

개인정보보호를 위한 현행 형벌체계의 문제점 검토*

이 성 대**

국 | 문 | 요 | 약

2011. 3. 29. 제정된 개인정보보호법의 제정과정에서는 규율대상, 보호범위, 피해구제제도, 개인정보보호위원회의 직제 및 권한 등에는 상당한 관심을 두었으나, 벌칙규정의 정비에 대해서는 상대적으로 관심이 부족했던 것으로 보인다. 이 논문은 기존형사법과의 관계에서 체계적 정합성을 확보하려는 목적의식을 기반으로 현행 개인정보보호법제상의 형사처벌규정의 문제점을 검토하였다.

먼저, 우리의 개인정보보호법제는 OECD가이드라인에 규정되어 있는 개인정보보호 8원칙에서 출발하고 있으며, 개인정보보호법을 비롯한 관련법률들은 유사한 형벌체계를 구성하고 있음을 지적함으로써 현행 개인정보보호법제를 개관하였다. 그리고 관련법률 사이의 관계에 대하여 살펴보았다.

다음으로 현행법체계상 개인정보의 개념과 관련한 문제를 검토하였다. 여기서는 개개의 형벌 규정의 적용에 있어 해석론을 통한 개인정보개념의 제한가능성도 일부 존재하기는 하지만, 개별적인 개인정보 침해유형과 관련한 구체적 해석의 문제는 여전히 남게 될 수밖에 없으므로 입법론적 관점에서 근본적인 문제해결이 필요하다고 보았다.

마지막으로 개인정보 보호법제상의 형벌체계의 부정합성을 지적하고 이를 기반으로 개인정보보호를 위한 현행 형벌체계의 정합성 확보를 위한 나름의 개선방안을 제시하고자 하였다. 그 결과 제시할 수 있는 현행 형벌체계의 문제점은 일률적인 중벌화경향, 과태료부과대상과 형벌부과대상의 교차현상, 관련법률상 처벌규정의 비통일성, 기존형사법 체계와의 부정합성 등을 들 수 있는데, 이러한 현행 법제상 형벌체계의 문제점은 개인정보개념의 불명확성보다도 형사처벌범위의 광범위성과 일률적인 중벌화의 경향에서 기인한다고 보았다. 이에 따라 형사처벌범위의 축소와 실질적 피해자보호대책의 마련이라는 방향성을 중심으로 현행 개인정보보호법제상의 형벌규정을 개선해야 한다는 결론을 제시하였다.

❖ 주제어 : 개인정보보호법, 개인정보보호를 위한 형벌체계, 개인정보 자기결정권, 개인정보침해, 정보주체

* 이 논문은 2013년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2013S1A5B5A07048827)

** 성균관대학교 법학연구소 선임연구원, 법학박사

I. 개인정보를 위한 현행 형벌체계의 검토 필요성

우리나라의 개인정보 보호체계는 개별영역별로 마련된 법률을 통한 규율방식을 취하고 있었으나 2011. 3. 29. 개인정보보호법이 제정됨에 따라 기존과는 달리 민간과 공공부분을 모두 포섭하는 통합적 방식을 취하게 되었다. 이에 따라 공공기관뿐만 아니라 법인·단체·개인을 포괄하는 사업자들도 개인정보를 보호해야할 의무를 부담하게 되었으며, 개인정보의 수집에서 파기에 이르는 전 과정에 걸친 공통된 기준이 마련되었다고 할 수 있다. 이와 같이 개인정보보호법의 제정은 개인정보보호의 범위와 내용을 충실히 하였다라는 점에서 그 자체만으로도 긍정적인 평가가 가능하다.

그러나 수범자의 입장에서 가장 민감한 부분인 형벌규정에 대한 충분한 검토가 이루어지지 않았다는 점은 문제가 아닐 수 없다. 즉, 통합개인정보보호법의 제정이 전부터 개인정보침해와 관련한 형사법적 관점에서의 다양한 검토가 이루어 졌음에도 불구하고 실제의 입법에서는 이러한 검토의 결과를 충분하게 반영하지 못한 것으로 보인다. 그 결과 개인정보보호법과 유관법률들 사이에는 체계상의 부정합성이 곳곳에서 발견되고 있을 뿐 아니라 개인정보보호법제상 형사처벌규정이 지니고 있는 문제점에 대한 지적은 어렵지 않게 찾아볼 수 있다. 여기에 통합개인정보보호법상의 벌칙규정에 대한 형사법적 관점에서의 면밀한 검토필요성이 존재한다.

이 논문은 기존형사법체계와의 정합성을 확보하고자하는 목적의식에 기반하여 현행 개인정보보호법제상의 형사처벌규정의 문제점을 검토하고자 한다. 이를 위하여는 먼저 개인정보보호법과 유관법률상의 형벌체계를 개관(II)할 필요가 있다. 그리고 구체적인 문제점으로서 대표적인 논란의 대상이 되고 있는 개인정보의 개념 및 범위와 관련한 문제(III)에 대하여 살펴보고, 현행 개인정보 보호법제상의 형벌체계의 부정합성(IV)을 지적하려 한다. 마지막으로 이상의 논의를 기반으로 개인정보 보호를 위한 현행 형벌체계의 정합성 확보방안에 대한 나름의 생각을 피력하고자 한다(V).

II. 개인정보보호관련 형벌체계의 개관

1. 개인정보 보호원칙과 개인정보보호를 위한 형벌체계

개인정보보호법 제3조는 ‘개인정보 보호 원칙’이라는 표제 하에 개인정보처리자가 타인의 개인정보를 취급함에 있어서 지켜야할 기본적 의무를 규정하고 있다. 이는 1980년 9월 OECD이사회가 채택·권고한 ‘개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: 이하 OECD가이드라인)’에¹⁾ 규정되어 있는 개인정보보호 원칙의 내용과 거의 동일하다.²⁾ 즉, OECD가이드라인 제2장(Part 2. Basic principles of national application)은 ① 수집제한의 원칙(Collection Limitation Principle), ② 정보내용정확성의 원칙(Data Quality Principle), ③ 목적 특정의 원칙(Purpose Specification Principle), ④ 이용제한의 원칙(Use Limitation Principle), ⑤ 안전확보의 원칙(Security Safeguards Principle), ⑥ 공개의 원칙(Openness Principle), ⑦ 개인참가의 원칙(Individual Participation Principle), ⑧ 책임의 원칙(Accountability Principle) 등 8개의 개인정보보호 원칙을 규정하고 있는데, 우리 개인정보보호법이 천명하고 있는 개인정보보호 원칙도 이를 반영한 것이다.³⁾ 이러한 개인정보 보호원칙은 개인정보처리자와 정보주체가 지니는 권리와 의무의 형태로 구체화되어 나타나는데, 이는 개인정보보호와 관련한 형벌체계의 핵심적 가치를 형성한다.

- 1) OECD가이드라인은 1970년대에 유럽과 북미지역을 중심으로 논의되기 시작한 개인정보 보호의 문제와 관련한 국제사회의 초기의 대응이라고 할 수 있는데, 이는 지금까지도 국제적인 영향을 미치고 있다. 최근(2013. 7.)에는 동가이드라인이 제정된 이후 처음으로 개정이 이루어지기도 하였다(개정된 OECD가이드라인의 구체적 내용에 대하여는 정효진/윤재석, “개정 OECD 프라이버시 가이드라인: 주요 내용 및 향후 전망”, 2014. 6. 4.자 주간기술동향, 정보통신산업진흥원, 4면 이하 참조).
- 2) OECD가이드라인이 규정하고 있는 개인정보보호 원칙의 자세한 내용은 황태정, “통합개인정보보호 법안의 입법체계 검토”, 형사정책연구 제20권 제1호, 2009, 620면 이하 참조.
- 3) 김주영/손형섭, 개인정보 보호법의 이해, 법문사, 2012, 167면. 다만 개인정보보호법 제3조는 OECD 가이드라인이 제시하고 있는 원칙에 덧붙여 최소침해의 원칙(동조 제6항)과 익명처리의 원칙(동조 제7항)을 추가하고 있으나 이는 OECD가이드라인 8원칙의 세부내용 혹은 실현수단으로서의 성격을 지니는 것으로 독자적 의미를 부여할 만큼 독창적인 규정이라 보기는 어렵다.

2. 개인정보 침해행위에 대한 형벌체계

개인정보의 보호를 위하여 형벌규정을 두고 있는 주요한 법률로는 ‘개인정보 보호법’, ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)’, ‘위치정보의 보호 및 이용 등에 관한 법률(이하 위치정보법)’, ‘신용정보의 이용 및 보호에 관한 법률(이하 신용정보법)’ 등을 거론할 수 있다. 그 외에도 형법을 비롯한 기타의 개별·특별법 중에도 개인정보보호와 관련된 규정들은 다수 존재한다. 이러한 현행 개인정보보호법제상의 형벌체계는 개인정보의 수집, 이용, 처리, 제공, 이전, 관리 등의 전 단계에 걸친 다양한 형벌규정으로 구성되어 있다고 할 수 있다.

현행 개인정보보호법제상의 일반법이라 할 수 있는 개인정보보호법⁴⁾ 정보주체의 동의없는 개인정보의 수집행위를 형사처벌의 대상으로 규정하고 있지는 않지만,⁵⁾ 위계 등에 의한 개인정보의 수집행위에 대하여는 형벌부과를 예정하고 있다(동법 제72조 제2호). 또한 개인정보의 이용, 처리, 제공, 이전 등의 단계에 대하여는 동법 제71조에 상세한 규정을 마련하고 있는데, 개인정보의 불법제공 등(제1호), 개인정보의 불법이용·제공 등(제2호), 민감정보의 불법처리(제3호), 고유식별번호의 불법처리(제4호), 업무상 지득한 개인정보의 누설·제공(제5호), 개인정보의 훼손·멸실·변경·위조·유출(제6호) 등이 그것이다. 그리고 개인정보의 관리단계와 관련해서는 개인정보의 분실·도난·유출·변조·훼손(제73조 제1호), 정정·삭제 등의 조치의 무 위반 등(동조 제2호), 개인정보 처리 중지의무의 위반 등(동조 제3호)과 같은 구체적인 침해유형에 대한 형벌규정이 마련되어 있다. 이외에도 개인정보보호법은 개인정보 변경 등 업무방해(제70조), 영상정보처리기기의 불법조작 등(제72조 제1호), 직무상 비밀누설 등(제72조 제3호)에 대한 형사처벌을 예정하고 있다.

한편 정보통신망법도 개인정보보호법과 유사한 형벌체계를 갖추고 있다고 할 수

4) 개인정보보호법은 제9장에서 형사처벌의 대상이 되는 위반행위들을 상세하게 규정하고 있다. 특히 동법은 각각의 위반행위들을 법정형을 기준으로 제70조(10년 이하의 징역 또는 1억원 이하의 벌금), 제71조(5년 이하의 징역 또는 5천만원 이하의 벌금), 제72조(3년 이하의 징역 또는 3천만원 이하의 벌금), 제73조(2년 이하의 징역 또는 1천만원 이하의 벌금)에 나누어 규정하고 있다. 또한 단순한 행정의무 위반 등 비교적 경미한 동법의 위반행위에 대하여는 과징금(동법 제34조의2)과 과태료(동법 제75조)의 부과를 규정하고 있다.

5) 다만 동법 제75조 제1항 제1호에 따라 5천만원 이하의 과태료를 부과하도록 규정하고 있을 뿐이다.

있다. 그런데 정보통신망법은 정보통신망 이용자의 동의를 받지 않은 개인정보의 수집행위에 대해서도 형사처벌을 예정하고 있다(동법 제71조 제1호, 제2호). 여기에서 정보통신망법과 개인정보보호법 사이의 뚜렷한 차이점 중 하나를 찾아볼 수 있다.⁶⁾ 이에 따라 법정대리인의 동의를 받지 않은 14세 미만인 아동의 개인정보를 수집하는 행위에 대해서도 개인정보보호법과 정보통신망법은 그 취급을 달리하고 있다(개인정보보호법 제75조 제1항 제2호 및 정보통신망법 제71조 제8호 참조). 그러나 정보통신망법이 형사처벌의 대상으로 삼고 있는 개인정보침해행위의 유형은 개인정보의 수집단계를 제외한 기타의 경우 앞서 언급한 개인정보보호법의 침해유형과 대동소이하다고 할 수 있다. 즉, 정보통신망이라는 적용대상의 특수성으로 인하여 일반법인 개인정보보호법과 구체적인 표현과 법정형에 있어 다소간의 차이를 나타내고는 있으나 양 법률이 규정하고 있는 개인정보침해행위의 유형은 거의 동일하다고 할 수 있다. 다만 정보통신망 및 정보통신서비스의 특성에 따라 정보통신망법이 요구하는 특수한 신고의무 등에 대한 처벌규정과 같은 부분에서 차이가 있을 뿐이다. 이는 위치정보법과 신용정보법 등에 마련되어 있는 형사처벌규정의 경우에도 마찬가지라 할 수 있다.⁷⁾

3. 개인정보보호와 관련된 법률들 사이의 관계문제

이상에서와 같이 개인정보의 보호를 위하여 우리 법률체계는 다수의 개별·특별법을 마련하고 있다. 그런데 각각의 법률은 개인정보침해행위에 대한 별도의 형사처벌규정을 두고 있으면서도 각 법률상의 구성요건들은 상호 유사한 내용을 담고 있다는 점에서 적용상의 혼선이 발생할 여지가 존재한다. 이에 대하여는 현행 개인정보보호법제상 일반법이라 할 수 있는 개인정보보호법이 제6조에서 ‘다른 법률과의 관계’라는 표제 하에 “개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다”고 명시함으로써 관련법률의

6) 정보주체의 동의없는 정보수집행위에 대한 개인정보보호법과 정보통신망법의 취급이 다른 이유에 대하여는 정보통신서비스, 정보통신서비스제공자, 정보통신이용자 등과 같은 특별법인 정보통신망법의 적용대상이 지니는 특수성을 감안한 것으로 이해할 수 있을 것이다.

7) 구체적인 처벌규정의 내용은 위치정보법 제39조 내지 41조와 신용정보법 제50조 참조.

적용에 있어서 발생할 수 있는 혼선을 미연에 방지하고 있는 듯이 보인다.⁸⁾

그러나 문제는 정보통신방법을 비롯한 개별·특별법에도 개인정보보호법 제6조와 유사한 규정이 존재한다는 점에 있다.⁹⁾ 즉, 현행 개인정보보호법제상의 법률들 사이에서 어떤 법률을 ‘다른 법률’로 볼 것인지의 여부에 따라 구체적인 적용법조가 달라질 수 있게 된다.¹⁰⁾ 물론, 현행 개인정보보호법제상 개인정보보호법이 일반법이며, 여타의 법률은 이에 대한 특별법이라는 간편한 이해가 가능하다. 이렇게만 보면 문제는 없어 보인다. 그러나 일반법과 특별법의 관계는 형식적인 법률의 명칭에 좌우될 것이 아니라 각 법률의 구체적 규정의 성격에 따라 개별적인 판단이 요구된다는 점에서 결코 간단하게 취급될 문제는 아니라고 할 수 있다. 뿐만 아니라 정보통신방법의 경우에는 개인정보보호법이 제정되기 전까지 폐지된 (구)공공기관의 개인정보보호에 관한 법률이 규율대상으로 삼았던 공공분야의 규율에 대비하여 민간분야에서 일반법으로서의 역할과 기능을 수행하고 있었으며, 지금도 정보통신분야에 있어서는 일반법적 지위도 함께 지니고 있다는 사실도 고려되어야 한다. 또한 각 법률을 개인정보보호법에 대한 특별법으로 단순하게 이해한다고 하여도 개인정보보호법의 일반적 규정에 대하여 특별법상 유사한 관련 규정이 존재하는 경우 무조건 개인정보보호법의 관련규정이 배제된다고 보아야 할 것인지(개인정보보호법 적용배제설) 혹은 개인정보보호법이 포괄적으로 적용되는 상태에서 특별법의 규정과 저촉되는 부분에 대하여만 개인정보보호법의 관련규정이 적용배제된다고 볼 것인지(개인정보보호법 포괄적용설)와 같은 이론상의 문제제기도 가능하다.¹¹⁾

이상과 같은 개인정보보호법제상 법률들 간의 체계문제는 법률의 적용범위에 대

8) 개인정보보호법과 다른 법률(정보통신방법 등) 사이의 적용범위와 관련한 문제는 이필재, “개인정보보호법과 관련 법률의 체계문제”, 한국위기관리논집 제10권 제1호, 2014, 93면 이하 참조.

9) 정보통신방법 제5조와 위치정보법 제4조가 대표적이다.

10) 이에 대한 문제제기와 구체적인 검토에 대하여는 박노형, “개인정보보호법과 정보통신방법의 관계분석”, 안암법학 제41권, 2013, 133면 이하 참조.

11) 물론 이 문제는 실제상 별다른 실익이 없는 부분이라 할 수 있을 것이나, 이 또한 개인정보보호관련 법률의 체계문제에 있어서 혼란을 유발케 한다는 점에서 검토가 필요하다. 이에 대한 자세한 검토는 박노형, “개인정보보호법과 정보통신방법의 관계분석”, 142면; 이창범, 개인정보보호법, 법문사, 2012, 70면 이하; 현대호, “개인정보 보호법과 다른 법률의 개인정보보호 규정과의 정합성 확보”, 「개인정보보호법」 제정에 따른 개인정보보호정책의 방향과 과제, 한국인터넷법학회 춘계공동학술대회 자료집, 2011.4.15., 40면 이하 등 참조.

한 일반적 부분에 있어서만 논의될 성질이 아니라 개개의 침해행위에 대하여 적용될 구체적 규정을 확정함에 있어서도 문제될 수 있다. 즉, 형벌규정의 해석에 있어서도 문제될 수 있는 부분인 것이다. 물론, 이와 같은 문제가 발생하더라도 형법 이론상의 죄수론 등을 토대로 어느 정도 해결이 가능할 것으로 예상된다. 그러나 일반법으로서의 개인정보보호법이 마련된 이상 동법을 중심으로 관련법체계가 통일되어야 할 필요가 있을 뿐만 아니라 적용순위와 범위의 문제가 형벌규정에 관련되는 경우에는 이를 명확히 하는 것이 바람직하다고 본다. 특히 우리 개인정보보호법제는 개별·특별법의 제정이 있는 후에 일반법인 개인정보보호법이 제정되는 통상적이지 않은 순서를 거쳤다는 점에서 태생적으로 법률들 사이의 관계가 문제되지 않을 수 없다는 점을 유념해야 할 것이다.¹²⁾ 따라서 향후 개인정보보호법제를 보완해 나감에 있어서도 지속적인 검토가 필요한 부분이라 생각한다.

Ⅲ. 개인정보 개념과 형벌규정의 해석

1. 개인정보보호관련 법률상 개인정보개념의 문제점

현행 개인정보보호법은 동법의 보호대상인 개인정보의 개념에 대하여 「“개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다」고 규정하고 있다(동법 제2조 제1호).¹³⁾ 즉, 현행 개인정보보호법제상 개인정보는 살아있는 개인

12) 개인정보보호법은 부칙 제2조에서 구법인 ‘공공기관의 개인정보 보호에 관한 법률’을 폐지한다는 점을 분명히 하면서, 부칙 제5조에서는 종전의 ‘공공기관의 개인정보보호에 관한 법률’을 위반한 행위와 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’을 위반한 행위에 대하여는 종전의 법률에 따른다는 점을 명시함으로써 예상되는 법률적용상의 문제점에 대한 최소한의 고려는 반영하고 있음을 알 수 있다. 그러나 중복규정으로 인한 혼란스러움, 벌칙들 간의 불균형성 등과 같은 문제는 여전히 남아있다고 할 수 있으며, 그 해결에는 개인정보보호법을 제정함에 투입된 것 보다 더 많은 시간과 노력이 필요할지 모른다는 우려적인 목소리도 존재한다(이에 대하여는 김정환, “개인정보 보호법에 대한 입법론적 검토”, 법학논총 제18집 제1호, 2011, 356면 이하 참조).

에 관한 것이라는 점을 전제로 하는 식별가능성과 정보성을 그 개념요소로 한다. 여기서 ‘정보’의 의미를 정의하는 방식에 따라 ‘개인정보’의 구체적인 범위와 내용에 있어서 차이가 존재할 수 있다.¹⁴⁾ 그러나 현행 법제는 정보의 의미에 대하여는 별다른 제한을 두지 않고 있으므로, 개인정보의 핵심적인 개념요소는 특정 개인에 대한 ‘식별가능성’이라 할 수 있다.¹⁵⁾

개인정보에 대한 이상과 같은 개념정의에 따르면 ‘식별가능성’의 유무에 따라 형사처벌의 범위가 결정된다는 결과에 이른다. 문제는 이에 따르면 개인정보의 범위를 명확하게 한정하는 것은 거의 불가능하게 되어 최소한의 예측가능성도 확보하기 어렵다는 점에 있다. 특히 ‘해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것’이라는 괄호안의 내용을 고려하면 실제 상 거의 모든 정보는 개인정보가 될 수 있는 가능성을 지니게 되며, 과학기술의 발달에 따라 현재는 개인정보로 취급되지 않는 것이라도 향후 개인정보의 범위에 포섭될 가능성은 상존하게 된다.¹⁶⁾ 뿐만 아니라 개인정보의 개념을 전제로 하는 ‘개인

-
- 13) 이와 관련하여 정보통신망법도 「“개인정보”란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 부호·문자·음성·영상 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다」(동법 제2조 제1항 제6호)고 하여 유사한 정의규정을 두고 있다. 다만 법률의 제정순서상 일반법인 개인정보보호법이 정보통신망법의 정의규정에 기반하고 있는 것으로 보인다. 위치정보법상의 ‘개인위치정보’의 개념정의도 또한 식별가능성에 중점을 두고 있다(동법 제2조 제2호).
- 14) 예를 들면, ‘정보’의 의미를 일반적 의미의 정보(Information)와 협의의 정보인 처리정보(Data)를 구별하는 방식이 대표적이다. 이러한 구별에 대하여는 김준규, “개인정보의 개념과 특징”, 토지공법연구 제18집, 2003, 243면 참조.
- 15) 다른 나라의 입법례도 개인정보의 개념은 식별가능성에 중점을 두고 있는 것이 일반적이다. 예를 들어, 앞서 언급했던 OECD가이드라인의 경우 ‘식별되거나 식별될 수 있는 개인에 관한 모든 정보(any information relating to an identified or identifiable individual)’를 개인정보라고 정의하고 있으며, 이에 기반하여 마련된 각국의 관련법률들도 이러한 식별가능성에 중점을 두고 있다고 할 수 있다. 개인정보의 개념정의와 관련한 각국의 입법례에 대하여는 전용준, “개인정보보호법률상 형사처벌규정의 적정성에 관한 연구, 정보법학 제17권 제2호, 2013, 219면 이하 참조.
- 16) 휴대폰 기기의 고유번호인 IMEI(International Mobile Equipment Identity)와 사용자의 개인식별정보 등이 들어있는 USIM(Universal Subscriber Identity Module)카드의 일련번호를 예로 들 수 있다. IME와 USIM번호는 전세계적으로 단 1개의 번호만 부여되는 것이지만, 그 각각의 일련번호만으로는 개인을 특정할 수는 없다. 하지만 다른 정보와의 조합(예를 들어, IMEI와 USIM번호의 결합 혹은 그 각각과 사용자의 전화번호의 결합)을 통해서도 얼마든지 개인을 특정할 수 있게 된다. 이와 같은 정보들은 과거에는 개인정보의 범위와의 관계에서 문제가 되지 않았던 것들이라

정보처리자(개인정보보호법 제1조 제5호)’ 등의 개념범위도 한정하기 어렵게 된다. 즉, 개인정보침해행위의 구성요건으로서 행위주체(개인정보처리자)와 행위객체(개인정보)의 범위가 지나치게 넓어지고 모호해진다는 것이다. 이는 “범죄의 구성요건이 추상적 또는 모호한 개념으로 이루어지거나, 그 적용범위가 너무 광범위하고 포괄적이어서 불명확하게 되어 통상의 판단능력을 가진 국민이 법률에 의하여 금지된 행위가 무엇인가를 알 수 없는 경우에 명확성의 원칙에 위배된다”는 판례의 입장에 비추어 보면,¹⁷⁾ 죄형법정주의의 세부원칙으로서 명확성의 원칙에 반하게 될 소지가 다분하다고 할 수 있다.¹⁸⁾

2. 개방적 개인정보개념의 필요성

개인정보보호법 제1조는 “이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다”고 규정함으로써 동법의 제정목적은 천명하고 있다. 이는 동법의 제정 과정에서 그 목적으로 논의되어 온 ‘정보주체의 권리보호’와 ‘개인정보의 적절한 이

할 수 있으나, 최근에는 이와 같은 정보도 개인정보의 범주에 포함될 수 있을지가 문제되고 있는 것이다. 이와 관련하여 우리 판례(서울중앙지법 2011. 2. 23, 선고 2010고단5343 판결)는 “정보통신망법 제2조 제1항 제6호는 ‘개인정보’란 해당 정보만으로 특정 개인을 알아볼 수 있는 정보와 다른 정보와 쉽게 결합하여 특정 개인을 알아 볼 수 있는 경우를 포함하는 것으로 정의하고, 이때 당해 정보와 결합가능한 다른 정보가 모두 동일인에게 보유하고 있는 것을 전제로 하지는 아니하고 있다. 한편 여기서 ‘쉽게 결합하여 알아 볼 수 있다’는 것은 쉽게 다른 정보를 구한다는 의미이기 보다는 구하기 쉬운지 어려운지와는 상관없이 해당정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다 할 것이다. 오늘날 정보화의 진전에 따라 종전에 쉽게 결합할 수 없었던 정보들이 쉽게 결합되어 개인을 식별할 수 있는 자료로 작용되기에 이르렀고, 따라서 기계적인 정보라 하더라도 특정 개인에게 부여되었음이 객관적으로 명백하고 이러한 정보를 통하여 개인이 식별될 가능성이 크다면 이를 개인정보로 봄이 상당하다”라고 판시하여 IMEI와 USIM번호는 개인정보에 해당한다는 결론을 제시하였다(이 판례에 대한 평석은 문재완 “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 2014, 61면 이하 참조).

17) 헌법재판소(전원재판부), 1997. 9. 25. 선고 96헌가16.

18) 형사처벌의 문제에서 만이 아니라 개인정보의 개념이 지나치게 광범위하다는 점으로 인하여 현실적으로 요구되는 건전한 정보이용마저도 불가능하게 될 수 있다는 점은 문제가 아닐 수 없다. 이에 따라 개인정보의 정의규정에서 괄호부분을 삭제하자는 다소 극단적인 주장(최경진, “빅데이터와 개인정보”, 성균관법학 제25권 제2호, 2013, 213면)도 제기되고 있다.

용 보장'이라는 두 가지 기본이념¹⁹⁾ 중에서도 정보주체의 권리보호에 무게중심을 두고 있는 것이라 할 수 있다. 이와 같이 정보주체의 권리보호에 충실하기 위해서는 동법의 적용대상을 가능한 범위 내에서 확대할 필요가 있으며, 이를 반영하고 있는 것이 동법의 개념규정이라 할 수 있다.

또한 동법이 예정하고 있는 개인정보의 보호를 위한 규제방법에는 형사처벌 이외에도 사법적 규제와 행정적 규제가 혼재하고 있다는 점도 고려해야 한다. 일반적으로 형사규제에 비해서 그 범위가 방대한 사법적 혹은 행정적 규제의 경우 현행법과 같이 개념범위를 설정하는 것도 충분히 가능하다고 할 수 있으며, 형벌규정의 적용에 있어서 문제되는 명확성만을 근거로 동법의 개념규정을 극단적으로 제한하는 것은 본말이 전도된 결과를 초래할 뿐이다.²⁰⁾ 따라서 개인정보보호법의 개념규정의 내용 중에서 괄호부분을 삭제하는 것과 같은 극단적인 방법보다는 결합의 용이성을 판단하는 주체와 대상을 명확히 하고 개인식별성이 높은 경우를 예시적으로 열거한 후 이에 준하는 정보침해에 대해서만 형벌규정을 적용하는 방안 등을 검토하는 것이 보다 현실적인 대안이라 생각한다.

3. 해석론적 제한 가능성의 검토

이상에서와 같이 개인정보개념의 개방성은 불가피한 측면을 지니고 있으므로, 해석론적 제한의 가능성을 검토해 볼 필요가 있다. 개인정보의 정의에 대한 해석론적 논의는 개인정보보호법 제2조 제1호의 괄호부분(“해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다”)의 의미를 어떻게 파악할 것이냐의 문제라 할 수 있는데, 이에 대하여는 두 가지의 언어적·논리적 해석가능성이 존재한다.²¹⁾

19) 개인정보보호법의 제정과정에서 논의되었던 법률안의 목적규정에 대한 검토는 황태정, “통합개인정보보호법안의 입법체계 검토”, 619면 이하 참조.

20) 산업기술의유출방지및보호예관한법률 제2조 등 위헌소원(헌법재판소, 2013. 7. 25. 2011헌바39 결정)에서 헌법재판소가 명시하고 있듯이 정의조항을 구성요건의 일부로 삼는 ‘처벌조항의 위헌성’의 문제와 처벌조항이 아닌 수의적 행정행위 등에 관한 다른 규정들과의 관계에서는 그 정의조항이 합헌적일 수 있다는 점은 유의할 필요가 있다.

21) 이러한 해석론적 가능성에 대한 문제제기는 정상조 외, “비식별개인정보의 보호 및 활용에 관한

먼저 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보라면, 실제로 다른 정보와 결합하여 특정 개인을 식별한 바 없더라도, 특정 개인을 식별할 수 있는 잠재적 가능성이 있는 이상 그 정보를 개인정보로 보아야 한다는 것이 그 하나이다.²²⁾ 그리고 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보가, 실제로 다른 정보와 결합하여 특정 개인을 식별할 수 있게 된 경우에 한하여, 그 정보를 개인정보로 보아야 하고, 다른 정보와 결합함이 없이 익명으로 처리되어 특정 개인을 식별할 수 없는 상태에서 이용된 비식별개인정보는 동법상의 개인정보로 볼 수 없다는 것이 다른 하나이다.²³⁾ 전자에 의할 때에는 정보주체의 권리를 두텁게 보호할 수 있다는 장점은 있겠으나 식별가능성이라는 불명확한 개념에 의하여 형사처벌의 여부가 결정될 수 있게 되어 결과적으로 형벌의 자의적 행사를 가능케 할 수 있다는 결정적인 결함이 존재하게 된다. 따라서 실제상 다른 정보와 결합하여 특정 개인을 식별할 수 있게 된 경우에만 개인정보로 인정하는 후자의 방법이 수범자에 대하여 보다 명확한 기준을 제시할 수 있는 해석방법이라 할 수 있다. 그러나 이는 개인정보보호관련 법률상 형벌규정의 적용에 있어서 명확성의 원칙을 관철하기 위한 방편으로 고려해야 할 것이며, 일반적인 개인정보의 개념을 논의함에 있어서는 전자와 같은 해석이 법률의 제정목적에 부합한다고 본다.²⁴⁾

다만 형벌규정의 적용에 있어서 이상과 같이 식별가능한 개인정보의 개념을 제한적으로 해석하더라도 개인정보보호법을 비롯한 개인정보보호 관련 법률들에 마련되어 있는 개별적인 행위유형과 관련한 구체적 해석의 문제는 여전히 남게 된다. 특히 개별행위유형과의 관계에서 각 구성요건상의 개인정보의 개념이 포섭하는 범위의 광협은 다시 달라질 수 있다는 점에서 개인정보 침해행위에 대한 형사법적 대응의 필요성과 범위에 대한 진지한 재검토가 필요하다고 본다.²⁵⁾ 최소한 형사처벌

연구”, 방송통신위원회 연구보고서, 2010, 39면. 다만 이 보고서에서는 정보통신망법상의 정의규정을 주로 문제삼고 있으나 현재의 개인정보보호법도 동일한 규정형식을 취하고 있으므로 동일한 관점에서 논의가 가능하다.

22) 전웅준, “개인정보보호법률상 형사처벌규정의 적정성에 관한 연구”, 224면.

23) 정상조 외, “비식별개인정보의 보호 및 활용에 관한 연구”, 39면.

24) 전웅준, “개인정보보호법률상 형사처벌규정의 적정성에 관한 연구”, 224면 이하는 전자의 해석방법이 타당함을 전제하면서도 형사처벌과 관련해서는 식별‘가능성’이 지니는 의미와 내용을 명확하고 제한적으로 해석할 필요가 있음을 지적하고 있다.

규정을 보다 명확하게 규정함으로써 적용범위의 불명확성을 제거하는 방법만큼은 고민되어야만 한다. 예를 들면, 개인정보의 개념을 개별구성요건에서 명확히 하거나 단순개인이정보가 아니라 민감정보나 고유식별정보와 같이 비교적 명확한 개념을 처벌대상으로 삼는 방안 등을 고려해 볼 수 있을 것이다.

IV. 개인정보보호를 위한 형벌규정의 체계적 정합성²⁶⁾

1. 공공기관의 개인정보보호에 관한 법률과의 비교

현행 개인정보보호법(여기서는 ‘신법’)은 동법의 제정에 따라 폐지된 (구)공공기관의 개인정보보호에 관한 법률(이하 ‘구법’)에서 출발하고 있다. 형사처벌규정에 한정해 보면, 구법은 제23조에서 공공기관의 정보처리업무를 방해할 목적으로 개인정보를 변경 또는 말소하는 행위(제1항), 개인정보취급자가 그 의무에 위반하여 개인정보를 누설 또는 권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적으로 사용하는 행위(제2항), 공익목적으로 설치된 폐쇄회로 텔레비전(CCTV)의 설

25) 개인정보의 개념분제와 마찬가지로 기술적 조치의 미이행을 처벌대상으로 하는 구성요건(개인정보 보호법의 경우 특히 제73조 제1호)의 경우에도 형법상의 명확성의 원칙과 관련한 문제가 존재한다. 즉, 기술적 조치의 미이행의 경우에는 그 전체적인 구성요건의 불명확성으로 인하여 실무상으로도 상당한 혼란을 유발하고 있으며, 실제상 사문화 되어가고 있다(이에 대하여는 김진환/조대회/이상진, “개인정보 보호조치 위반 사건 수사의 문제점과 대책”, 경찰학연구 제13권 제3호, 2013, 67면 이하 참조). 따라서 이 경우에도 그 구성요건의 명확성 확보를 위한 법률의 정비가 필요한 상황이라 할 수 있는데, 사건으로는 이를 형사처벌의 대상으로 하는 것 보다는 과징금 및 과태료의 부과대상으로 삼아 적극적인 행정지도를 부여하는 방안을 고려함이 바람직하다고 생각한다.

26) 개인정보보호법을 비롯한 현행 개인정보보호법제상 마련되어있는 형벌규정의 적정성을 검토함에 있어서는 다양한 측면에서 논의가 가능하다. 예를 들면, 비교법적 관점에서 현행 형벌규정의 적정성을 검토하거나 보다 근본적인 관점에서 개인정보에 대한 형법적 보호의 타당성 등을 검토하는 것도 가능하다. 그러나 이들 문제에 대하여는 다수의 선행연구에서 이미 논의가 이루어진 부분이라 할 수 있으므로 여기서는 기존의 선행연구들을 토대로 현행 개인정보보호체계상의 형벌규정들에서 발견되는 체계부정합성의 문제를 중심으로 논의를 진행하고자 한다. 이를 위해서는 통합개인정보 보호법이 제정됨에 따라 폐지된 (구)공공기관의 개인정보보호에 관한 법률상의 처벌규정과 비교, 형사처벌의 대상이 되는 침해행위유형과 과태료부과 대상행위 사이의 차이점 검토, 일반형법을 비롯한 기존형사법 체계상의 관련규정과 비교하는 등의 방법이 유효할 것이라 생각되며, 이하에서 순차적으로 살펴보고자 한다.

치목적을 넘어 부정한 목적으로 임의조작하는 행위·다른 곳을 비추는 행위·녹음기능을 사용하는 행위·거짓 등의 부정한 방법으로 공공기관으로부터 처리정보를 열람 또는 제공받는 행위(제3항)를 형사처벌의 대상으로 삼고 있는데 반하여, 앞서 살펴본 바와 같이 신법은 구법상의 구성요건에 대응하는 유사한 규정과 보다 구체화된 구성요건을 마련하고 있을 뿐만 아니라 나아가 별도의 새로운 구성요건도 마련하고 있다. 전반적으로 형사처벌대상을 확대한 것으로 볼 수 있는데, 특히 신법은 구법과는 달리 과징금 및 과태료의 부과 대상이 되는 행위들도 상세하게 규정함으로써 개인정보침해행위의 유형에 따라 복층적인 규제체계를 갖추고 있다는 점에서 양 법률은 본질적인 차이점을 보이고 있다.

그리고 구법상의 구성요건에 대응하는 신법상의 처벌규정의 법정형을 검토해 보면, 구법에 비하여 전체적으로 상향된 법정형을 규정하고 있다는 점 또한 하나의 특징이라 할 수 있다. 먼저, 구법 제23조 제2항의 경우 3년 이하의 징역 또는 1천만원 이하의 벌금을 규정하고 있음에 반하여, 신법 제71조는 침해행위의 내용을 보다 명확함과 동시에 5년 이하의 징역 또는 5천만원 이하의 벌금을 법정형으로 규정하고 있다.²⁷⁾ 또한 구법 제23조 제3항은 2년 이하의 징역 또는 700만원 이하의 벌금형을 규정하고 있음에 반하여, 신법은 제72조를 통하여 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 규정하고 있다.

이상을 종합해 보면, 신법은 그 적용범위를 민간부문까지 확대했을 뿐임에도 구법에 비하여 그 법정형을 전반적으로 중하게 설정하고 있음을 알 수 있다. 그런데 이와 같은 신법의 태도가 과연 타당한 것인지에 대해서는 상당한 비판의 여지가 존재한다. 법률의 적용범위가 민간부문을 포섭하는 형태로 확대되었다 하더라도 개인정보와 자기결정권이라는 행위객체와 보호법익에는 변화가 없기 때문이다. 또한 우리 형법이 업무방해행위에 대하여 공무집행방해죄(형법 제136조)와 업무방해죄(형법 제314조)로 나누어 구성요건을 마련하고 있으면서도 그 법정형에는 큰 차이를 두지 않고 있는 점과 비교해 보면, 법정형을 거의 일률적으로 상향해야 할 특별한 근거는 찾기 어렵다고 본다.

27) 다만 구법상의 행위유형 중 개인정보의 누설행위(개인정보보호법 제72조 제3호)에 대하여는 벌금형에 있어서만 법정형을 상향하고 있다.

2. 과징금 및 과태료 부과대상과 형벌부과대상의 준별

현행 개인정보보호법은 제75조에서 과태료의 부과대상이 되는 행위유형을 나열하고 있는데, 이는 동법상 형벌부과의 대상이 되는 의무위반에 이르지 아니한 전단계의 행위들을 유형화한 것이라 할 수 있다. 문제는 일응 형벌부과 대상행위의 전단계에 해당하는 경우로 분류할 수 있는 유형 중에는 그 이후의 단계인 형벌부과 대상행위와 명확하게 구분되지 않는 것도 있다는 점이다. 대표적으로 개인정보보호법 제36조 제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 경우를 예로 들 수 있는데, 단순한 조치미이행의 경우 동법 제75조 제2항 제11호에 따라 과태료를 부과하는 반면에 이를 넘어 개인정보를 계속 이용하거나 제3자에게 제공하게 되면 동법 제73조 제2호에 따라 형벌을 부과하도록 규정되어 있다. 단순한 조치미이행과 이를 넘어 개인정보를 계속 이용하거나 제3자에게 제공하는 행위를 엄격하게 구분할 수 있는지가 쟁점이라 할 수 있는데, 수집된 개인정보는 전산상 자동적으로 처리되는 경우가 많다는 점을 고려해 보면 양자를 명확하게 구분하기란 쉽지 않다. 이러한 문제점은 정보통신망법에서도 그대로 나타나고 있다.²⁸⁾ 이러한 문제상황은 결국 죄형법정주의의 세부원칙으로서의 명확성의 원칙 및 형벌적정성의 원칙과의 관계에서 관련법률상의 형벌체계를 재검토해야 할 필요성을 제기하게 한다.²⁹⁾ 물론 형벌부과대상과 과태료부과대상을 구분하는 것은 원칙적으로 입법재량의 범위에 놓

28) 또한 개인정보보호법 등에 규정되어 있는 ‘안전성 확보에 필요한 조치의 미이행’이라는 의무위반유형에 대해서도 동일한 문제제기가 가능하다. 이와 관련해서는 개인정보보호법의 경우 75조 제2항 제6호의 과태료부과대상과 동법 제73조 제1호의 형벌부과대상의 준별이 문제된다고 할 수 있으며, 정보통신망법의 경우에는 동법 제73조 제1호의 벌칙규정과 제76조 제3호의 과태료규정이 문제된다. 개인정보 보호법제상 안전성 확보조치의 미이행이라는 의무위반유형과 관련한 문제점의 검토에 대하여는 김진환/조대희/이상진, “개인정보 보호조치 위반 사건 수사의 문제점과 대책”, 61면 이하 참조.

29) 이외에도 개인정보보호법은 정보주체의 동의를 받지 않은 개인정보의 제3자 제공과 그 정보의 습득행위에 대하여만 제71조 제1호를 통하여 5년이하의 징역 또는 5천만원 이하의 벌금의 부과 대상으로 규정하고 있는데, 동법 제75조 제1항 제1호는 단순한 개인정보수집행위를 5천만원 이하의 과태료부과대상으로 규정하고 있다. 그런데 정보주체의 동의를 받지 아니한 정보수집행위라는 측면에서 본다면 제71조 제1호의 개인정보를 제공받은 자의 입장에서 동등한 의미를 갖는다고 할 수 있음에도 형벌 혹은 과태료의 부과여부가 달라진다는 것 또한 문제가 아닐 수 없다.

여 있는 것이라고 할 수 있겠으나 이상과 같은 문제를 유발한다는 것은 이미 입법재량의 범위를 일탈한 것으로 밖에 볼 수 없다.

3. 관련법률상 처벌규정의 비통일성

현행의 법률체계상 개인정보 침해행위에 대한 형벌규정을 두고 있는 법률들이 유사한 형벌체계에 근거하고 있음은 이미 앞서 언급한 내용이다. 그렇지만 각 법률들에 규정되어 있는 처벌규정들 간에는 다소간의 모순점이 발견되기도 한다. 동의없는 개인정보수집의 금지의무를 위반한 경우가 대표적이라 할 수 있다. 즉, 개인정보보호법은 정보주체의 동의를 받지 않고 개인정보를 수집하는 행위에 대하여 동법 제75조 제1항 제3호에서 5천만원 이하의 과태료부과를 예정하고 있는 반면에 정보통신망법은 제71조 제1호에서 5년이하의 징역 또는 5천만원 이하의 벌금을 부과하도록 규정하고 있다. 마찬가지로 14세 미만의 미성년자의 개인정보를 수집함에 있어서 법정대리인의 동의를 받을 것을 요구하고 있는 양 법률상의 의무에 위반한 경우에 대하여도 개인정보보호법은 과태료(제75조 제1항 제2호)를 정보통신망법은 형벌(제71조 제8호)을 부과하도록 규정하고 있다. 이는 동의확보를 전제로 하는 개인정보의 수집행위에 대하여 본질적으로 다른 형태의 취급을 규정하고 있는 것이라 할 수 있다. 물론 이는 정보통신망법의 적용대상이 지니는 특수성에 근거한 입법적 판단에 따른 것으로서 입법재량의 일탈을 문제삼을 수는 없다고 본다. 그러나 단순히 개인정보보호법의 적용을 받는 개인정보처리자인지 혹은 정보통신망법의 적용을 받는 정보통신서비스 제공자인지의 여부에 따라 그 취급을 달리함에는 쉽사리 수긍하기 어려운 부분이 존재할 뿐만 아니라 정보통신서비스 제공자도 기본적으로는 개인정보처리자라는 점에서 양자를 구분하는 것이 항상 명백한 것은 아니라는 점을 지적하지 않을 수 없다. 또한 인터넷을 비롯한 정보통신망의 사용이 일상화되어 있는 오늘날의 정보화사회에서 정보통신서비스 제공자라는 특정 부류의 개인정보처리에 대하여 별개의 법률을 존치시키는 것은 바람직하지 않다는 지적에도 귀를 기울일 필요가 있다고 본다.³⁰⁾

30) 이러한 관점에 대하여는 박노형, “개인정보보호법과 정보통신망법의 관계분석”, 134면 이하.

그리고 정보통신망법과 개인정보보호법 사이에는 그 제정시기의 차이로 인하여 미세한 법률구성상의 차이도 발견된다. 예를 들면, 개인정보보호법은 개인정보를 정보주체의 동의없이 제3자에게 제공하는 경우 이를 제공받은 자에 대한 형사처벌을 명시하고 있는데(동법 제71조 제1호), 이에 대응하는 정보통신망법 제71조 제3호는 ‘영리 또는 부정한 목적’을 별도로 요구하고 있다. 이와 관련하여 정보통신서비스 제공자가 개인정보를 정보주체의 동의없이 제3자에게 제공하는 경우 그 상대방에게 ‘영리 또는 부정한 목적’이 없다면, 정보통신서비스 제공자도 기본적으로 개인정보보호법상의 개인정보처리자이므로 개인정보보호법 제71조 제1호에 따라 처벌해야 할 것인지 아니면 정보통신망법을 적용할 수 없는 경우이므로 처벌할 수 없다고 보아야 할지는 명백하지 않다. 이와 같은 경우는 개인정보보호법 제6조의 다른 법률에 특별한 규정이 ‘있는’ 경우가 아니라 다른 법률에 특별한 규정이 ‘없는’ 경우라고도 볼 수 있기 때문이다.

개인정보보호법 관련 법률들 사이에서 발견되는 이상과 같은 형벌체계의 비통일성은 개인정보보호법을 제정하는 과정에서 기존의 형벌체계를 충분히 검토하지 않은 결과인 것으로 보인다. 물론 이러한 문제들은 향후 입법을 통하여 서서히 바로잡아 나가게 될 것이며, 실제로도 후속입법을 통하여 각 법률들 사이의 불일치가 제거되고 있다.³¹⁾ 그러나 형사처벌의 영역에서 발견되는 이상과 같은 문제는 형벌 자체의 타당성에 대한 의문을 발생하게 한다는 점에서 결코 사소한 문제라 할 수 없다. 따라서 현행 개인정보보호법제상 발견되고 있는 이러한 문제점들은 통일된 법리에 근거하여 체계적으로 정비되어야 마땅하다.

31) 예를 들어, 개인정보보호법은 고유식별정보의 처리를 원칙적으로 금지하면서 이를 위반하는 경우 형사처벌을 규정(동법 제71조 제4호)하는 반면에 정보통신망법은 고유식별정보의 일종이라 할 수 있는 주민등록번호의 수집·이용을 원칙적으로 금지하면서도 이를 위반한 경우 3천만원 이하의 과태료를 부과하도록 규정하고 있었다(동법 제76조 제2호 전단). 이 또한 동일한 성격의 개인정보 처리에 대하여 적용되는 법률에 따라 차별적 취급을 예정하는 것이라 할 수 있는데, 2013.8.6. 개인정보보호법이 개정되면서 신설된 동법 제24조의2에 정보통신망법과 유사한 의무규정을 도입하고 이에 위반하는 경우 과태료를 부과하도록 함으로써 개정법률의 시행일인 2014. 8. 7.부터는 이러한 차별적 취급의 가능성은 제거되었다(동법 제75조 제2항 제4호의2).

4. 기존형벌규정과외의 불균형성

개인정보침해행위를 대상으로 하는 법률들은 비교적 최근에 마련된 것이라 할 수 있으나, 이러한 법률들이 규정하고 있는 개개의 구성요건들 중에는 과거의 일반형법으로는 대응할 수 없었던 새로운 것들이 존재하기도 하는 반면에 기존의 일반형법상에도 존재했던 구성요건을 기반으로 재구성된 것들도 존재한다.³²⁾ 특히 후자의 경우에는 기존의 일반형법과의 관계에서 그 체계적 정합성의 확보여부를 검토해볼 필요가 있다.

먼저, 개인정보보호법 제70조의 공공기관이 처리하는 개인정보에 대한 침해행위에 대한 검토가 가능하다.³³⁾ 동조는 공무원에 대한 침해행위(형법 제136조)가 아니라 공공기관에서 처리하는 개인정보를 대상으로 할 뿐이므로 공무집행방해죄의 행위와는 구별된다. 오히려 그 행위유형은 일반업무방해죄(형법 제314조)의 행위유형에 가까운 것으로 판단된다.³⁴⁾ 즉, 개인정보보호법 제70조의 구성요건은 공공기관이 처리하는 개인정보침해를 통하여 공공의 업무를 방해하는 행위의 경우 일반형법의 규정에는 포섭이 어렵다는 점을 반영하고 있는 것으로 이해할 수 있다. 그리고 동조는 “10년 이하의 징역 또는 1억원 이하의 벌금”을 법정형으로 규정하고 있는데, 일반형법이 “5년 이하의 징역 또는 1천만원 이하의 벌금(제137조)” 혹은 “5년 이하의 징역 또는 1천500만원 이하의 벌금(제314조)”을 규정하고 있는 것과 비교해 보면 과도한 법정형이 설정이 아닐 수 없다. 물론 이는 업무방해행위와 손괴행위의 결합 유형으로서 광범위한 입법재량의 범위에 충분히 포섭가능하다. 그러나 공공기관이 처리하는 개인정보가 아닌 일반의 개인정보를 침해하는 형태로 동일한 행위를 하는 경우에는 결국 일반형법상의 업무방해의 행위유형으로 포섭할 수밖에 없는데, 형법에서 공무방해와 업무방해를 구별하여 규정하면서도 양자를 유사한 법정형의 범위

32) 통합개인정보보호법이 제정되기 전 우리나라의 개인정보보호관련 법제의 현황과 그 검토에 대하여는 전지연, “개인정보보호 관련법제의 형사정책적 검토”, 형사정책연구 제16권 제3호, 2005, 52면 이하 참조.

33) 이에 대응하는 (구)공공기관의 개인정보보호에 관한 법률 제23조 제1항의 구성요건에 대한 분석은 이경렬, “개인정보 침해의 형법적 대응”, 비교형사법연구 제12권 제2호, 2010, 594면 참조.

34) 정해욱, “개인정보보호법상의 형사처벌 규정에 관한 연구”, 법학논문집 제35집 제3호, 2011, 116면.

에 두고 있다는 점과 비교할 때에는 그 체계적 정합성의 확보여부가 문제될 소지는 충분하다고 본다.

다음으로, 개인정보침해행위의 유형 중 가장 일반적인 행위유형은 ‘비밀누설’의 행위유형이라 할 수 있는데, 이러한 비밀누설에 해당하는 경우에 대하여는 다양한 법률에서 관련규정을 찾아 볼 수 있다. 즉, 개인정보보호법을 비롯한 관련법률들은 이러한 비밀누설행위와 관련하여 개인정보취급자의 비밀준수의무를 규정함과 동시에 이를 위반한 경우 ‘3년 이하의 징역 또는 3천만원 이하의 벌금’(개인정보보호법 제72조 제3호, 정보통신망법 제72조 제1항 제5호) 혹은 ‘5년 이하의 징역 또는 5천만원 이하의 벌금’(신용정보보호법 제50조 제1항 제6호, 위치정보법 제39조 제2호)을 법정형으로 설정하고 있다. 일반형법이 공무상비밀누설행위(제127조)에 대하여는 ‘2년 이하의 징역이나 금고 또는 5년 이하의 자격정지’를 업무상비밀누설(제317조)에 대하여는 ‘3년 이하의 징역이나 금고, 10년 이하의 자격정지 또는 700만원 이하의 벌금’을 법정형으로 규정하고 있다는 점에 비추어 보면 일견 기존의 형법규정과 어느 정도는 균형을 유지하고 있다고 할 수 있다. 그리고 여기서 신용정보보호법 등의 경우는 현저한 재산적·인격적 가치를 지니는 개인정보를 침해하는 행위에 대하여 그 불법을 기증하고 있는 것으로 이해할 수 있을 것이다.

그런데 특수한 개인정보의 누설을 규정하고 있는 법령 중에는 현행 개인정보 보호체계와는 어울리지 않는 법정형을 규정하고 있는 경우도 찾아 볼 수 있다. 성폭력범죄의 처벌 등에 관한 특례법(이하 ‘성폭력특례법’)의 경우가 대표적이라 할 수 있는데, 동법 제50조 제2항은 성폭력피해자의 신원과 사생활의 비밀 등을 누설한 자에 대하여 ‘2년 이하의 징역 또는 500만원 이하의 벌금’에 처하도록 하고 있다. 이는 개인정보보호와 관련한 일반법인 개인정보보호법상의 처벌규정이 특별법인 성폭력특례법상의 처벌규정보다 중하게 규정되어 있는 경우라고 할 수 있는데, 성폭력범죄 피해자의 개인정보가 누출 혹은 침해되는 경우 발생할 수 있는 다양한 위험성을 고려할 때 과연 타당한 것인지 의문을 제기하지 않을 수 없다. 물론 이와 같은 법정형의 설정은 통합개인정보보호법이 제정되기 이전에 기존의 일반형법상의 비밀침해규정을 고려한 것으로 생각되지만, 기왕에 마련된 개인정보보호법제와의 균형을 확보할 필요는 있다고 본다. 따라서 성폭력특례법상의 개인정보침해행위의 법

정형을 특별히 가볍게 규정해야 할 근거를 찾을 수 없다면, 현행 개인정보보호법제와의 체계적 정합성을 확보한다는 취지에서 재검토가 이루어져야 할 것이다. 문제는 이와 같은 예가 다수의 개별·특별법에 존재할 가능성이 농후하다는 점이며, 개인정보보호법의 제정 이전에 마련된 규정이라면 더욱 그러할 것이다. 성폭력특례법 이외에도 검토가 이루어져야 할 법률로는 ‘특정범죄신고자 등 보호법’, ‘성폭력 방지 및 피해자보호 등에 관한 법률’, ‘아동·청소년의 성보호에 관한 법률’, ‘가정폭력 방지 및 피해자보호 등에 관한 법률’ 등을 거론할 수 있다. 이 중에는 성폭력특례법과 같이 극단적으로 개인정보보호법제에 부합하지 않는 법정형을 규정하고 있는 경우도 존재하고 일응 타당해 보이는 경우도 존재하지만, 개인정보보호법제의 체계적 정합성의 확보라는 차원에서 재검토되어야 할 필요가 있다고 본다.

5. 소 결

이상에서 검토한 결과에 따르면 현행 개인정보보호법제상 형벌규정들은 상향된 법정형의 근거부족, 형벌부과대상과 과태료부과대상에 대한 구별의 모호성, 개인정보보호를 위한 형벌규정을 마련하고 있는 법률들 간의 비통일성, 기존의 형법 및 개별·특별법상 관련규정들과의 불균형성 등과 같은 체계적으로 다양한 문제점을 노출하고 있음을 알 수 있다. 요컨대 현행 개인정보보호법제상의 형벌규정들은 그 체계적 정합성의 확보에 실패하고 있다는 평가가 가능하다. 이러한 체계적 부정합성의 문제는 개인정보침해행위에 대한 규제를 내용으로 하는 법률들이 과연 통일적인 법리에 근거하여 마련된 것인지를 의심케 하는 요인이 되지 않을 수 없다. 따라서 통합개인정보보호법의 법리를 기반으로 관련법률 및 규정들을 재검토하고 현행 개인정보보호법제상의 형벌규정들이 체계적 정합성을 확보할 수 있는 방안을 고민해야만 할 것이다.

V. 개인정보보호를 위한 형벌규정들의 체계정합성 확보를 위한 제언

이 논문은 개인정보보호를 위한 현행 형벌체계의 문제점을 살펴보고자 하였는데, 그 검토결과에 따르면 현행 개인정보보호법제상의 형벌체계는 통합개인정보보호법이 제정되고 4년여의 시간이 흐른 지금까지도 통일적 법리에 근거한 체계구축으로서는 부족한 부분을 다수 노출하고 있음을 알 수 있다. 이로 인하여 개인정보침해행위를 대상으로 하는 형벌규정들을 해석하고 적용함에 있어서도 법리상 그리고 실제상으로 다양한 문제가 발생하지 않을 수 없는 것이다. 따라서 관련법률상의 형벌규정들에 대한 체계정합적 관점에서의 정비가 필요하다고 할 것인데, 여기서는 이를 위한 나름의 방향성을 제시함으로써 결론에 갈음하고자 한다.

1. 정보주체의 실질적 권익향상

먼저, 개인정보주체의 실질적 권익향상이 최우선적 과제라 할 수 있다. 현행 개인정보보호법제상의 개별법률들은 정보주체의 동의여부를 전면에 내세우고 있으나, 이는 정보주체의 권리보호보다는 정보처리자의 면책을 위한 요건이라는 의미에 중점을 두고 있다는 인상을 지우기 어려운 것이 사실이다. 그러나 개인정보자기결정권은 단순한 동의권이 아니라 정보통제권을 그 본질적 내용으로 하는 것이므로 자신의 정보에 대한 실질적 통제권의 확보에 정책의 중점이 놓여야 한다. 따라서 정보통제권의 실질화를 위한 제도적 보완작업은 앞으로도 계속되어야 한다. 다시 말해서, 현행법상의 정보열람·정정·삭제 청구권을 비롯한 개인정보 유통통지 등에 더하여 되도록 정보주체가 개인정보의 유통단계 중 어느 단계에서도 자기결정권을 행사할 수 있는 절차적 보장장치가 보충되어야 한다는 것이다. 예를 들어, 개인정보보호법상의 개인정보 열람권, 정정·삭제 및 처리정지 요구권 등의 행사방법 및 절차를 용이하게 하는 것은 정보주체의 권익향상에 실질적인 의미를 지닌다고 할 수 있다. 다만 이 부분은 기술의 발전에 따라 구체적인 대응방법도 달라질 것이라는 점에서 향후 지속적인 관심이 필요하다고 본다.

또한 정보주체의 권익향상은 형식적인 권리강화에만 중점을 두어서는 안될 것이다. 이는 공공적 관점에서 요구되는 개인정보의 적절한 이용을 제한하는 요인이 될 수 있기 때문이다. 즉, 공공재로서의 개인정보를 이용함에 있어서 실질적인 정보주체의 권익을 침해하지 않는 한도에서는 개인정보의 이용을 적극적으로 장려해야 하지만, 지금과 같이 형식적인 동의획득과 통지여부에만 중점을 두는 제도의 운용은 형식에 얽매어 정보주체의 불편만을 조장할 뿐 권리보호에는 별다른 도움이 되지 않는다는 점을 유념해야 할 것이다. 따라서 개인정보의 효율적 이용과 정보주체의 편의를 고려하여 정보주체의 진의에 근거한 유효한 동의를 전제로 어느 정도 포괄적인 동의의 획득방법을 인정함으로써 개인정보취급자와 개인정보주체 상호간 이익의 조화를 도모할 수 있다고 본다.

2. 처벌대상의 축소

다음으로 형사처벌의 범위와 수위의 조절이 필요하다고 본다. 현행 개인정보보호법제의 형벌규정은 다른 법제에서는 그 유래를 찾아보기 어려울 정도로 광범위하고 강력한 형사처벌을 예정하고 있다. 이에 따라 형벌규정이 근거하고 있는 개인정보보호법 및 관련법령상의 개인정보개념이 지나치게 광범위하다는 점에 대한 비판이 단골소재가 되지 않을 수 없는 것이다. 그러나 개인정보개념 자체의 개방적 혹은 포괄적 성격이 아니라 형사처벌범위의 광범위성에 문제의 본질이 놓여있지 않을까 한다. 앞서서도 언급했듯이 다소 불명확한 개인정보의 개념설정은 불가피한 측면을 지니고 있으므로, 형사처벌의 대상을 축소하는 방향으로 법률을 정비해야 한다고 본다. 따라서 형사처벌의 대상은 민감정보나 고유식별정보의 침해 등으로 제한하고 여타의 경우는 행정형벌이나 사법상의 구제방법을 통하여 규제하는 방법을 고려하는 것이 보다 현실적인 방향이라 생각한다. 특히 정보주체의 입장에서는 정보침해를 행한자의 처벌보다는 그에 따른 손해의 방지와 구제에 더 큰 관심을 가지고 있을 것이므로 형사처벌의 문제보다는 사법적·행정적 구제방법을 보다 확실하게 보완하는 것이 정보주체의 권익향상이라는 측면에서 보면 더 절실한 문제이기 때문이다. 또한 사법적·행정적 규율이 가능한 영역이라면 굳이 형법적 규제를 전면에 등장시

킬 필요는 그다지 크지 않을 뿐 아니라 개인정보침해에 대한 사회적 인식이 성숙하지 않은 시점에서 처벌대상과 그 수위만 광범위하게 설정하는 것은 그 처벌규정의 정당성 확보에도 부정적인 영향을 미치게 될 것이다. 따라서 지금과 같은 광범위한 중벌화의 경향에 대해서는 제동이 필요하다. 물론, 특별입법을 통한 중벌화의 경향이 개인정보의 보호와 관련된 영역에서만 문제되는 것은 아니지만, 비교적 새로운 범죄유형이라 할 수 있는 개인정보침해범죄에 대하여는 사회적 인식이 확립될 때까지 그 처벌여부와 경중에 대한 지속적인 고민이 요구된다고 할 것이기 때문이다.

3. 형벌규정의 체계정합적 정비

마지막으로 이상의 전제위에서 개인정보보호법제상의 형벌규정들에 대한 체계정합적 정비가 이루어져야 할 것이다. 형벌규정의 체계정비에 있어서는 관련규정들 사이에서 발견되는 모순점의 제거와 형사처벌범위의 축소에 중점이 놓여야 한다. 하지만 이와 더불어 개인정보 침해행위의 유형에 대한 본질적 관점에서의 검토를 기초로 형벌체계를 전반적으로 정비하는 것 또한 필요하다. 그리하여 궁극적으로는 현행 개인정보보호법제상의 형벌규정들은 일반법인 개인정보보호법으로 최대한 통합하고 각 개별법에 특수한 구성요건들만을 남겨두는 형태로 체계정비가 이루어져야 한다. 이러한 방향성에 따른 형벌체계의 정비가 이루어진다면 과태료부과대상과 형벌부과대상의 간섭에 대한 조율, 관련법률상 처벌규정의 법리일치 그리고 기존형사법 체계와의 정합성확보라는 과제는 근본적인 해결이 가능하다고 본다.

이러한 형벌규정의 체계적 정비에 있어서는 특히 개인정보보호 8원칙이 하나의 기준점으로 작용할 수 있을 것이다. 앞서 언급했듯이 개인정보 보호원칙은 개인정보보호와 관련한 형벌체계의 핵심적 가치를 형성하고 있기 때문이다. 따라서 동원칙에 기반하여 관련법제의 체계정비를 시도한다면, 개인정보보호와 관련한 형벌규정들 사이의 통일적 체계정립이 가능할 것이라 생각한다.

4. 결 어

이상의 논의결과는 개인정보보호법제의 정비과정에 투입된 그 동안의 노력에 대한 부정적 평가를 전제로 하는 것이라는 점에서 조심스러운 부분이 없지 않다. 하지만 사회적 합의 혹은 규범의식이 미성숙한 지금의 시점에서 관련법률상의 형벌규정들이 단순한 상징적 의미에 머물지 않도록 하기 위해서는 반드시 해결되어야 할 과제임도 분명하다. 우리 사회에서 정보통신분야와 관련한 기술의 발전에 있어서는 최근까지도 세계최초 혹은 세계최고라는 수식어가 자주 등장해 왔으며, 많은 사람들이 이에 열광해 온 것도 사실이다. 그러나 형사처벌을 대상으로 하는 법률분야에서는 이와 유사한 수식어의 사용은 경계의 대상이 되어야 한다. 형벌은 다른 수단으로는 그 목적달성이 어려운 경우에 한하여 투입되어야 한다는 점에서 보다 신중한 검토가 요구되기 때문이다. 그럼에도 불구하고 우리 개인정보보호법제에 형벌규정을 도입하는 과정에서는 이러한 검토의 과정이 충분하지 못했던 것이 아닌지에 대한 진지한 성찰이 필요한 시점이라 생각한다. 향후 현행 개인정보보호법제상의 형벌규정에 대한 전향적 관점에서의 재검토가 이루어지기를 기대한다.

참고문헌

- 김주영/손형섭, 개인정보 보호법의 이해, 법문사, 2012.
- 이창범, 개인정보보호법, 법문사, 2012.
- 정상조 외, 비식별개인정보의 보호 및 활용에 관한 연구, 방송통신위원회 연구보고서, 2010.
- 행정안전부, 개인정보보호법령 및 지침고시 해설서, 2011/12.
- 길준규, “개인정보의 개념과 특징”, 토지공법연구 제18집, 2003.
- 김정환, “개인정보보호법에 대한 입법론적 검토”, 법학논총 제18집 제1호, 2011.
- 김진환/조대희/이상진, “개인정보 보호조치 위반 사건 수사의 문제점과 대책”, 경찰학연구 제13권 제3호, 2013.
- 문재완 “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 2014.
- 박노형, “개인정보보호법과 정보통신망법의 관계분석”, 안암법학 제41권, 2013.
- 이경렬, “개인정보 침해의 형법적 대응”, 비교형사법연구 제12권 제2호, 2010.
- 이필재, “개인정보보호법과 관련 법률의 체계문제”, 한국위기관리논집 제10권 제1호, 2014.
- 전응준, “개인정보보호법률상 형사처벌규정의 적정성에 관한 연구, 정보법학 제17권 제2호, 2013.
- 전지연, “개인정보보호 관련법제의 형사정책적 검토”, 형사정책연구 제16권 제3호, 2005.
- 정효진/윤재석, “개정 OECD 프라이버시 가이드라인: 주요 내용 및 향후 전망”, 주간기술동향, 정보통신산업진흥원, 2014/6/4.
- 정혜옥, “개인정보보호법상의 형사처벌 규정에 관한 연구”, 법학논문집 제35집 제3호, 2011.
- 최경진, “빅데이터와 개인정보”, 성균관법학 제25권 제2호, 2013.
- 현대호, “개인정보 보호법과 다른 법률의 개인정보보호 규정과의 정합성 확보”, 「개인정보보호법」 제정에 따른 개인정보보호정책의 방향과 과제, 한국인터넷법학회 춘계공동학술대회 자료집, 2011.4.15.
- 황태정, “통합개인정보보호법안의 입법체계 검토”, 형사정책연구 제20권 제1호, 2009.

A Study on Problems of Current Sentencing System for Personal Information Protection*

LEE, SUNGDAE**

The Act on Personal Information Protection that was enacted on March 29, 2011 covered not only private sector but also public sector. In other words, not only public agencies but also corporate, group and personal operators had obligation of personal information protection to enact standards of all of the processes from collection to destruction of personal information. The enactment of the act paid considerable attention to regulation subject, scope of the protection, damage relief system, and organization and authority of the committee of personal information protection, and paid less attention to modification of punishment regulations. As a result, systematic mismatching and problems were found between the Act on Personal Information Protection and associated laws.

The study investigated problems of criminal sentencing regulations of the Act on Personal Information Protection for the purpose of matching with existing system of the criminal act:

At first, sentencing systems of the Act on Personal Information Protection and associated laws were: Like other personal information protection laws, current personal information protection system started from eight principles of personal information protection of ‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ and regulated considerably heavy statutory penalty to differ from other legal systems.

And, the study investigated problems of sentencing system concerning concept

* This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government(NRF-2013S1A5B5A07048827)

** Senior Researcher, Institute of Law Research Units, Sungkyunkwan University

of personal information of current legal system to examine validity of concept of personal information of the personal information protection system according to principle of legality. Application of each sentencing regulation had limitation on personal information concept at theory of analysis, and concrete analysis on infringement upon individual personal information was still left to solve fundamental problems from point of view of legislation.

Lastly, the study found out incoherence of sentencing system of protection law system of personal information to give reformation to get matching of current sentencing system to protect personal information. The study examined legal punishment regulation on public agencies' personal information protection cancelled at enactment of general personal information protection law to investigate difference between infringement behavior criminally punished and behavior being given penalty, and to investigate comparison with regulations according to general criminal law and existing criminal law systems. Current sentencing system had problems: uniform sentencing of severe punishment, crossing of both imposing of fine and punishment, ununiformity of punishment regulations of associated laws and regulations, and mismatching with existing systems of criminal laws. Current legal system's sentencing had problems of wide and uniform heavy punishment rather than uncertainty of personal information concept, so that scope of criminal punishment should be lessened to protect actual victim and to reform current personal information protection legal system.

❖ Keyword: Personal Information Protection Act, sentencing system for personal information protection, the right to informational self-determination, infringement of the personal information, data subsection

투고일 : 2월 26일 / 심사(수정)일 : 3월 20일 / 게재확정일 : 3월 20일
--