연구논문 정보화정책 제23권 제4호, 2016년 겨울호, pp.38~58

우리나라의 개인정보 보호제도 분석*
– 인증 및 평가제도와 개인식별번호를 중심으로 –

김 민 천**

요 약

빠르게 변화하는 인터넷 환경과 미디의 변화는 온라인상에서 소통이라는 새로운 커뮤니케이션 방식을 만들고 있다. 누리꾼들은 온라인상에서 이전보다 더 많은 서비스를 제공받고, 이런 서비스를 통해 서로가 어려움 없이 소통할 수 있게 되었다. 하지만 이런 변화를 통해 얻어진 소통의 자유 확대는 이전보다 더 많은 개인 정보의 노출과 더 쉬운 개인 정보의 유출로 이어지고 있다. 더 큰 문제는 지금의 상황에서 개인 정보 유출을 통제하는 것이 과거보다 더 어렵게 되었다는 것이다. 우리 정부는 지속적으로 발생하는 개인정보 유출 사건을 해결하고 예방하기 위해서 개인정보 보호와 관련된 여러 정책들을 개발하고 시행하고 있다. 이 연구는 이렇게 시행되고 있는 개인정보 보호제도의 문제점을 찾아내고 대안을 모색하고자 한다.

주제어: 개인정보 보호제도, 정보보호 준비도 평가, 개인정보, 개인정보식별번호, 인증제도(ISMS 등)

Analysis of Personal Information Protection System in Korea
– Focus on Certification & Evaluation System and Personal Identification Number –

Kim, Min-Chen

Abstract

The ever-evolving Internet environment along with changes in the mass media has been creating a new way of communicating in the virtual cyber world. The Internet users have more services at their disposal to communicate with ease. Such a new way of communication styles, however, makes them vulnerable to personal information leakage, increasing the concerns of cyber security. A thorny issue is how we can control the disclosure of personal information. Lately, the Korean government implemented privacy policies to resolve and prevent personal information leakage incidents that incur social problems. Here, we seek to identify problems in the privacy policies for better solutions.

Keywords: Personal Information Protection System, SECU STAR, Personal Information, Personal Identification Number, ISMS

2016년 8월 23일 접수, 2016년 8월 29일 심사, 2016년 11월 3일 게재확정

* 이 논문은 2011년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 연구되었음(NRF-2011-35C-B00460)

** 한국정보방송통신대연합 차장(kimminchen@gmail.com)

Ⅰ. 서론

우리나라는 1978년 제1차 행정전산화 사업(1978~1982년)을 시작으로 2차에 걸친 행정전산망 사업(1987~1996년)을 거쳐 행정정보화 촉진 시행사업(1996~2000년)을 시행하는 등 우리나라를 정보 사회로 이끌기 위해 노력해왔다. 우리 정부의 이런 노력은 우리나라를 빠르게 변화하는 정보화 사회로 이끌었고, 이를 통해 2010년부터 2014년까지 UN이 정한 전자정부 지수 세계 1위, 2014년 ITU전권회의 개최(제19회)[1] 등 세계 최고 수준의 ICT 강국으로 위상을 다지게 했다. 이와 같은 정보화의 노력에 따른 ICT의 발전은 국민 생활의 편리성, 기업 활동의 효율성, 정부 업무의 능률성을 향상 시켰다.

ICT의 발전은 최근 우리 사회의 오프라인과 온라인을 자연스럽게 연결시키고 있다. 특히 2010년부터 본격적으로 보급된 개인용 휴대용 단말기는 가상공간 접속을 더 활발하게 만들고 있다. 또 페이스북(facebook), 트위터(twitter), 카카오톡(Kakao Talk) 등 SNS(Social Networking Service)[2]의 등장은 더 많은 사람들을 온라인으로 결집시키고 있다.

이와 같이 가상공간에서의 활발한 활동은 사람들에게 새로운 재미와 생활의 편리함 등을 제공해주지만, 동시에 개인정보 유출로 인한 피해의 가능성을 높이고 있다. 개인정보 유출 사례는 2007년 8월 케이티(KT)와 하나로 텔레콤 등이 보유한 고객 730만 여 명의 개인정보 유출(한겨레신문, 2007/0810), 2008년 3월 LG 텔레콤의 800만 여명의 개인정보 유출(머니투데이, 2008/04/22), 2008년 4월 옥션의 1,081만 명 개인정보 유출(한국경제신문, 2008/04/18), 2008년 9월 GS 칼텍스의 1,125만 명 개인정보 유출(경향신문, 2008년 9월 5일),[3] 2011년 5월 현대캐피탈 175만 명 고객정보 유출(2011/05/18),[4] 2011년 5월 휴대폰 커뮤니티 '세티즌', 140만 개인정보 유출(뉴시스, 2009/05/21),[5] 2011년 7월 강남구청 공무원의 520명의 개인 정보 유출(매일경제, 2011/07/04),[6] 2011년 7월 초중고생 65만 명의 개인 정보 유출(뉴시스, 2011/07/07),[7] SC · 씨티은행도 구멍 '뻥'… 고객정보 13만여 건 유출(국민일보 쿠키뉴스, 2013/12/12)[8] 등으로 끊이지 않고 이어지고 있다. 2014년은 금융권, 이통사 등을 포함하여 50여 건이 발생했다(보안뉴스, 2014/06/25, 2014/12/31. 기사 참고).

정부의 개인정보 보호 대책이 매년 이어지고 있지만 개인정보 보호와 관련된 문제는 해가 거듭될수록 문제성이 심각해지고 있다. 여러 사례에서도 나타나고 있듯이 개인정보 유출은 단지 유출로만 그치는 것이 아니라 2차 · 3차 피해의 우려를 낳고 있다. 신원도용, 보이스피싱, 금품갈취 등의 사기 · 협박의 피해로 이어질 수 있다는 것이다.

1) ITU는 유엔 산하 정보통신을 담당하는 국제기구로, ITU 전권회의는 정보통신기술(ICT) 올림픽으로 불리며 4년마다 열린다. 전 세계 193개국 IT 장관들이 총집합해 향후 4년간 세계 ICT 관련 정책과 표준을 확정하고 앞선 ICT를 공유하는 글로벌 축제로 부산 ITU 전권회의는 아시아태평양 지역에서는 1994년 일본에 이어 두 번째로 열렸다.

2) SNS는 가상공간에서 지인을 포함한 불특정 다수의 타인과 인맥을 형성할 수 있는 서비스이다. SNS 이용자들은 해당 서비스를 통해 새로운 인맥을 쌓거나, 자신의 평소 지인과의 관계를 강화시킬 수 있다. 우리나라 최초의 SNS는 10여 년 전 잠시 붐을 일으켰던 '아이러브스쿨'이라 할 수 있으며, 현재 대표적인 우리나라의 SNS는 가상공간에서 일촌맺기가 가능한 '싸이월드'를 들 수 있다. 현재 세계적으로 SNS의 인기는 높아지며 이용자의 수도 폭발적으로 증가하고 있다. 현재 세계를 대표하는 SNS는 페이스북과 트위터라 할 수 있다.

3) 모 법무법인의 사무장이 집단 소송 사건의 수임을 노리고 GS칼텍스 고객 1,125만 명의 개인 정보를 빼내 유출하였다.

4) 현대캐피탈은 해킹을 당해 175만 명의 개인정보를 유출시켰다.

5) 휴대폰 커뮤니티인 '세티즌'은 해킹을 당해 140만 건의 개인정보를 유출시켰다.

6) 서울 강남구 모 주민자치센터 8급 공무원과 7급 공무원은 주민등록등 · 초본은 건당 5만 원, 가족관계등록부는 건당 10만 원씩, 모두 520여 건을 넘겨 2천600만 원을 챙겼다.

7) 모 소프트웨어 개발업체 대표가 전국 시 · 도 교육청의 학교도서관 정보시스템(DLS)을 해킹, 초중고생 65만여 명의 개인정보를 팔아 부당이득을 챙겼다.

8) 한국스탠다드차타드(SC)은행과 한국시티은행의 곡개 13만여 건이 대출업자들에게 유출되었으며, 이는 은행권 개인정보 유출 사고로는 사상 최대 규모이다.

개인정보 보호 문제가 정보보호의 넓은 범위 내에서 일부분에 속한다고 볼 수도 있겠지만, 매년 반복되는 사례들에 무뎌지고 이를 간과해 버린다면 국가 사회 전체의 신뢰도 하락을 피할 수 없음은 물론, ICT 중심의 국가 발전에도 저해요인으로 작용할 수 있다.

Ⅱ. 연구 배경 및 목적

1. 연구 배경

우리나라는 세계에서 유일하면서 확실한 개인식별번호인 주민등록번호 제도를 운영하고 있다. 정보화가 시작되던 시기에 주민등록번호의 온라인 사용에 대한 정확한 기준이 없었기 때문에 오프라인과 마찬가지로 온라인에서도 본인확인 용도로 주민등록번호가 사용되었다. 우리나라의 주민등록번호는 개인을 확인할 수 있는 가장 확실한 수단의 개인 식별 번호이며, 태어나서 죽을 때까지 나만의 '고유불변'의 번호이다. 우리나라의 국민으로 태어난 지 1개월 이내에 출생 신고를 한 뒤, 주민등록번호라는 이름으로 국가로부터 부여받는 것이다.[9] 또 주민등록번호는 우리나라에서 살아가기 위한 우리나라의 국민이라면 무조건 부여받아야만 하는 강제성의 성격도 가지고 있다.(김민천, 2009)

주민등록번호를 활용한 명의 도용은 우리나라 가상공간에서 가장 일반적인 범죄 행위이다. 범죄자가 타인의 이름과 주민등록번호로 특정 웹 사이트에 가입하여 악의적인 목적으로 명의를 도용하는 등 가상공간에서 행하는 여러 가지 행위들은 물질적인 피해를 입히지 않더라도 명의 도용을 당한 당사자에게 정신적인 충격을 줄 수도 있다. 실제로 주민등록번호 등 개인 정보가 유출되어 수십여 곳의 성인 사이트에 당사자도 모르게 가입되어, 당사자가 정신적인 피해를 입은 사례가 언론에 보도되기도 했다(김민천, 2010).

스미싱(Smishing), 파밍(Pharming), 피싱(Phishng) 등 개인정보 침해 수법도 점점 다양해지고 있다. 2015년 6월에는 신종 대포통장을 이용한 스미싱 수법으로 돈을 가로챈 일당이 검거되기도 했다.[10] 개인정보가 금전적 이익을 취하는 등 악의적인 목적으로 사용되기 때문에 개인정보 유출은 또 다른 피해로 이어져 심각한 사회 문제로 인식되고 있다. 정보시대에 살고 있는 우리의 개인 정보들은 보호되기보다 돈의 가치로 매겨져 불법적으로 유통 · 판매되고 있다. 이렇게 불법적으로 유출된 개인 정보는 불법거래 사이트에서 밀거래되거나, 타인의 명의 도용 등으로 개인정보 침해의 수단으로 사용된다.

개인정보보위원회에 따르면 2015년 주민등록번호 등 타인 정보의 훼손 · 침해 · 도용 관련 민원으로 전체 개인정보 침해 민원건수의 절반이 넘는 51%를 차지하고 있는 것으로 나타났지만, 이 민원 유형은 2012년 13만 9,724건, 2013년 12만 9,103건, 2014년에 8만 3,126건으로 감소하는 동향을 보였고, 2015년 역시 7만 7,598건으로 2014년 대비 11.9% 감소하였는데, 이는 지난 4년 동안에 걸쳐 절반에 가까운 44.5%나 감소한 것이다. 이런 결과에 대해 개인정보보호위원회는 2012년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법')」 개정으로 2012년 8월부터 온라인상에서 주민등록번호 신규수집이 전면 금지되었고, 2013년 「개인정보 보호법」개정으로 2014년 8월부터 법령 등의 근거가 없는 주민등록번호 처리가 원칙적으로 금지되는 등 처벌이 강화되었을 뿐 아니라, 2015년 7월에는 고유식별정보(주민등록번호 등) 분실 · 도난 등의 경우 5억 원 이하의 과징금부과, 주민등록번호의 암호화 의무 등을 내용으로 「개인정보 보호법」이 개정됨에 따라 개인정보처리자가 주민등록번호 수집 · 이용 등 처리에 대하여 경각심을 가지게 되었기 때문으로 보고 있다. 그

9) 가족관계의등록등에관한법률 제44조 ① 출생의 신고는 출생 후 1개월 이내에 하여야 한다.
10) 아주경제 (2015). "신종 대포통장 이용 스미싱 인출책 검거." 6월 12일.

러나 이 유형은 전체 개인정보 침해 민원 건수의 51%나 차지하고 있기 때문에 주민등록번호 등에 대한 개인정보 오남용이 여전히 심각한 문제임을 보여 주고 있다. 그리고 이 유형을 '기타 개인정보 침해' 60,480건과 합칠 경우 138,078건으로 전체 대비 90.75%의 높은 비중을 차지하고 있으며, 침해유형에 포함되지 않은 '기타 개인정보 침해' 유형은 2014년 대비 2,775건으로 4.8% 증가하는 등 개인정보 보호에 대한 노력이 여전히 미흡함을 알 수 있다.(2016 개인정보보호 연차보고서, 개인정보보호위원회. 참고)

2. 연구의 목적

이 연구는 온라인에서 발생하는 개인정보 유출, 개인정보 보호의 필요성 등 해당 문제의 심각성을 인식하고 우리나라 개인정보 보호제도를 분석하여 보완점을 찾기 위한 논문이다. 현재 우리 정부의 주민등록번호제도와 관련된 제도를 분석하여 효율적인 제도 활용 방안을 모색하고자 하였다.

구체적인 연구 목적은 다음과 같다.

첫째, 우리나라에서 시행되고 있는 개인정보 보호 관련 인증 및 평가제도의 현황을 파악하고 이를 분석하여 보다 효과적인 인증 및 평가제도 운영방안을 모색하고자 하였다.

둘째, 우리나라의 개인식별번호 제도를 파악하여 보다 효율적인 개인정보 보호 방안을 제시하고자 하였다.

셋째, 앞에서 밝혀진 내용들을 토대로 우리나라의 개인정보 보호제도의 문제점을 파악하고 보다 효율적인 방안을 모색하고자 하였다.

이렇게 분석된 결과를 바탕으로 개인정보 보호제도가 보다 나은 방향으로 나아가기 위해 어떤 것들이

〈표 1〉 개인정보침해 접수 유형 분석

(단위: 건)

침해유형	2009	2010	2011	2012	2013	2014	2015
정보주체의 동의 없는 개인정보 수집	1,075	1,267	1,623	3,507	2,634	3,923	2,442
개인정보 수집 시 고지 의무 불이행	15	75	53	396	84	268	65
과도한 개인정보 수집	115	146	379	847	1,139	1,200	868
고지한 범위를 넘어선 목적 외 이용 또는 제3자 제공	1,171	1,202	1,499	2,196	1,988	2,242	3,585
개인정보 취급자에 의한 훼손 · 침해 또는 누설	158	158	278	941	1,022	1,086	857
개인정보 처리 위탁 절차 위반	6	25	36	125	44	40	22
영업의 양수 등의 통지의무 불이행	6	22	64	44	47	54	41
개인정보 보호(관리)책임자 미지정	10	21	38	48	51	39	48
기술적 · 관리적 조치 미비로 인한 개인정보 유출 등	819	1,551	10,958	3,855	4518	7,404	4,006
수집 또는 제공받은 목적 달성 후 개인정보 미파기	294	323	488	779	602	686	767
열람 또는 정정, 삭제, 처리정지 요구 불응	680	826	662	717	674	792	957
동의철회 · 열람 · 정정을 수집보다 쉽게 해야 할 조치 미이행	603	630	800	660	510	352	381
법정대리인의 동의 없는 아동의 개인정보 수집	19	35	71	47	36	33	34
주민등록번호 등 타인 정보의 훼손 · 침해 · 도용	6,303	10,137	67,094	139,724	129,103	88,126	77,598
기타 개인정보침해	23,893	38,414	38,172	12,915	35,284	57,705	60,480
합 계	35,167	54,832	122,215	166,801	177,736	158,900	152,151

출처: 개인정보보호위원회(2016), 『2016년 개인정보 보호 연차보고서』

필요한지에 대해 논의하고, 개인정보 보호를 위한 대응책을 모색하고자 하였다.

Ⅲ. 연구방법 및 범위

1. 연구 방법

이 논문에서는 우리나라의 개인정보 보호제도 분석 틀을 구성하기 위해 우리나라 개인정보 보호 관련 인증제도와 법 등 그리고 관련된 국내외 문헌자료 등 다양한 연구 자료들을 검토하고자 하였다. 「개인정보 보호법」이 제정된 지 몇 년 지나지 않았지만, 현재와 지금까지의 문제점을 파악하기 위해 여러 사례들과 관련 연구 자료를 수집하고 분석 자료로 활용하였다.

첫째, 개인정보 보호 관리체계(Personal Information Management System, 이하 'PIMS'), 개인정보 보호 인증(Personal Information Protection Level, 이하 'PIPL'),[11] 정보보호 준비도 평가(SECU-STAR) 등 국내에서 시행되고 있는 인증 제도를 분석하였다.

둘째, 본인확인 수단으로 사용되는 i-PIN(이하 '아이핀'), My-PIN(이하 '마이핀')을 분석하였다.

기존의 관련 저서와 논문, 개인정보 보호제와 관련된 실무 기관의 자료(행정안전부, 방송통신위원회, 한국인터넷진흥원, 한국정보화진흥원 등 여러 정부기관의 연구보고서, 정기간행물, 발간자료 및 기타자료), 개인정보 보호제도와 관련된 정책 자료, 인터넷 웹 사이트 등을 분석 대상으로 삼았다.

연구 분석 방법으로는 우리나라의 개인정보 보호제도의 현황과 내용을 파악하고, 선행 연구 자료 등을 검토하여 변수를 추출하고 분석을 시도하였다.

이렇게 분석된 결과를 토대로 우리나라의 개인정보 보호제도에서 나타나는 문제점을 찾아내고, 이를 근거로 삼아 우리나라 개인정보 보호제도의 문제점을 논의하고 효율적인 방안을 제시하고자 하였다.

2. 연구 범위

이 연구는 우리나라의 개인정보 보호제도를 분석하여 문제점을 진단하고 그 개선점을 찾기 위한 것이다. 국내기관에서 시행하고 있는 PIMS, PIPL, 정보보호 준비도 평가 등 국내 기관에서 민간 자율로 시행하고 있는 인증제도의 현황 그리고 주민등록번호를 대체하는 수단으로 등장한 아이핀, 마이핀 등과 같은 개인식별번호 현황을 파악하고 분석하였다.

Ⅳ. 선행연구 검토 및 분석의 틀

1. 개인정보 보호제도 연구내용 검토

최광희 외(2012)는 우리나라의 개인정보 보호체계의 문제점으로 '과도한 주민등록번호 수집 및 이용', '개인정보 보호 조치 구축에 소극적', '개인정보 보호를 위한 이용자 참여 저조'를 지적하고 있다. 이창범(2012)은 「개인정보 보호법」의 특징', '개인정보 보호기구의 설치', 「개인정보 보호법」의 집행체계', '영세 · 소 사업자 등에 대한 적용제한', '목적 외 이용 및 제공 제한', '개인정보 취급위탁 공개 · 고지 의무' 등에 대해 논의하고 있다. 이들은 우리나라 개인정보 보호체계의 여러 문제점을 지적하면서 법 내용의 수정 보완 등을 주장하고 있다.

김민천(2010)은 주민등록번호 대체수단으로서의 아이핀의 정책 집행에 대해 성공보다는 실패에 초점을 맞추면서 가상공간에서 주민등록번호를 활용한 개인식별번호의 폐지 또는 현재 아이핀 정책이 보다 적극적일 필요가 있다고 주장하고 있다. 염흥열(2005)은 아이핀 이용을 유도하는 법적 근거 마련의 필요성을 제기하고, 동시에 기술적 개발이 이루어져야 한다

11) 2016년부터 PIMS로 통합되어 운영되나, 전체적인 제도의 이해를 돕기 위해 분석에 포함시켰다.

고 주장하고 있다.

김재광(2012)은 '정보 주체의 자기정보결정권'과 「개인정보 보호법」 상 정보주체의 권리' 에 대해 그리고 민윤영(2011)은 '인터넷 사용과 개인정보 노출'에 대해 문제점에 대해 분석하면서 개인정보 주체들의 권리의 확립에 대해 논의하고 있다.

김일환(2011a;b)은 '현행 「개인정보 보호법」제의 개관과 과거의 법제정비'와 '공공부문에서 개인정보 보호의 원칙과 기준', '민간부문에서 개인정보 보호의 원칙과 기준'에 대해 논의 하면서 개인정보 보호에 명확한 원칙과 기준을 법에 명시할 것을 지적하고 있다. 배대현(2012)은 '법률에 정한 자율규제 검토', '「개인정보 보호법」과 「정보통신망법」과의 관계', '손해배상책임 규정', '개인정보의 처리' 등을 논의했다. 그리고 '「개인정보 보호기본법」', '개인정보 보호 전담조직' 등의 분석을 통해 개인정보 보호 강화의 필요성을 주장했다.

방동희(2015)는 '개인정보자기결정권의 실현과 국가 · 지자체의 강한 책무부여', '인증제도의 의의와 기능', '인증제의 기능과 필요성' 등을 논하면서 우리나라 인증제도의 현황과 문제점을 통해 개선방향을 제시했다.

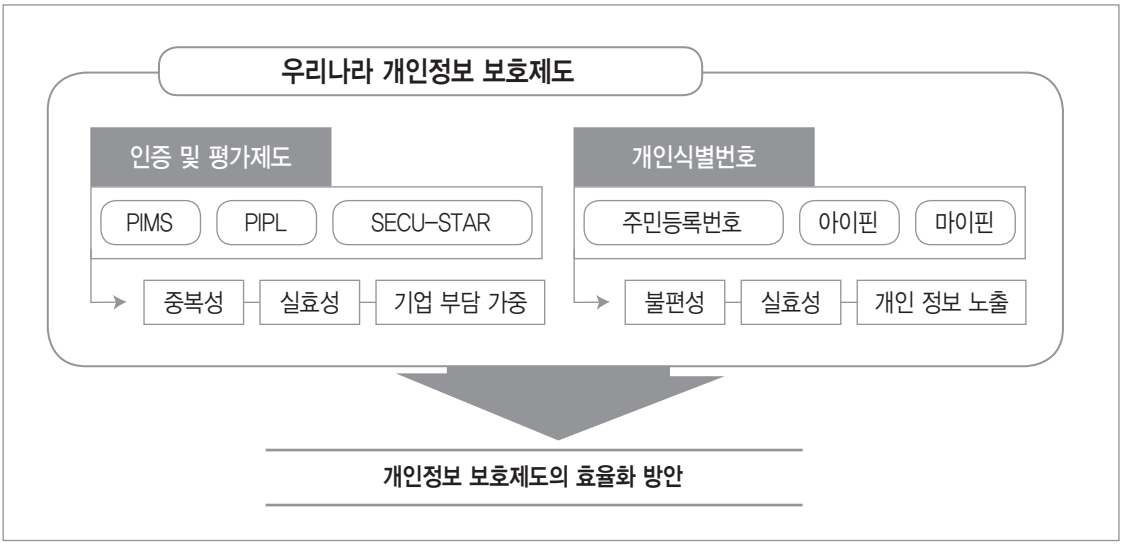
대부분의 연구자들은 개인정보 보호에 대한 구체성과 명확성을 강조하며 보다 적극적인 개인정보 보호를 위한 제도 및 기준의 필요성을 주장하고 있다.

2. 분석의 틀

이 연구는 우리나라의 개인정보 보호제도의 현황을 파악하고 보다 효율적인 개선 방안을 모색하기 위한 것이다. 물론 우리나라의 개인정보 보호제도 전체를 파악하고, 분석하는 것이 가장 최적화된 연구이겠지만, 방대한 개인정보보호 범위를 고려한 이 연구는 〈그림 1〉과 같이 개인정보 인증제도와 평가제도와 개인식별번호에 초점을 맞추어 진행하였다.

먼저 개인정보 인증제도 및 평가제도는 PIMS, PIPL, 정보보호 준비도 평가 등 기업 및 기관의 개인정보를 인증하고 평가하는 제도를 중심으로 현황을 파악하고, 중복성, 실효성, 기업 부담 가중 등의 변수를 설정하여 분석을 시도하였다.

개인정보 보호 인증과 평가라는 이름으로 진행되고 있는 제도들을 비교하여 제도 간의 중복성 및 현



〈그림 1〉 분석의 틀

재 혼재되어 있는 제도들의 실질적인 효과는 어느 정도인지를 중심으로 분석을 시도하였다. 이를 통해 실제 적용 대상인 기업의 부담 등을 서술하고 시행중인 제도의 개선 방향을 모색하였다.

우리나라는 주민등록번호라는 강제불변[12]의 개인식별번호가 모든 국민에게 부여되기 때문에 대한민국 국민으로 당연히 가지고 있어야 하는 번호이다. 주민등록번호는 국민 관리에 아주 효율적인 제도이지만, 온오프라인에서 야기되는 개인정보 유출 및 피해 문제의 중심에 있다. 이와 같은 문제를 해결하기 위해 정부가 마련한 것이 또 다른 개인식별번호인 아이핀과 마이핀이다. 이 연구에서는 우리나라 개인정보 보호 문제에서 빠질 수 없는 개인식별번호 제도의 현황을 파악하고 이를 분석하기 위해 불편성, 실효성, 개인정보 노출 등을 주요 변수로 설정하여 문제점 및 개선방안을 모색하고자 하였다.

이와 연구 분석 틀을 토대로 인증 및 평가제도와 개인식별번호에서 설정된 변수에서 드러나는 문제점과 개선점을 파악하고, 개인정보 보호제도의 효율성을 높일 수 있는 방안을 도출하고자 한다.

Ⅴ. 우리나라 개인정보 보호 제도

1. 우리나라의 개인정보 보호 인증제도

1) PIMS(Personal Information Management System, 개인정보 보호 관리체계)

PIMS는 〈표 2〉와 같이 2006년부터 개인정보 침해관련 민원이 급증한 것을 우려하여 2010년 11월에 시행하였다. 당시 개인정보침해사고 발생 시 집단소송 등을 통해 적극적 배상요청이 보편화 되는 추세였고, 법률 분쟁 시 개인정보 보호 노력을 객관적으로 증빙할 수 있는 인증 제도의 필요성이 제기되었다. 또 이미 영국과 일본 등 해외에서는 BS10012(영국), 프라이버시 마크제도(일본) 등 개인정보 보호와 관련하여 기업들에게 인증 및 마크를 부여하는 제도를 이미 시행하고 있었다. 이에 2009년 인증제도의 기반을 마련하고, 2010년 공청회 등을 거쳐 최종 확정되었다.

PIMS는 기업이 고객의 개인정보 보호를 체계적이고 지속적으로 수행하기 위해 필요한 보호조치로 이해할 수 있다. 즉 기업의 개인정보자산의 보호에 관련된 위험을 관리하기 위한 것이다. 인증심사 기준은 개인정보 관리과정, 보호대책, 생명주기 및 권리보장 3개 분야 등 86개 통제항목[13][14]으로 구성되어 있다.[15] 개인정보 보호에 대한 기술적 · 관리적 · 물리적 보호조치 및 준거성을 달성하기 위해 위험 정도를 평가하고 위험을 예방하기 위한 대책을 수립 · 운영하고자 하는 것이다. 이를 바탕으로 개인정보 보호 활동을

〈표 2〉 개인정보침해신고센터 신고 · 상담 접수 추이(2007~2015)

년도	2007	2008	2009	2010	2011	2012	2013	2014	2015
신고	847	988	2,139	1,788	2,556	2,058	2,347	2,992	2,316
상담	25,118	38,823	33,028	53,044	119,743	164,743	175,389	155,908	149,835
합계	25,965	38,911	35,167	54,832	122,215	166,901	177,736	158,900	152,151

출처: 개인정보보호위원회 (2016). 「2016 개인정보보호 연차보고서」.

12) 최근 소송 등을 통해 변경하는 사례도 있지만, 특별한 상황이 발생하지 않는 이상 우리나라 국민들에게 주민등록번호는 강제불변의 국민등록번호로서의 역할을 하고 있다.
13) 2016년 1월 1일부터 공공기관 86개, 대기업 또는 정보통신 서비스 제공자 83.개, 중소기업 74개, 소상공인 47개로 구분하여 적용한다.
14) 세부항목은 현재 작업 중에 있으며 현재는 이전의 310개의 세부점검 사항으로 진행하고 있다.
15) 2016년 1월 1일 이전 인증심사 기준은 개인정보 관리과정, 보호대책, 생명주기 3개 분야 등 124개 통제항목, 310개의 세부점검 사항으로 구성되어 있다.

체계적이고 지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 PIMS 인증을 부여하는 제도이다. 인증기관은 한국인터넷진흥원이다.[16][17]

PIMS 인증의 근거는 '개인정보 보호 관리체계 인증 등에 관한 고시'(행자부고시 제2015-52호, 방통위고시 제2015-29호)[18]와 「정보통신망법」 제47조의3(개인정보 보호 관리체계의 인증)에 있다. 그러나 법적근거를 지니고 있다 해도 강제성은 없는 인증제도이다. 기업이 스스로 필요하다고 판단되면 담당기관에 인증을 의뢰하는 방식이다. PIMS 인증의 유효기간은 3년(매년 사후관리)이며, 기업은 이를 위해 1,000만 원 이상의 비용을 부담해야 한다(기업 규모에 따라 차이는 있으며, 개인정보취급자 수와 서버급 컴퓨터 대수에 따라 비용과 심사기간이 달라진다). 심사기간은 약 10일 이상이 소요되며, 심사를 받기 위해 개인정보보호관리체계를 구축하고 2개월 이상 운영해야 한다. 2010년 말에 시행된 PIMS 인증은 2016년 8월 기준 총59건이다.

2) PIPL(Personal Information Production Level, 개인정보 보호 인증)[19]

PIPL은 2011년 「개인정보 보호법」 제정 이후 여전히 미흡했던 기업 및 기관들의 개인정보 보호 수준을 우려하여 2013년 11월 29일 시행하였다.

PIPL의 심사기준은 심사영역 9개, 심사목적 26개, 심사항목 65개로 구성되어 있다. 이 중 심사기준 항목의 내용은 ①「개인정보 보호법」 기반의 법적 요구사항, ②개인정보 보호체계 수립 및 이행, ③개인정보 흐름분석을 통한 위험분석 및 위험관리, ④경영진 참여 및 의사결정, ⑤개인정보 보호 강화를 위한 보호대책으로 구성되어 있는데 유형별로 차등 적용하고 있다. 유형별로는 공공기관과 대기업이 각각 65개, 63개 항목으로 ①~⑤의 내용을, 중소기업은 52개 항목으로 ①~③의 내용을, 소상공인은 ⑤의 내용을 적용하고 있다. 인증기관은 한국정보화진흥원이며, 행정자치부가 인증 관련 법 · 제도 개선 및 정책 결정을 담당하고 있다.

PIPL은 기업 및 기관의 개인정보처리자에게는 개인정보 보호 활동의 기준 제시 및 일정 수준 이상의 자율적 개인정보 보호가 가능하도록 하고, 정보주체에게는 개인정보가 안전하게 관리되고 있음을 인식할 수 있는 기준을 제공하기 위함이다. 즉, PIPL은 개인정보처리자의 개인정보 보호 관리체계 구축 및 개인정보 보호조치 사항을 이행한 공공기관과 민간기업의 개인정보 보호 수준을 점검하고 PIPL 인증마크를 부여하는 제도이다.

PIPL의 법률적 근거는 「개인정보 보호법」 제13조

〈표 3〉 연도별 PIMS 인증 추이

년도	2011	2012	2013	2014	2015	2016*	계
건 수	2	7	8	6	14	22	59

* 2016년은 8월 기준
출처 : 한국인터넷진흥원(http://isms.kisa.or.kr)

16) 2016년 1월 1일 이전 인증기관 지정 및 감독 업무를 담당하는 인정기관은 방송통신위원회이며, 인증심사 수행 및 결과를 보고하는 인증기관은 한국인터넷진흥원이었다.
17) 정책기관은 방송통신위원회와 행정자치부가 공동으로 맡고 있다.
18) 2016년 1월 1일 이전 PIMS 인증의 근거는 '개인정보 보호 관리체계 인증 등에 관한 고시'(제2013-17호) 제15조(인증의 신청 등)와 '정보통신망법' 제47조의3(개인정보 보호 관리체계의 인증)이었다.
19) PIPL은 2016년 1월 1일부터 PIMS로 통합되어 운영된다. 2016년 1월 1일부터 PIMS와 통합 운영되기 때문에 신청기업 및 기관은 2016년 12월 31일까지 PIPL과 PIMS 중 하나를 선택하여 받을 수 있다(단, 최종인증서는 PIMS로 발급).

(자율규제의 촉진 및 지원), '개인정보 보호 인증제 운영에 관한 규정' 제2014-1호(행정자치부고시)에 있다.

PIPL 인증의 유효기간은 3년(매년 유지관리심사)이며, 기업은 이를 위해 1,000만 원 이상의 비용을 부담해야 한다(기업 규모에 따라 차이는 있으며, 개인정보취급자 수, 개신정보처리시스템 수, 정보주체 수 등에 따라 비용과 심사기간이 달라진다). 심사기간은 약 5일 이상이 소요되며, 심사를 받기 위해 신청기업은 개인정보보호 관리체계 및 대책들이 효과적으로 이루어지고 있는지에 대해 상시 점검활동 등을 3개월 정도 지속적으로 진행해야 하는 등의 준비과정을 거쳐야 한다. 2013년 말에 시행된 PIPL 인증은 2015년 12월 말 기준 총 16건이다.

3) 정보보호 준비도 평가(SECU-STAR)

정보보호 준비도 평가는 정부의 노력에도 불구하고 지속적인 개인정보 유출 사고 그리고 최근 이어지는 금융권의 개인정보 대량 유출 사고(2011년 현대캐피탈, 하나 SK카드, 삼성카드, IBK캐피탈, 2012년 한국스탠다드차타드은행, 2013년 시티은행, KB카드, 롯데카드, NH카드 등)에 대한 우려가 커짐에 따라 국민들의 우려를 불식시키기 위해 2014년 11월부터 시행하였다. 기반지표(정보보호 리더십, 정보보호 자원관리), 활동지표(관리적 보호활동, 물리적 보호활동, 기술적 보호활동), 선택지표(개인정보보호) 등 3개 지표 30개 항목 117개[20] 세부지표로 구성되어 있다.

정보보호 준비도 평가는 2014년 11월 기업의 자발적인 노력과 정보보호에 대한 투자 활성화를 유도하여 국내 기업들의 정보보호 역량 강화 및 정보보호 사각지대를 해소하기 위해 만들어졌다. 기존 제도들의 한계점을 극복하기 위해 평가 기간, 비용 등을 감소시켰고, 이는 기업의 재정 · 물리적인 부담을 완화시켜주기 위함이었다. 또 컨설팅과 자문의 개념을 강화시킨 것이 정보보호 준비도 평가의 특징이다. 정보보호 준비도 평가는 기업의 정보보호 수준을 평가하기 전에 정보보호에 대한 사전 컨설팅과 자문을 진행함으로써 기업이 정보보호에 대한 인식을 높이고 충분히 준비할 수 있도록 평가 준비기간을 부여해 주었다. 2014년 출범부터 2015년까의 체계는 인증기관과 평가기관으로 구성되어 있었으며, 인증기관은 한국정보방송통신대연합(이하 'ICT대연합'), 평가기관은 한국정보통신진흥협회(이하 'KAIT'), 한국정보통신기술협회(이하 'TTA'), 한국침해사고대응팀협의회(이하 'CONCERT')가 역할을 담당하였다.

정보보호 준비도 평가 대상은 국내 모든 산업(비ICT 포함)군을 포함하고 있다. AAA~B까지 5단계의 등급 체계를 갖추고 있고, 개인정보보호 평가를 선택하여 받을 시 등급에 'P'마크를 부여하고 있다. 등급 부여는 인증기관에서 최종 진행하지만 평가의 공정성과 신뢰성 확보를 위해 인증기관이 10명으로 구성된 심의위원회(외부전문가로 구성)를 운영하고 있다.

정보보호 준비도 평가 민간의 자율적인 정보보호 활성화를 목표로 하였기 때문에 2014년 11월 출범당시 명확한 법적 근거를 가지고 시행되지 않았다.[21] 그러나 정보보호 산업의 활성화의 필요성을 인지하고,

〈표 4〉 정보보호 준비도 평가 등급 인증 추이

년도	2014	2015	2016*	계
건 수	19	8	24**	51

* 2016년은 8월 기준
** 2016년 개정된 제도 기준으로 진행된 인증은 1건임
출처: 한국정보방송통신대연합

20) 표개인정보보호 세부지표 17개.

2015년 5월 53일 「정보보호 산업 진흥에 관한 법률」이 제정되면서 법령 근거가 마련되었다. 동법 제12조(정보보호 준비도 평가 지원 등)에 대한 내용이 포함되면서 정보보호 준비도 평가 제도의 필요성이 강조되었다. 정보보호 준비도 평가 등급의 유효기간은 1년이며, 평가를 받기 위한 비용은 500만원 미만이다. 평가기간은 3일(서면평가 1일, 현장평가 2일)이며 타 제도와 달리 체계 구축 운영기간이 없다. 2014년 말에 시행된 이 제도의 등급 인증은 2016년 8월 기준 총 51건이다.

그러나 2015년 12월 「정보보호 산업의 진흥에 관한 법(이하 '정보보호산업법')」이 시행되면서 지금까지 진행되었던 체계가 많이 바뀔 것으로 예상된다. 한국인터넷진흥원이 전담기관으로 지정되어 평가기관을 등록받도록 하고 있다. 이에 따라 평가기관으로 등록받고자 하는 기관 및 기업은 평가 결과에 대한 심의를 담당하는 기구 또는 기관을 별도로 구성 또는 지정을 해야 한다.[22] 평가비용 역시 평가기관별로 책정이 가능해졌으며, 기존에 진행되어왔던 측정지표 역시 바뀔 제도에 맞게 수정될 것으로 보인다.

2. 우리나라의 개인식별번호

1) 주민등록번호

1942년 시행된 기류제도에서 비롯된 주민등록번호 제도는 1962년 법률 제1067호로 「주민등록법」이 공포되면서 처음 실시되었다(김일환, 2004. 참고). 주민등록번호는 1968년 1차 개정에서 「주민등록법시행령」에 처음으로 명문화 되었으며, 당시에는 12자리로 이루어져 있었다. 현재 우리가 사용하는 13자리[23]의 주민등록번호는 1975년 「주민등록법시행령」과 시행규칙의 개정으로 이루어졌다.

우리나라 주민등록제도의 목적은 "시(특별시 · 광역시 제외하고, 특별자치도 포함) · 군 또는 구(자치구)의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것"으로 규정하고 있다.[24]

주민등록번호의 체계는 총 13자리(YYMMDD-ABCDEFG)로 이루어져 있으며, 'YYMMDD'에 부여되는 여섯 자리는 생년월일을 나타낸다. 'A'는 출생 연대와 성별, 'BCDE'는 출생 신고지의 지역번호, 'F'는 출생 신고지에 출생 신고된 순서, 마지막 'G'는 주민등록번호의 진위 여부를 확인하는 오류 검증 번호로 구성되어 있다. 우리나라의 국민들은 태어난 지 1개월 이내에 출생 신고를 한 뒤, 주민등록번호를 국가로부터 부여받는다. 주민등록번호는 법으로 규정되어 있는 제도이기 때문에 우리나라에서 살아가기 위한 우리나라의 국민이라면 무조건 부여받아야만 하는 강제성의 성격도 가지고 있다(김민천, 2009. 참고).

2) 아이핀

아이핀[25]은 정보통신부[26]가 대면 확인이 불가능한 인터넷 상에서 주민등록번호를 대신할 수 있는 개인식별번호의 목적으로 2005년 7월에 도입하였다. 인터넷 상에서 주민번호를 대신하여 아이디와 패스워드를 이용하여 본인확인을 하는 수단으로 4개 발급기관(민간 3개,[27] 공공 1개)[28]에서 아이핀을 발급하고 있

21) 법적 근거는 없었지만, 평가를 위한 측정 지표는 「정보통신망법」, 「개인정보 보호법」을 준수하여 구성이 되어 있다.
22) 인증기관의 내용이 법에 규정되지 않으면서 심의기구 또는 심의기관으로 그 기능이 명시되었다.(동법 시행령 (별표1) 참고).
23) 「주민등록법」 시행규칙 제2조 (주민등록번호의 작성)「주민등록법」제7조제3항에 따른 주민등록번호는 생년월일 · 성별 · 지역 등을 표시할 수 있는 13자리의 숫자로 작성한다.
24) 「주민등록법」 제1조(목적) 참고.
25) '아이핀'이라는 용어는 2006년 10월부터 사용하였다(이전에는 발급 기관별로 가상주민번호, 개인ID인증, 개인인증키 등의 용어로 지칭되었음)(김민천, 2009).
26) 1994년 「정부조직법」 개정에 따라 과학기술처 · 공보처 및 상공자원부의 정보통신 관련 기능을 흡수 · 통합하여 정보통신부로 개편되었다가, 2008년 「정부조직법」 개정에 따라 해체되고 그 기능이 산업자원부, 과학기술부, 지식경제부, 문화체육관광부, 방송통신위원회, 미래창조과학부(2008년 신설)로 이관되었다.

다.[29] 아이핀은 이용자가 발급기관 사이트에서 이름과 주민등록번호를 입력하고 아이디와 비밀번호를 입력하고, 3개의 신원확인수단(휴대폰, 공인인증서, 대면확인) 중 하나는 선택하여 신원확인을 받으면 발급된다. 아이핀은 이용자가 언제든지 폐지 및 재발급이 가능하며, 미성년자도 부모의 확인이 있으면 발급이 가능하다. 아이핀은 「정보통신망법」 제23조 제2항(주민등록번호의 사용 제한)을 배경으로 하고 있으며, 그 운영은 한국인터넷진흥원이 전담기관으로 담당하고 있다.

3) 마이핀

마이핀은 일상생활에서 사용할 수 있는 본인확인 수단으로 개인식별정보가 포함되지 않은 13자리의 무작위 번호로 온라인에서 사용하던 아이핀을 오프라인까지 확대 제공하는 서비스로 「개인정보 보호법」 개정에 따라 2014년 8월부터 시행하였다. 공공 1개,[30] 민간 3개[31]의 온라인 기관이 있으며, 전국 읍/면사무소 및 동민센터에서도 방문 발급이 가능하다.[32] 마이핀은 이용대상이 전국민이나, 의무사항은 아니다. 개인정보를 포함하고 있지 않은 임의의 13자리 숫자를 신청인에게 부여하고, 신청인은 연 5회에 걸쳐 부여받은 번호의 변경이 가능하다. 발급한 마이핀 번호의 유효기간은 3년이다.

아이핀이 온라인 전용이라면 마이핀은 오프라인에서 주민등록번호 대신 제시하는 번호로 만들어졌다. 멤버십카드 발급, ARS 상담, 도서대여 등 주민등록번호 대신 사용할 수 있는 번호이다. 「개인정보 보호법」 제24조의2(주민등록번호처리의 제한)에 따른 주민등록번호 수집법정주의 시행으로 마련되었으며, 안전행정부(현행정자치부)가 시범운영을 거쳐 총괄 운영하고 있다.

Ⅵ. 우리나라 개인정보보호 제도의 문제점 분석 및 효율화 방안

1. 개인정보보호 인증제도

본 연구에서 소개한 PIMS와 PIPL은 기업의 개인정보관리 체계를 심사하여 그 결과를 인증하는 제도이고, 정보보호 준비도 평가는 기업의 정보보호 및 개인정보보호 수준을 평가하여 그 결과에 따라 최종등급을 부여해주는 제도이다.

1) 중복성

우리나라의 개인정보보호 인증제도는 국민들의 개인정보를 안전하게 보호하고 있는지에 대한 공인된 기관에서 검증해주고, 해당 기업의 개인정보보호 활동의 적극성을 판단하도록 해주지만, 꾸준히 중복성의 문제가 제기되어 왔다. 특히, PIMS와 PIPL의 중복성 문제에 대한 논의가 끊이지 않고 있다. 정부도 2014년 7월에 발표한 '개인정보보호 정상화 대책'에서 안행부, 미래부, 방통위 등이 각각 운영하는 유사 인증제도간 중복을 해소한다는 내용을 담으며 인증제도의 중복에 대한 문제점을 지적하고 있다. 이에 따라 2014년 8월 범부처 인증제도 개선방안을 발표하면서 PIMS와 PIPL 통합 안을 내놓기도 했다. 2014년 10월 국감에서도 PIMS와 PIPL의 통합 운영의 필요성을 제기하였다.[33] 이는 두 제도 인증항목의 유사성 때문이다.

PIPL 제정이 추진되던 2013년 5월 안전행정부(현행정자치부)의 '개인정보 보호 인증제' 추진과 운영에

27) 서울신용평가정보, 나이스신용평가정보, 코리아크레딧뷰로.
28) 공공 I-PIN센터.
29) 인터넷 이용자는 i-PIN과 공공I-PIN 중 하나만 발급받으면 공공사이트와 일반사이트 어디서든 사용할 수 있다.
30) 공공 I-PIN센터.
31) 나이스아이핀, 사이렌아이핀, KCB아이핀.
32) 민간본인확인기관 본사 및 지사 방문 발급도 가능.
33) 유승희 의원(새정치민주연합, 미래창조과학방송통신위원)은 PIMS, PIPL 인증 제도를 통합 운영해야 된다고 지적함.

〈표 5〉 각 인증제도의 주요 평가 내용

PIMS*	PIPL*	PIA	정보보호 준비도 평가
– 개인정보 정책수립 – 관리체계 범위설정 – 위험관리, 구현 – 사후관리	– 「개인정보 보호법」 기반의 법적 요구사항	– 기관 내부의 개인정보 보호체계, 규정, 조직 현황 등	– 개인정보 최소수집
– 개인정보 보호 정책 – 개인정보 보호 조직 – 개인정보 분류 – 교육 및 훈련 – 인적보안 – 침해사고처리 및 대응절차 – 내부검토 및 감사 – 기술적 · 물리적 보호조치	– 개인정보 보호체계(관리체계) 수립 및 이행	– 개인정보취급자 (정보시스템관리자, 접근자 등), 위탁업체 등에 대한 내부 규정 및 관리 · 교육 체계	– 개인정보 수집 고지 및 동의획득
– 수집, 이용 및 제공 – 관리 및 파기	– 개인정보 흐름분석을 통한 위험분석 및 위험관리	– 개인정보 보호 정책 환경 분석	– 개인정보 취급방침
	– 경영진 참여 및 의사결정	– 영향평가 대상사업의 특수성을 반영한 정책 환경	– 이용자 권리 보호
	– 개인정보 보호 강화를 위한 보호대책	– 정보시스템을 통해 수집되는 개인정보의 양과 범위가 해당 사업 수행의 적절성	– 개인정보의 관리적 보호조치
		– 정보시스템의 외부연계 여부 검토	– 개인정보의 기술적 보호조치
			– 개인정보 파기

* 2016년부터 통합 운영

관한 규정 마련을 위한 검토회의에서도 유사인증제도(PIMS)와의 중복 문제가 중요한 논의 주제로 다루어지기도 했다. 방동희(2014)는 이에 대해 「개인정보 보호법」제정 이후로 PIPL의 완성도를 높이기 위해 고시 마련의 필요성을 주장하면서도 이미 수행되고 있던 PIMS와의 중복 문제를 가장 큰 걸림돌이라고 했다. 이에 대해 정부 역시 유사인증 제도간 중복을 해소하고 상호 인정범위를 확대 할 것을 2014년 7월 "개인정보보호 정상화 대책"에서 언급하면서 제도의 중복성을 인지하고 있었다.

우리나라의 모든 개인정보보호 인증 및 평가는 개인정보보호 법률의 준수 사항을 기본으로 하고 있기 때문에 유사성을 가질 수밖에 없다. 위의 〈표 5〉에서 볼 수 있듯이 각 인증 제도는 유사한 항목들을 주요 평가 내용으로 삼고 있다. 평가 항목들 역시 큰 틀을 벗어나지 않고 유사하게 구성되어 있다. 그럼에도 불구하고 지금처럼 운영되고 있는 이유는 담당기관이 모두 다르기 때문이다. PIMS는 한국인터넷진흥원, PIPL은 한국정보화진흥원이 운영했고, 정보보호 준비도 평가는 한국정보방송통신대연합에서 2015년까지 운영했다. 이중 PIA는 공공기관만을 대상으로 한다는 특징을 가지고 있기 때문에 그 성격이 다르다고 할 수 있다. 또 정보보호 준비도 평가는 개인정보보호만을 평가하는 제도가 아니라 기업의 정보보호 현황 전체를 평가하는 제도이기 때문에 PIMS와 PIPL보다는 평가 범위가 넓다. PIMS와 PIPL은 개인정보보호만을 다루고 그 대상 또한 겹치기 때문에 중복성이 아주 강한 제도들이다.

2) 실효성

PIMS, PIPL 그리고 정보보호 준비도 평가는 기업 및 기관의 개인정보보호를 평가하고 인증하기 위해

시행된 제도들이다. 이중 특히 PIMS와 PIPL은 기업 및 기관의 개인정보보호만을 심사하고 결과에 따라 인증서를 발급하고 있다(정보보호 준비도 평가는 정보보호 전체에서 개인정보보호 분야를 포함하고 있음). 이 때문에 앞서 언급했듯이 제도의 중복성 문제가 많이 대두되었다.

〈표 6〉에서 볼 수 있듯이 PIMS는 2016년 8월까지 약 5년여 동안 59건, PIPL은 2년여 동안 16건에 불과하다. 그리고 정보보호 준비도 평가는 총 51건이다. 그러나 이 중 개인정보보호를 받은 기업은 1건이다.[34] 정보보호 준비도 평가의 경우 시행된 지 1년이 되지 않은 상황에서 시장이 형성되었다고 보기 어렵기 때문에 현재의 수치로 실효성을 논하기는 어렵다. 그러나 PIMS의 경우 시행 6년째에 접어들었고, PIPL은 2년차에 있는 제도이다. 이 두 제도는 개인정보 유출사고가 빈번하게 발생함에도 불구하고 여전히 시장을 확보하지 못하고 있는 것으로 볼 수 있다. 이는 PIPL의 경우 의무제도가 아니다 보니 취득하려는 기업이 많지 않고, PIMS 인증을 취득하기도 사실상 쉽지 않으며, 기업에서 개인정보관리체계를 강화하지 않고는 고시 기준에 맞춰 구축 · 운영하는 게 어렵기 때문이라는 것이다. 또한 PIMS와 PIPL의 통합[35][36] 이후 인증 취득여부를 결정하려는 기업이 상당수 있다는 것이다(보안뉴스, 2015년 6월 24일 참고).

3) 기업의 부담 가중

개인정보보호 인증제도는 국내 기업들의 개인정보보호 수준을 향상시키고 개인정보보호 산업을 활성화시키기 위해 추진된 제도이다. 그러나 우리나라 기업 구조는 2013년 기준으로 1인 기업이 82.3%, 2~9인 기업 13.9%, 10~49인 기업 3.2%, 200~299인 기업과 300인 이상 기업이 각각 0.1%의로 이루어져있다. 2013년 우리 기업생태계는 49인 이하 기업이 99.3%를 차지하고 있다(2015, 전국경제인연합회). 즉 우리나라 기업의 99% 이상이 중소기업으로 구성되어 있다는 것이다. 여기에 더해 한국인터넷진흥원(2014)에 따르면 정보보호 예산 편성을 하지 않는 기업이 89.5%에 달한다고 한다. 즉, 국내 기업 분포 구조상 대부분의 기업 매출액이 낮음을 유추할 수 있다.

기업들은 PIMS 인증을 받기 위해 최소 1,000만 원 이상의 비용을 지출해야만 한다. 3년 주기로 되어 있으나 사후평가 등이 실시되기 때문에 기업들은 매년 적지 않은 예산을 인증비용을 지출하여야만 한다. 정보보호 준비도 평가를 받기 위해서는 최소 500여만 원[37]의 비용을 지불해야만 한다. 정보보호 준비도 평가의 비용에는 기업의 개인정보 보호[38]와 정보보호

〈표 6〉 각 인증제도의 주요 평가 내용

구분	PIMS	PIPL*	정보보호 준비도 평가
출범년도	2010	2013	2014
총 인증 수(건)	59	16	51

* PIPL은 2016년 1월 1일부터 PIMS와 통합되었기 때문에 16건을 끝으로 사라지게 되었다.
※ PIA는 공공기관만을 대상으로 하고 있기 때문에 실효성 분석에서 제외하였다.

34) 정보보호 준비도 평가의 경우 시행된 지 1년여가 지났고, 「정보보호 산업 진흥에 관한 법률」이 뒤늦게 제정되면서 제도가 변하였기 때문에 현 시점에서 구체적인 시장이 형성되었다고 보기 힘들다.
35) 2014년 8월 5일 제2기 규제개혁위원회에서 2014년 3월 20일 제1차 규제개혁 장관회의의 후속조치 일환으로 '범부터 인증제도 개선방안'을 통의하고, 25개 부처 139개 임의인증을 원점에서 검토하여 유사인증을 통합 및 감축하기로 하였다.
36) 2014년 7월 방송통신위원회는 사업자들의 혼란을 줄이기 위해 PIMS, PIPL, ISMS(정보보호관리체계)의 통합 추진 계획을 발표하였다.
37) 「정보보호산업법」 제정 이전에는 중소기업의 경우 30% 할인율 적용(약 340만 원).
38) 개인정보보호는 기업의 선택사항으로 규정하고 있다.

전체 평가가 포함되어 있다. 정보보호 준비도 평가의 경우 기업이 개인정보 보호 수준을 평가 받기 위해서는 고정비용[39]이 지출되지만, PIMS의 경우는 기업 및 기관의 규모와 종류에 따라 비용이 차등 적용된다. 기업의 상황에 따라 인증 비용이 1,000만 원을 쉽게 넘어설 수 있다는 것이다. 중·소·벤처기업이 대다수인 우리나라의 기업 분포 상 고가의 인증비용은 대부분의 기업들에게 큰 부담으로 작용할 것이다.

4) 개인정보보호 인증제도의 효율화 방안

정부는 최근 인증제도 간의 중복성 문제를 해결하기 위해 PIMS와 PIPL을 통합하는 정책을 시행했다. 국내에서 개인정보보호 관련 인증제도는 이제 하나의 제도로 합쳐진 것이다. 그러나 여전히 타 제도와의 중복성 문제는 남아있다. 타 제도는 개인정보보호만을 다루고 있지는 않지만 개인정보보호를 포괄한 채 운영되고 있기 때문에 정부에서 운영하고 있는 정보보호제도 간의 조정 또는 통합 문제는 지속적인 논의가 필요한 것으로 보인다. 2016년부터 정보보호 준비도 평가, ISMS, PIMS 등 정부가 시행하고 있는 정보보호 인증제도의 전담기관은 한국인터넷진흥원으로 일원화되었다. 이제 인증제도 전담기관 간의 분쟁 요인은 제거된 것으로 볼 수 있다. 따라서 현재 시행되고 있는 인증제도 중 정보보호 준비도 평가와 ISMS의 명확한 구분을 해야 할 필요가 있다. 그리고 중복성 논란을 사라지게 할 수 있는 PIMS만의 필요성 마련 등으로 통해 시장의 혼란(기업의 입장에서는 어떤 인증을 받아야할지 대한 고민)을 없앨 수 있는 정책을 수립해야 한다.

〈표 6〉과 같이 2016년 현재 인증제도가 5년 이상 운영되었음에도 불구하고 시장은 여전히 활성화되지 않고 있다. 우리나라 전 산업의 정보보호 수준 향상을 위해 시행을 했지만, 지금과 같은 결과에 대해서는 제도의 실효성과 정책의 변화를 신중히 고민해봐야 할 것이다. 정부는 산업의 개인정보 보호 향상을 위해 오랜 기간 연구하여 지금의 정책들을 만들고 시행하고 있지만, 많은 기업들은 아직 그 필요성을 명확히 인지하고 있지 못하고 있다. 2015년 국내 정보보호산업 실태조사(한국정보보호산업협회, 한국인터넷진흥원, 2015)에 따르면 국내 기업이 IT 예산 중 정보보호에 투자하는 비율이 3%에 그친다. 5% 이상을 투자하는 비율이 40%인 미국과 50%인 영국에 비하면 비교자체가 불가한 수준이다. 그리고 5인 이상의 국내 기업 중 정보보호 예산을 편성하고 있는 기업은 20.9%에 불과하다. 개인정보 보호를 정보보호의 범주에 포함시킬 때 국내의 정보보호 시장은 여전히 열악한 상황으로 볼 수 있다. 이와 같은 결과는 기업입장에서 필요성을 느끼지 못하는 것도 큰 요인으로 볼 수 있다. 매년 이어지는 정보유출 사고가 발생하지만 대부분의 기업들은 스스로 위험성을 느끼지 못하고 있는 것이다. 정부는 운영 중인 인증 제도를 활용하여 기업의 개인정보보호 필요성에 대해 보다 적극적으로 나서야할 것으로 본다. 그리고 현재 국내의 시장 상황의 어려움에 대해서는 기업의 정보보호에 대한 인식의 변환이 반드시 이루어져야 할 부분이다.

기업의 인증에 대한 부담을 해결하기 위해서는 각 인증제도 간의 명확한 구분이 우선시 되어야 할 것이다. 예들 들면 기업규모·특성별 인증제도 구분, 기업과 기관의 구분 등을 통해 비용을 책정하는 것이다. 현재 각 인증 제도별로 구분을 하고 있으나, 각각의 시행보다는 규모별 기업의 의견과 시장상황을 고려하여 먼저 전체 제도 간의 명확한 구분을 통해 비용을 재산정하는 것이 시장의 혼란과 기업의 부담을 경감시킬 수 있을 것이다.

국제적으로는 영국에서 제정되어 국제적으로 활용되고 있는 BS10012,[40] ISO/IEC 27001[41]이 있다.

39) 「정보보호산업법」 제정 이후 기업 규모별로 평가 비용 책정 예정(평가기관별로 각각 다른 비용 책정 가능).
40) 영국 표준협회(BSI, British Standard Institute)가 개인정보의 효과적 관리체계에 관한 표준으로 국제규격에 맞게 설계한 인증 제도.
41) 기업 정보보안 운영을 위해 정보보호정책, 조직체계, 운영, 접근통제 등의 통제항목으로 구성된 국제 표준 정보보안 인증(영국표준(BS)이었으나 2015년 11월 ISO로 승격).

BS10012는 개인정보보호, ISO/IEC 27001은 기업의 정보보호 운영에 적용할 수 있도록 설계되었다. 특히 개인정보보호 국제규격으로 제정된 BS10012는 개인정보보호 및 관리를 위한 계획수립, 이행, 운영, 감시, 검토, 유지관리 및 지속적 개선이 효과적으로 수행될 수 있도록 하고 있다. 두 제도는 명확한 영역 구분을 통해 이 연구에서 지적하고 있는 중복성, 실효성, 기업 인증의 부담 등의 문제를 해소했다고 볼 수 있다. 또한 국제규격이기 때문에 인증을 받은 기업들에게는 대외적으로 높은 정보보호 수준을 자랑하는 제도이기도 한다. 이와 같은 사례를 참고하여 우리 인증 제도를 국제 규격과의 연계,[42] 인증제도 개선 등의 방안을 마련한다면 보다 효율적인 제도의 확립이 가능할 것이다. 최근 국내 정보보호 인증 기준이 국제 표준에 반영[43]되는 등 국내 인증 제도의 발전을 위한 우리 정부의 많은 노력이 있기 때문에 분명 지금보다는 효율적인 인증제도로의 발전이 가능할 것으로 기대된다.

2. 개인식별번호

1) 불편성

아이핀, 마이핀은 주민등록번호를 대체하기 위해 만들어진 개인식별번호이다. 주민등록번호는 1962년 법령 제정과 함께 시행되어 지금까지 우리나라 국민들을 식별할 수 있는 유일한 번호로 인식되어 왔다. 주민등록번호의 개념보다는 국민등록번호의 개념이 강한 제도로 우리나라 국민이라면 당연하게 받아들여온 세계 유일의 번호이다. 특히 국내에서 안정적인 생활을 유지하기 위해서는 필수적인 번호로 자리매김해 왔다. 정부와 국민, 민간기업까지 국내에서의 주민등록번호 사용을 당연하게 받아들였던 것이다.

그러나 1990년대 중반 인터넷이 등장하면서 주민등록번호 사용의 문제점이 강하게 대두되었고, 이에 따라 아이핀과 마이핀이 주요 대체수단으로 등장하였다. 그러나 이 번호는 주민등록번호처럼 국가에서 지정되어 나오는 의무적인 고유 번호가 아닌, 이용자의 신청에 의한 발급번호이다. 즉, 아이핀은 이용자가 국가 지정 온라인 사이트에서 발급받고, 마이핀은 주민센터 방문을 통해 발급받을 수 있다. 두 번호 모두 13자리의 무작위 숫자로 구성되며, 아이핀은 온라인 대체수단, 마이핀은 오프라인 대체수단으로 기능을 하고 있다.

주민등록번호를 대체할 수 있는 수단이 생겨났기 때문에 외형적으로는 개인정보의 안전성이 확보된 것처럼 보인다. 하지만 이는 우리나라 국민들이 개인식별번호를 최대 3개씩이나 가지게 되면서 노출할 수 있는 개인정보 수단이 확대된 것으로도로 볼 수 있다. 또 주민등록번호의 위험성을 극복하기 위해 만들어진 아이핀과 마이핀은 발급 받을 시 반드시 주민등록번호를 입력하거나 제출해야하는 문제점을 가지고 있다. 국민들은 또 다른 개인식별번호를 발급받기 위해 지정된 사이트나 주민센터를 방문하여야 한다는 것이다. 그러나 한 번의 발급만으로 끝나는 것이 아니라 개인정보유출 방지를 위해 이들 번호를 주기적으로 바꾸어야 한다.[44] 개인정보 유출의 위험이 줄어들기 보다는 더 증가한 것으로 볼 수 있다. 개인정보보호를 위해 어느 정도의 불편을 감수할 수 있겠지만, 주민등록번호 대체수단의 등장은 우리나라 국민들로 하여금 개인식별번호에 대한 관리 부담과 사용의 불편함을 오히려 가중시키고 있다.

2) 실효성

아이핀은 2005년부터 온라인상에서 주민등록번호

42) 2016년 9월 한국인터넷거버넌스포럼에서는 ISMS와 ISO/IEC 27001의 상호인증에 대한 논의가 활발하게 이루어지기도 했음.
43) 2016년 8월 29일부터 9월 7일까지 개최된 정보보호 국제표준화 회의'에서 한국ITU연구위원회 정보보호연구반의 'X.805 보안 영역의 구현을 위한 기술적 보안 대책'이 국제표준(ITU-T X.1039)으로 최종 채택.
44) 아이핀은 수시로 변경이 가능하며, 마이핀은 1년에 5회로 제한되어 있음.

를 대체하기 위해 지금까지 시행되고 있다. 방송통신위원회에 의하면 현재 아이핀은 2015년 7월 기준으로 2,215만개가 발급되었으며, 약 2만여 개 웹사이트에서 사용이 가능하다.[45] 2014년부터 시행된 마이핀은 2015년 4월 기준으로 275만 명이 발급받았으며, 129개(2015년 6월 기준)[46] 기관이 도입하고 있다.

아이핀과 마이핀은 우리나라 온 · 오프라인에서 주민등록번호를 대체할 수 있도록 만들어진 것이다. 지속적으로 이어지는 개인정보 유출의 문제를 해소하기 위한 제도이다. 그러나 2015년 2월 28일에서 3월 2일 사이에 75만 건의 공공아이핀이 부정 발급되는 등 공공아이핀센터가 해킹 피해를 입는 사건이 발생했다. 주민등록번호를 대체하는 번호를 만들어 정보유출을 방지하겠다는 정부의 의지와는 달리 또 다른 문제를 양산하고 있는 것이다. 또 위에서 언급한 발급 절차의 불편성과 새로운 번호에 대한 낯설음 등이 더해져 가입자들의 실제 사용률은 높지 않을 것으로 보인다.[47] 2013년 2월 18일부터 24일까지 일주일간 '카페24'[48] 회원가입 방식은 휴대폰 인증 사용 비율이 89%로 나타났다. '카페24'는 아이핀도 회원가입 방식으로 구축하고 있었으나 상대적으로 편리한 휴대폰 인증의 비율이 더 높게 나타난 것이다(DATANET, 2013년 3월 05일 참고). 이는 온라인 상에서 주민번호 수집이 중단된 상황에서의 결과이기 때문에 주민등록번호 대체 수단으로서 실질적인 효과를 나타내고 있지 않은 것으로 파악할 수 있다.

3) 개인정보 노출의 다각화

앞서 언급한 것과 같이 아이핀과 마이핀이 등장하면서 우리 국민들의 개인식별번호는 3개로 늘어났다. 물론 아이핀과 마이핀이 의무 가입 사항도 아니고 강제로 부여하는 번호가 아니지만, 국민들의 입장에서는 온 · 오프라인에서의 번호가 각 한 개씩 더 늘어난 것이다. 그리고 이 번호가 주민등록번호의 정보 유출을 방지하기 위해 등장한 번호들이지만 이들 번호 역시 정보보호를 위한 확실한 안전성을 담보하지는 못한다는 것이 문제이다. 2015년 발생한 공공아이핀 부정 발급, 금융기관과 통신사 등에서 끊임없이 발생하는 주민등록번호 유출 사고 등은 늘어난 개인식별번호가 오히려 유출의 범위를 확대시키고 있음을 보여주는 사례이다. 마이핀의 경우 시행된 지 얼마 지나지 않아 그 사례를 파악하기 어렵지만, 이 번호들이 국민 개개인을 식별하는 번호임이 분명하기 때문에, 언제든지 침해의 대상이 될 수 있다.

특히, 아이핀이 주민등록번호 대체수단의 성격을 띤다고는 하지만 우리나라 어느 법에도 아이핀 관련 내용은 명시되어 있지 않다(현재는 「정보통신망법」 제23조 ②의 내용의 근거함).[49] 또 아이핀은 특정기관에 주민등록번호를 집중시키는 결과를 만든다. 현재 아이핀을 발급하는 기관은 민간 3개 기관과 정부 1개 기관이다. 주민등록번호를 대체하는 수단인 아이핀을 발급받기 위해서는 주민등록번호를 제공해야 하는데 발급기관 4개 중 3개가 민간기관이다. 민간기관의 신뢰가 무조건적으로 낮다고는 할 수 없지만, 국민들의 정보를 관리하는 정부기관보다 민간기관에 더 많은 개인정보가 저장되고 있다는 것은 개인정보 유출에 대한 위험성이 여전히 크게 노출되어 있는 것으로 이해된다. 개인정보 유출 사건의 대부분은 민간기관에서 발생하고 있다.[50]

민간과 공공기관의 역할은 확실히 다르다. 공공기관은 공익을 위하지만, 민간기관은 공익보다 사익추구가 우선인 것이 사실이다. 그리고 최근에 유출된

45) 2015년 9월 9일 방송통신위원회 보도자료 '이기주 상임위원, 아이핀 본인확인기관 간담회 개최'.
46) http://www.g-pin.go.kr/center/note/sub_01.gpin.
47) 전체 아이핀과 마이핀 가입자의 실제 사용률에 대한 정확한 수치는 현재 없음(발급 건수만 강조하고 있음).
48) www.cafe24.com.
49) 제23조의2(주민등록번호의 사용 제한) ② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집 · 이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.
50) 최근에 발생한 D-Dos 공격과 같은 사례들로 볼 때 공공기관도 정보 유출의 위험에서 자유로울 수는 없다.

개인정보가 관리적인 실수 보다는 개인정보 유통의 상황에서 발생하는 경우가 더 많다는데 그 위험성이 더 높아 보인다.

4) 효율적인 개인식별번호 정책 방안

우리나라 국민 개개인의 개인정보를 보호하기 위해 시행된 현재 개인식별번호 정책에 대해서는 재검토가 필요하다. 이미 우리 제도 깊숙이 자리하고 있는 주민등록번호는 제외하더라도 10여 년 전부터 등장한 온라인상에서 주민등록번호 대체수단인 아이핀에 대해서는 정책의 변화를 도모해야할 시점이다. 온라인상에서 주민등록번호를 대체한다고는 하지만, 여전히 우리나라는 주민등록번호를 최우선의 개인식별번호로 인식하고 있기 때문에 새로운 대체수단으로서 등장한 아이핀은 충실한 역할을 수행하고 있지 못하고 있다. 시행초기이기는 하지만 오프라인 상에서의 마이핀 역시 아이핀을 교훈 삼아 제도의 필요성을 다시 한 번 검토해야 할 것이다. 향후 많은 연구가 필요하겠지만 현재 제도의 재검토를 통해 전체 개인식별번호에 대한 변화를 도모하고 이를 통해 개인정보보호 수준을 향상시키는 방안을 모색해야 한다.

우리나라의 주민등록번호 제도가 급격한 사회의 온라인화 이후 여러 문제점을 야기하고 있지만 정부 운영의 측면에서 볼 때는 세계에서 유래를 찾기 어려울 정도로 관리적 측면에서는 매우 효율적인 제도이다.

주민등록번호를 통한 개인정보보호 문제 발생 이유는 정보보호에 대한 인식 없이 온라인상에서 주민등록번호를 오프라인에서 사용하는 똑같이 방식을 적용했다는 것이다. 즉, 인터넷 공간의 특성을 충분히 파악하지 못했다는 것이 문제의 출발점이었다. 이런 문제를 외면한 채 온라인상에서 주민등록번호를 대체하는 수단인 또 다른 개인식별번호만 생성하여 활용한다는 것은 우리나라 국민들의 식별번호 개수를 늘리고 개개인들의 관리번호 수만 늘어나게 할 뿐 근본적인 해결책이 아닌 것 같다. 오히려 주민등록번호 활용 분야를 명확히 규정하는 등 철저한 관리 정책을 구상하는 것이 더 나을 것으로 보인다.

먼저 공공부분의 사용처를 명확히 규정하는 방안이 있다. 공공 분야에서 주민등록번호 활용 방법(업무 성격에 따라 확인, 적용, 제출, 관리 등으로 구분)을 구체적으로 수립하는 것이다. 이를 통해 공공과 민간 영역의 주민등록번호 사용 방법을 확실히 구분할 수 있으며 주민등록번호 유출이 사전에 차단될 수 있는 사전 예방책을 마련할 수 있다.

물론 이와 같은 방법이 구체화되기 위해서는 주민등록번호만의 문제로 해결할 수 있는 것이 아니다. 이미 주민등록번호는 우리나라 공공 업무 깊이 자리잡고 있기 때문에 그 활용 영역이 아주 광범위하다. 그렇기 때문에 행정자치부를 포함하여 범부처의 공공업무의 개혁이 수반되어야만 한다. 우리 정부의 전자정부 서비스(2002년 11월 1일) 이후 민원인들의 불편을 해소하고 업무의 복잡성을 간소화시키기 위해 진행되어오고 있는 민원서류 구비 부담을 줄인 행정정보 공동이용 정책은 전자정부 수출실적으로 이어져 2015년 대비 12% 증가한 5억3,404만달러를 기록하는 등 가시적인 성과를 보이고 있다.[51] 주민등록번호와 민원서류 업무의 성격은 다르지만 업무의 효율화 측면에서는 효과적인 주민등록번호 정책에 도움이 될 수 있을 것이다.

개인정보보호를 위한 개인식별번호 정책은 사용성, 효율성 등 사용자 측면에서의 논의가 우선시 되어야 한다. 수요자이자 사용자인 국민의 입장이 고려되지 않은 채 공급자의 입장에서 생산해내는 개인정보보호 정책은 불편성, 실효성 등의 논란에서 자유로울 수 없다. 매년 이어지는 개인정보 유출 사례가 새로운 개인식별번호 정책을 추구하고 있는 현재 우리나라의 개인정보보호 제도에 대해 이미 많은 변화를 요구하고 있는 것이다. 주민등록번호를 대체하는 개인식별

51) 대한민국 전자정부는 UN평가 지수 2010년, 2012년, 2014년까지 3회 연속 세계 1위를 달성했다(2016년은 영국, 호주에 이어 3위)-http://www.unpan.org.

번호 정책은 2016년 현재까지 10년 이상 이어져왔다. 여전히 수요자의 외면을 받고, 지속적으로 많은 문제점을 야기하는 정책이라면 현행 아이핀, 마이핀 폐지 또는 주민등록번호 제도 내에서 효과적인 정책 수립 등의 정책적 변화를 도모해야 한다.

Ⅶ. 결론

인터넷 환경과 미디의 빠른 변화는 가상공간속에 소통이라는 새로운 커뮤니케이션 방식을 만들고 있다. 누리꾼들은 가상공간에서 이전보다 더 많은 서비스를 제공받고, 이런 서비스를 통해 서로가 어려움 없이 소통할 수 있게 되었다. 하지만 이런 변화를 통해 얻어진 소통의 자유 확대는 이전보다 더 많은 개인 정보의 노출과 더 쉬운 개인 정보의 유출로 이어지고 있다. 더 큰 문제는 지금의 상황에서 개인 정보 유출을 통제하는 것이 과거보다 더 어렵게 되었다는 것이다. 우리 정부는 지속적으로 발생하는 개인정보 유출 사건을 해결하고 예방하기 위해서 개인정보 보호와 관련된 여러 정책들을 개발하고 제도화시켜 시행하고 있다. 2011년에 제정된 「개인정보 보호법」, 2014년「개인정보보호 정상화 대책」, 2015년「K-ICT 시큐리티 발전 전략」 역시 같은 맥락으로 볼 수 있다. 하지만 '소통'이라는 단어가 화두가 된 지금 개인정보 보호에 대한 명확한 규정과 피해구제라는 사후 대책보다는 사전 예방의 필요성이 더 강조되고 있다.

본문에서 여러 차례 언급한 것과 같이 시행이후 중복문제가 끊이지 않았던 PIPL은 2016년부터 PIMS로 흡수되어 한국인터넷진흥원이 운영한다. 그러나 여전히 중복성의 논란은 남아있다. 기업의 정보보호 체계를 인증해주는 ISMS(정보보호 관리 체계 인증)의 경우 「정보통신망법」 제47조와 동법 시행령 제49조에 인증을 받아야하는 의무대상자가 명확하게 규정되어 있지만, PIMS는 그 범위가 구체적으로 명시되어 있지 않다. 그렇기 때문에 2014년 시행하고, 2016년(한국인터넷진흥원 전담기관 지정) 새롭게 시작하는 정보보호 준비도 평가와의 중복성 문제는 여전히 남아있다. 정보보호 준비도 평가에서 기업의 개인정보보호에 대한 부분은 선택사항이지만, 그 내용은 PIMS와 대동소이하다고 할 수 있다.

중복성 논란을 없애거나 최소화시키기 위해서는 공존하고 있는 두 제도의 효율적인 운영방안을 찾아야 한다. 예컨대, 기업규모에 따라 어떤 제도를 이용해야 하는지 규정해두는 방안이다. PIMS도 ISMS와 같이 「정보통신망법」에 의무대상자를 규정해두고, 정보보호 준비도 평가와의 차별성을 확보하는 것이다. PIMS는「정보통신망법」 제47조의3에 인증에 대한 내용이 명시되어 있기 때문에 향후 법 개정을 고려할 필요가 있다. 정보보호 준비도 평가는「정보보호산업법」 제12조에 명시되어 있으나, 제도에 대한 내용보다는 평가기관 등록에 관한 내용으로 구성되어 있기 때문에 이 또한 해당 법 개정을 고려해야 한다.

정부는 과거 실패사례에서 나타는 원인을 분석하고 현재 추진되고 있거나, 향후 추진될 제도 실패의 재발 방지를 위한 제도 정비의 필요성을 인식해야 한다. 현재시행되고 있는 정보보호 인증 및 평가 제도는 2004년 7월 시행된 '정보보호 안전진단(이하 '안전진단')' 제도와 그 맥을 같이 한다. 안전진단은 2004년 1월「정보통신망법」 개정을 통해 진행(2012년 폐지)되었다. 안전진단은 민간기업(보안업체, 회계법인, 감리법인, SI업체 등)[52]들을 지정하여 시행한 제도이다. 안전진단은 의무대상자 등 그 내용이「정보통신망법」에 명확하게 규정되어 있었음에도 실패하였다. 안전진단을 받은 기업의 개인정보 침해사고가 지속적으로 발생하면서 안전진단은 실효성 문제가 끊임없이 이어지다가 결국 ISMS와 PIMS로 대체되면서 폐지되었다. 여러 가지 원인이 있겠지만, 기술적인 이유보다는 민간 기업의 정보보호 진단을 민간 기

52) 영「정보통신기반보호법」 제17조(정보보호컨설팅전문업체의 지정)(2009. 5. 22. 삭제)의 규정에 의한 '정보보호컨설팅전문업체'(2004. 1. 29. 신설, 2012. 2. 17. 삭제).

업이 했다는 것이 주요 원인 중의 하나이다. 민간 기업의 1차 목표는 이윤창출이다. 안전진단을 시행하는 기업으로 지정된 기업은 그 무엇보다 이윤창출이 큰 목표였을 것이다. 정부는 안전진단을 위한 민간기업의 지정을 통해 정보보호 시장을 확대시키고, 민간의 정보보호 수준을 향상을 기대했겠지만, 철저한 안전진단이 아닌 이윤창출을 위한 형식적인 안전진단은 제도 출범 10년이 채 되지 않아서 폐지되었다. 민간기관의 평가 및 인증 참여가 주는 실패사례는 농림축수산부의 친환경농산물 인증제도(2001. 7. 1. 시행)에서도 확인할 수 있다. 농림축수산부는 인증기관으로 민간 기업을 지정하였으나, 인증기준을 준용한 심사보다 수익 목적의 인증업무 수행 등 부실인증 사례가 이어져 2014년 10월 공공성 등을 갖춘 기관 또는 단체가 인증업무를 수행할 수 있도록 인증기관 지정기준을 강화하였다. 민간의 이윤창출 목적이 친환경농산물 자체에 대한 국민들의 우려와 불신을 가중시킬 것을 우려한 조치이다.

이런 사례에도 불구하고 2014년 11월 시행한 정보보호 준비도 평가 제도는 2015년 「정보보호산업법」 제정 및 시행과 함께 과거 친환경농산물 인증제도와 유사한 체계로 변해버렸다. 정보보호 준비도 평가는 출범 당시 인증기관 1개, 평가기관 3개를 지정하여 운영하였고, 참여기관은 모두 비영리법인이었다. 그러나 2015년 6월 제정된 「정보보호산업법」에서는 인증기관이 사라지고, 평가기관의 역할만 강조되었다. 정부는 민간주도를 강조하면서 민간기업도 정보보호 준비도 평가기관으로 등록할 수 있도록 확대하고, 평가기관이 자체심의 기구[53]를 구성하여 평가결과에 대한 자체 검증 및 등급인증을 허용하고 있다. 평가결과에 대한 공정성과 신뢰성을 확보하기 위한 인증기관의 권한이 평가기관으로 모두 이관된 것이다. 이에 따라 평가기관은 자체 평가결과를 자체 심의하여 등급을 인증할 수 있게 되었다. 범국가적인 정보보호 인식 향상이라는 측면에서 제도의 민간 확대는 긍정적이라 할 수 있지만, 민간이 민간의 정보보호 수준을 평가하여 등급을 부여한다는 것은 과거 친환경농산물 인증의 실패를 우려하게 한다. 정보보호 준비도 평가와 유사한 정보보호 인증제도인 ISMS와 PIMS는 인증기관을 「정보통신망법」에 규정하고 있음을 볼 때, 법 규정과 함께 재정비된 정보보호 준비도 평가 체계가 얼마나 성공적으로 정착을 할 수 있을지 많은 의문을 가지게 한다.[54]

개인정보 보호 제도는 기술의 발달과 함께 다양하게 전개될 것이라 예상한다. 이 연구에서는 주민등록번호, 아이핀 등의 번호와 인증제도에 대한 언급을 주로 다루었지만, 지문인식, 홍채인식 등의 새로운 기술 적용 그리고 제4차 산업혁명에 따라 변화할 패러다임 등에 대응할 수 있는 개인정보 보호 제도의 방향성과 효율성 확보를 위해 향후 지속적인 연구가 필요할 것으로 본다.

■ 참고문헌

길준규 (2012). “통합개인정보 보호법과 효과적인 개인정보의 보호.” 「토지공법연구」, 57: 213-234.

김민천 (2008). “가상 공간에서 수집되는 개인 정보의 비교분석.” 「사회과학연구」, 24(3): 1-28.

김민천 (2009). 「안전한 전자정부 구현을 위한 i-PIN 정책집행 과정 분석」, 경성대학교 대학원 박사학위 논문.

김민천 (2010). “i-PIN의 활성화를 위한 정책집행 과정 분석.” 「정보화정책」, 17(1): 43-62.

김일환 (2011a). “개인정보 보호법제 정비에 대한 비판적 고찰-새로운 개인정보 보호법안을 중심으로-.” 「토지공법연구」, 52: 269-294.

김일환 (2011b). “개인정보의 보호와 이용법제의 분석을 위한 헌법적 고찰.” 「헌법학 연구」, 17(2): 353-389.

53) 「정보보호산업법」 시행령 제6조(정보보호 준비도 평가기관 등록 요건 · 절차) 별표1'에는 타기관도 심의위원회 운영기관으로 지정할 수 있도록 하고 있다.

54) 정보보호 준비도 평가 관련 조항이 포함된 「정보보호산업법」은 의원입법(새누리당 권은희 의원)으로 발의 되었으며, 제정 당시 기존에 제도를 운영하고 있던 인증기관과 평가기관의 의견 수렴 과정 및 공청회가 없었다.

김재광 (2012). “개인정보 보호법에 관한 새로운 법적 문제.” 「강원법학」, 36: 95-120.
마크로밀엠브레인(2015). “주민등록대체 및 공공아이핀 관련 인식 조사,” 「리서치보고서」 3월호.
민윤영 (2011). “인터넷 상에서 잊혀질 권리와「개인정보보호법」에 대한 비교법적 고찰,” 「고려법학」, 63: 287-316.
방동희 (2014). “개인정보 보호 제도에 있어 인증제의 정립과 개선에 관한 소고.” 「공법학연구」, 15(1): 263-300.
배대현 (2012). “잰걸음으로 나선 개인정보 보호법을 보완하는 논의: 개인정보 보호법 개정 논의 및 관련법률 검토.” 「IT와 법 연구」, 6: 1-33.
염흥열 (2005). “인터넷 상에서 주민등록번호 대체수단.” 「언론과 법」, 4(2): 83-110.
염흥열 (2005). “국제 개인정보보호 표준화 동향 분석.” 「정보보호학회지」, 26(4): 6-10.
유종락 (2011). “디지털시대의 개인정보 보호 -새로운 개인정보 보호법을 중심으로-.” 「디지털정책연구」, 9(6): 81-90.
이창범 (2012). “비교법적 관점에서 본 개인정보 보호법의 문제점과 개정방향: 한국 · EU · 일본을 중심으로.” 「Internet and Information Security」, 3(2): 65-95.
전국경제인연합회 (2015). 「우리나라 기업생태계, -대기업 · 중소기업 비중 분석-」, 통권 제214호.
정혜영 (2011) “개인정보 보호법의 내용과 체계에 관한 분석.” 「공법학연구」, 12(4): 407-435.
최광희 · 정연수 · 이재일 (2012). “개인정보 보호 신규 제도와 정책 변화.” 「정보보호학회지」, 22(6): 34-38.
한혜경 · 김유정 (2011), “인터넷 실명제와 우회로의 선택: 인터넷 공론장 참여자들의 자기검열과 우회로 선택 의향을 중심으로.” 「한국언론정보학보」, 55: 50-73.
황지은 (2016), “개인정보 제도개선 관련 최근 입법동향.” 「경제규제와 법」, 9(1): 269-274.
개인정보보호위원회 (2016). 「2016 개인정보보호 연차보고서」. 서울: 개인정보보호위원회.
한국정보보호산업협회, 한국인터넷진흥원. (2015). 「2015 국내 정보보호산업 실태조사」. 서울: 한국정보보호산업협회, 한국인터넷진흥원.
한국인터넷진흥원 (2011). 「2010 개인정보분쟁조정사례집」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2013). 「2012 개인정보분쟁조정사례집」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2014). 「2013 개인정보분쟁조정사례집」. 서울: 한국인터넷진흥원.
한국인터넷진흥원(2011). 「2011년도 개인정보보호관리체계(PIMS) 구축 및 운영 교육 실무자 과정 교재」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2015). 「개인정보보호 관리체계(PIMS) 인증신청 가이드라인」. 서울: 한국인터넷진흥원.
한국정보방송통신대연합 (2015). “정보보호 준비도 평가.” http://www.kfict.or.kr. (검색일: 2016.07.05.)
한국정보화진흥원 (2015). 「개인정보 보호 인증(PIPL) 안내서」. 서울: 한국정호봐진흥원.
한국정보화진흥원 (2015). 「개인정보 영향평가 수행 안내서」. 서울: 한국정호봐진흥원.
관계부처 합동 (2014). “개인정보보호 정상화 대책.” http://www.msip.go.kr. (검색일: 2014.08.20.)
미래창조과학부 (2015). “정보보호가 기본이 되고 창조경제 먹거리 산업화를 위한 K-ICT 시큐리티 발전 전략 -세부 추진계획-.” http://www.msip.go.kr. (검색일: 2015.08.05.)
경향신문 (2008). “1125만여 명 개인 정보 새나갔다.” 9월 5일.
노컷 뉴스 (2008). “훔친 명의 수백 개로 인터넷가입, 억대 수당 챙겨.” 9월 30일.
뉴스토마토 (2013). “현대캐피탈 ‘개인정보 유출’ 해커 징역 1년6월 선고.” 2월 21일.
머니투데이 (2008). “공공사이트서 주민등록번호 입력 안해도 된다.” 3월 20일.
방송통신위원회 보도자료 (2015), ‘이기주 상임위원, 아이핀 본인확인기관 간담회 개최.’ 9월 9일.
보안뉴스 (2008). “한심한 아이핀 · G-PIN…개인 정보 노출 심각!!.” 10월 4일.
보안뉴스 (2014). “6.25사이버테러 1주년, 개인정보 유출은 여전히 ‘핵폭탄’.” 6월 25일.
보안뉴스 (2014). “[연말마감] 2014년 하반기 개인정보 유출사건 총결산.” 12월 31일.
보안뉴스 (2015). “개인정보보호 관련 인증 취득, 저조한 이유 3가지.” 6월 24일.
아주경제 (2015). “신종 대포통장 이용 스미싱 인출책 검거”, 6월 12일.
재외동포신문 (2005). “신분도용범죄 조심.” 12월 16일.
전자신문 (2005). “주민등록번호 대체 수단 의무화 추진에 인터넷업계 강력 반발.” 8월 5일.
전자신문 (2005). “2007년 주민등록번호 없이 인터넷 회원가입.” 11월 1일.

전자신문 (2009). “2015년부터 주민등록번호 온라인서 사용 못한다.” 3월 5일.
DATANET (2013). “휴대폰 본인인증, 아이핀 사용률 월등히 앞서.” 3월 5일.
YTN (2008). “포털 대체주민등록번호 ’아이핀‘ 이용률 저조.” 6월 22일.