형사정책연구 Korean Criminological Review
제25권 제3호(통권 제99호, 2014 · 가을)

SNS상 개인정보 무단 수집·보관·유포 및 타인사칭에 대한 형사법 연구*

이 상 현**

국 | 문 | 요 | 약

SNS의 활용이 연령을 넘어 점차 대중화되어 감에 따라 소위 신상털기 기타 개인정보 무단 수집 및 유포, 타인 사칭과 같은 SNS를 이용한 일탈행위의 피해 확산에 대한 우려가 커지고 있다. 또한, 이러한 사건이 실제 발생함에도 현재 우리의 정보화 관련 입법, 특히 형사입법과 실무는 이러한 일탈행위에 대해 아직 실체법적으로 충분한 대비책을 갖추지 못하고 있다. 또한, 국경을 넘어서는 인터넷의 이용 확대는 해외 소재 SNS 사업자-페이스북 또는 트위터-에 대한 우리나라의 법 적용 역시 법적 근거가 확립되지 않고 있다.

본 논문은 SNS상 개인정보 무단 수집, 유포 및 무단 타인사칭에 대한 우리의 대응 입법, 판례를 검토한 후, 미국, 캐나다, 영국과 독일의 형사법제 및 EU와 UN의 법제를 비교 분석하였다. 이를 토대로 SNS상 개인정보 무단 수집보관, 유포, 타인사칭에 대한 범죄화 입법을 구체적으로 제안하고, 외국 소재 SNS사업자에 대한 법의 실효성 확보를 위한 법리 개발 및 SNS사업자에 대한 법적 의무 부과방안을 모색해 보았다. 세계 선진국 수준의 SNS 이용율을 나타내는 우리나라에서 개인정보 무단 수집 및 타인사칭에 대한 형사법제 수준은 선진국에 미치지 못하고 있는 점을 고려해 이 부분의 형사제재가 시급히 개선될 필요가 있다.

❖ 주제어 : 개인정보, SNS, 개인정보 무단 수집, 아이디절도, 무단 타인 사칭

* 본 연구는 한국연구재단의 2014년 신진연구자 지원사업의 재정 지원으로 행해졌음을 알리고자 한다. 또한, 연구에 필요한 자료를 수집하는 등 성실한 조력을 아끼지 않은 김명훈 석사, 김연희 양(숭실대 법학과 4학년)과 이충호 군(숭실대 국제법무학과 4학년)이 본 논문 작성에 커다란 힘이 되었음을 밝힌다.

** 법학박사(S.J.D), 미국 뉴욕주 변호사. 소속: 숭실대학교 법과대학(Soongsil Univ. College of Law) 국제법무학과(Department of Global Law). 직위: 조교수(associate professor)

Ⅰ. 서론

한국사회에서 2000년대 초·중반 유선인터넷 시대의 '싸이월드', 2010년대에 진입하며 스마트폰 등 모바일 인터넷 시대의 페이스북(Facebook)[1], 카카오스토리, 트위터(twitter)로 대표되었던 소셜네트워크서비스(Social Network Service(Site)이하 SNS)[2]는 정보통신기술의 습득에 빠른 젊은층에서 애용되어 왔었다. 그런데, 2010년대 중반에는 시간과 장소에 구애 받지 않고 실시간 인터넷의 이용을 가능하게 하는 스마트폰 등 모바일기기의 대중화와 함께, 밴드(BAND), 링크드인(LinkedIn) 등 새로운 SNS의 이용이 전 연령대의 국민을 대상으로 급속히 확산되고 있다.[3] 이들 SNS는 글, 사진, 동영상과 인터넷 링크 등을 자신의 계정에 올려 이를 다른 이들과 공유하고 이에 대해 타인들이 댓글을 달 수 있도록 하는 등 다양한 방법으로 짧은 시간에 다수인과의 소통을 가능케 하고 있다.

SNS는 휴대용 모바일기기를 통한 실시간 접속 및 빠른 전파력, 다수와의 소통 편이 측면의 사적 그룹내 소통수단이나 기업홍보 수단으로 기능하면서, 종래 전형적인 사이버범죄-예를 들면, 명예훼손, 음란물 유포 등-의 수단으로 악용되기도 했다.[4] 그러나, 이를 넘어서서 3천만명의 가입자를 가졌던 싸이월드 해킹 사건으로

---

1) 종래 자신이 원하는 사람에게만 정보 노출을 허용하는 싸이월드(일촌맺기)가 해킹 및 대규모 개인정보(비밀번호 포함) 유출로 쇠락하는 사이 미국에 기반을 둔 페이스북(Facebook)이 그 자리를 대체하고 있다.

2) 관심, 활동 또는 학교 등의 일정한 관계를 공유하는 개인들이 자신의 프로필을 올리고 서로 인맥을 구축할 수 있도록 하는 웹에 기반한 기술 서비스로 정의된다. Danah M. Boyd & Nicol B. Ellison, Social Network Site: Definition, History & Scholarship, Journal of Computer-Mediated Communication, Volume 13, Issue 1, Article first published online (2007)

3) 연합뉴스 최인영 기자, 50대 '디지털 신중년층' 증가…메시지·SNS 이용률 증가, 2014년 3월 27일 (http://www.yonhapnews.co.kr)(2014년7월9일 검색)(미래창조과학부가 발표한 '2013년 정보문화 실태조사' 결과-만6세 이상 인터넷이용자 4천6백5십명 대상-에 따르면 50대의 SNS 이용률은 2012년 26.2%에서 2013년 39.1%로 늘었으며, 60대의 SNS 이용률도 10.1%에서 21.7%로 각각 두 배 이상 증가했다. 50·60대의 활약에 힘입어 SNS 이용률도 60.2% (2012년)에서 63.3% (2013년)로 3% 이상 증가)

4) 정보통신망법상 명예훼손에 대해서는 서울북부지방법원 2012. 11. 28. 선고 2012고단1594, 2054(병합) 판결(연예기획사 대표가 전속모델에 관한 허위사실을 트위터에 게시하여 정보통신망법상 명예훼손 유죄)과 서울중앙지방법원 2012. 8. 16. 선고 2012고단552 판결(롯데OOOO의 소주가 독극물과 유사한 물로 만들어졌고 불법적으로 면허를 받았다는 등 허위의 사실을 트위터를 이용하여 전파하여

인한 개인정보 유출, 고도의 정보 수집 기술 및 빅데이터 분석 기법 등의 개인정보 획득·분석 능력을 악용한 개인정보침해, 이로 인한 2차 피해-예를 들면, 피싱(phishing)[5], 스미싱(smishing)[6] 등 신종 금융사기-에 대한 SNS 이용자들의 우려 역시 확산[7]되고 있다. SNS 가입시 실명인증을 요구하지 않는 점[8]을 악용한 타인 명의의 계정을 통한 타인 사칭 SNS 이용도 2차 피해인 사기, 명예훼손의 피해 발생 전에 차단하기가 쉽지 않다.

이러한 기술 진보에 따른 신종 사이버범죄 또는 SNS를 통한 일탈행위에 대한 범죄화 및 형법 투입에 대해, 한편에서는, 사적 소통 수단인 SNS의 특징과 표현의 자유를 강조하면서 이러한 소통을 형법의 적용에서 제외해야 한다는 주장[9]을 제기한다. 반면, 새로운 양상의 법익 침해행위에 대해 기존 형법 및 형사소송법 규정의 적절성과 효과성을 재고해야 한다는 주장[10]도 설득력있게 제기되고 있다.

본 연구는 SNS의 이용 확산에 따른 여러 다양한 일탈행위 중 지면 관계상 논의를 개인정보 무단 수집·보유·누설 등 침해행위와 온라인상 타인 사칭행위로 제한

정보통신망법상 명예훼손과 형법상 신용훼손 유죄)를 참조하라. 또한, 형법상 협박죄와 정보통신망법의 음란물유포죄에 관해서는 청주지방법원 2013. 11. 15. 선고 2013고단1284 판결(종전 연인에 대해 성관계 및 나치 장면 동영상을 페이스북에 올렸고, 계속 만나주지 않으면 일반 공개로 설정하겠다고 협박하여 협박죄, 정보통신망법 음란물 유포 유죄) 등이 있다.

5) 조종엽 기자, SNS에 공개한 자녀이름-학교, 피싱 먹잇감으로 노출, 동아일보, 2014.2.4. (http://news.donga.com 에서 검색 가능)

6) SK 브로드밴드 블로그, SMS에서 SNS로 진화하는 스미싱, 2014.1.2.(http://blog.skbroadband.com)

7) 연합뉴스, 앞의 기사(개인정보와 콘텐츠를 무단으로 이용하는 행위의 심각성을 인식하고 있다는 답변도 각각 89.6%에서 93.3%로, 76.6%에서 83.4%로 증가)

8) 헌법재판소는 정보통신서비스 제공자 중 정보통신서비스의 유형별 일일 평균 이용자 수가 10만명 이상인 대통령령으로 정하는 기준에 해당되는 자에게 본인확인조치 의무를 부과했던 정보통신망법 제44조의 5에 대해 표현의 자유, 사생활의 비밀과 자유, 정보의 자기결정권을 침해한다며 2012년 위헌(2010헌마47·252(병합))결정을 내렸다. 미국에서 실명정책을 고수했던 페이스북도 최근 일부 이용자에 대한 가명, 예명 사용을 허용하기로 결정했다. 임세정 기자, 페이스북 '100% 강제실명제' 포기, 국민일보, 2014년 10월 4일자, 11면.

9) 박경신, SNS의 매체적 특성과 법적용의 한계, 인하대 법학연구 제15집 제3호, 127-152면 (2012). 사이버선거운동에 선거법상 벌칙 규정 적용에 소극적 입장으로 지영환, 전현욱, SNS上의 선거운동에 대한 형사법적 규율, 경희법학 48권 4호, 83-107면 (2013).

10) 임채곤, 사이버 범죄에 관한 연구 - 허위사실유포죄, 사이버모욕죄, 인터넷 실명제 중심으로, 경상대학교 박사학위 논문, 2013; 이상현, 전홍식, 사이버선거운동의 자유화 및 사이버선거범죄에 대한 공직선거법상 형사제재의 대응 : SNS를 중심으로, 법학연구 제46집, 261~290면(2012).

하고, 관련 현행법제의 문제점을 지적한다. 다음으로, 이러한 범죄유형에 대한 SNS 및 모바일기기 이용이 보편화된 미국, 캐나다와 영국, 독일 등 EU의 입법을 조사·검토한다. 위의 검토를 토대로, 본고는 현행 형사법제 개선방안을 제안한 후, 결론을 제시한다.

Ⅱ. SNS를 통한 개인정보 무단 수집 및 타인 사칭

1. SNS에 의한 범죄적 일탈행위의 유형: 개인정보 무단 수집 및 타인 사칭

SNS를 이용한 범죄적 일탈행위는 다양하게 나타나고 있으며[11] 향후 기술의 진보에 따라 그 변화가 예측하기가 쉽지 않다. 본 연구는 SNS를 이용한 일탈행위의 범위를, 지면과 시간의 한계를 고려해, 개인정보와 프라이버시 침해 유형, 이용자 사칭 등 인격권 침해 및 기업 상표 침해 유형으로 제한하고자 한다.

먼저, SNS의 이용은 개인정보를 공개하여 프라이버시 침해의 가능성을 높게 한다. SNS 이용자는 자신의 이름, 이메일, 나이, 생년월일 및 사진, 가족과 친구의 이름 및 사진, 자신의 직업, 소속기관, 현재 상황과 관심사를 타인에게 노출하며, 나아가 거주지 주소, 전화번호, 가족관계의 상세사항 등 정보를 다른 이용자에게 노출하는 경우도 많다. SNS 사업자 측면에서는 이런 정보가 마케팅이나 비즈니스 목적으로 매우 유용한 정보로 수집할수록 이익이 되며 실제 페이스북은 이러한 정보를 이용하여 관련된 이용자들의 사진을 보여주면서 친구맺기를 유도하고 있다. 기술적 제한을 통해 자신이 공개에 동의한 이용자에게만 정보를 노출하도록 하는 것이 원칙이나 SNS 이용자가 올린 개인정보의 제3자에 대한 노출을 완벽히 차단시킬 수는 없다.[12] 실제로는 SNS상에서는 동의를 받은 이용자(페이스북의 '친구')

11) 디지털 형태의 음란물의 유포, 허위 사실의 유포 뿐만 아니라 저작권을 침해하는 문서나 디지털 파일의 유포가 손쉽게 가능하게 되었다. 이 부분에 대한 논의는 다른 논문에서 제시하고자 한다.

12) 한 팔레스타인 페이스북 이용자는 친구가 아님에도 페이스북 회장의 개인정보를 유출시켜 프라이버시 보호의 기술체제의 허점을 노출시켜 보이기도 했다. Associate Press, Palestinian hacks Mark

의 새로운 동의(페이스북의 '좋아요' 버튼)를 통해 또는 동의 없는 경우에도 퍼나르기(트위터상 '팔로워'의 '리트윗')를 통해 자신의 글 등이 제3자에게 손쉽게 공유되고 있다.

둘째, SNS 이용자를 이름과 아이디를 사칭하여 자신이 그 이용자인 것으로 행세하면서 그 이용자의 명예, 인격을 침해하거나 자신이 경제적, 사회적, 정신적 이익을 취득하는 사례들이 나타나고 있다. 이러한 SNS 이용 일탈행위에 대해서는 아직 범죄화 논의가 충분히 제기되고 있지 않으며 기존의 형사법적 대응으로는 신속성, 효과성, 처벌의 적절성의 측면에서 문제가 되고 있다.

2. 당벌성과 형벌 필요성

가. 개인정보 무단 수집 및 유포

모바일 인터넷 및 SNS 대중화 시대에서 개인정보는 헌법상 보장되는 사생활의 비밀(제17조), 통신의 비밀(제18조), 인격권(제10조) 뿐만 아니라 최근 출시된 SNS상 소액 결재와 인터넷 뱅킹의 연계 서비스의 예를 통해서 볼 때 재산권(제23조)와도 직접 관련이 있는 법익이다. 따라서, 개인정보는 형법 투입을 위한 보호법익으로 인정될 수 있다. 이를 전제로 개인정보의 온라인상 무단 유포는 그 자체로 법익침해의 결과불법와 사회적 비난가능성이 높은 행위로서 행위불법이 인정된다. 한편, 무단 개인정보 수집·보유행위는 그 자체로 결과불법이 인정되며, 범죄 목적을 위한 수단인 경우 상당한 행위불법도 인정된다.

범죄화 입법의 필수적 요건인 당벌성(strafwuerdigkeit)에서 '정의(Gerechtigket)'로부터의 판단기준에 따르면, 법익침해 빈도, 사회적 결핍정도 및 그 침해가 야기하는 위협감정을 고려해야 한다.[13] 인터넷상 개인정보의 이용확대는 모바일 인터넷 기술, SNS의 이용 확대, 수집 및 분석기술의 발전과 결부되어 그 침해 빈도의 증가

Zuckerberg's personal Facebook page, NYDailyNews, Aug.19, 2013 (http://www.nydailnes.com에서 검색).

13) Winfrid Hassemer, Kommentar zum Strafgesetzbuch, Band 1, Rn 199-200 (Luchterhand 1990).

를 야기하고 있다. 아래 <표 1>에서는, 스마트 기기의 보급이 확산된 2008년 이후 개인정보 침해(유출)를 경험한 응답자 비율이 200% 넘게 증가하였음을 보여주고 있다.

〈표 1〉

조사연도	2006	2008	2011
개인정보 침해(유출) 경험자의 수 (비율)	455 (18.9%)	1,184 (29.6%)	817 (81.7%)
총 설문 조사 대상자의 수	2,402	4,000	1,000

출처: 미래창조과학부, 정보보호실태조사(개인부문)[14]과 트렌드모니터, 개인정보 유출 관련 인식조사(2011)[15]

사회적 결핍 정도의 관점에서도 SNS 실시간 이용 확대는 개인정보 노출을 증가시키고 있으며,[16] IT기술 및 빅데이터(big data) 분석기법의 급격한 발전에 따라 기망적 수단의 이용이 없이도 개인정보의 수집 및 분석 수준의 지속적 상승이 예견되어 개인정보 보호에 대한 사회적 결핍은 증가하리라 예상된다.

나아가, 이렇게 SNS와 인터넷을 통해 수집된 개인정보와 분석 결과를 지능적으로 범죄에 이용하는 사례[17]가 등장하고 있다. 이에 따라, SNS를 이용하는 일반인들 사이에 개인정보 침해에 대한 우려는 급증하고 있다. 아래 [그림 1]은 한국인터넷진흥원에 접수된 인터넷상 개인정보 침해 상담 건수의 추이를 나타내고 있는데, 2010년에 비해 2011~2013년의 상담 건수는 100~200%를 초과하는 급격한 증가세를 나타내며 인터넷 이용자들의 개인정보 침해 우려의 급증을 여실히 보여주고 있다. 또한, 실제 개인정보 침해가 발생한 경우에도 침해 상담을 하는 비율이 10% 미만에

14) 개인정보 피해 경험 유무(2006), 개인정보/프라이버시 침해 경험(2008), (http;//www.kosis.kr 에서 검색)

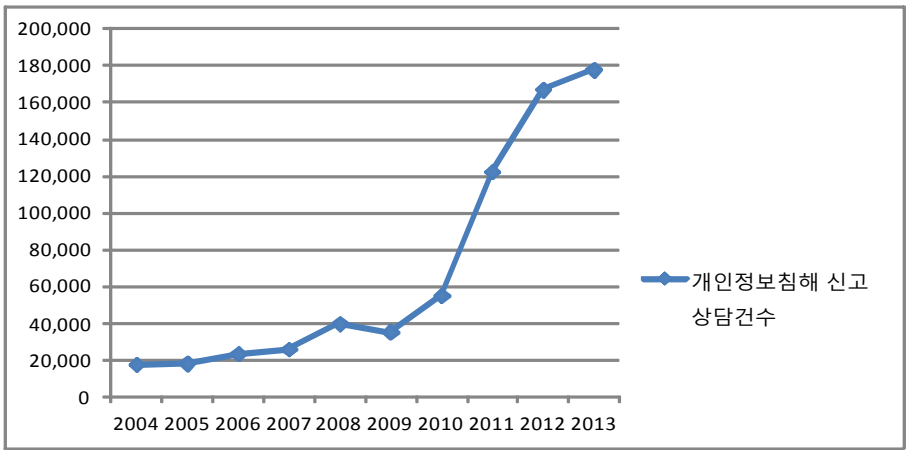
15) 트렌드모니터, 개인정보 유출 관련 인식조사, 리서치보고서 Vol.2011 No.9,p.16(2011)

16) 실제로 SNS상에서 수집가능한 개인정보의 범위는 5~6년 전보다 훨씬 증가하였다. 앞으로도 증가할 것으로 예상된다.

17) SNS가 우리나라보다 더 빨리 자리 잡은 미국의 경우, 절도범이 '집에 혼자 있다'는 내용을 키워드로 삼아 구글 검색을 통해 혼자 지내는 여성, 주택의 확실한 위치 등을 확보하여 지능적인 절도와 강도 범행을 저지르는 사례가 발생하였다. 국민권익위, 블로그.

머무르는 것으로 조사된 설문 결과[18]를 고려하면 실제 피해 사례는 상담 건수의 10배를 훨씬 초과할 것으로 추측된다.

[그림 1] 연도별 개인정보침해 신고 상담 건수



출처: 인터넷 침해대응 지원센터

그러나, 범죄에 활용할 목적으로 SNS나 인터넷상 개인정보를 수집, 분석 하는 경우를 대비한 형사 처벌 규정은 현재 존재하지 않는다. '범죄를 범할 목적으로' 정보통신망 특히 SNS를 통해 노출된 개인정보를 수집, 분석하고 이렇게 분석된 개인정보(분석자료 포함)를 보유, 유출하는 SNS 이용자에 대한 형사입법이 시급히 필요하다.

나. 온라인상 타인 사칭

범죄화 요소로 볼 때 또한, 타인 사칭 행위는 헌법상 보장된 인격권을 침해하는 행위로 사기죄, 명예훼손, 모욕죄 등의 2차 피해로 이어지기 쉽다. 우리 형법에서

18) 만12세~59세까지의 인터넷 이용자를 가진 304,367개 조사구를 대상으로 진행된 설문 조사에서 개인정보·프라이버시 침해 피해를 경험한 인터넷 이용자 중 '관련기관에 신고 또는 상담한 경험이 있다'는 응답 비율은 전체 설문 대상자의 9.7%로 나타났다. 미래창조과학부, 한국인터넷진흥원, 정보보호 실태조사 개인편 -2013, 93면 (2013.12).

명예훼손죄와 모욕죄에 미수범 처벌 규정이 없다는 점을 보면, 현행법제상 타인 사칭행위는 형법 적용 범위 밖에 있음을 보여준다. 하지만, 손해배상 청구소송, 가처분 등 민사적 구제수단이 실효성이 없는데다 정보통신망법상 제재수단이 전술한 바 효과적이지 못한 점을 고려하면, 이 부분에 대한 형사입법의 필요성이 높다.

현재 정보통신망법에서는 사이버 명예훼손죄(제70조) 해당 행위를 3년 이하의 징역, 금고 또는 2천만원 이하의 벌금에 처하도록 규정함과 동시에, 음란정보 유통금지죄(제44조의 7 제1항 제1호), 불안감 야기 정보 유통금지죄(동조 동항 제3호)를 통해 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하고 있다. 또한 성폭력범죄의 처벌 등에 관한 특례법에서는 사이버성폭력에 관한 규정[19]을 도입하고 있다. 이러한 입법적 대처 상황은 (구)정보통신부 정보통신윤리위원회가 규정한 사이버 폭력의 유형, 즉 ①사이버 명예훼손, ②사이버 성폭력, ③음란물 유통, ④사이버 스토킹, ⑤사생활 침해와 신상정보 유통 중 앞의 네 유형에 대한 입법은 어느 정도 확보되었음을 보여주고 있다. 그러나, SNS의 대중화와 함께 문제되고 있는 마지막 ⑤유형 특히 신상정보 유통에 대한 처벌 입법이 불충분함을 보여주고 있다.[20]

3. 현행 형사법적 제재와 문제점

가. SNS를 통한 개인정보 무단 수집, 보관 및 누설에 대한 법제

먼저 형법 비밀침해죄(제316조 제2항)는 '봉함 기타 비밀장치한 .. 사람의 편지, 문서, 도화 또는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸' 행위를 범죄화하여 형사처벌[21]하고 있는데, 이는 개인정보에 일반적으로 적용되는 규정이 아닐 뿐더러 비밀장치과 기술적 수단의 이용을 요구하여, SNS와

19) 한 예로, 통신매체 이용 음란죄(제13조)에서 '자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화, 우편, 컴퓨터, 그 밖의 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말, 음향, 글, 그림, 영상 또는 물건을 상대방에게 도달하게 한 사람을 2년 이하의 징역 또는 500만원 이하의 벌금'에 처하게 하도록 규정한다.

20) 가상준·김강민·임재형, SNS 사용문화가 청소년의 학교폭력 및 사이버폭력에 미치는 영향, 분쟁해결연구 제11권 제1호, 166면 (단국대 분쟁해결연구소, 2013).

21) 구체적으로 3년 이하의 징역, 금고나 500만원 이하의 벌금에 처할 것을 규정하고 있다.

같은 정보통신망상 인적 네트워크에서의 개인정보 무단 수집 등에 적용하기에 적합하지 않다. 한편, SNS와 같은 인터넷기반 서비스에 적용되는 정보통신망 이용촉진 및 개인정보 보호에 관한 법률(이하 정보통신망법)에서는 정보 침해를 금지하는 법 규정과 처벌규정을 아래와 같이 규정하고 있다.

> 제49조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.
>
> 제71조 다음 각호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
> 11. 제49조를 위반하여 타인의 정보를 훼손... 한 자.
>
> 제49조의2(속이는 행위에 의한 개인정보의 수집금지 등) ① 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다.
>
> 제72조 제1항 다음 각호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
> 2. 제49조의2 제1항을 위반하여 다른 사람의 개인정보를 수집한 자
>
> 제73조 다음 각호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
> 7. 제49조의 2 제1항을 위반하여 개인정보의 제공을 유인한 자

개인정보에는 '타인의 비밀'에 해당하는 부분-병력(病歷), 연봉, 가족사(家族史) 등-도 존재하나, 비밀이 아닌 개인정보-생년월일, 주민등록번호, 휴대전화 번호, 자택 전화번호 및 주소 등-도 있으며 SNS상 이용자가 일정 범위 지인에게 스스로 노출하는 것은 주로 후자이다. 이러한 개인정보에 대해서는 정보통신망법상 '훼손'(제49조), '속이는 행위로 수집', '정보를 제공하도록 유인한 행위'(제49조의 2)만을 금지하고 있다. 기술적 수집, 분석기법 등을 이용하여 주체의 동의 없이 수집, 보관, 누설하는 것은 '훼손', '속이는 행위로 수집' 또는 '유인'한 것은 아니어서, 결국 이러한 행위가 명예훼손, 모욕죄가 되지 않는다면, 정보통신망법과 형법의 적용 범위 밖에 있는 것이다.

한편, 개인정보 보호를 다루는 또다른 법률로서 '개인정보보호법'은 정보주체의

동의 없는 개인정보 수집 및 제3자 제공을 금지하고 그 위반 시에 형벌을 규정하고 있다.[22] 그런데, 이 개인정보보호법 벌칙규정의 수범자는 '업무를 목적으로 개인정보파일의 운영을 위해 개인정보를 처리하는' '개인정보처리자'[23] 그로부터 개인정보 처리업무를 수탁받은 자, 개인정보처리자였던 자로 제한되어 있다. 즉, 개인정보 침해에 대한 범죄화 기획시 형사처벌 범위를 제한하기 위해 범죄 주체를 전·현직 '개인정보처리자'와 그러한 업무의 수탁자·양수자로 한정하는 진정신분범 형식과 개인정보를 양수한 공범 형식의 범죄화 입법[24]을 채택하고 있다. 유일한 예외 규정(제70조)은 공공기관의 개인정보를 변경, 말소하여 공공기관 업무에 심각한 지장을 초래하는 행위를 대상으로 하는 결과, 개인정보처리자와 관계 없이 독자적으로 행해진 일반 이용자-업무에 의하지 않는-의 SNS상 개인정보 무단 수집, 보관, 유포행위에 대한 형벌규정은 존재하지 않는다. 이에 따라, 범죄를 목적으로 SNS를 통해 개인정보를 획득·보관·유포하는 일반 SNS이용자(잠재적 범죄인)에 대해서는 적용할 벌칙 규정이 없는 상황이다.

형법외 다른 규제는 실효성이 떨어진다. 현재 정보통신망법상 게시중단 제도,[25] 손해배상 청구가 활용된다. 정보통신망에 게시된 정보가 사생활 침해 등을 야기하는 경우 피해자는 게시중단 요청을 정보통신서비스 제공자-SNS사업자-에 할 수 있는데, 서비스 제공자가 이를 거절하는 경우에는 손해배상 청구소송외에는 별다른 강제력 확보 수단이 없다. 하지만, 이마저도, 대법원 판례에 따르면, 게시중단 요청에 대해 즉시 아닌 상당한 기간 내에 문제된 컨텐츠를 삭제한 경우 홈페이지 운영자에 대해 손해배상책임을 부정하고 있고,[26] 명예훼손 등 2차 피해가 아직 발생하지

22) 개인정보보호법 제71조, 제72조, 제73조는 개인정보처리자에 대한 형벌을 규정하고 있다.

23) 개인정보보호법 제2조 5호.

24) 제26조, 제27조에 대한 벌칙 규정(제71조)를 참조하라.

25) 제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제 등"이라 한다)를 요청할 수 있다. ② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. ... ⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

26) 대법원 2003.6.27. 선고 2002다72194 판결 (그 운영자가 이를 알았거나 알 수 있었다는 사정만으로

않은 상황에서 적절한 배상액 산정이 어렵기에 게시중단 가처분의 인정 여부가 불확실한 점에서 효과적인 규제로 평가되기 어렵다.[27] 이에 따라 개인정보를 무단 유포하는 이용자, 이에 대한 즉각적 차단조치를 취하지 않은 사업자에 대한 효과적 제재수단이 갖추어지지 않은 상태이다. 한편, 정보통신망법에서는 개인정보 수집, 처리에 관한 몇 개의 규정들을 위반한 사업자에 대해 방송통신위원회의 과징금 부과권한을 인정(제64조의 3)하고 있고, 개인정보보호법에서도 법위반행위를 한 개인정보처리자에 대해 과태료 부과를 인정하고 있다(제75조). 하지만, SNS 글로벌화 시대에 트위터, 페이스북 등 외국에 본사를 가진 SNS에 대해 이러한 규제가 어느 정도 영향을 미칠지는 아직 예측하기 어렵다.[28] 그에 따라, SNS를 통한 개인정보 무단 수집 및 유포-소위 '누리꾼의 신상털기'[29]-는 법의 흠결 속에 더욱 기승을 부리고 있다.

나. SNS상 타인 사칭

또한, SNS와 정보통신망의 비대면성을 이용하여 다른 사람을 속일 목적으로 타인으로 행세하면서 그 타인에게 해를 가하거나 자신에게 이익을 가져오게 하는 행위에 대해서 재산상 이해관계인 경우 형법상 사기죄, 허위사실 적시에 의한 인격권

항상 운영자가 그 글을 즉시 삭제할 의무를 지게 된다고 할 수는 없음); 대법원 2009.4.16. 선고 2008다53812 (상당한 기간 내에 삭제할 의무를 불이행하여 손해가 발생하면 손해배상책임을 짐)

27) 같은 취지로 김경환 변호사 [ICT법 바로알기] 인터넷·SNS 타인명의 사칭의 법적 문제, 디지털데일리 2013.9.11. (http://www.ddaily.co.kr) (2014년 7월 11일 마지막 방문)

28) 제64조의 3 제2항에서는 '과징금을 부과하는 경우 정보통신서비스 제공자 등이 매출액 산정자료의 제출을 거부하거나.. 경우 해당 정보통신서비스 제공자 등과 비슷한 규모의 정보통신서비스 제공자 등의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 이하의 과징금을 부과할 수 있다'고 규정한다. 외국에 본사를 둔 사업자의 법규 불준수에 대한 대책으로 입법된 것으로 보이나, 어느 정도 실효성을 가질지 지켜봐야 한다.

29) 명예훼손, 모욕죄의 대상이 되지 않는 단순한 개인정보의 SNS상 공개에 대해서 형사처벌이 불가능하다. 한 예로, 대통령 선거 전 여론조작 의혹을 받고 있는 국정원 직원의 신상을 트위터에 공개한 혐의로 고발당한 소설가 OO와 교수 OO에 대해 서울 수서경찰서는 "트위터에 주민등록번호를 구체적으로 거론한 것이 아니고 그냥 어디 아파트라고 주소가 떠도는 것을 가지고 법을 위반했다고 볼 수 없다"고 밝혔다. 윤해성, SNS 환경에서의 범죄현상과 형사정책적 대응에 관한 연구, 한국형사정책연구원 연구보고서.

침해의 경우는 명예훼손죄, 인격 침해의 언사인 경우 모욕죄가 적용될 수 있다. 그런데, 대법원 판례는 일정한 용도로 사용하도록 타인으로부터 허락 받은 ID와 비밀번호를 자기의 이익을 위해 그 타인을 사칭하여 사용함으로써 권한을 남용한 경우 정보통신망법상 무단 침입-소위 해킹-에 대한 형벌 규정의 적용범위에 포섭되는 것으로[30] 해석하고 있다.[31] 그러나, 해킹은 기술적 수단을 이용하여 정보통신망에 침투하는 행위로, 전술한 행위들은 그 특성상 기술적 수단을 이용하지 않은 무단ID 사용 또는 타인 사칭으로서 해킹에 적용되는 정보망 부단침입 처벌규정에 포섭될 행위로는 적절하지 않다.

SNS가 기업홍보 수단으로 사용되고 있음을 악용하여 무단으로 해당기업을 사칭하는 경우는 상표법 규정의 적용이 문제될 수 있다. 상표법상 '상표권 ...의 침해행위를 한 자'에 대해 7년 이하의 징역 또는 1억원 이하의 벌금에 처한다고 규정한 제93조는 인터넷 거래 사이트에서 유사 상표를 사용하는 상거래를 한 사업자에게 적용을 검토했던 대법원 판례가 나옴으로써,[32] 향후 SNS에서의 상표권 침해행위에 대한 고소가 있는 경우에도 적용될 것으로 예상된다. 그러나, 페이스북, 트위터 등 SNS가 기업홍보의 수단으로 사용됨에 따라 역으로 상표권 침해 없이 특정 기업의 이름을 포함하는 아이디(ID)를 사용하는 무단 기업 사칭에 대해 처벌규정의 공백이 나타난다. 2차적으로 공정거래법, 부정경쟁방지법 위반 행위가 나타나지 않는 1차적 기업 무단 사칭행위에 대해서는 현재 민사적 불법행위로 인한 손해배상 청구 외에 실효성이 떨어지는 정보통신망법상 아이디 사용 금지 요청으로써만 규제될 수

30) 정보통신망법 제48조 제1항 "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망(이하 망)에 침입하여서는 아니된다"고 규정하며, 제72조 제1항 제1호에서는 제48조 제1항의 규정에 위반하여 망에 침입한 자를 '3년 이하의 징역 또는 3천만원 이하의 벌금'에 처하는 것으로 규정한다. 참고로 제48조의 제2항과 제3항은 각각 악성 프로그램의 전달, 유포의 금지와 DDos공격에 의한 망의 장애 야기 금지를 입법화하고 있다(제71조).

31) 대법원 2005.11.25.선고 2005도870 판결 (업무상 알게 된 직속상관의 ID, 비밀번호를 이용, 군 내부 전산망 등에 접속하여 직속상관의 명의로 군사령관에게 'O대위(피고인을 지칭)를 징계하려고 했던 것에 피가 거꾸로 솟구친다'는 식의 이메일을 보낸 행위를 무단 침입죄에 해당함을 판시)

32) 울산지방법원 2013. 7. 12. 선고 2012노788 판결 (옥션(http://www.auction.co.kr)에 상표 등록되어 있는 PSPGO 게임기기의 케이블에 정품 상표와 유사한 FOR PSP go, PSP go를 부착한 케이블을 판매한다고 게시하였으나, 다양한 비정품 주변기기가 판매되고 있는 점, For라는 접두어를 사용하여 정품 게임기기에 사용되는 호환케이블임을 밝히고 있는 점, 인터넷상 제품의 상세정보란에 '정품은 아니지만 저렴한 가격에 좋은 품질'이라는 문구가 있는 점 등에서 무죄로 판단)

있을 뿐이다.

현재 연예인, 정치인 등 유명인과 유명 기업에 국한되어 있던 이러한 SNS상의 타인사칭 사건들은, 사기, 명예훼손 등 2차 피해가 발생하지 않는 한, SNS 사업자의 게시중단 조치의 시행 여부의 재량 및 내부적 기술적 조치 여하에 규제 가능성이 맡겨져 있는 상황이라 판단된다.[33] SNS 대중화와 함께 카카오톡, 페이스북 등 SNS가 금융계정과의 연동 시도[34] 등 기능 확대와 함께 일반인들의 개인정보 침해로 인한 대한 피해가 급속도로 확대될 것이 예상되는데, 이러한 형사입법의 흠결은 조속히 시정될 필요가 있다.

Ⅲ. SNS상 개인정보 무단 수집 및 타인사칭에 대한 외국의 입법례

1. 미국

가. 아이디절도(ID THEFT)

미연방법은 사적 영역에서의 포괄적인 프라이버시 보호법을 도입하고 있지는 않지만, 주로 연방거래위원회(Federal Trade Commission)가 주도하는 일정한 프라이버시 보호 정책 또는 개인정보의 기만적 이용에 대한 규제는 행해지고 있다. 이러한 개인정보에 관한 규제 중에서 개인정보 무단 취득 또는 '아이디절도(identity theft)'는 연방법에 의해 범죄로 규정되어 있다. 이에 따르면, '아이디절도'는 다른 사람의 생년월일, 연방정부가 발행하는 social security number, 사업자번호, 납세

33) 손해액이 불명확한 민사상 손해배상은 부적절하고, 공인이나 유명인, 기업을 공식 인증하는 '인증표시(이름 옆에 위치한 파란색 체크표시)'를 페이스북 페이지에 도입한 것이 거의 유일한 기술적 예방조치라고 보는 의견으로, 김경환 변호사, 앞의 글.

34) "페이스북, 국외송금서비스로 금융사업 진출", 연합뉴스, 2014.4.14.(http://www.yonhapnews.co.kr): 이관범, 박정경 기자, '카톡 뱅크' 초읽기 – 국내은행 비상, 문화일보, 2014.7.21. (http://www.munhwa.com)

자번호나 사기업 발행의 신용카드 번호 및 이용기한 등 일련의 숫자와 이름과 같이 그 자체로 또는 다른 개인정보와 함께 특정한 개인을 식별하게 해 주는 개인정보(identification, 이하 개인식별정보)[35]를 무단 수집, 이용하여 행해지는 사기(a fraud)로 정의된다.[36] 그런데, 이 아이디절도에 대한 가중처벌법(the Identity Theft & Penalty Enhancement Act of 2004)이 2004년 제정되면서 일정한 중범죄(felony)를 행하는 과정에서 또는 그 중범죄와 관련하여 행해지는 아이디절도를 가중된 형벌에 의해 처벌토록 하는 법규가 마련되었다.[37]

미연방법률 제18장 제1028A조 (a)항에 따르면, 열거된 중범죄(felony)[38]의 범행 중 그리고 그와 관련하여 적법한 권한 없이 다른 사람의 개인식별정보를 고의로 전달, 소지 또는 사용하는 경우, 그 중범죄의 형 외에, 2년 이내의 징역형을 부과하고 있다.[39] (b)항에서는 (1)아이디절도의 선고형에서 집행유예(probation)를 금지하고, (2)중범죄로 인해 선고된 형이 징역형인 경우 위 (a)항에 근거해 선고된 징역형을 병과하며, (3)법원이 중범죄의 선고형을 고려해 아이디절도의 선고형을 감경하지 못하도록 규정하고 있다.

대다수의 주에서는 아이디절도를 형사처벌하는 법이 제정되었다. 캘리포니아 주법은 연방법과 달리 중범죄와의 관련성을 요구하지 않고 개인정보의 무단 수집 및

35) A means of identification is a "name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any name, social security number, date of birth, ... employer or taxpayer identification number." 18 U.S .C. § 1028(d)(7); see United States v. Mitchell, 518 F.3d 230, 234 (4th Cir.2008)

36) 15 U.S.C. sec.1681A [Definitions; rules of construction] (q) (3) (4) identity theft definition : ‘a fraud committed using the identifying information of another person, subject to such further information as the Bureau may prescribe by regulation’.

37) 18 U.S.C. 1028A (ID절도및횡령억제법)

38) 18 U.S.C.1028A조(c)항 (1)에서 (11)호까지 열거된 중범죄이다. 공금횡령, 절도, 은행직원에 의한 횡령, 배임, 횡령, 미국시민권 사칭, 사기 또는 허위진술 관련 장의 모든 범죄, 우편사기(mail fraud), 전신사기(wire fraud), 여권 및 비자 관련 장의 모든 범죄, 기망에 의한 고객정보 획득죄, 외국인등록 중 위조 및 추방명령 불이행죄, 이민법 위반 범죄, Social Security Act 위반의 허위진술 관련 범죄들이 규정되어 있다.

39) aggravated identity theft under 18 U.S.C. § 1028A(a)(1) requires proof that the defendant "(1) knowingly transferred, possessed, or used, (2) without lawful authority, (3) a means of identification of another person, (4) during and in relation to a predicate felony offense." United States v. Abdelshafi, 592 F.3d 602, 607 (4th Cir.2010).

불법적 사용을 금지하고 있다. 캘리포니아주법 제530.5조(a)항에 따르면 “다른 사람의 개인식별정보(the personal identifying information)를 의도적으로(willfully) 획득하여 그 사람의 동의 없이 불법 목적(a unlawful purpose)[40]으로 사용하는 행위”를 처벌한다. 캘리포니아 주 대법원에서는 ‘불법 목적’이라 함은 형법 위반의 범죄뿐만 아니라 다른 법, 판례법 기타 다른 법적 기준에 대한 위반 행위도 모두 포함된다고 해석하고 있다.[41]

또한, 아동의 온라인 프라이버시 보호법(Children's Online Privacy Protection Act (COPPA))은 웹사이트 운영자, 온라인 서비스 제공자에게 어린이의 개인정보를 무단 수집하는 행위를 금지하고 있다. 어린이의 개인정보는 특별히 중범죄와의 관련성이나 불법 사용 없이도 무단 수집 그 자체를 처벌하고 있는 것이다.

나. 타인사칭(on-line impersonation)

한편, ‘타인사칭(impersonation)’은 다른 사람을 속이거나 특정인에 손해를 가하기 위해 또는 자신 또는 타인이 이익을 얻을 목적으로 일정한 사람으로 행세하는 것을 말한다.[42] 여기에는 온라인상에서 특정 개인을 사칭하면서 타인을 속이는 행위도 포함된다. 캘리포니아, 루이지애나, 와이오밍 주 등 상당 수의 주에서 온라인 타인사칭(on-line impersonation)을 독자적 범죄로 만들어 처벌하는 입법을 도입하고 있다.[43] 예를 들면, 캘리포니아 주법 § 528.5 [인터넷 기타 전자적 수단에 의한

40) 신용(credit), 재화, 서비스, 부동산 또는 보건 정보(medical information)의 획득을 불법 목적의 예로 들고 있다, 제530.5조를 참조하라.

41) People v. Rosa, 2013 WL 941728, at 10 (Cal.App.5 Dist.)

42) ‘Impersonation’: NY Penal Code 190.25 a person is guilty when he or she impersonates another and does an act in such assumed character with intent to obtain a benefit or to injure or defraud another.

43) Wyoming State Code sec.6-3-902 “any person who knowingly and without consent intentionally impersonates another actual person through or on, an internet website or by other electronic means, including, but not limited to spoofing and causes or attempts to cause harm, is guilty of a misdemeanor punishable by a fine of not more than $1,000, imprisonment for not more than one year or both“: : Lousiana Revised Statute sec.14:70.10 [Online Impersonation] A (1) It shall be unlawful for any person, with intent to harm, intimidate, threaten, or defraud, to intentionally impersonate another actual person, without the consent of the person, in order to engage in any

실존인물에 대한 신뢰할 만한 사칭]에서 '다른 사람을 가해, 협박, 위력 또는 기망을 하기 위해 동의 없이 인터넷 웹사이트 또는 다른 전자적 수단(electronic means)에 의해 자신을 실존하는 다른 사람으로 신용할 정도로 사칭한 사람은 1년 이하의 징역, 1,000달러 이하의 벌금 또는 병과형에 처한다'고 규정한다. (c)항에서는 전자적 수단에는 다른 사람의 이름으로 이메일 계정을 열거나, 소셜네트워크 서비스에서 계정이나 프로필을 여는 것을 포함한다고 규정함으로써, 본 범죄가 SNS에서의 타인사칭을 포함하고 있음을 분명히 규정하고 있다.

이에 관해 많은 판결 중 뉴욕주 대법원 판결(People v. Raphael Golb)[44]을 소개하면 다음과 같다. Golb 교수의 아들 피고인 라파엘(Raphael Golb)이 부친 Golb 교수의 연구 성과에 반대하거나 이를 지지하지 않는 학자들의 이름을 사용한 이메일 계정을 만든 뒤 Golb교수의 저작물에 대한 표절을 자인하거나 Golb교수를 비판했던 것은 실수였음을 인정한 이메일을 사칭한 계정을 통해 언론기관과 대학·학계 관계자들에게 보내는 사건이 있었다. 주 대법원은 피고인 라파엘의 반대파 학계 인사 사칭 이메일 송부행위에 대해 타인사칭(impersonation)의 유죄를 인정하였다.[45]

2. 캐나다

캐나다 연방법률은 21세기 초반까지도 컴퓨터 비밀번호, 신용카드 정보 등 몇 가지 예외를 빼고는 사인에 의한 개인정보 무단 수집에 대해 별도의 규제 입법을 하고 있지 않았다.[46] 그러나, 그러한 법의 허점을 막기 위해 2009년 형법 개정을 통해

of the following:

(a) open an electronic mail account, any other type of account, or a profile on a social networking website or other Internet website,

(b) post or send one or more messages on or through a social networki9ng website or other Internet website.

44) Court of Appeals of N.Y, 2014 N.Y. Slip Op. 03426 (2014)

45) People v. Golb 960 NYS2d 66 (2013): impersonation, id theft 유죄 인정 (Pigott, J. dissenting)

46) 컴퓨터 비밀번호와 신용카드 정보는 sections 342.1(1)(d) and 342(3)에서 각각 사기임이 입증된 경우 또는 보유의 정당한 권원 없음이 입증된 경우는 금지됨을 규정하였다.

일정한 범죄를 행할 것이 예상되는 상황에서의 개인정보 무단 수집을 범죄화하였다.[47] 두 차례의 규제 입법 시도[48] 끝에 아이디절도(identity theft)(제402.2)를 범죄화하는 규정을 채택한 것이다. 또한, 아이디사기(identity fraud)(제403조)를 통해 개인정보 무단 수집과 연계된 타인사칭을 처벌하고 있다. 특히, SNS나 인터넷을 수단으로 하는 범죄에 대한 별도의 규정은 없지만, 아이디절도(제402.2조)와 아이디사기(제403조)의 적용을 통해 해결하고 있는 것으로 보인다.

먼저, 제402.2조(1)항은 아이디절도(identity theft)에 대해 규제하고 있는데, "다른 사람의 개인식별정보(identity information)[49]가 사기 또는 허위를 구성요건요소로 포함하고 있는 범죄를 범하는데 사용되어질 것이라는 합리적인 추론이 가능한 상황임을 알면서 그 개인식별정보를 획득 또는 보유하는 행위'를 정식기소 될 수 있는 범죄를 범한 것으로 규정한다. 또한, 5년 이하의 징역 또는 약식판결로 형사처벌하도록 규정한다.[50]

다음으로, 제403조에서 다음의 네가지 목적을 가지고 생존인 또는 사자를 불문하고 타인을 기만적으로 사칭하는 행위를 처벌하고 있다. 이러한 네 가지 목적에는 (a) 자신 또는 다른 사람이 이익을 얻을 목적으로, (b) 어떤 재산 또는 재산에 대한

---

47) http://www.bearpaweducation.ca CIPPIC, Identity Theft: Introduction and Background, CIPPIC Working Paper No.1 (ID Theft Series), (Ottawa: Canadian Internet Policy and Public Interest Clinic, April 2007),

48) 캐나다 형법을 개정하려는 두 번의 시도가 있었다. 먼저, 2005년 개정법안(Bill C-359)은 개인정보의 무단 수집과 유통을 처벌하는 규정을 담고 있으나 의회 승인을 받지 못했다. 다음으로, 2006년의 개정법안(Bill C-299)은 사기 또는 타인사칭에 의해 개인정보를 획득하는 행위를 처벌하는 규정을 담고 있었다.

49) 이름, 주소, 생년월일, 지문 이미지, DNA 프로파일, 신용카드 번호, 은행계좌번호, 여권번호, 운전면호증 번호, 비밀번호 등 그 정보만으로 또는 다른 정보와 결합하여 개인을 식별하게 해주는 정보를 identity information 으로 정의하고 있다. Canadian Federal Statute Criminal Code sec.402.1[정의규정]을 참조하라.

50) Sec.402.2(1) Identity theft Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence. Sec. 402.2(5)은 402.2(5) PunishmentEveryone who commits an offence under subsection (1) or (2) (a) is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or (b) is guilty of an offence punishable on summary conviction.

이해관계를 얻을 목적으로, (c) 사칭된 사람 또는 다른 사람에게 손해를 가할 목적으로, 또는 (d) 체포, 기소를 면하거나 형사사법의 진행을 방해, 왜곡 또는 파괴할 목적(obstruct, pervert or defeat the course of justice)이 규정되어 있다. 이러한 아이디사기를 범한 자는 정식기소될 수 있는 범죄를 범한 것으로 10년 이하의 징역 또는 약식판결(summary conviction)으로 처벌될 수 있는 범죄를 범한 책임이 있음[51]을 규정하여 엄격히 처벌하고 있다.

3. 유럽연합과 국제연합

가. 유럽연합(European Union, EU)의 정보보호법

EU 차원에서는 정보보호법(data protection law)이 그러한 개인정보의 유출에 관해 규제하고 있다.[52] 하지만, 이러한 정보보호법(data protection (DP) law- Directive 95)은 누구든지 인터넷상에서 접근할 수 있는 정보의 사적 수집, 처리에 적용되는 것이 아니라 접근이 제한된 정보를 처리하고 있는 공적·사적 기관, '개인정보 관리자(Personal Data Controller)'에게 적용되는 법이다.[53] 이 때 '개인정보 관리자'는 SNS 제공사업자를 포함하는데, EU는 이 문언의 해석범위를 지역적, 대상적으로 확대하여 정보보호법의 적용범위를 넓혀가고 있다. 지역적으로 '개인정보 관리자'는 주사무소(headquarters)가 EU 영토 밖에 있는 미국회사인 마이스페이스(MySpace), 페이스북(Facebook)을 포함한다. EU 개인정보보호 사무국(Data Protection Working Party)은 SNS 자체가 EU 밖에서 제공되더라도 '쿠키(cookies)[54]가 EU 내에 있는 웹

51) Canadian Federal Statute Criminal Code sec.403(1)과 (3)을 참조하였다.

52) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. data protection (DP) law is seen as the key legal regime regulating the collection, processing, sharing, selling and deletion of personal data on SNSs.

53) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) based on Article 95 of the Amsterdam Treaty (currently Article 114 of the TFEU).

페이지 방문자의 컴퓨터에 있다면 그러한 컴퓨터는 자동화된 장치로서 자격을 갖추며 EU와 회원국의 정보보호법을 적용할 수 있게 해 준다'는 점을 근거로 외국 소셜 네트워크서비스 제공자에도 EU법과 회원국의 법이 적용될 수 있음을 제시하였다.[55] 이러한 논리는 베를린 항소법원 등 EU회원국 내의 지역 법원에서 수용되고 있다.[56]

대상적으로도, 우리 법과 같이 업무로서 개인정보파일을 운영하는 자 외에 일반 인터넷·SNS 이용자도 ① 클럽, 단체 또는 회사를 대신하여, 또는 ② 상업적, 정치적, 또는 자선 목적(charitable purpose)을 위해 글을 올리는 등 포스팅을 하는 경우 '개인정보 관리자'에 포함될 수 있다.[57] 하지만, 순수하게 사적 또는 가사 활동 중인 이용자의 행위(activities which are carried out in the course of private or family life of individuals)는 적용제외 규정(Article 3.2)에 따라 정보 관리자의 금지행위에 포함되지 않는다. 그런데, 유럽연합법원(ECJ)은 Sweden v. Lindqvist 판결을 통해 적용제외 규정의 적용범위를 축소하였다. 이 사건은 교회 자원봉사에 참여했던 18명의 개인식별정보-전화번호, 이름, 취미와 직장과 업무, 심지어 상해 관련 정보까지-를 개인이 만든 웹사이트에 자원봉사자의 동의 없이 올린 행위가 문제되었는데, 유럽연합법원은 '인터넷 개인 웹페이지에 개인정보를 게시(publication on the internet)한 행위는 많은 사람들에게 개인정보를 접근가능하게 하기 때문에 적용제외 규정(Article 3.2)이 적용되지 않아 순수하게 사적 활동중인 이용자의 행위로 해석될 수 없으며 개인 정보 관리자의 금지된 행위에 해당한다'며 300파운드 가량의 벌금 부과하였다.[58]

---

54) 웹페이지(SNS 포함)에 접속했던 기록을 이용자 컴퓨터에 저장해 놓은 일종의 문서를 말한다.

55) Jan Dhont, Lorenz, EU Extends Privacy on Social Networking Sites (http://www.hg.org) (2014년 7월10일 마지막방문).

56) German Court rules against Facebook's "Friend Finder" (http://www.lexology.com)

57) Social Networking Giants are subject to EU data protection laws, say regulators(유럽 정보보호 규제담당 위원회(EU committee of data protection regulators 또는 Europe's privacy watchdog)가 확인) (http://www.out-law.com)(2014년 7월10일 마지막 방문)

58) Case C-101/01, Sweden v. Lindqvist, 2003 E.C.R. I-12971, 42-47.

나. 국제연합(United Nations, UN)조약 가안

한편, 사이버공간을 위한 국제형사재판소에 관한 UN조약 가안(假案)(Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace)[59]은 현실적인 법적 효력은 갖고 있지 않으나 입법화 논의 과정에 있는데, 개인정보 무단 수집에 관해 규정을 포함하고 있다. 컴퓨터 시스템, 정보시스템, 데이터, 소셜 네트워크나 관련 국제형사법에서 보호되는 다른 자산에 대해, 국제사이버범죄법 위반으로서 아이디절도(identity theft)나 전세계적 관심의 대상인 소셜 네트워크에 대한 중대한 범죄와 같은 전세계적 관심의 대상인 중대한 사이버범죄를 범한 사람을 기소할 수 있는 권한을 국제형사재판소에 부여하고 있음이 특징이다.[60]

4. 영국

1998년 정보보호법(Data Protection Act 1998)에서 개인정보의 불법획득을 형사처벌하는 규정을 다음과 같이 도입하였다.

> "제55조 개인정보(personal data)의 불법획득 등
> (1) 누구든지 정보관리자(data controller)의 동의 없이 고의로 다음의 행위를 해서는 안된다.
> (a) 개인정보에 포함된 자료(information) 또는 개인정보의 획득 또는 공개
> (b) 개인정보에 포함된 자료의 다른 사람에 대한 누설

59) At the 13th International Criminal Law Congress in Queenstown Judge Stein Schjolberg of Norway presented a paper on and the arguments for an International Criminal Tribunal for Cyberspace (Stein Schjolberg is an extraordinary Court of Appeal Judge in Norway).

60) Article 4 (Social networks & identity theft)
The International Tribunal shall have the power to prosecute persons committing or ordering to be committed of the most serious cybercrime of global concern as violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, social networks, information or other property protected under the relevant international criminal law;
a) identity theft
b) other most serious crimes on social networks of global concern

(2) 제1항은 다음 중 하나를 입증한 사람에게는 적용되지 않는다.
(a) 획득, 공개 또는 누설이 (i) 범죄 억제 또는 탐지 목적으로 필요하거나, (ii) 입법, 법에 의한 승인 또는 법원의 명령에 의해 요구 또는 허용되었음
(b) 그 정보 또는 자료를 획득, 공개 또는 누설할 권리를 가지고 있다는 합리적인 신뢰에 의해 행동했음
(c) 정보관리자가 그 사정을 알았다면 그가 동의했었을 것이라는 합리적인 신뢰에 의해 행동했음, 또는
(d) 그 행위들이 특정한 상황에서 공익에 부합하는 것으로 정당화되었음
(3) 제1항에 위반한 자는 범죄에 해당한다.
(4) 제1항에 위반하여 개인정보를 획득했다면, 그가 그 개인정보를 판매하는 행위는 범죄에 해당한다.
(5) 제1항에 위반하여 개인정보를 획득했거나 추후 획득하게 되는 경우, 획득한 자가 그 개인정보를 판매하려는 제공하는 행위도 범죄에 해당한다.
(6) 제5항과 관련하여, 개인정보가 판매용 또는 판매가능함을 적시한 광고는 개인정보를 판매하려는 제공에 해당한다.”

한편, 제7항에서는 제4항 내지 제6항에서 개인정보(“personal data”)는 개인정보에서 추출된 자료(information)를 포함한다고 규정하여, 데이터에 대한 새로운 분석 기술을 통해 추출된 정보 역시 보호되는 개인 정보에 해당함을 명시하였다. 제55조를 위반한 경우의 형벌은 벌금형(제60조)이다.

5. 독일

독일은 정보보호법(Data Protection Act)에 근거하여 이메일, 사진 기타 생체 정보와 같은 개인정보를 당사자의 동의 없이 수집하는 것을, 부정경쟁방지법을 통해 개인정보를 당사자의 동의 없이 상업적으로 이용하는 것을 금지하고 있다. 또한, 업로드된 사진 등을 통해 개인 생체 정보를 분석, 수집하는 행위에 대해 지역 정보보호기구에서 법 위반사항을 지적한 바 있다.[61] 또한, 친구찾기(Friend Finder) 기능을 통해 이용자의 전체 이메일 주소록 기타 개인정보를 동의 없이 이용하려고 했던

61) Telegraph, German accuses Facebook of privacy ‘breaches’, (http://www.telegraph.co.uk)(2014년 7월 10일 마지막 방문). 그러나, 이에 대한 형사처벌은 없는 것으로 보인다.

페이스북에 대한 소비자단체의 위법행위 금지 청구를 베를린 항소법원에서 인용하기도 하였다.[62] 독일은 소비자단체의 단체소송 또는 행정법적 제재를 통해 SNS에서의 개인정보 침해 문제를 해결하고 있는 것으로 보인다.

6. 비교법적 분석과 시사점: SNS상 개인정보 무단 수집과 타인 명의 도용

선진각국의 입법례 조사의 결과, 아래 <표 2>에서 보듯, 개인정보의 동의 없는 수집, 소지, 타인에게의 제공을 범죄화하여 형사처벌하고 있는 입법은 미국, 캐나다, 영국의 법제임을 알 수 있다. 특히, 미국, 캐나다, 영국의 법제 중 미국과 캐나다는 징역형을 부과하고 있는 반면, 영국은 벌금형만을 규정하고 있는 것이 특징이다. 한편, 독일은 개인정보를 당사자의 동의 없이 수집하는 것을 금지하면서도 범죄화 입법 대신 행정법적 제재, 단체 소송에 의한 규제 방식을 채택하고 있었다.

〈표 2〉 선진 각국의 개인정보 무단 수집 범죄화 입법

미국 연방법	아이디절도 가중처벌법(18 U.S.C.1028A(a)): 열거된 중범죄의 범행 중이거나 그와 관련해 권한 없이 타인의 개인식별정보를 고의로 전달, 소지 또는 사용하는 행위- 2년 이하의 징역 캘리포니아주법 제530.5조(a) : 타인의 개인식별정보를 악의적으로 획득하여 그의 동의 없이 불법목적으로 사용
캐나다 연방법	다른 사람의 개인식별정보가 사기, 허위를 구성요건요소로 하는 범죄를 범하는데 사용되어질 것이라는 합리적 추론이 가능한 상황임을 알면서 그 정보를 획득, 보유하는 행위 - 5년 이하의 징역
영국 정보보호법	정보관리자의 동의 없는 개인정보의 획득, 공개, 누설- 벌금형
독일 정보보호법	개인정보를 당사자의 동의 없이 수집- 단체소송, 행정규제

62) Karin Retzer, Morrison & Foerster LLP, German Court rules against Facebook's "Friend Finder", Mar.3, 2014 (http://www.lexology.com) (2014년 7월10일 마지막 방문)

또한, 유럽연합법원은 Sweden v. Lindqvist 사건을 통해 자선목적의 종교기관 소모임의 개인정보의 무단 인터넷 게시도 '정보처리자'의 '무단 개인정보 처리'에 해당함을 인정하여 개인정보보호법의 적용범위를 확대해 나가고 있다. 이에 반해, 우리법제는 일반 SNS 이용자가 개인정보를 무단으로 수집·보관하는 행위는 기만적 방법을 사용하지 않는다면 아무런 법적 제재를 받지 않는다. 무단 유포의 경우, 명예훼손, 모욕죄에 해당하지 않는다면, 실효성이 떨어지는 손해배상청구, 게시중단 요청만이 존재한다.

온라인상 타인사칭의 경우, 미국의 다수 주의 법률과 캐나다 연방법률에서는 온라인상 타인 사칭을 사기의 일종인 아이디사기로 규정하여 형사처벌하고 있다. <표 3>에서 보듯 캐나다 연방법률은 특히 재산상 기타의 이익을 취득할 목적, 피사칭인 등에 손해를 가할 목적 및 형사사법을 방해할 목적을 규정하면서 생존인 사인을 불문하고 타인 사칭에 대해 장기 10년의 징역형을 부과하는 중범죄(felony)로 규정하고 있다.

〈표 3〉 선진 각국의 타인 사칭에 대한 범죄화 입법

미국 다수 주의 법률	캘리포니아주법 제528.5조: 다른 사람을 가해, 협박, 위력 또는 기망을 하기 위해 동의 없이 인터넷 웹사이트 또는 다른 전자적 수단에 의해 자신을 실존하는 다른 사람으로 신용할 정도로 사칭- 1년 이하의 징역, 1,000달러 이하의 벌금 또는 병과형
캐나다 연방법률	제403조 생존인, 사자를 불문하고 (a)자기·타인이 이익을 얻을 목적, (b)어떤 재산·이해관계를 얻을 목적, (c)사칭된 사람·타인에게 손해를 가할 목적, (d)형사사법 진행을 방해,왜곡,파괴할 목적으로 타인을 기만적으로 사칭- 10년 이하의 징역

우리 법제에는 아이디사칭에 대해 사기죄 외에는 별도의 입법이 없다. 따라서, 재산상 이익 취득 목적 또는 가능성이 전혀 없는 타인사칭- 예를 들면, 자신의 명성을 높이기 위한 타인 사칭-은 사기죄의 포섭범위 밖에 남아 있게 되어 형사절차에 의한 제재가 거의 불가능하다.

Ⅳ. SNS상 개인정보 무단 수집, 유포 및 타인사칭에 관한 형사법적 대응방안

1. SNS를 통한 소통과 형법 투입

SNS는 콘텐츠를 볼 수 있는 사람들이 사적인 관계로 제한되어 공적 소통이라기보다는 사적 소통의 공간으로 평가된다는 주장이 강하다.[63] 자신이 선택한 사람들-페이스북 친구맺기, 트위터 팔로우-에게 자신의 올리는 정보를 공유한다는 사적 공간의 특징이 존재하고 있지만, 자신이 선택하지 않은 사람들도 설정에 따라 노출되는 기본정보를 볼 수 있다는 점을 고려하면, 기술적인 측면에서 SNS가 사적 소통만을 위한 것이라고 단정할 수는 없다. SNS 일반 이용자, Google 등 검색 사이트 이용자들도 SNS상에서 일반 공개로 설정해 놓은 정보의 경우 검색이 얼마든지 가능하며, SNS별로 일정한 개인정보-페이스북의 경우 생일, 이메일, 출신학교, 트위터는 이메일과 개인프로필-는 통상적으로 일반 공개를 기본으로 하고 있는 점에서 대중적 소통과 네트워킹의 기회를 제공하는 공적인 면도 무시할 수 없다. 실제로 연예, 스포츠 등 문화 및 정치 분야와 학계 인사들은 SNS를 통해 자신들의 메시지를 대중들에게 전달하고 있어 SNS는 새로운 형태의 소셜 미디어(social media)로서 기능하고 있다.[64] 현재 활발하게 기능하고 있는 SNS 사업자-예를 들면, 페이스북-는 보유하고 있는 기술력을 활용하여 이용자의 개인정보를 수집, 분석하여 이를 통해 더 많은 인적 네트워킹(networkding, 인맥)과 더 많은 정보의 공유를 하도록 유도하고 있는 추세이다.

구성원간 공유된 정보의 외부 유출을 하지 않기로 하는 암묵적 신뢰가 형성되는 사적 공간과 달리 SNS에서는 구성원간 정보 공유라는 점에서는 같으나 그 목적이 타인과의 교제와 소통을 전제로 하는 것이어서, 일단 가입하여 활동하고 있는 이상

63) 박경신, SNS의 매체적 특성과 법적용의 한계, 인하대 법학연구 제15집 제3호, 140-141면 (2012).

64) Sam Borden, With tweets and snaps, Cup stars embrace social media, International NY Times, Jul. 8, 2014 (2014년 브라질 월드컵에서 브라질 네이마르 선수를 부상시킨 콜롬비아 선수, 또 비신사적 행동으로 물의를 일으킨 우루과이 수아레즈 선수들이 페이스북을 통해 자신의 입장을 전달하며 전 세계의 축구팬들이 그들에게 트위터와 페이스 북을 통해 비난의 메시지를 전달함을 보도).

정보의 노출은 피할 수 없다. 나아가, 자신이 선택하지 않은 사람들에도 최소한의 정보-페이스북의 경우 이름, 이메일, 사진-는 공개된다. 이는 인맥쌓기(네트워킹)을 활성화를 위한 SNS의 속성에서 나온 것으로 자신이 찾지 않은 사람이 자신과의 연결(정보 공유)를 요청하는 것을 알려 주는 경우가 종종 발생한다.

실제의 활용예를 보아도, 장소적 시간적 제약이 있는 오프라인상의 일정한 사적 공간에서 한 번에 모여 대화를 나누는 친구들의 수가 통상 대여섯 명이라고 볼 때, 통상 SNS에서 자신이 소통하는 사람들은 일반적으로 수십에서 수백명-페이스북에서 자신의 정보를 공유하며 소통하는 친구의 수는 통상 수 백명-에 이른다는 점에서 순수한 사적공간에서의 사교(私交)가 아니라 공적인 성격을 함축한 집단 내의 교제인 사교(社交, group)가 이루어지고 있다고 평가되어야 한다. 이용자들 스스로도 스마트폰에 탑재된 SNS를 통한 소통이 단순한 사적 소통이 아닌 사적이면서도 공적인 특징을 가지고 있음과 이로 인한 개인정보 노출의 문제점을 인식하고 있다.

2. SNS 이용자의 개인정보 무단 수집(획득)·보관·유포에 대한 범죄화

SNS상에서도 표현의 자유는 존중되어야 한다. 그러나, 그 표현의 자유에는 헌법 제21조 제3항과 제37조 제2항에서 규정하듯이 법적 한계가 있다. 타인의 명예훼손, 모욕 뿐만 아니라 범죄를 목적으로 한 개인정보의 무단 획득·보관 및 무단 유포는 사회 질서 유지, 사생활 비밀 및 인격권의 침해행위이다. 그럼에도, 개인정보보호법은 ‘업무로 개인정보파일을 운영하는’ 개인정보처리자에 대해서만 무단 수집, 유포를 범죄화하고 있으며, 정보통신망법은 기망적 수단을 통한 개인정보 수집만을 범죄화하고 있다. 이는 선진각국의 법제상 개인정보를 형벌 투입을 통해 보호하는 추세에 못 미치고 있다고 평가된다. SNS의 활용에 따른 개인정보 및 프라이버시 노출이 갈수록 증가하는 상황에서, 무단수집·보관된 개인정보를 통해 2차범행이 현실될 수 있다. 따라서, 모욕, 명예훼손, 강요죄 등 미수범 처벌규정, 사기죄의 예비 처벌규정이 존재하지 않는 점을 고려할 때, 2차범죄의 발생을 형법적으로 차단할 수 있는 법적 근거가 필요하다. 또한, 소위 ‘신상털기’ 등 개인정보의

무단 유포는, 모욕죄에 이르지 아니하는 경우에도, 그 자체로 사생활의 비밀과 인격권을 침해하는 행위로 무단 수집 및 보관보다 결과불법과 행위불법이 크다. 더 중한 형벌 투입을 통한 규제가 필요하다. 다만, 사적 영역에 대한 지나친 형법의 투입을 막기 위해 반의사불벌죄로 입법하여 사적 합의에 의한 형벌권의 차단을 허용할 필요가 있다. 이같은 제안을 구체화하면 다음과 같은 입법안을 제시해 볼 수 있을 것이다.

제0조 ① 누구든지 불법적 이용을 목적으로 개인정보를 정보주체의 동의 없이 수집하여 보관하는 행위는 1년 이하의 징역 또는 3백만원 이하의 벌금에 처한다.
② 누구든지 정보주체의 동의 없이 보관하고 있던 개인정보를 그의 동의 없이 인터넷 또는 소셜네트워크서비스상에 올리는 행위는 2년 이하의 징역 또는 6백만원 이하의 벌금에 처한다.
③ ①항과 ②항의 죄는 정보주체의 명시적 의사에 반하여 소추하지 못한다.

3. 온라인상 무단 타인 사칭에 대한 범죄화

현재 무단 타인사칭에 대해서는 전혀 형사입법이 마련되어 있지 않은 점은 문제이다. 미연방 다수의 주, 캐나다에서 타인사칭(impersonation), 아이디사기(identity fraud)에 관한 형사입법이 채택되어 왔음을 유의해야 할 것이다. 대면 접촉이 없는 온라인·네트워크상 타인의 무단 사칭행위는 SNS 이용자 확대와 함께 많은 피해를 야기할 수 있는 행위이며, 그 자체로 인격권 침해이자 변형된 형태의 명예훼손, 모욕죄로 평가된다. 현재 사기의 예비죄, 또는 명예훼손, 모욕죄의 미수범 처벌규정이 없으며 인터넷실명제가 위헌결정으로 폐지된 상황에서 타인사칭에 대한 인격 침해에 대한 별도의 형사입법이 절실히 필요하다. 다만, 사소한 침해에 대한 사적 화해 유도의 측면, 인격권이 핵심적 보호법익이기에 사칭된 본인의 의사를 존중하는 점에서 친고죄 입법이 타당하다. 이를 고려한 입법안을 제시하면 다음과 같다.

제0조 ① 누구든지 자기·제3자가 이익을 얻을 목적으로 또는 사칭된 타인 또는 제3자에게 손해를 가할 목적으로 온라인상에서 동의 없이 타인을 사칭하는 자는 1년 이하의 징역 또는 3백만원 이하의 벌금에 처한다.
② 전항의 죄는 사칭된 사람의 고소가 있어야 공소를 제기할 수 있다.

4. 외국 소셜네트워크서비스 제공자에 대한 형사책임 부과

외국 SNS 서비스 제공자에 대해서도 EU 국가들이 자국법을 적용하여 온 판례의 법리를 벤치마킹하여 국내법을 적용토록 하는 법리 개발이 필요하다. 전술한 유럽연합의 개인정보보호국(Data Protection Working Party)이 '쿠키가 EU 내에 있는 웹페이지 방문자의 컴퓨터에 있다면, 그러한 컴퓨터는 자동화된 장치로서의 자격을 갖추며 EU 회원국의 정보보호법을 적용할 수 있는 근거가 된다'는 논리를 개발해 베를린 항소법원 등 EU 회원국내 사법부에서 역외적용의 근거법리로 수용되고 있다는 점은 주목할 만하다. 국제화되어 가는 SNS와 인터넷서비스의 추세를 고려할 때 국내법의 외국 소재 소셜네트워크서비스 제공자에 대한 역외적용을 위한 입법 내지 법리 개발이 시급하다.

5. 소셜네트워크서비스 제공자에 대한 컨텐츠 관리를 위한 법적 의무 부과

현재 아동 청소년 성보호에 관한 법률 제17조 제1항 자신이 관리하는 정보통신망에서 아동·청소년이용음란물을 발견하기 위하여 대통령령으로 정하는 조치를 취하지 아니하거나, 발견된 아동·청소년이용음란물을 즉시 삭제하고, 전송을 방지 또는 중단하는 기술적인 조치를 취하지 아니한 "온라인서비스제공자"는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 다만, 온라인서비스제공자가 정보통신망에서 아동·청소년이용음란물을 발견하기 위하여 상당한 주의를 게을리하지 아니하였거나 발견된 아동·청소년이용음란물의 전송을 방지하거나 중단시키고자 하였으나 기술적으로 현저히 곤란한 경우 면책을 인정한다. 그러나, 비단 아동청소년이용음란물에 그치지 않고, 소셜네트워크서비스 제공자에게도 온라인서비스제공자로서 다른 법규에 저촉되는 위법한 게시물, 영상물, 링크에 대한 차단 조치를 취할 의무를 부과하고, 또한 발견된 위법한 게시물 등은 즉시 삭제, 전송을 중단하는 조치를 취할 의무를 부과하여 이를 불이행한 자를 형사처벌하는 입법-진정부작위범 형식-을 고려할 필요가 있다. 또한, 위반행위자 개인 외에 그 개인을 관리하는 사업주도 고의의 부작위로 인한 범죄에 대한 형사책임을 인정하는 양벌규정 입법도 뒤따라야 할

것이다. 하지만, 수 없이 확대되는 네트워크상의 소통을 온라인서비스제공자(OSP)가 현실적으로 점검하기란 지극히 어려운 일이므로 이용자에 대한 주의조치, 교육 등을 법적 의무화[65]하여야 하며, 신고와 적발을 용이하게 하는 기술적 조치를 취한 경우 면책을 인정하는 입법과 판례를 통해 자기책임 원칙과의 조화를 마련해야 할 것이다.

V. 결론: SNS를 통한 사이버범죄에 대한 효과적인 형법적 대응의 필요성

앞에서 검토한 바와 같이, SNS라는 소통수단을 악용한 개인정보의 무단 수집, 보유, 타인의 아이디와 비밀번호 무단 사용을 통한 타인 사칭과 같은 일탈행위와 그에 따른 피해 확산에 대한 우려가 커지고 있다. 이러한 일탈행위가 증가하고 있으며 그로 인한 피해자들이 발생하고 있음에도, 기술적 수단에 대한 형법 투입의 자제, 사적 영역 소통론과 연계된 표현의 자유 논리에 의해 일탈행위에 대해 형사입법은 충분하고도 효과적인 대응책을 갖추지 못하고 있다. 실체법으로서의 형법은 물론, 정보통신망법과 개인정보보호법 역시 적절한 형사처벌 규정을 갖추고 있지 못하다.

반면, 미국, 영국, 독일 등 EU의 주요 국가들은 우리보다 SNS의 이용도나 표현의 자유를 보장하는 수준이 결코 낮지 않음에도 SNS의 남용으로 인한 위와 같은 일탈행위들에 대해 형사법의 개정 및 제정을 통한 구성요건 및 처벌규정들을 도입, 시행해 오고 있다. 이는 기술적 수준과 정치적 기본권의 입법 측면에서 글로벌 스턴더드를 따라가고자 부단히도 노력하는 입법 및 사법의 전문가들에게 과제를 던져주고 있다. 오히려 선진각국에서는 사이버 범죄를 규제하기 위한 체계적 입법과 해석

65) 예를 들면, 아청법 제17조 제2항은 ‘「저작권법」 제104조에 따른 특수한 유형의 온라인서비스제공자(OSP)((다른 사람들 상호간 컴퓨터를 이용하여 저작물 등을 전속하도록 하는 것을 주된 목적으로 하는 OSP))는 이용자가 컴퓨터 등에 저장된 저작물 등을 검색하거나 업로드 또는 다운로드를 할 경우 해당 화면이나 전송프로그램에 “**아동·청소년이용음란물을 제작·배포·소지한 자는 처벌을 받을 수 있다**”는 내용이 명확하게 표현된 경고문구를 대통령령으로 정하는 바에 따라 **표시할 의무가 있음을 규정한다. 위 OSP가 제17조 제2항상의 작위의무를 위반한 경우는** 3천만원 이하의 과태료를 부과하고 있다 (아청법 제67조 제1항).

을 통해 엄격한 처벌을 부과하고 있다. 모바일인터넷 환경에서 발생하는 SNS를 이용한 일탈행위에 대해서도 마찬가지로, 개인정보의 보호를 위한 입법과 판결을 통해 실시간 소통에 의해 나타나는 피해 확산에 대한 형사법적 대처방안을 마련해 오고 있다. 나아가, 이미 국제화되어 버린 사이버범죄의 특징을 고려하여 사이버범죄 방지를 국제적 협약의 제정, 가입국 확대의 노력을 기울이고 있다.

우리나라에서 SNS의 이용은 대중화단계로 나아가고 있으며 SNS를 통해 발생하는 사생활에 관한 피해가 이들 국가에 비해 결코 작지 않다. 기술적 수단의 이용에 관한 보호와 표현의 자유가 법적 보호에 핵심적인 부분이나, 법적 제재로부터 영구히 자유로워야 할 영역은 아니며 이용자들에 대한 교육이 확대됨에 따라 이에 대한 법적 규제가 도입될 필요가 있다. 더더군다나 그 피해 범위가 확대되고 사회 일반인의 위협감정도 증가하고 있음에도 SNS상 무단 타인 사칭 행위가 경범죄로서의 입법조차도 이루어지지 않고 있는 점, 기존 형법상 범죄화 대상 일탈행위와는 그 피해 확산의 신속성과 파급효과가 현저히 차이가 있음에도 기존의 법정형보다 경한 처벌을 두거나 이를 그대로 적용해 오고 있다는 점은 유의해야 할 대목이다. SNS의 대중적 사용에도 불구하고 법적 정의는 뒤따르지 못하고 있다는 비판이 대두되고 있는 현 상황에서, SNS 남용으로 인한 일탈행위에 대해서 사이버 공간을 공적 제재가 투입되지 않거나 경한 제재에 맡겨 두는 것은 사적 보복을 유도하는 문제를 낳을 수 있다. 신중한 형사입법을 위한 시간의 경과 속에서 SNS상에서는 점점 더 많은 일탈행위자들과 피해자들이 생겨나고 있음을 기억해야 할 것이다.

참고문헌

윤해성·박성훈, SNS 환경에서의 범죄현상과 형사정책적 대응에 관한 연구, 한국형사정책연구원 연구보고서, 2014.

강동범, 사이버범죄 처벌규정의 문제점과 대책, 형사정책 제19권 제2호, 2007, 33~54면.

가상준·김강민·임재형, SNS 사용문화가 청소년의 학교폭력 및 사이버폭력에 미치는 영향, 분쟁해결연구 제11권 제1호, 단국대학교 분쟁해결연구소, 2013.

김봉수, SNS범죄에 대한 의미론적 고찰-사이버범죄로의 포섭 및 그 한계를 중심으로, 법학논총 제33권 제3호, 전남대학교 법학연구소, 2013.

김희수, 개인정보 수집, 저장, 이용의 적법성과 한계: 정보인권 관점 등에서 본 형사사법통합정보체계, 국가인권위원회, 2006.

백승주, 미국의 압수수색 영장 일부기각 및 압수방법 제한에 관한 실무연구- 특히 디지털 증거를 중심으로, 법조 제62권 제7호, 법조협회, 2013.

박경신, SNS의 매체적 특성과 법적용의 한계, 인하대 법학연구 제15집 제3호, 2012.

이성식, 소셜네트워크 서비스(SNS)상에서의 불법행동과 그 원인으로 사회자본과 그 쟁점: 트위터와 페이스북의 비교, 형사정책연구 제24권 제2호, 한국형사정책연구원, 2013.

이원상, 허위사실유포 관련 범죄에 대한 고찰, 형사정책연구 통권 제95호, 57-84면 (2013.9)

이상현·전홍식, 사이버선거운동의 자유화 및 사이버선거범죄에 대한 공직선거법상 형사제재의 대응 : SNS를 중심으로, 법학연구 제46집, 한국법학회, 261p ~ 290p (2012)

지영환·전현욱, SNS上의 선거운동에 대한 형사법적 규율, 경희법학 제48권 제4호, 84-106면(2013)

임명성, 개인정보 유출 사고 후 웹사이트 가입 지속 및 프라이버시 무관심에 영향을 미치는 요인에 관한 연구, 디지털정책연구 Vol.11 No.1 [2013]

임채곤, 사이버 범죄에 관한 연구- 허위사실유포죄, 사이버모욕죄, 인터넷 실명제 중심으로, 경상대학교 박사학위 논문, 2013.

진성철·김인경, 인터넷 이용자의 개인정보 유출 가능성에 대한 심리적 불안에 관한 연구: 성별, 이용량, 이용 빈도를 중심으로, 전자통신학회 논문지 Vol.6 No.5 (2011)

편집부, 개인정보 유출관련 인식조사, 리서치보고서, Vol.2011 No.9 (2011)

허진성, SNS의 개인정보 침해문제와 그 대응방안에 관한 연구, 언론과법 제9권 제2호, 한국언론법학회, 2010.

한국인터넷진흥원, 개인정보 침해 신고 및 상담사례집, 2013.

Danah M. Boyd & Nicol B. Ellison, Social Network Site: Definition, History & Scholarship, Journal of Computer-Mediated Communication, Volume 13, Issue 1, Article first published online, 2007.

인터넷 자료

김경환 변호사 [ICT법 바로알기] 인터넷·SNS 타인명의 사칭의 법적 문제, 디지털데일리 2013.9.11. (http://www.ddaily.co.kr) (2014년 7월 11일 마지막 방문)

Canada Department of Justice, A Handbook for Police & Crown Prosecutors on Criminal Harassment, Part 1, 1.6 (http://www.justice.gc.ca)

CIPPIC, Identity Theft: Introduction and Background, CIPPIC Working Paper No.1 (ID Theft Series), (Ottawa: Canadian Internet Policy and Public Interest Clinic, April 2007), (http://www.bearpaweducation.ca)

FACEBOOK, Information for Law Enforcement Authorities (https://www.facebook.com/safety/groups/law/guidelines)

German Court rules against Facebook's "Friend Finder" (http://www.lexology.com)

Jan Dhont, Lorenz, EU Extends Privacy on Social Networking Sites (http://www.hg.org) (2014년 7월10일 마지막방문).

Karin Retzer, Morrison & Foerster LLP, German Court rules against Facebook's "Friend Finder", Mar.3, 2014 (http://www.lexology.com) (2014년 7월10일 마지막 방문)

Social Networking Giants are subject to EU data protection laws, say regulators(유럽

정보보호 규제담당 위원회(EU committee of data protection regulators 또는 Europe's privacy watchdog)가 확인) (http://www.out-law.com) (2014년 7월 10일 마지막 방문)

Telegraph, German accuses Facebook of privacy 'breaches', (http://www.telegraph.co.uk) (2014년 7월 10일 마지막 방문)

Research on Criminal Legislations against Identity Theft & Impersonation through Social Network Services

Lee, Sanghyun

As social networking service (SNS) has been widely used with popularity, such abuses of the SNS as identity theft and identity fraud (impersonation) have been under concerns of SNS users. Although cases involving the abuses come up, current legislations, particularly criminal law, in Korea has been less prepared for penalizing the criminals who cause the cases. This thesis reviewed current legislations and cases of the Supreme Court in Korea, those of the United States, Canada, United Kingdom, and Germany. Additionally, it searched international law of EU and UN. Legislations of Korea where SNS has been widely used as much as above-mentioned advanced countries have exposed some loopholes regarding identity theft and impersonation compared to the advanced countries. There should be consideration for adopting criminal provisions against identity theft and impersonation with appropriate penalties. Some model provisions are suggested.

❖ Key words: personal identification information, impersonation, Social Networking Service (SNS), identity theft, unauthorized collection of identification information

투고일 : 8월 31일 / 심사(수정)일 : 9월 19일 / 게재확정일 : 10월 1일