이터를 표준 형식으로 변환한다. 즉, 개별 기업들은

29) Article 29 Working Party, 앞의 가이드라인, 16-18면.

30) Data Transfer Project, "About us", https://datatransferproject.dev/ (2020. 6. 2. 확인)

31) Oscar Borgogno/Giuseppe Colangelo, 앞의 논문.

개별적으로 API를 개발하여 제공하되, 사업자의 API를 통해 제공되는 데이터는 변환기를 통해 표준화된 데이터 모형으로 변형될 수 있다. 'Data Transfer Project'를 통해 실제 개인정보 전송이 활발히 이루어지고 있는지에 대한 평가는 별론으로 하더라도, 위 프로젝트에 참여하는 IT 기업들은 기존 API를 계속 운영하는 한편, 데이터 형식을 표준화함으로써 일단의 상호운용성을 확보하고자 한다. 이러한 방식은 기존 서비스 방식이나 인증 메커니즘 등에 대한 전면적인 변화 없이, 산업 전반에서 데이터의 이동성을 증진시키기 위한 목적이라고 이해될 수 있다.[32)]

'Data Transfer Project'의 접근법과 달리, 개인정보처리자에게 상호호환 가능한 표준화된 API를 사용하도록 강제하는 것은 사실상 불가능할 수 있다. 여러 산업군마다 서로 다른 형식과 민감 수준을 가진 개인정보가 처리되고 있고, 그에 따라 정보주체에 대한 인증 방식이나 보안 수준 또한 제각기 다를 수 있기 때문이다. 그래서 개인정보에 관한 일반법인 개인정보 보호법이 표준화된 API의 사용하도록 강제하거나, 특정한 기술적인 방식을 요구하기란 어렵다. 개인정보 보호법 개정안 제35조의2 제2항도 상호운용성을 위한 최소한의 기준을 제시하고 있지, 이를 구현하기 위한 구체적인 요건까지 규정하고 있지는 않다.

이러한 여건 하에서 개인정보처리자 간의 일반적인 상호운용성을 확보하는 것은 쉽지 않은 과제가 될 수 있다. 각각의 시장참여자들 간의 개인정보 이동성 확보에 대한 인센티브가 일치하지 않고, 기술력 격차가 존재하는 상황에서 표준화된 API가 도입되고 운영되지 못할 수도 있다. 또한 기술력이 충분하지 못한 개인정보처리자가 보안성이 부족하고 결함 있는 API를 도입할 경우 개인정보 유출 공격 등에 노출될 위험도 있다. 오히려 표준화가 혁신성을 저해하는 원인으로 지적되는 점도 문제이다.[33)]

하지만 특정 산업 분야, 특히 규제 산업 분야에 있어서는 표준화된 API를 제정하고 상호운용성 확보를 위한 의무를 부과하는 것이 상대적으로 용이하고 또한 실현될 수 있다. 금융 분야 마이데이터 사업과 의료 분야 마이데이터 사업이 그 예이다. 금융 분야 마이데이터에 관하여는 다음 장에서 상세하게 살펴보고, 본 장에서는 우선 의료 분야 마이데이터의 주요 사항들을 본다.

3. 마이 헬스웨이 플랫폼과 API 활용

4차산업혁명위원회는 2021. 2. 환자, 예방 중심으로 의료서비스의 축이 전환되고 있는 상황에서 본인 주도 하에 의료데이터를 공유, 활용함으로써 의료서비스를 혁신하기 위한 '마이 헬스웨이(My Healthway)', 즉 의료 분야 마이데이터를 추진하겠다고 발표했다. 이와 관련하여, 의료법이 2020. 3. 4. 개정되어, 의료인은 전자문서 형식으로 환자 또는 다른 사람에게 의료 기록 전부 또는 일부분을 확인하게 할 수 있게 되었다.[34)]

마이 헬스웨이 플랫폼은 정보주체 동의 하에 다양한 기관이 보유한 의료데이터를 조회, 저장, 전송하는 '네트워크 허브'로서 기능한다. 의료기관 등은 본인 동의 하에 전송받은 개인 의료데이터를 활용하여 건강 관리 서비스를 제공한다. 여기에는 특히, 의료데이터의 시각화와 설명(예: 생애주기 건강검진 알림, 개인 맞춤 건강관리 등), 정밀 진단 및 진료 등이 포함되며(예: 외래진료 중복 처방 방지, 응급상황 정보 공유 등), 사용자는 '나의 건강기록' 앱을 통해 활용기관으로 데이터를 전송함으로써 의료데이터를 조회, 저장, 활용하게 된다.

마이 헬스웨이 도입 방안에는 4개 분야, 12개의 추진 과제들이 포함되어 있다. 의료데이터가 수집되는 기관(공공기관, 의료기관, 웨어러블 디바이스 등)별로 플랫폼을 통해 공유, 활용되는 항목들을 정의하고, 이를 표준화하여야 하는 과제들이 존재하며, 특히 의료기관들이 인프라를 구축, 플랫폼에 참여하는 방향으로 유도하는 것이 관건이다. 이와 관련하여, 수혜자가 제증명수수료를 지급하거나(의료법 제45조의3), 활용기관에서 의료데이터를 정기적으로 제공받는 대신 수수료를 지급하는 비용 지불 체계 등이 고려되고 있다.

API는 특히 마이 헬스웨이 플랫폼을 구축하는 단계에서, 의료데이터가 연계되는 네트워크 구축 시 사용되는 표준연계형식으로 정해졌다.[35)] 의료데이터를 교환하기 위한 표준화된 형식으로 HL7(Health Level Seven International)의 FHIR(Fast Healthcare Interoperability Resources) 프레임워크를 채택하였으며, 예를 들어, 약물 처방 내역 API, 검체 검사 결과 API, 병리검사 결과 API 등이 포함된다.

Ⅳ. 금융 분야 마이데이터와 API의 활용

1. 배경 — 오픈 뱅킹의 도입

은행권에서는 2016. 8. 오픈플랫폼을 구축하고 API를 통해 지급결제망과 데이터를 제공하기 시작하였는데, 이를 오픈뱅킹(Open Banking)이라 한다. 여기에는 잔액 조회, 거래 내역 조회, 출금 및 입금 이체 API를 비롯하여 20여 가지의 금융 API가 포함되어 있다. 이는 금융결제원이 관리하는 플랫폼에 핀테크 기업이 API를 사용하여 접근할 수 있도록 한 것으로서, 표준화된 API가 본격적으로 도입되었다기보단, 기존 금융공동망을 통해 금융결제원이 은행으로부터 데이터를 받아 간편 결제, 간편 송금 등 다양한 사업을 수행하고 있는 이용기관에 전달하는 방식이었다. 한편, 이는 농협은행, 하나금융그룹, 신한금융그룹 등의 금융회사에서 개별적으로 제공하고 있는 여러 유형들의 Open API와는 별개의 인터페이스이다. 예를 들어, 부동산을 중개하는 서비스인 '다방'을 이용하는 고객들이 별도 애플리케이션, 검색 없이 바로 전세자금대출 한도 조회 서비스를 이용할 수 있는 것은 앞의 공동 Open API에 의한 것이 아닌, 신한은행에서 제공하는 전세자금대출 한도조회 API에 의한 것이었다.[36)] 결국, 오픈뱅킹 서비스는 금융결제원이 기존 인프라를 활용하여, 마치 앞의 'Data Transfer Project'와 같은 공동 플랫폼을 운영하는 것이라고 볼 수 있다.

32) 권헤진, "신용정보 공유 활성화를 위한 API 표준화 방안 및 이에 따른 법적 쟁점 검토", Law & Technology 16 (2020), 5-6면.
33) Oscar Borgogno/Giuseppe Colangelo, 앞의 논문, 10-11면.
34) 의료인, 의료기관의 장 및 의료기관 종사자는 「전자서명법」에 따른 전자서명이 기재된 전자문서를 제공하는 방법으로 환자 또는 환자가 아닌 다른 사람에게 기록의 내용을 확인하게 할 수 있다(의료법 제21조 제5항).
35) 4차산업혁명위원회, 앞의 글.
36) 금융위원회, "[알기쉬운 핀테크] 금융권 Open API" (2019), 9면.

오픈 뱅킹(Open Banking) 정책으로 말미암아, 신규 핀테크 서비스가 다수 등장하는 등의 정책적 성과가 도출되었다. 다만, 참여 기업들이 수익 악화 우려 등을 우려하여 데이터 공유에 소극적이었고, 고가의 수수료 때문에 신규 사업자가 이를 활발하게 이용하지 못했다는 비판 또한 존재하였다.[37)]

2. 본인신용정보관리업 신설과 Open API 도입

핀테크 산업의 지속적 확산에 따라 금융위원회는 2018. 7. '본인신용정보관리업'을 신설하고, 금융 데이터를 조회, 전송하는 Open API를 도입하기 위한 정책들을 추진하겠다고 발표하였다.[38)] 금융위원회는 이후 지급결제, 송금 등을 실행하는 '실행형 API'와 데이터를 전송하는 '조회형 API'를 구분하고, 조회형 API와 관련하여 금융회사 참여 하에 표준화된 개방형 API를 구축하겠다고 발표했다. 예를 들어, 스마트폰 앱을 통해 잔액 조회 서비스를 이용하면, 잔액 조회 Open API를 통해 계좌 관련 데이터가 송신, 수신됨으로써 고객에게 제공되는 방식이다. 2020. 2. 신용정보의 이용 및 보호에 관한 법률(이하 '신용정보법') 개정에 따라 '본인신용정보관리업'이 법에 명문화되어 도입되면서 이러한 정책이 현실화되었다.

금융 분야 마이데이터 사업은 결국 이와 같이 Open API를 통해 개인신용정보를 송수신할 수 있도록 한 것이다. 금융위원회는 이를 통해 지급결제 및 금융데이터에 대한 제3자 접근성을 높이고, 금융업의 경쟁성과 혁신성을 촉진할 수 있으며, 맞춤형 금융서비스 제공의 기반이 마련될 것으로 기대하였다.[39)]

유사한 정책은 해외 사례에서도 확인된다. 금융 분야 Open API를 도입하고 있는 EU PSD2, 영국 Open Banking Initiative, 일본 은행법이 그 예이다. 예를 들어, EU PSD2는 핀테크 산업이 부상하고 있는 환경에서, 결제서비스 시장에서의 경쟁을 촉진시키고 효율적으로 만들기 위하여 도입된 것으로서,[40)] 국내 오픈 뱅킹 서비스와 마찬가지로 계정 정보 및 결제 서비스에 대해 고객 동의하에 지급지시전달업자(Payment Initiation Service Providers)와 본인계좌정보관리업자(Account Information Services Provider)가 접근하는 것을 허용하고 있다. 이 때, 안전하고 효율적인 채널(safe and efficient channels)로 데이터를 전송해야 한다고만 규정하고 있고, 세부 지침(Regulatory Technical Standards) 또한 API를 명시하고 있는 것은 아니라고 한다.[41)] 그럼에도 불구하고, 이는 통상 API를 의미하는 것이라고 해석되고 있다. 이는 일반적으로 API가 안전성과 신뢰성을 갖춘 기술로서 간주되고 있기 때문이다. 또한, 영국 Open Banking Initiative는 API를 구축해야 함을 명시하고 있다.[42)]

37) 문병순, "은행의 API 공개를 촉진하기 위한 법제도의 모색-신용정보의 이용 및 보호에 관한 법률 개정안을 중심으로", 은행법연구 12 (2019), 117-118면.
38) 금융위원회, "소비자 중심의 금융혁신을 위한 금융분야 마이데이터 산업 도입방안" (2018), 12-18면.
39) 금융위원회, "[알기쉬운 핀테크] 금융권 Open API", 10-11면.
40) Markos Zachariadis/Pinar Ozcan, 앞의 논문, 5-7면.
41) 문병순, 앞의 논문, 124면.
42) Markos Zachariadis/Pinar Ozcan, 앞의 논문, 5-7면.
43) 금융위원회/금융보안원, "금융분야 마이데이터 기술 가이드라인" (2021), 21-23면.
44) 법 제22조의9제4항에서 "대통령령으로 정하는 방식"이란 제3항에 따른 방식 외의 방식으로서 다음 각 호의 요건을 모두 갖춘 방식을 말한다(신용정보법 시행령 제18조의6 제7항). 1. 개인신용정보를 전송하는 자와 전송받는 자 사이에 미리 정한 방식일 것 2. 개인신용정보를 전송하는 자와 전송받는 자가 상호 식별·인증할 수 있는 방식일 것 3. 개인신용정보를 전송하는 자와 전송받는 자가 상호 확인할 수 있는 방식일 것 4. 정보 전송 시 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하는 방식일 것

3. Open API를 통한 데이터의 전송 과정

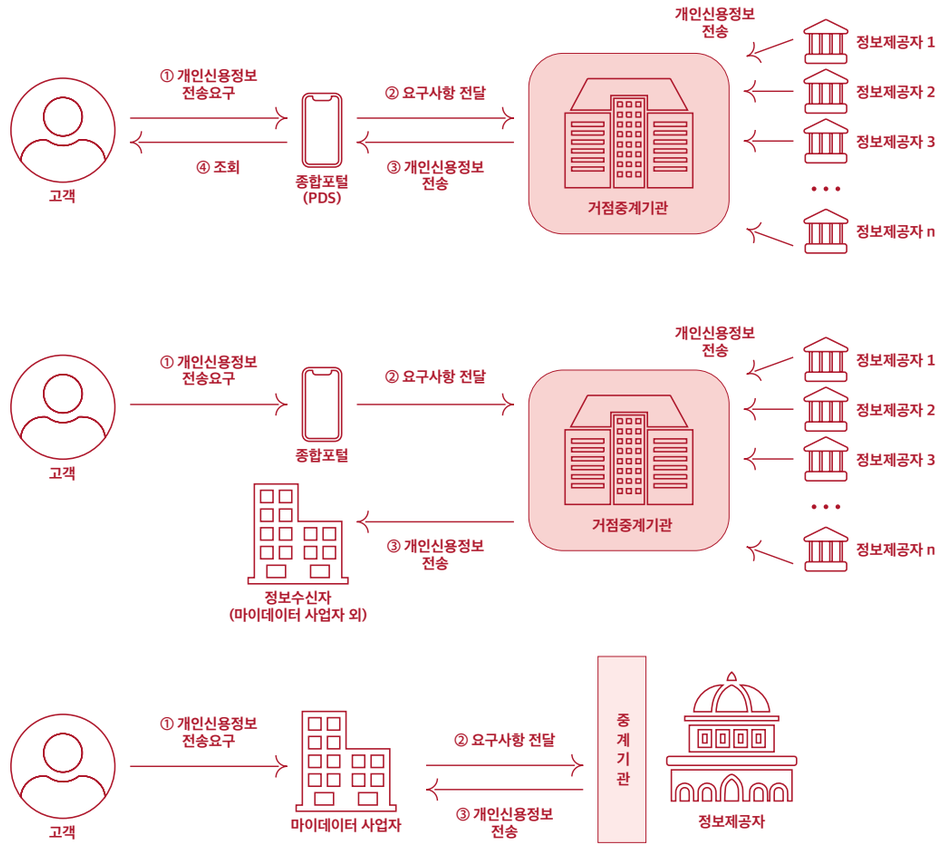

그림 4 개인신용정보 전송 유형[43)]

Open API를 통해 개인신용정보가 전송하는 과정은 ① 개인신용정보 전송요구, ② 고객 본인인증, ③ 개인신용정보 전송 3단계로 구성된다. 금융회사, 공공기관, 본인신용정보관리회사 등 정보제공자는 고객, 본인신용정보관리회사, 금융회사 등 정보수신자에 대해 직접 또는 중계기관 등을 통해 컴퓨터 등 정보처리장치로 처리할 수 있는 형태로 데이터를 전송하게 된다. 최초 전송 단계에서, 정보제공자는 정보수신자가 자격 있는 자에 해당하는지를 확인한다. 그로부터 '접근토큰(access token)'이라 하는 권한 증명서가 생성, 발급되며, 이를 제시함으로써 정보수신자는 1년 동안 자신의 권한을 증명할 수 있다.

신용정보제공·이용자는 안전성과 신뢰성이 보장될 수 있는 방식으로 개인신용정보를 전송해야 한다(신용정보법 제22조의9 제4항). 이와 관련하여, 송신자와 수신자는 상호 식별·인증 및 확인 가능하며, 안전하게 암호화된 방식으로 미리 정하여야 한다.[44)] PSD2 사례와 같이 이는 Open API를 의미하는 것이라고 해석되며, 금융위원회/한국신용

정보원과 금융위원회/금융보안원의 가이드라인도 같은 취지이다.[45] 이처럼 본인신용정보관리회사 간의 개인신용정보 전송 방식으로 API 방식이 정해져 있으므로, 사업자는 개인신용정보 전송요구 관련하여 API를 개발하고 관리해야 하며, 특히 표준 API에 맞게 개발되었는지 API 테스트베드를 이용하여 확인해야 한다.

본인신용정보관리회사 간의 개인신용정보 전송과는 달리, 신용정보주체 본인에게 전송되는 경우 마이데이터 종합포털(Personal Data Storage)에서, 본인신용정보관리회사 외 기관에 전송되는 경우 업권별 거점중계기관(한국신용정보원, 코스콤, 금융결제원)에서 이를 중계한다.[46] 다시 말해, 신용정보주체 본인이나 본인신용정보관리회사 외 기관에게 전송하는 경우에는 API를 사용하여 전송해야 하는 것은 아니다. 따라서, 이메일이나 메신저 등으로 전송하는 것도 불가능하지는 않을 수 있다. 그러나 금융위원회/한국신용정보원 가이드라인은 특히 정보주체 본인에 대한 전송의 경우 PDS(Personal Data Storage)에 전송하는 방식만을 고려하고 있다.[47] PDS는 신용정보주체가 자신의 정보를 저장하고 관리하는 플랫폼으로서, 주로 클라우드 DB(Database) 서비스로 운영될 것으로 보인다. 참고로, EU GDPR에서도 본인에게 데이터를 전송하는 경우 상호운용성의 최소 요건들을 충족하는 방식으로 해야 한다고 규정하고 있으나, 어떠한 형식과 내용을 사용하면 그 요건을 갖추게 되는 것인지는 명확하지 않은 상황이다. EU에서의 경우, 실무상 CSV, XML, JSON 형식이 선택되었으나, PNG, JPEG, PDF, DOCX 등 형식이 선택된 사례도 있었다고 한다.[48]

4. 표준화된 API 사용과 스크레이핑 방식의 금지

스크레이핑 방식은 원래 인간 이용자를 대상으로 작성된 웹 문서를 '그 자체로' 읽고 분석하여 데이터를 수집하는 방식이다. 종래 신용정보 관리 모바일 앱들은 사전에 수집된 고객의 인증정보를 기초로 금융회사에 접속해 이러한 방식을 통하여 신용정보를 수집하여 왔다. 그렇지만, 스크레이핑에 대하여는 여러 측면에서 문제점이 제기되어 왔다.

고객의 인증정보가 고객의 단말기 내지는 사업자 서버에 추가적으로 저장되므로 유출의 위험이 증가되고, 금융기관이 보안정책과 기술을 적용할 수 없게 한다는 것이 주된 비판의 논거였다. 스크레이핑으로 인한 금융기관의 서버 과부하 문제도 지적되었다. 미국의 한 은행이 통신 부하를 이유로 핀테크 회사가 스크레이핑 방식을 통하여 데이터를 수집하는 것을 금지하였으나, 이후 협의를 통해 API를 제공한 사례도 있다.[49] 스크레이핑 방식에 의해 금융 데이터가 전송되는 것이 개인정보의 제3자 제공에 해당하는지, 고객의 동의를 별도로 받아야 하는지, 모바일 앱에서 스크레이핑이 이루어는 '클라이언트 스크레이핑(client scraping)' 방식을 이용할 때에도 그러한 것인지 등 법적 문제도 제기되었다.[50]

금융 분야 마이데이터 제도에 따라 표준화된 API를 사용하게 됨에 따라 이러한 스크레이핑은 사실상 금지되었다.[51] 즉, 스크레이핑 방식은 안전성과 신뢰성이 보장되는 방식으로 볼 수 없다는 것이다. 금융위원회와 한국신용정보원의 가이드라인 또한 개정 신용정보법 제22조의9 제4항의 시행일인 2021. 8. 4. 이후에는 스크레이핑이 금지됨을 명시하고 있다.[52] 다만, 공인인증서를 위탁받아 수집하는 방법 이외에 규모, 거래빈도 등에 따라 중계기관 활용, 신용정보주체로부터의 개별 정보제공동의, 오픈뱅킹 API를 활용하는 등의 방법으로 수집하는 것은 허용된다.[53]

스크레이핑 방식이 금지된 주된 이유는 그것이 '안전성과 신뢰성이 보장되는 방식'으로 '직접' 전송하는 형태에는 해당하지 않는다는 것이라고 볼 수 있다. 스크레이핑 방식에 비해 현재의 표준화된 API 방식에서는 인증정보가 아니라 허용권한증표를 활용하므로, 개인신용정보를 제공하는 금융기관이 보안정책과 기술을 적용할 수 있다는 보안상 장점이 있다고 알려져 있고, 안전한 프로토콜을 통하여 고객의 정보가 전송되므로 신뢰할 수 있다.

스크레이핑 금지에 대한 비판도 존재한다. 비판의 핵심은 '본인신용정보관리업' 허가를 받지 못한 사업자는 API를 사용하지 못하고, 스크레이핑도 할 수 없게 되어, 결국 데이터를 얻을 수 있는 경로가 차단됨으로써 경쟁력을 잃게 되는 상황에 놓을 것이라는 점이다. 또한 스크레이핑 방식은 웹상에서 입수할 수 있는 다양한 정보를 수집할 수 있어 장점도 있다. 이에 API 방식의 일률적 적용을 의무화하는 것보다, 마이데이터 시장의 발전과 상황에 따라 스크레이핑 방식을 허용할 필요가 있다는 주장도 제기된다.[54]

Ⅴ. 결론

API는 기술상으로나 사업상으로나 여러 장점이 있다. 특히, 사물인터넷(IoT)과 인공지능을 활용한 애플리케이션을 통해 수집, 이용하는 데이터가 광범위해지고, 플랫폼 간의 상호운용성을 확보하기 위한 노력들이 이루어지고 있는 상황에서, API 방식의 데이터 전송은 더 빈번히 고려될 것이다.[55] 특히, API의 상호운용성과 모듈성은 서비스 확장을 용이하게 한다는 점에서 그 활용 가능성이 크다.

API를 통한 상호운용성을 높이기 위해서는 이를 표준화할 필요가 있기도 하다. 하지만 누가 어떻게 API를 정의하고 활용할 것인지에 대해서는 명확히 합의된 바가 없다. EU 기관들은 기업들이 공개되어 있는 표준 API를 사용하는 것을 고려토록 권고하고 있고, 주로 금융, 의료 등의 제한적인 분야에서 표준화된 API 활용의 움직임이 나타나고 있다.

한편, API의 무분별한 이용으로부터 기인하는 프라이버시 침해 가능성도 유의할 필요가 있다. API는 정보주체가 충분히 인식하지 못하는 상황 하에서 개인정보처리자가 개인정보를 추가적으로 수집하고 축적할 수 있는 채널로 기능할 가능성도 있다. 많은 논란이 제기된 케임브리지 애널리티카(Cambridge Analytica) 사건은 "당신의디지털생활(Thisisyourdigitallife)"이라는 페이스북 앱으로부터 수집된 개인정보가 정치적 목적으로 활용된 것이었다. 이 때 개인정보 수집의 도구로 페이스북의 Open Graph API가 활용되었다는 사실을 유념할 필요가 있다.

45) 금융위원회/금융보안원, 앞의 글, 37면; 금융위원회/한국신용정보원, "금융분야 마이데이터 서비스 가이드라인" (2021), 19면.
46) 금융위원회/금융보안원, 앞의 글, 8-29면.
47) 금융위원회/한국신용정보원, 앞의 글, 59-61면.
48) Janis Wong/Tristan Henderson, "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", 9 International Data Privacy Law 186-188 (2019).
49) 문병순, 앞의 논문, 118-120면.
50) 김준영/전보미/박지영, 금융데이터의 수집과 공유-개정 신용정보법 하에서의 변화, DAIG 1 (2020), 90-93.
51) 금융위원회/한국신용정보원, 앞의 글, 15, 72-73면.
52) 금융위원회/한국신용정보원, 앞의 글, 15면.
53) 제4항에도 불구하고 신용정보 제공·이용자등의 규모, 금융거래 등 상거래의 빈도 등을 고려하여 대통령령으로 정하는 경우에 해당 신용정보제공⊠이용자등은 대통령령으로 정하는 중계기관을 통하여 본인신용정보관리 회사에 개인신용정보를 전송할 수 있다(신용정보법 제22조의9 제5항).
54) 고환경/손경민/주성환, 앞의 글, 36-37면.
55) Oscar Borgogno/Giuseppe Colangelo, 앞의 논문, 2-4면.