https://doi.org/10.33778/kcsa.2023.23.1.035

개인정보보호법 적용 대상에 대한 개선 방안 연구
(안전성 확보조치 기준 의무 대상 중심으로)

장 상 수*

요 약

우리나라는 2011년에 개인정보보호법이 제정되어 국민의 개인정보를 안전하게 보호하고 권익을 보호하는 많은 역할을 해오고 있다. 개인정보처리자는 안전한 개인정보 관리를 위하여 안전성 확보 조치 기준을 의무적으로 준수해야 한다. 이렇게 행정 규제가 수반되는 문제임에도 누구에게 언제 어떻게 적용되는지가 명확하지 않다. 법 적용의 원칙은 법의 적용 범위나 대상이 명확해야 하고 대상자의 법적 안정성과 예측 가능성에 있어야 한다는 것이다. 의무 부과에 따라 대상자에 대한 범위, 기준, 안전조치 항목, 절차 등이 명확하고 구체적으로 명시되어야 하지만 현행법 제도는 미흡하다. 따라서 본 연구에서는 선행연구와 개인정보보호 실태조사 자료를 기반으로 적용 대상자 분류 기준, 대상 판단 근거 기준, 안전성 확보 조치 기준 등에 대한 문제점과 합리적인 개선 방안을 제시하였다. 이를 통해 적용 범위와 기준을 명확화, 구체화하여 합리적인 방안을 제시하여 제도의 실효성을 높이는데 기여하고자 한다.

A Study on Improvement Plans for Application of the Personal Information Protection Act(Based on the Subject to Duty of Safeguards)

Jang Sang Soo*

ABSTRACT

Since the Personal Information Protection Act was enacted in 2011, it has played a role in safely protecting people's personal information and protecting their rights. Personal information controller must comply with the duty of safeguards for safe personal information management. Even though administrative regulation is an accompanying issue, it is not clear to whom, when and how it applies. According to the imposition of duties, the scope, standards, safety measures, procedures, etc. for the target person should be clearly and specifically specified, but the current legal system is insufficient .In this study, problems and reasonable improvement plans were presented for the classification criteria for applicable subjects, the criteria for the criteria for determining the targets, and the criteria for measures to ensure safety. Through this, we intend to contribute to enhancing the effectiveness of the system by presenting reasonable measures by clarifying and specifying the scope and standards of application.

Key words : Personal Information, Personal information Controller, Duty of Safeguards, Measures, Legal System

접수일(2023년 02월 01일), 수정일(2023년 03월 17일), 게재확정일(2023년 03월 24일)

* 한국인터넷진흥원 연구위원

1. 서 론

우리나라는 2011년에 개인정보의 유출 등 침해로부터 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로「개인정보보호법」이 일반법으로 제정되었다. 이 법은 이전에 공공기관에 적용하던 것을 공공기관과 민간 기업을 확대하여 적용 범위를 개인정보처리자 모두에게 적용하게 되었다. 그러나 대상을 개인정보처리자로 한정하고 보유량에 따라 공공기관과 민간기업으로 대상을 구분하다 보니 의무 적용 대상 여부 판단에 여전히 혼란을 가중하고 있다.

안전성 확보 조치 기준 의무 대상자 입장에서 개인정보 처리에 관하여 다양한 법적 의무를 부여하고 이를 위반할 경우 강력한 행정 규제를 하고 있기 때문에 법 적용 범위가 중차대한 문제가 아닐 수 없다. 그러나 현행 「개인정보보호법」은 누구에게 언제 어떻게 적용되는지가 명확하고 타당해야 하나 법 시행 10년이 지난 지금까지도 논란의 소지가 발생하고 있다. 행정 규제가 수반되는 법적용의 원칙은 법 적용 범위나 대상이 명확해야 하고 대상자의 법적 안정성과 예측가능성에 있어야 한다는 것이다. 이렇다 보니 현행 「개인정보보호법」상 범위 및 대상 기준의 모호함으로 인한 혼란과 불편을 겪을 수밖에 없다. 「개인정보보호법」 의무 적용 대상을 개인정보처리자 유형과 개인정보 보유량에 따라 분류하고 있어 분류 기준에 대한 객관성이나 개인정보처리자에 대한 해석 문제, 개인정보 보유량의 신뢰성, 객관성 부족 문제가 제기 되고 있어 법 제도 운용의 실효성에 의문시 되어 왔다[1].

그간 개인정보보호 분야 대한 많은 연구가 진행되어 왔으나 「개인정보보호법」 적용 범위나 대상에 대한 연구는 미흡한 것이 사실이다[2]. 본고에서는 「개인정보보호법」상 개인정보의 안전성 확보 조치 기준 중심으로 의무 적용 대상과 적용 기준에 대한 문제점을 파악하고 합리적인 개선 방안을 제시하고자 한다. 개인정보보호 분야의 특성상 접근 가능한 자료가 제한적이고 공개된 양적 데이터는 거의 존재하지 않기 때문에 관련 선행 연구와 개인정보보호위원회의 개인정보보호 실태조사[2] 자료를 기반으로 분석하여 문제점을 도출하고 전문가에 대한 델파이 기법으로 대상 기준 항목을 선정하고 합리적인 개선 방안을 제시하였다.

본 연구를 통해 그동안 지속적으로 문제가 제기되왔던 개인정보의 안전성 확보 조치 기준 준수 의무 대상자에 대한 모호한 기준을 새롭게 정립함으로써, 향후 합리적인 「개인정보보호법」 정책 수립과 제도 운용의 실효성 확보, 법 적용 대상에 대한 보다 명확성과 객관성을 확보할 수 있을 것으로 기대한다.

2. 관련 선행 연구

본 연구 주제뿐만 아니라 현실적으로 제도 운용 측면에서 「개인정보보호법」의 적용 대상과 의무 대상 주체인 개인정보처리자의 범위를 구체화, 명확히 확정하는 것이 현재 무엇보다 시급하고 중요한 과제이다[3][4]. 이와 관련하여 김민호[5]는「개인정보보호법」을 개정하여 개인정보처리자를 업무를 목적으로 스스로 또는 다른 사람을 통하여 개인정보를 처리하여 개인정보 파일을 운용하는 공공기관, 법인, 단체 및 개인 등으로 한정·구체화할 것을 제안하였다. 김민호 외[6]는 「개인정보보호법」의 일관된 법 집행이 가능해야 하며 공공부문과 민간부문을 구분해서 적용해야 할 필요성이 있다고 주장하였다. 물론 동법에서는 공공과 민간에 동일하게 적용되는 것으로 해석할 수 있으나, 공적인 정보(행정 정보)의 경우 대부분 엄격한 법률상의 규제를 통해 보호를 받는 반면에, 민간의 경우 원칙적으로 자유롭게 정보를 처리할 자유를 갖는다는 점에서 차이가 있다. 따라서 이러한 특성을 고려하여 해당 영역을 구분해서 규정해야 할 필요성이 있 하였다. 김진환[7]은 개인정보 개념의 합리적 해석의 또 다른 시도로서 개인정보는 기존 제2조 제1호상 정의에서 좀 더 나아가 살아 있는 개인을 알아볼 수 있는 정보로서 개인정보 파일의 형태로 운용되는 정보라고 이해하

는 것이 적절하다고 주장한다. 주민철[8], 김진환[9]은 개인정보의 기술적 보호 조치의 경우 장비를 설치· 운영 뿐 만 아니라 접근제한과 개인정보 유출시도 탐지, 보안정책을 반영하여 지속적으로 감시, 분석, 대응을 해야 한다고 하였다. 김일환[10]은 「개인정보보호법」을 추상적이고 일반적인 목적을 위한 포괄적·전체적인 적용 배제하는 식의 입법 방식은 문제가 있다고 전제하고 개인정보처리자나 개인정보의 종류 등에 따라 개별적으로 법 적용의 정도를 결정하는 방식으로 규정할 필요가 있다고 하였다.

이와 같이 선행 연구에서의 견해처럼 개인정보 규제의 대상과 기준에 대한 구체적이고 명확하고 투명하고, 객관적이며 형평성을 고려한 「개인정보보호법」 준수가 매우 중요한 기본 원칙이라 하겠다.

3. 「개인정보보호법」 적용 대상 문제점

3.1 의무 적용 대상 모호

「개인정보보호법」 제정 이전에 적용하던 공공기관에서 법 제정을 통한 민간영역을 확대하면서 민간 부문에 대한 적용 대상의 해석적 차원에서 민간 기업을 포괄적 대상자에 포함하면서 형평성과 혼란과 혼선을 야기하고 개인정보의 중요성을 감안하더라도 의무 대상자 입장에서는 지나친 규제로 비치고 있는 것이 사실이다.

공공기관의 경우 민간과 달리 업무 특성상 광범위하게 국민의 개인 정보에 접근할 수 있는 만큼 민간에 비해 높은 수준의 법령 준수 의무와 책임감이 요구되지만 민간의 경우는 안전성 확보 조치 기준 준수 의무를 사업 특성이나 규모, 개인정보처리 여부 등 사업자별 특성을 고려하지 않고 모는 사업자에게 부과하는 것이 혼선과 과도한 규제로 비칠 수 있기 때문이다. <표 1>와 같이 공공기관은 개성정보 중요성 고려하여 개인정보처리 및 운용할 경우 모두 포함돼야 타당하나 민간의 경우 유형 1에서 개인정보 1만명 미만인 소상공인, 단체, 개인도 모두 의무 적용 대상에 포함이 된다는 것이다[4].

<표 1> 개인정보처리자 유형 및 개인정보 보유량에 따른 적용 대상

유형	적용 기준 (보유량)	적용 대상
유형1	1만명 미만	소상공인, 단체, 개인
유형2	100만명 미만	중소기업
	10만명 미만	대기업, 중견기업, 공공기관
	1만명 이상	소상공인, 단체, 개인
유형3	10만명 이상	대기업, 중견기업, 공공기관
	100만명 이상	중소기업, 단체

「개인정보보호법」 취지상 엄격하게 법이 집행이 돼야 함에도 불구하고 <표 2>에서 알 수 있듯이 민간기업 71.9%가 안정성 확보 조치를 전혀 안 하고 있고 최소한의 필수 보호 조치조차 안 하는 것은 법 적용 대상 범위가 문제가 있거나 구체적이고 명확하지 않다 보니 해석적이고 자의적 판단에 이행 여부를 맡기는 것은 아닌지 더 나아가 이는 제도 운용의 실효성 문제로 볼 수 있다[11].

3.2 안전성 확보 조치 기준 획일적

개인정보의 안전한 관리를 위한 안전성 확보 조치인 기술적·관리적 보호 조치 기준은 대상자에 대한 명확한 기준과 대상 특성별 최소한의 의무 준수 항목을 적용할 필요가 있다. <표 2>과 같이 현행 적용 방식은 기본적으로 특정한 보호 조치의 이행·불이행 여부를 가지고 획일적으로 의무를 부과함으로써 적확하지 않은 규제를 적용할 여지가 있다[11]. 또한 기술이 발전하고 서비스 환경이 바뀌면 이에 걸맞은 새로운 개인정보보호 요구사항을 반영하기 위해서는 일정한 절차가 소요되어 끊임없이 발전하는 IT 기술에 당연히 뒤처질 수밖에 없다[11].

「개인정보보호법」 제29조와 정보통신서비스제공자등에 적용하는 제48조의2 개인정보의 안전성 확보 조치에 관한 특례 규정에 따라 이행, 불이행 등으로 획일적으로 적용하고 항목별로 100% 준수하고 있다는 것을 증명하기도 어렵다는 문제가 있다.

<표 2> 안전성 확보 조치 기준 비교

보호 조치 기준 항목	「개인정보보호법」	「정보통신망법」
개인정보처리시스템 접근권한 차등 부여	O	O
접근권한 부여・변경・말소 내역 보관	O	O
전보・퇴직자 접근권한 말소	O	O
책임 추적성 확보(사용자계정 공유 금지)	O	-
접속 비밀번호 작성규칙 운용	O	O
방화벽, IDS, IPS 등 설치・운영	O	O
외부접속시 안전한 인증수단 적용	O	O
망분리	-	O
고유식별정보 처리 시 주기적 취약점 점검	O	-
개인정보 외부공개 방지	O	O
로그온 타임아웃	O	O
업무용 모바일 기기 분실 대비	O	-
개인정보의 암호화 저장 및 전송	O	O
접속기록 위・변조 방지 및 일정기간 이상 보관	O	O
악성프로그램 방지(자동업데이트, 백신 등 사용)	O	O
관리자용 단말기 안전조치	O	-
내부관리계획 수립・시행	O	O
물리적 보안	O	O
재해・재난 대비(위기대응 매뉴얼, 백업 및 복구)	O	-
개인정보의 파기	O	-
출력・복사시 보호 조치, 개인정보 마스킹 조치	-	O

3.3 보유량에 따른 적용 기준 획일적

개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증 책임은 당해 개인정보처리자가 부담하라고 하고 있다[12]. 그러나 개인정보 보유량만을 가지고 적용 여부를 판단하는 기준으로는 한계가 있다는 것이다. <표 3>과 같이 종업원 300명 이상의 민간기업의 경우 1천명 미만 개인정보 보유가 37.3%로 나타났다[2]. 이는 민간기업 대부분이 개인정보를 보유하지 않거나 아주 적은 수의 보유를 하고 있다는 것이며 대부분이 법 준수 의무 대상이 아닐 수 있다는 것이다. 보유량만을 기준으로 대상 여부를 판단하기에는 많은 기업들이 제외될 가능성이 존재한다.

<표 3> 보유량에 따른 분류(단위:%)

구분	1천명 미만	1천명 ~100만명	백만명 이상
공공기관	28.4	55.2	16.4
민간기업 (300인 이상)	37.3	47.8	14.9

민간 영역은 개인정보 수집 형태나 목적이 다양하기 때문에 개인정보 보유량만으로 대상을 차별화하는 것이 불합리할 수 있다. 적용 기준을 현재의 개인정보 보유량도 중요한 요소이지만 보유량에 대한 신뢰성, 객관성을 담보하기 어려운 문제가 발생하고 있어 이에 대한 개선이 필요하다.

3.4 의무 대상자 적용 기준의 불합리

「개인정보보호법」 상 의무 준수 규정인 안전성 확보 조치 기준(기술적・관리적 보호 조치 기준)[4]은 기본적으로 법적 제재를 부과하는 기준이면서 주의의무 위반의 기준도 일부 될 수 있다. 규제 대상에 포함이 안 된다 하더라도 민사상 주의 의무 준수의 기준이 될 수 있다는 의미이다. 다시 말하면 기술적・관리적 보호 조치 기준을 정한 행정규칙은 법령상 책임 여부를 판단하기 위한 근거 규정이다. 이러한 법령 기준에 의하면 법규 준수 대상자는 모두 법령에서 요구하는 모든 안전조치를 취해야 한다[13]. 대상의 적용 여부와 그에 따른 보호조치 기준의 명확화와 영세사업자에 대한 완화된 보호조치 기준이 필요하다. 법 제도의 형식적 운영이나 선언적 규제 보다는 제도의 실효성을 높일 수 있는 방안을 마련해야 한다.

2021 개인정보호 실태조사 결과[2]를 분석해보면 <표 4>와 같이 민간기업의 경우 300이상 종사자 기

준으로 개인정보처리자를 위한 개인정보보호 정책 우선순위를 조사한 결과 개인정보 보유 규모 등을 고려한 처벌 규정의 차등화와 합리화가 34.2%, 기술지원(28.1%), 인재양성(25.8%)로 조사된바 민간 기업들은 여전히 이무 준수 규정 적용 기준을 차등화하거나 합리적 기준을 제시해 줄 것을 요구하고 있다[2].

<표 4> 개인정보 정책 우선순위 조사 결과

순위	공공기관	민간기업
인재양성	60.4%	25.8%
처벌규정의 차등화·합리화	27.0%	34.2%
기술개발	53.8%	24.9%
교육홍보	46.7%	21.4%
기술지원	13.9%	28.1%

4. 개선 방안

4.1 의무 대상자(공공, 민간)에 대한 개선 방안

법 적용에 있어 규제 대상이 되는 행위의 구성요건을 정한 법률 조항은 명확해야 하고 일률적으로 집행될 수 있어야 한다. 그렇지 않으면 규제 대상이 되는 주체나 허용되는 행위 사이의 구분이 애매해지고 주체별 자의 해석에 따라 처벌 여부가 좌우될 수 있어 법치주의를 해치게 된다[13]. 현행 「개인정보보호법」 상 안전성 확보 조치 기준 의무 적용 대상을 공공부문과 민간부문으로 구분하고 있으나 민간 부문에 대한 보다 구체적이고 세분화된 법 취지에 맞는 대상자가 의무 대상자로 포함될 수 있도록 하여 법 실효성을 높여야 할 필요가 있다.

따라서 첫째, 안전조치 의무 대상을 유형별로 보유량에 따라 적용 대상을 구분하는 방식을 개선하여 <표 5>과 같이 공공영역과 민간영역으로 구분하고 보유 개인정보의 형태나 규모 등을 고려하여 사각지대가 발생하지 않도록 유형을 세부화할 필요가 있다. 공공기관에서 보유 및 처리하는 개인정보나 고유식별정보는 민간기업의 수집 이용하는 정보와는 형태나 특성이 다르고 매우 중요하게 다루어져야 하기 때문에 공공기관은 보유량에 관계없이 처리 및 운용을 하게 되면 모두 적용대상으로 보는 것이 타당하다.

<표 5> 적용 대상 및 적용 기준 개선(안)

적용 대상	적용 기준
공공기관	개인정보 보유량에 관계없이 개인정보를 처리 및 운용하는 자(기관)
민간기업	일정규모 이상의 개인정보 보유량, 총매출액, 종원원수을 충족하는 자

두 번째, 문제가 되고 있는 개인정보 보유량에 대한 자의적 판단을 줄이고 규제의 객관성과 공정성 확보를 위하여 공공과 민간 분야에 대한 개인정보 파일 보유량을 매년 등록하도록 할 필요가 있다. 세 번째, 적용 대상을 보유량뿐만 아니라 다양한 개인정보처리시스템 규모, 매출액, 종업원 수 등 측정 가능한 요소들을 반영하여 적용 대상을 세분화할 필요가 있다. 현행 개인 보유량 측정 시기나 방법이 자의적인 경우가 대부분으로 객관성 확보를 위해서는 확정된 적용 요소들에 대한 정확한 측정 시기와 방법을 제시해야 한다.

네 번째, 규제 대상이 명확하게 구체화되고 정해지면 대상자별 세부 안전성 확보 조치 기준을 마련하여 실효성을 높여야 한다.

4.2 의무 대상자 적용 기준 개선 방안

「개인정보보호법」 준수 의무 대상자에 대한 명확한 기준을 정립하기 위해서는 개인정보의 형태나 목적, 정보보호의 특성, 대상자의 사업 형태, 보호 목적 등 다양하고 복잡한 현실을 고려하여 객관성, 공정성, 신뢰성을 확보하는 것이 무엇보다 중요하다. 대상을 보다 명확하게 정의하기 위해서는 개인정보보호의 특성, 준수 대상자의 형태, 규모 등 현실적인 문제를 고려하여 대상 여부 판단 기준을 정하기 위하여 SMART(Specific, Measurable, Attainable, Realistic, Timeline) 기법을 활용하였다.

SMART 기법은 1981년 경영 컨설턴트인 조지 도란(George T. Doran)이 개발한 목표 설정 기법으

로 SMART에서는 S(Specific, 항목 설정에 대한 목표가 구체적), M(Measurable, 항목 설정 목표가 측정이 가능), A(Attainable, 항목 설정값이 활용이 용이), R(Realistic, 항목이 현실적으로 적용이 가능), T(Timeline, 기간 내에서 정확히 판단 가능) 등의 5가지 관점에서 목표를 점검하고 목표의 수준을 조정할 수 있는 방법론이다.

「개인정보보호법」 의무 준수 대상자를 판단하기 위하여 선정된 항목(POOL)을 <표 6>과 같이 SMART 기법을 이용한 가중치를 부여하여 4.0 이상의 항목을 중심으로 세부적인 분석하였다. 공공, 민간, 학교, 업체 등 이해당사자 등 전문가 10명으로 구성하여 델파이 기법으로 1, 2, 3차에 걸쳐 기준 항목을 도출하고 평가하였다. 항목으로는 고객 관점, 재무 관점, 정보자산 관점으로 각각 2개의 항목을 분석하였다. 항목 중에서 가중치를 고려하여 3점 이상인 항목을 중심으로 상세하게 분석하였고 개인정보에 영향을 미치는 정도로 가중치를 1점에서 3점으로 구분하여 측정하였다. 항목 데이터에 대한 구별 여부와 산출물 생성 가능성을 등급으로 표시하고 1점에서 5점 척도로 산출하였다.

- 5(아주 명확하게 구별, 산출물 충분함)
- 4(약간 명확하게 구별, 산출물 약간 충분함)
- 3(보통 명확하게 구별, 산출물 약간 어려움
- 2(명확하게 구별되지 않고 산출물 약간 곤란)
- 1(명확하게 구별되지 않고 산출물 아주 곤란)

기준 항목에 대한 분석 측정 결과 4.0이상의 대상자 선정 항목 중에 가장 높게 반영된 항목은 6개 항목으로 총매출액(5.0), 종업원 수(4.8), 개인정보보유량(4.6)이고, 정보통신매출액(4.2), 일평균이용자수(4.2), 개인정보보호 관련 설비수(4.2)순으로 분석되었다.

<표 6> 기준항목별 대상자 판단 기준 분석

기준 항목	대상선정판단기준(등급)							
	S	M	A	R	T	계	평균	선택
총매출액	5	5	5	5	5	25	5.0	O
개인정보 매출액	4	4	3	3	4	18	3.6	X
정보통신서비스 매출액	5	4	4	4	4	21	4.2	O
정보화투자액	3	3	5	4	4	19	3.8	X
개인정보보호투자액	3	3	5	4	4	19	3.8	X
개인정보 보유량	5	4	5	4	5	23	4.6	O
일평균이용자수	5	4	4	4	4	21	4.2	O
전체 종업원 수	5	5	4	5	5	24	4.8	O
개인정보보호 관련 설비수	5	4	4	4	4	21	4.2	O
정보보호 직원 수	4	4	4	3	4	19	3.8	X
개인정보보호 직원 수	4	4	4	3	3	18	3.6	X

법 적용 의무 대상자 기준 항목 중에서 대상 항목 중 3개가 기준 값 이상이면 의무 대상 대상자로 선정하는 방법이 있다. 공공기관은 기준 값을 상향 조정할 필요가 있으며 민간 기업의 경우 기준 값 이상 기업을 대상자로 선정하는 방안(3개 이상)은 현재 적용하고 있는 개인정보 보유량 기준에 총매출액과 종업원 수를 선정 기준으로 설정하는 것을 보완할 필요가 있다. 그중에서 총매출액, 종업원 수를 측정하여 기준 값의 범위 안에 포함하여 반영하는 것이 바람직하다. <표 7>와 같이 1차적으로 적용 대상별 기준은 먼저 공공기관과 민간 기업으로 구분하고 공공기관은 보유량에 관계없이 개인정보를 처리 및 운용하는 자, 민간 기업은 일정 규모 이상의 개인정보 보유량, 총매출액, 종업원수로 구분하여 3개의 조건 모두 충족 시 대상자로 확정할 필요가 있다.

<표 7> 적용 대상 별 적용 기준 개선(안)

공공기관	민간기업
개인정보 보유량에 관계없이 개인정보를 처리 및 운용하는 자	일정규모 이상의 개인정보 보유량, 총매출액, 종원원수을 충족한자

<표 6>에서 도출된 대상 기준안을 <표 8>과 같이 다시 고객 관점, 재무 관점, 정보자산 관점으로 분류하였다. 고객 측면에서 고객중심의 데이터를 입력하기 위하여 신속성, 객관성, 타당성을 고려한다면

업체의 이용자 수와 회원 수를 파악할 수 있는 방법을 중장기적으로 검토하고, 개인정보 보유량을 10만명 이상으로 반영하여 관리하는 방법을 제안한다. 민간의 경우 보유하고 있는 개인정보가 대부분 이용자나 회원 수가 많기 때문에 고객수를 반영한다면, 기업체들이 고객 보유수를 정확하게 산정하여 제시한다고 해도 투명하게 확인할 수 있는 방법은 없지만, 회사마다 이미지 확보를 위하여 잠재 고객, 휴면 고객 등을 포함하여 실제적으로 활동하는 고객을 정의하는 것이 필요하다.

재무 관점에서는 총매출액과 정보통신서비스 매출액이 고려 대상일 수 있다. 민간기업의 경우 온라인 사업 중심의 개인정보 수집 형태가 대부분임 점을 감안하면 정보통신서비스 매출액 기준이 적정해 보이나 기업 측면에서는 별도 매출액을 구별하기가 어렵다는 단점이 있다. 개인정보를 보유하면서 매출액이 높다라면 개인정보에 미치는 영향이 높을 것으로 판단된다. 따라서 현행법에서 대상 선정 기준으로 많이 적용하고 있는 매출액 100억원 이상으로 설정이 필요하다.

또한 정보자산 관점에서는 개인정보보호 관련 설비나 시스템 수가 적정해 보이나 이는 대상 사업자의 자의적 판단에 근거하기 때문에 객관성을 담보하기 어려워 보인다. 정보시스템 설비 수는 무결성, 정확성, 안정성 등 한계를 극복하기 위한 많은 노력이 필요하다. 또한 개인정보 보유 기업은 개인정보보호 업무만을 수행하는 것보다는 정보통신업과 일반 업무를 수행하는 전체적인 인원을 선정하는 것이 바람직하다. 따라서 현행법에서 대상 선정 기준으로 많이 적용하고 있는 종업원 300명 이상으로 설정이 필요하다.

이와 같이 대상자를 선정하는 기준을 새롭게 선정하면 기존의 항목보다 신뢰성, 파악 용이성, 객관성 등이 높아질 것이다.

<표 8> 민간기업 기준 항목별 개선 방안(안)

관점	항목	현재	개선 방안	비고
고객	개인정보	1만 미만	10만명	개선
관점	보유량	~100만명 이상	이상	
	개인정보처리시스템 일평균이용자수	없음	10만명 이상	검토
재무 관점	총매출액	없음	100억 이상	추가
	정보통신서비스 관련 매출액	없음	50억 이상	검토
정보 자산 관점	전체 종업원 수	없음	300명 이상	추가
	개인정보보호 관련 설비수	없음	10대 이상	검토

4.3 중소·영세사업자에 대한 규제 합리화 방안

중소기업 및 소상공인은 인력 및 예산 부족 등으로 개인정보 보호 조치에 어려움을 겪고 있는 것이 사실이므로 일정 기준 이상의 사업자만 의무 대상에 포함하고 나머지 업체에게는 법 적용을 유예하고 기술지원, 교육 및 홍보, 인식제고 등 개인정보의 안전성을 확보하기 위한 정부 차원의 지원이 필요하다. 또한 안전성 확보 조치 기준도 중소기업에 준하는 적합한 보호조치 기준 마련이 필요하다.

2021 개인정보보호 실태조사[2] 결과에 민간기업의 경우는 85.4%에 달하는 것으로 조사됐다[2]. 이는 공공기관의 경우와는 다르게 민간기업의 개인정보 보유량만을 보면 1천명 미만이 85.4%, 1만명 미만이 무려 98%로 법 적용 대상을 명확하게 하고 확대 해석보다는 현실적으로 규모가 큰 기업 위주로 강화하여 실효성을 높일 필요가 있다.

따라서 첫째 안전조치 의무 대상자에 대한 명확한 보호조치 기준을 개선하여 개인정보 유출에 영향이 미비한 영세사업자를 대상에서 제외할 필요가 있다. 둘째, 제외된 업체에 대해서는 사각지대가 발생하지 않도록 지속적인 지원과 교육 및 홍보가 필요하다. 세 번째, 개인정보기술지원센터를 확대 개편하여 영세소상공인을 대상으로 잠재 법규 위반 사업자가 되지 않도록 맞춤형 개인정보보호에 대한 경제적, 기술적 지원을 토록 해야 한다. 현행 컨설팅 중심의 방식에서 개인정보보호 솔루션 개발·보급, 시스템 도입 지원, 맞춤형 기술 지원 등 다양한 형태의 지원이 시급하다.

5. 결 론

5.1 정책적 제언

본 논문에서는 현행 개인정보보호법과 제도의 투명성, 객관성, 공정성, 실효성을 높일 수 있도록 다음과 같은 몇 가지 정책적인 제언하고자 한다.

첫째, 개인정보 보유량에 따라 적용 대상을 구분하는 방식을 개선하여 대상을 크게 공공영역과 민간영역으로 구분하고 보유 개인정보의 형태나 규모 등을 고려하여 유형을 세분화할 필요가 있다. 두 번째, 개인정보 보유량에 대한 자의적 판단을 줄이고 규제의 객관성과 공정성 확보를 위하여 공공과 민간 분야에 대한 개인정보 파일 보유량을 매년 등록하도록 제도화할 필요가 있다. 세 번째, 적용 대상 적용 기준을 측정 가능한 요소들을 반영하고 적용 대상을 세분화하여 대상자별 세부 안전성 확보 조치 기준을 개선하여 실효성을 높여야 한다. 마지막으로 개인정보 유출에 영향이 미비한 영세사업자를 대상에서 제외할 필요가 있다. 제외된 업체에 대해서는 사각지대가 발생하지 않도록 지속적인 지원과 교육 및 홍보가 필요하다. 제외된 영세소상공인을 대상으로 맞춤형 개인정보보호에 대한 경제적, 기술적 지원을 강화하는 '개인정보보호지원센터'를 확대 개편해야 한다.

5.2 시사점 및 기대 효과

본 연구는 개인정보보호 관련 기업 및 정책 기관 등 이해관계자에게 다음과 같은 실무적 시사점을 제공하고 있다. 「개인정보보호법」 시행 이후 정책 효과나 문제점을 분석하여 법과 제도의 발전 방안에 대해 이론적 근거를 마련하는데 의의가 있으며 「개인정보보호법」 적용의 효과를 극대화할 수 있는 정책적 시사점을 제시하고 있다. 또한 관련 정책 기관에서는 「개인정보보호법」 적용의 타당성과 합리적인 대상 기준 마련 등 법 제도 개선 필요성 인식과 개인정보보호 정책 개선 방안을 마련하는 데 기틀을 마련하였다. 제시된 개선안 중심으로 제도를 도입함으로써 제도 시행의 실효성과 객관성, 공정성 확보가 가능할 것으로 판단된다. 의무 대상자 입장에서는 개인정보보호 관련 정책의 필요성, 참여율 제고, 합리적인 이행 방안 등에 대해 시사점을 제시하였다는 점에서 실무적으로 가치가있다. 불합리한 대상 기준을 명확하게 함으로써 제도의 실행력 제고와 개인정보보호 수준 제고를 통해 국민의 개인정보를 한층 더 안전하게 보호하고 활용하는데 기여할 것으로 기대한다.

5.3 연구의 한계 및 향후 연구 방향

본 연구에 있어 한계점은 공공기관이나 민간기업의 개인정보 보유 현황에 대한 자료가 없어 정확한 대상자 수를 파악하기 어려웠으며, 「개인정보보호법」 적용의 투명성과 객관성, 공정성, 실효성 확보를 위한 선행 연구들이 많지 않았다. 또한 본 연구는 「개인정보보호법」 운용에 대한 정책적, 제도적 제언으로 제시한 개선 방안에 대한 실효성과 타당성을 검증하기에는 한계가 있다.

향후 연구 방향으로는 제시한 개선 방안에 대한 구체적인 수행 방법과 시행 효과에 대해 면밀한 분석이 필요하다. 공공기관과 민간 기업에 대한 정확한 개인정보 보유 현황 파악과 대상자 판단 기준 마련에 대한 연구가 활발히 진행되어야 할 것이다.
본 연구에서 제시된 제언이 개인정보보호와 관련된 유관기관에서 국내 주요 정책 수립에 유용한 기초자료로 활용을 할 수 있을 것으로 기대한다.

참고문헌

[1] 개인정보보호위원회, "2022년 개인정보보호 연차 보고서", 2022.
[2] 개인정보보호위원회(한국인터넷진흥), "2021 개인정보보호 실태조사 보고서", 2022.
[3] 법제처, "개인정보보호법, 시행령", 제16930호, 제32813호, 2022.
[4] 개인정보보호위원회, "개인정보의 안전성 확보 조치 기준", 제2021-2호, 2021.
[5] 김민호, "개인정보처리자에 관한 연구", 성균관법학, 제26권 제4호, 2014.

[6] 김민호 외 6인, “개인정보보호 규제 합리화 방안”, 개인정보보호법학회, 2013.
[7] 김진환, “개인정보 보호의 규범적 의의와 한계 연구” 한국법학원, 통권144호, pp43-87, 2014.
[8] 주민철, “개인정보 보호 조치 위반의 형사적 책임 연구”, 서울대학교., 2015.
[9] 김진환 외 2인, “개인정보 보호 조치 위반 사건 수사의 문제점과 대책 연구”, 경찰학연구, 제13권 제13호, 2014.
[10] 김일환, “개인정보보호법 적용대상의 합리화 방안”, 한국공법학회, 43(1), pp31-54, 2014.
[11] 김일환, “초연결사회에서 개인정보보호법제 정비방안”, 성균관법학, 29(3), pp35-74, 2017.
[12] 전승재, 권헌영, “해킹을 방지하지 못한 사업자의 법적 책임 판단기준의 문제점”, 정보법학 제21권 제2호, 2017.
[13] 김용일, 김유정, “우리나라 개인정보보호 법제의 개선방안에 관한 연구”, 법과정책 제27권 제1호, 2021.
[14] 법제처, “정보통신망이용촉진및정보보호등에 관한 법률, 제18871호, 2022.

〔저자소개〕

장 상 수 (Sang-soo Jang)
1989년 2월 한국항공대학교 학사
2003년 2월 동국대학교 석사
2011년 8월 전남대학교 박사
2000.5 ~ 현재 한국인터넷진흥원 연구위원
email : ssjang0116@gmail.com