진화하는 온라인 사칭과 세 개의 문(門)

서유경 법률사무소 아티스 대표변호사·법학박사

I. 들어가며

디지털 시대에 접어들면서 연예인, 기업인, 교수 등을 사칭한 온라인 사기 범죄가 급증하고 있다. 2024년 상반기에는 이러한 문제에 대응하기 위해 '유명인 사칭 온라인 피싱범죄 해결을 위한 모임'(이하 '유사모')이 결성되었으며, 사칭 범죄에 대한 경각심과 대응의 필요성이 강조되고 있다. 그러나 우리나라에서는 여전히 온라인 사칭을 규제할 법적 장치가 부족해 피해가 실시간으로 계속 발생하고 있는 상황이다.

온라인 사칭은 단순히 혼란을 초래하는 것을 넘어, 다양한 범죄로 이어질 수 있는 복합적인 문제를 내포하고 있다. 그러나 현재로서는 사칭 자체를 규제하기가 어려워, 각 행위를 개별적인 법규로 제재할 수밖에 없는 실정이다. 이로 인해 피해는 빠르게 확산되지만, 법적 공백으로 인해 피해자들은 자력구제로 나아갔다가, 사적 제재라는 새로운 사회적 문제를 야기하고 있다.

또한 플랫폼의 자율규제라는 명목 아래 실제로는 방치되거나 비협조적인 태도가 문제를 더욱 악화시키고 있으며, 국가 간의 법적 차이로 인해 수사도 상당한 어려움을 겪고 있다. 이러한 상황 속에서 피해자는 계속해서 늘어나고 있다. 이번 글에서는 이러한 온라인 사칭 범죄의 현황과 이를 해결하기 위한 법적 대응 방안을 구체적으로 살펴보고자 한다.

II. 사칭, 그 자체만으로 범죄이거나 불법행위인가?

1. 사칭이란 무엇인가?

온라인에서 의도적으로 타인을 흉내내거나 타인인 것처럼 행동하는 행위를 온라인 타인 사칭(online impersonation)이라고 한다.[1] 우리나라 형사법상 단순히 사칭하는 것만으로 처벌하는 조항은 없다.[2] 따라서 단순히 '말'로만 사칭한 경우, 윤리적 비난을 받을 수는 있으나 이를 범죄로 보기 어렵다. 물론 사칭이 단순한 말에 그치지 않고 ① 문서로 표시된 경우, 문서와 관련된 범죄가 성립할 수 있으며 ② 재물을 교부받거나 재산상 이익을 취한 경우, 사기죄(컴퓨터 등 사용 사기 포함)가 성립할 여지는 있지만 추가적인 구성요건이 충족되어야 하므로 상당히 제한적이다.

2. 사칭에 대한 법적 공백

사칭에 대한 기존 「형법」의 한계를 드러내는 판결로, 대법원 2016년 3월 24일 선고된 2015도10112 판결이 있다. 이 사건에서 피고인은 피해자의 사진, 이름, 생년월일 등을 이용해 소개팅 어플리캐이션(application)에 가입한 후, 피해자의 사진과 이름 등을 프로필에 게시하고 다른 남성 회원들과 대화하며 전화번호를 제공했다. 이에 대해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 제70조 제2항에 따른 사실적시 명예훼손죄로 기소되었으나, 대법원은 이를 '사실'을 적시한 것으로 볼 수 없다는 이유로 범죄의 증명이 부족하다고 판단했다. 이 사건은 1심, 2심, 대법원까지 모두 무죄로 판단되었다는 점에서 주목할 만하다. 이와 유사한 취지의 판결로 대법원 2018년 5월 30일 선고된 2017도607 판결이 있다.

결국 온라인에서 타인을 사칭하는 행위만으로는 정보통신망법상 명예훼손죄가 성립하지 않는다. 따라서 사칭 행위에 대해서는 오로지 플랫폼의 자율규제에 의존할 수밖에 없는 상황이다.

민사상에서도 사칭 그 자체만으로는 불법행위로 보기 어렵다. 첫째, 형사적 판단과 유사하게, 사칭 행위가 '위법행위'인지가 불명확하며, 앞서 언급한 대법원 2015도10112 판결과 2017도607 판결에 따르면 위법행위로 인정되지 않을 가능성도 있다. 설령 위법행위로 간주되더라도

---

1) 온라인 타인사칭의 방법은 ① 프로파일 스쿼팅(profile squatting: 실제로 존재하는 타인의 신상정보를 사칭하여 그 타인인 것처럼 행세하는 것)과 ② 캣피싱(catfishing: 가공의 인물을 설정하여 실제로 존재하는 것처럼 행세하는 것), ③ 신원절도(identity theft: 의도적으로 다른 사람의 신분을 사용하는 불법행위) 등으로 나뉜다. 정완·안아름 (2018). 온라인 타인사칭의 법적책임에 대한 연구. 〈홍익법학〉, 제19권 제2호 참조.

2) 「형법」상 '사칭(詐稱)'이라는 용어가 사용되는 법조문은 오로지 제118조의 공무원자격사칭죄 밖에 없는데, 구성요건은 공무원 자격의 사칭과 직권의 행사 두 가지여서 사칭 그 자체를 처벌하지 않는다.

타인에게 손해가 발생하여야 비로소 불법행위가 성립할 수 있다. 따라서 손해가 발생하였음을 입증하고 그 손해액을 산정하여야 하는데, 이 모든 과정은 결코 쉽지 않다. 향후 민법상 인격권이나 인격표지영리권이 입법되지 않는 한, 인격적 이익 침해를 주장하고 이를 입증하는 것은 매우 어려운 과제다.

3. 사칭과 법적 제재 가능성

결국 사칭 그 자체는 현행 법체계에서 법적 책임을 묻기가 매우 어렵다고 볼 수 있다. 따라서 로맨스 스캠(romance scam), 투자 사기, 공동구매 사기, 문서위조에 의한 피해 등 구체적인 사건이 발생해야만, 추가적인 요건을 검토하여 범죄의 구성요건을 충족하는지를 판단한 후, 각 개별 범죄의 성립 가능성을 평가하고 형사절차를 통해 범죄자에 대한 처벌을 구한 뒤 민사절차를 통해 피해 구제를 받을 수밖에 없다. 그렇다면, 사칭이 무해한 행위인가? 그렇지 않다.

사칭은 범죄로 이어질 수 있는 일종의 예비적 행위로 볼 수 있다. 결국, 사칭은 사람의 신뢰를 이용해 타인을 기망하는 행위에 해당하기 때문이다. 따라서 사칭은 사기 범죄의 기망에 착수하기 위한 일종의 음모 또는 예비행위로 판단할 수 있다. 그러나 우리 「형법」 제28조는 범죄의 음모 또는 예비행위는 법률에 특별한 규정이 없는 한 처벌하지 않는다고 규정하고 있으며, 사기죄에는 음모 또는 예비행위에 대한 처벌 조항이 없기 때문에, 사기를 목적으로 신원을 속이는 사칭행위 자체는 처벌할 수 없다. 결론적으로 범죄 행위가 발생해 미수든 기수든 결과가

나타나야만 사칭범에 대해 민형사적 조치를 구할 수 있게 된다.

국회에 정보통신망법 개정법률안은 2015년의 개정안(의안번호: 1914659, 1916055) 및 2016년의 개정안(의안번호: 2000735)이 상정되었으나 모두 폐기된 상황이다.

비교하여, 미국은 각 주(州)법에 따라서 '사칭(criminal impersonation)' 그 자체를 처벌하기도 한다. 15개 주에서 기존의 「형법」상 '사칭' 조항을 마련하고 있으며, 특히 뉴저지주, 캘리포니아주, 와이오밍주, 뉴욕주 등 8개 주에서 온라인 타인사칭 조항을 별도로 마련하였다.[3] 또한 루이지애나주, 로드아일랜드주, 미시시피주, 텍사스주에서는 컴퓨터 범죄의 하위규정으로 온라인 타인사칭 조항을 별도로 규정하였다.[4]

Ⅲ 온라인 사칭 범죄, 법적 공백과 사적 제재

1. 플랫폼의 자율인가, 방치인가

우리나라 법제도는 빠르게 변화하는 사회와 기술 환경을 충분히 반영하지 못하고 있어, 온라인 사칭에 의한 법적 공백이 발생하고 있다. 특히 온라인 사칭 범죄와 같은 신종 행위는 범죄로 취급되어야 함에도 불구하고, 기존 법체계에서는 이러한 행위들을 충분히 규제하지 못하고 있다. 그 결과, 유명인들의 초상권과 개인정보가 무분별하게 사칭당하고 이를 악용한 다양한 범죄가 발생하고 있음에도 속수무책으로 당할 수밖에 없는 상황이 초래되고 있다.

이러한 법적 공백 속에서 기대할 수 있는 것은 플랫폼의 자율규제에 불과하다. 그러나 현실에서는 SNS를 통해 타인을 사칭하는 계정들이 여전히 활발히 활동하고 있으며, 플랫폼들은 자율규제라는 명목 하에 이러한 문제를 사실상 방치하고 있다. 사칭 행위만으로는 법적 제재를 가하기 어려울 뿐 아니라, 사칭자를 적발하는 것도 플랫폼의 협조 없이는 매우 어려운 실정이다. 플랫폼은 커뮤니티의 생태계와 표현의 자유를 보호한다는 명목을 내세우지만 이는 사실상 자사의 영업적 이익을 우선시하는 방관에 불과하다.

최근 걸그룹 아이브 멤버 장원영이 미국의 디스커버리 제도를 활용해 범죄자의 신원을 밝혀낸 사례가 주목받고 있지만, 이러한 제도를 활용하기 위해서는 먼저 사칭 행위가 범죄임을 입증해야 한다. 즉, 범죄가 성립하지 않는다면 사칭자의 신원을 알아내는 것조차 불가능하다. 문제는 우리나라 법률상 사칭 그 자체만으로는 처벌하기 어렵다는 점이다. 이로 인해 사칭범들은 플랫폼의 보호 아래 규제와 견제 없이 활동하며 무제한의 자유를 누리고 있는 실정이다.

---

3) 정완·안아름 (2018). 앞의 글, pp.402–403.

4) 정완·안아름 (2018). 앞의 글, pp.403.

2. 사칭범, 추적의 실패와 수사중지

'유사모' 발족의 계기가 된 주진형 전 한화투자증권 대표의 사례는 이러한 문제의 심각성을 잘 보여준다. 주 전 대표는 자신의 이름과 얼굴을 사칭해 온라인에서 불법 광고를 한 범죄자를 고소했지만, 수사기관으로부터 "귀하 사건의 페이스북 계정 가입자 정보를 확인하였으나 피의자 인적사항을 특정할 만한 수사단서를 확보하지 못하는 등 현재로서는 범인 검거를 위한 단서를 발견하기 곤란해 수사중지 예정입니다"라는 통지서만 받았다.[5)]

빅테크 온라인 플랫폼의 방치 아래, 디지털 시대에 불법적인 증권 광고와 유명 인물 사칭은 일상적인 일이 되었다. 이러한 사칭 행위는 단순히 법규를 위반하는 것에 그치지 않고, 투자자의 신뢰를 저하시켜 금융시장의 안전성까지 위협하는 심각한 문제를 야기한다. 그러나 이와 같은 사칭 범죄에 대한 법적 규제는 여전히 공백 상태에 있으며, 플랫폼 자율규제의 한계는 이러한 상황을 더욱 악화시키고 있다. 더구나 딥페이크(deepfake), 딥보이스(deepvoice)와 같은 첨단 AI(Artificial Intelligence) 기술이 사칭에 악용되면서, 실제와 구분하기 어려운 영상이나 음성을 통해 타인을 속이는 수법이 점점 더 정교해지고 있다. 이는 단순한 사기를 넘어 대중의 신뢰를 악용하고, 사회 전반에 걸친 불신을 조장하는 심각한 문제로 이어지고 있다.

3. 자력구제와 사적제재로 내몰리는 피해자들

이러한 법적 공백은 사적 제재를 정당화하는 상황을 초래하고 있다. 법적 제재가 효과적으로 이루어지지 않는 상황에서 피해자들은 스스로를 보호하기 위해 사적 제재에 나서고 있는데, 이는 또 다른 사회적 혼란을 불러일으킬 수 있다. 법적 보호가 미비한 상황에서 사칭 피해자들이 스스로 정의를 실현하려는 비질란테(vigilante) 즉, 자경단(自警團) 현상으로 이어지고 있다. 이는 피해자가 자신의 피해를 직접 해결하려는 행동으로, 종종 법적 절차를 무시하고 무분별한 방식으로 이루어진다. 예를 들어, 사칭 범죄자를 공론화하거나 온라인 상에서 개인의 신상을 공개하는 행위는 쉽게 명예훼손이나 「개인정보보호법」 위반으로 이어질 수 있다. 이러한 사적 제재는 결과적으로 무고한 사람들에게 피해를 입히는 악순환을 초래하며, 사회의 법질서와 신뢰를 무너뜨린다.

실제로 사칭 범죄와 관련된 오인이나 추정에 의해 무고한 사람들이 피해를 입는 사례가 발생하고 있다. 전화번호가 비슷하다는 이유만으로 협박과 문자 폭탄에 시달리거나, 잘못된 정보로

5) 임지선·박지영 (2024. 3. 25). [단독] 주진형 사칭 온라인피싱, 검·경은 수사중지 통보만. 〈한겨레〉. URL: https://www.hani.co.kr/arti/economy/economy_general/1133652.html

인해 사회적 매장을 당하는 등의 사례가 대표적이다.[6] 피해자들은 법적 보호를 받지 못한 채 심리적, 경제적 피해에 노출되고 있으며, 이로 인해 더욱 큰 사회적 문제가 발생할 가능성도 높아지고 있다.

결국 이러한 법적 공백은 사적 제재를 정당화시키고 그로 인해 더 큰 사회적 혼란과 갈등을 초래할 위험이 있다. 법적 구제의 공백을 메우고 피해자들이 스스로 사적 제재에 나서지 않도록 공적 제재의 역할을 강화하는 것이 중요한 과제이다.

Ⅳ. 해외 주요국의 온라인 사칭 규제 동향

1. 미국

미국 연방거래위원회(Federal Trade Commission, 이하 'FTC')는 정부 및 기업 사칭에 대한 규칙(Rule on Government and Business Impersonation, 이하 '사칭 규칙(impersonation rule)')을 마련하였고, 동 규칙은 2024년 4월 발효되었다.[7]

'사칭 규칙'이 입법되면서 FTC는 정부기관 또는 기업을 사칭하는 사기범을 직접 단속하고 규제할 수 있는 강력한 권한을 얻게 되었다. 구체적으로, FTC는 사칭 사기범을 상대로 연방법원에 직접 소송을 제기하여 피해자들에게 금전적 보상을 제공하고, 사기범들이 불법적으로 얻은 수익을 회수할 수 있으며, 규칙 위반자들에게 민사 과징금(civil penalties)를 부과함으로써 사기행위를 억제할 수 있다. 이는 미국 연방 대법원의 2021년 4월 AMG Capital Management, LLC v. FTC 사건에 대한 판결[8]에 비추어볼 때, FTC가 소비자 보호를 위한 매우 중요한 권한을 얻은 것으로 평가된다.[9]

'사칭 규칙'은 정부와 기업에 대한 사칭에만 초점을 맞춘 것이나, FTC는 2024년 2월 개인 사

---

6) 김용재 (2024. 8. 30). "가해자 우리가 찾겠다"…디지털 장의사·경찰 사칭 등장. 〈헤럴드경제〉. URL: https://news.heraldcorp.com/view.php?ud=20240830050105

7) Federal Trade Commission, "FTC Announces Impersonation Rule Goes into Effect Today", April 1 2024. URL: https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today (최종방문일: 2024년 8월 28일).

8) AMG Capital Management, LLC v. Federal Trade Commission, 593 U.S. ___ (2021). 미국 연방대법원은 2021년 4월 22일, 만장일치로 FTC가 「연방거래위원회법」(FTC Act) 제13(b)조에 따라 불공정 거래를 위반한 업체들로부터 금전적 구제(환수 또는 몰수)를 청구할 권한이 없다고 판결하였다. 미국 연방대법원은 FTC가 다른 절차를 통해 금전적 구제를 청구하거나 의회에 추가 권한 부여를 요청할 수 있다고 판결문에 기재하였으며, 이 판결로 인해 FTC의 권한 강화를 위한 입법 필요성이 제기되었다.

9) Federal Trade Commission, "FTC Proposes New Protections to Combat AI Impersonation of Individuals", February 15 2024. URL: https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals (최종방문일: 2024년 8월 28일).

칭(impersonation of individuals)까지 포함하여 규제하기 위한 보충 통지[10]를 발표하였으며, 2024년 4월 30일까지 대중의견을 수렴[11]한 다음, '사칭 규칙'의 개정에 관하여 검토하기로 하였다. '사칭 규칙'이 개인 사칭까지 확장될 경우, FTC의 권한이 개인 사칭으로 인한 피해자들에 대한 구제책에도 적용될 것으로 예상된다.

2. 유럽연합(EU)

EU는 디지털 서비스와 디지털 시장의 규제와 보호를 목적으로 디지털 서비스 법 패키지(The Digital Services Act package)[12]를 채택하여, EU 전역에서 통일된 규칙을 적용하여 디지털 서비스 이용자들의 기본권을 보호하고자 한다. 동 패키지는 디지털 시장에서 공정한 경쟁을 촉진하기 위하여 '게이트키퍼 플랫폼(gatekeeper platform)'을 규제하는 「디지털 시장법」(Digital Market Act, 이하 'DMA')[13]과 온라인에서의 안전성과 투명성을 높이기 위한 「디지털 서비스법」(Digital Services Act, 이하 'DSA')으로 구성된다.

그 중 DSA는 온라인 이용자의 안전을 도모하고 기본권을 보호하기 위한 법으로서, DSA는 온라인 중개자와 플랫폼을 포괄하여 적용하며, 허위 정보, 불법 콘텐츠[14] 및 기타 사회적 위험과 관련하여 온라인 플랫폼의 책임에 대한 기준을 제시하는 것을 목표로 한다.[15] 특히 대규모 온라인 플랫폼(Very Large Online Platform, VLOP)과 대규모 검색엔진(Very Large Online Search Engine, VLOSE)은 그 규모와 영향력을 고려하여 보다 엄격한 규제를 받는다. DSA를 집행하는 위원회는 조사 및 감독에 대한 권한을 가지며, DSA를 위반한 플랫폼에게 전 세계 매출의 최대 6%에 달하는 벌금이 부과될 수 있다. 이러한 규정에 따라, 온라인 사칭은 불법 콘텐츠나 허위 정보로 분류될 수 있으며, 플랫폼에 대한 규제와 책임 강화의 일환으로 처

---

10) Federal Trade Commission, "Proposed Amendments to Trade Regulation Rule on Impersonation of Government and Businesses". URL: https://www.ftc.gov/system/files/ftc_gov/pdf/r207000_impersonation_snprm.pdf)(최종방문일: 2024년 8월 28일).

11) Federal Trade Commission, "FTC Seek Comment for Trade Regulation Rule on Impersonation of Government and Businesses", March 1 2024. URL: https://www.regulations.gov/document/FTC-2023-0030-0031)(최종방문일: 2024년 8월 28일).

12) European Commission, "The Digital Services Act package". URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package)(최종방문일: 2024년 8월 30일).

13) 게이트키퍼 플랫폼은 연간 매출액, 월간 활성 사용자 수, 연간 활성 비즈니스 사용자 수와 같은 특정 기준을 충족하는 대형 온라인 플랫폼(예: 온라인 검색엔진, 앱스토어, 메신저 서비스 등)을 말한다. 이들 플랫폼은 시장에서 독과점적인 영향력을 행사할 수 있으며, 다른 기업들이 소비자에게 접근하는 경로를 통제할 수 있는 능력을 가지고 있다. 이러한 힘을 통해 공정한 경쟁을 저해할 수 있는 위험이 있기 때문에, DMA는 게이트키퍼 플랫폼을 특별히 규제하여 시장의 투명성과 공정성을 높이고자 한다. European Commission, "The Digital Markets Act". URL: https://digital-markets-act.ec.europa.eu/index_en)(최종방문일: 2024년 8월 30일).

14) DSA는 "오프라인에서 불법인 것은 온라인에서도 불법"이라는 취지에서 '불법 콘텐츠(illegal contents)'라는 개념을 광의로 파악한다. Anna Pingen, "EP Adopted Position on Digital Services Act", 25 February 2022. URL: https://eucrim.eu/news/ep-adopted-position-on-digital-services-act/ (최종방문일: 2024년 8월 30일).

15) European Commission, "Digital Services Act: Questions and Answers". URL: https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers (최종방문일: 2024년 8월 30일).

리될 것으로 전망된다.

플랫폼은 이용자가 불법 콘텐츠나 상품을 신고할 수 있도록 일관되고 사용하기 쉬운 신고 시스템(flagging system)을 갖추어야 한다. 구체적으로, 플랫폼은 신고를 접수하면 신속하고 신중하게 처리하고 신고자에게 진행 상황을 지속적으로 업데이트하여 알려주어야 한다. 또한 온라인에서 상품이나 서비스를 구매할 때, 이용자에게 판매자에 대한 명확한 정보를 제공하여 누구로부터 구매하고 있는지 명확히 알 수 있게 해야 한다.[16]

DSA에 따라서 허위정보의 확산을 방지하기 위해서는 다음과 같은 네 가지 내용이 중요하다.[17] VLOP와 VLOSE는 ① 서비스와 관련한 다양한 요소에 대한 위험평가를 수행하여야 하고, ② 허위정보가 전파되거나 증폭되는 것을 방지하기 위한 위험 완화조치를 이행하고 위기대응 메커니즘을 갖추어야 한다. DSA는 ③ 플랫폼이 허위정보에 관한 자발적 실천 강령(The 2022 Code of Practice on Disinformation)[18]에 가입할 것을 권장하며, ④ 타겟 광고로 인해 허위정보가 확산되는 것을 방지하기 위하여 VLOP, VLOSE로 하여금 공공 광고 저장소(public advertisement repository)를 유지하게 함으로써, 새로운 위험을 연구하는데 필요한 자료를 얻고자 한다.

3. 영국

영국은 2023년 「온라인 안전법」(Online Safety Act)[19]을 제정하여 온라인에서 아동과 성인을 보호하기 위한 새로운 법적 규제 체계를 도입하였다. 이 법은 플랫폼에게 사용자 안전을 보장할 의무를 부과하며, 불법적인 활동에 사용되거나 불법 콘텐츠가 나타났을 때 이를 신속하게 제거하도록 요구한다. 오프컴(Ofcom)은 이 법의 시행을 감독하는 독립 규제기관으로서, 플랫폼이 의무를 이행하지 않을 경우 최대 1,800만 파운드 또는 전 세계 매출의 10%에 해당하는 벌금을 부과할 수 있으며, 필요한 경우 법적 조치를 취할 수 있다. 이에 따라 플랫폼은 온라인 사칭과 같은 불법행위나 범죄를 방지하기 위한 시스템을 설계하여야 하며, 이를 적절히 이행하지 않을 경우 법적 제재를 받을 전망이다.

---

16) European Commission, “DSA: Making the online world safer”. URL: https://digital-strategy.ec.europa.eu/en/policies/safer-online (최종방문일: 2024년 8월 30일).

17) European Commission, “Digital Services Act: Questions and Answers”. URL: https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers (최종방문일: 2024년 8월 30일).

18) European Commission, “The 2022 Code of Practice on Disinformation”. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (최종방문일: 2024년 8월 30일).

19) UK Department for Science, Innovation & Technology, “Online Safety Act: explainer”, 8 May 2024. URL: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (최종방문일: 2024년 8월 30일).

4. 일본

일본은 총무성의 주도로 '디지털 공간에서의 정보 유통의 건전성 확보 방법에 관한 검토회'를 개최했다. 가장 최근인 2024년 5월 15일 회의에서 제출된 플랫폼 사업자 청문 결과[20]에 따르면, 대부분의 일본 국내 사업자들이 허위 및 오정보에 대한 별도의 정책을 마련하지 않았으며, 콘텐츠 모더레이션(삭제, 계정 정지 등)에 대한 구체적인 대응 기준에 대해서도 명확한 답변을 제공하지 않았다는 점이 지적되었다. 또한, 정기적인 정책 검토와 외부 기관에 의한 리뷰에 대한 답변도 부족했다.[21] 더 나아가, 일본 내외의 많은 사업자들이 사실관계 확인 기관과의 협력, 모니터링 대응, 관계 기관과의 협력, 향후 대응 계획 등에 대해 명확한 답변을 하지 않은 것으로 나타났다.[22] 사이버 보안 및 허위 정보 유통과 관련해서도 사칭 웹사이트나 계정에 대해 사이버 보안 관련 기관과 협력한 활동을 수행한 사업자는 일부에 불과했으며, 그 외에는 허위 정보의 유통 및 확산에 대한 명확한 대응이 부족한 상황이었다.[23] 일본은 이러한 검토회를 지속하며, 관련 법안 및 규제에 대한 논의를 이어갈 것으로 전망된다.

V. 마무리하며

디지털 시대에 우리는 세 개의 중요한 문 앞에 서 있다. 첫 번째 문은 '사칭'이라는 문이다. 이 문은 누군가가 타인의 신원을 도용하거나 거짓 신분으로 행세할 수 있게 만드는 출입구이다. 세계 각국은 이 첫 번째 문을 닫기 위해 다양한 노력을 기울이고 있다. 예를 들어, 미국은 사칭 행위에 대한 형법적 처벌 조항을 강화하고, FTC의 권한을 확대하여 신종 사칭 사기에 대응하고 있다. EU와 영국은 플랫폼의 책임을 강화하는 규제를 통해 이 문을 단단히 잠그려 하고 있다. 일본도 온라인 플랫폼의 실태를 면밀히 조사하며 대응책을 모색하고 있다. 이와 같은 글로벌 동향은 사칭이라는 첫 번째 문을 확실히 닫아야만 한다는 시대적 당위성을 보여준다.

그러나 우리나라의 경우, 이 첫 번째 문이 여전히 열려 있는 상태다. '사칭' 자체에 대한 법적 규제가 미비하여, 이를 단순한 '거짓말'로만 취급하고 있다. 이 문을 닫지 않으면, 사칭을 통해

---

20) URL: https://www.soumu.go.jp/main_sosiki/kenkyu/digital_space/02ryutsu02_04000475.html

21) 日本 総務省, デジタル空間における情報流通の健全性確保の在り方に関する検討会(第19回)配付資料 ※ワーキンググループ(第19回)合同開催 , 資料19-1-2 プラットフォーム事業者ヒアリングの結(暫定版), pp.1-14. URL: https://www.soumu.go.jp/main_content/000946387.pdf

22) 日本 総務省. 앞의 글, pp.22-24.

23) ① 사이버 보안 기관 관련 협력 활동의 예시로 일본 사이버 범죄 대책 센터(JC3)와 피싱 대책 협의회에 회원으로 참여하여 해당 서비스에 관계 없이 피싱 사이트 정보나 가짜 사이트와 같은 위협 정보를 제공받고, 자사에서 발견한 피싱 사이트 정보를 협의회를 통해 JPCERT/CC와 공유하여 사이트 폐쇄조치를 지원하는 것이 있다. ② SNS 가짜 계정에 대한 대응으로 사내 조사 및 사내외 CSIRT 창구로부터 접수된 통보를 통해 자사와 관련된 SNS 가짜 계정을 발견하고 허위 또는 오정보의 유통 및 확산에 대응하기 위해 계정 중지 등의 조치를 취하는 것이 있다. 日本 総務省. 앞의 글, pp.30-31.

두 번째 문이 열리게 된다. 이 두 번째 문은 사칭으로 인해 파생되는 사기, 문서 위조, 명예훼손과 같은 범죄들로 이어지는 출입구다. 따라서 사칭이라는 첫 번째 문을 닫는 것이 필수적이며, 이를 통해 그 이후에 이어질 수 있는 범죄들의 두 번째 문을 차단할 수 있다.

세 번째 문은 '플랫폼의 책임'이라는 문이다. 현재 각 플랫폼마다 신고 절차와 기준이 제각각이어서, 피해자들은 불안정한 상황에 처해 있다. 플랫폼의 자의적 판단에 따라 차단되지 못한 정보가 확산되면, 2차 피해가 발생할 가능성이 크다. 따라서 이 세 번째 문을 강화하고, 플랫폼의 부작위 또는 방치에 대한 강력한 책임을 부과해야 한다. 이는 빅테크 기업들이 그들의 강력한 영향력에 상응하는 책임을 다하도록 요구하는 중요한 과제이다.

결국, 우리나라 정부와 입법기관은 이 세 개의 문을 모두 단단히 잠그는 법적 장치를 마련해야 한다. 첫 번째 문인 '사칭' 자체를 규제하고, 두 번째 문인 사칭으로 인한 범죄의 발생을 막으며, 세 번째 문인 플랫폼의 책임을 강화하는 것이다. 이를 통해 디지털 사회의 안전성과 신뢰성을 확보하고, 피해자들이 신속하고 효과적인 구제를 받을 수 있는 환경을 조성할 수 있다. 이제는 이 세 개의 문을 단단히 잠글 시점이다.