



저작자표시-비영리-동일조건변경허락 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



동일조건변경허락. 귀하가 이 저작물을 개작, 변형 또는 가공했을 경우에는, 이 저작물과 동일한 이용허락조건하에서만 배포할 수 있습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

법학석사 학위논문

개인정보 유출로 인한  
기업의 책임  
- 손해배상책임을 중심으로

2015년 2월

서울대학교 대학원  
법학과 지식재산전공  
신재형

# 개인정보 유출로 인한 기업의 책임

- 손해배상책임을 중심으로

지도교수 정 상 조

이 논문을 법학석사 학위논문으로 제출함  
2014년 10월

서울대학교 대학원  
법학과 지식재산전공  
신 재 형

신재형의 석사 학위논문을 인준함  
2014년 12월

위 원 장 \_\_\_\_\_ (인)

부위원장 \_\_\_\_\_ (인)

위 원 \_\_\_\_\_ (인)

## 국문초록

정보화 사회의 진전에 따라 사회·경제·문화 등 사회 전 영역에서 개인정보를 활용한 서비스의 제공활동이 증대하였다. 개인정보의 수집 및 활용이 갖는 순기능은 정보의 가치를 극대화하고 이를 통하여 개인과 사회가 부담해야 하는 비용과 위험을 감소시킨다는 것이나, 반면 그 과정에서 개인정보자기결정권 또는 프라이버시권 등의 인격권이 침해될 우려가 높고, 무단으로 수집·가공·유통되는 개인정보는 여러 유형의 범죄에 활용될 위험성도 높다.

개인정보의 침해에 대해 손해배상과 같은 민사적 구제가 충실히 이루어진다면 합리적인 사업자들은 개인정보의 침해에 따른 손해배상책임을 부담하는 것보다 그 유출이나 도용을 사전에 방지하기 위한 노력을 기울일 것이다. 그러나 손해배상책임의 정도가 미미하다면 그 사업자는 개인정보의 보호를 위한 투자를 할 필요가 크지 않다고 판단하게 될 것이고, 그 결과 개인정보의 보호가 무색하게 될 염려가 있다.

그렇다고 손해배상액의 산정이 아무런 기준 없이 법원에 의하여 자의적으로 이루어지는 것 또한 곤란하므로, 개인정보 침해로 인한 손해배상액의 산정에 가급적 자의성을 배제하고, 예측가능성과 검증가능성을 높이기 위하여 손해배상액 산정에 있어서의 고려요소들을 체계화·유형화 할 필요성이 있다.

이에 본 논문에서는 개인정보의 유출로 인한 손해배상을 검토

하기 위한 논의의 전제로서 개인정보의 개념과 특성 및 개인정보 유출의 개념을 소략하게 검토하였고, 개인정보와 침해와 손해의 구별 논의 및 재산적 손해와 정신적 손해의 구별 논의를 검토하였다.

정신적 손해배상액 산출을 위하여 국내외에서 논의되고 있는 위자료 판단의 고려요소들을 개인정보 자체, 피해자 측 요소 및 가해자 측 요소로 범주화하여 정리하였으며, 이를 토대로 4단계에 걸친 통합적 손해배상액 산출모델을 제시하였다. 해당 모델은 기존에 많은 논의가 이루어지지 않았던 개인정보의 유형에 따른 손해의 정량적 판단 그리고 가해자 측의 참작요소를 구체화·세분화하였다는 점에서 그 의미가 있다.

통합적 산출모델에서는 다음의 단계를 통하여 구체적인 최종 손해배상액을 도출하도록 하였다. 우선 재산적 손해와 정신적 손해를 구분하여 재산적 손해에 해당하는 부분을 확정한다. 다음으로 객관적 요소에 해당하는 유출된 개인정보의 유형 및 개인정보 침해 사고의 태양을 확정하여 기초적 손해배상액을 산출한다. 여기에 주관적 요소인 피해자 측 참작요소와 가해자 측 참작요소를 종합적으로 고려하여 손해배상액을 최종적으로 산출한다. 위와 같은 단계적 판단과정을 통하여 개인정보 유출로 인한 손해배상액 판단에 있어서의 정형성과 예측가능성을 도모할 수 있을 것으로 기대한다.

**주요어:** 개인정보, 개인정보보호, 개인정보유출, 손해배상, 정신적 손해, 위자료.

**학 번:** 2013-21304

# 목 차

제1장 서론 .....	1
제1절 개인정보의 관리 및 보호 현황 .....	1
I. 정보화 사회와 개인정보 .....	1
1. 개인정보의 필요성 .....	1
2. 개인정보의 양면성 .....	2
3. 개인정보의 활용성 .....	2
4. 개인정보의 위험사회 .....	3
II. 개인정보보호 관련법규의 개정 .....	4
1. 개편의 필요성 .....	4
2. 개인정보보호법의 제정 .....	4
3. 개인정보보호법의 개정 .....	5
4. 정보통신망법의 개정 .....	5
5. 검토 .....	6
제2절 연구의 목적·범위 .....	6
제2장 개인정보 보호체계 .....	8
제1절 개인정보의 의의 및 인정범위 .....	8
I. 개인정보에 대한 정의 .....	8
II. 개인정보의 인정범위 .....	10
1. 학설 .....	10
2. 우리나라의 판례 .....	10
3. 미국의 판례 .....	11
4. 검토 .....	12
제2절 개인정보보호의 법적근거 .....	12
I. 헌법적 근거 .....	12
II. 법률적 근거 .....	14

1. 간접 적용설 .....	14
2. 민법상 채무불이행책임과 불법행위 .....	14
3. 개인정보보호법 및 정보통신망법 .....	14
<b>제3절 개인정보의 보호범위 .....</b>	<b>14</b>
I. 재산권으로 보는 견해 .....	15
II. 인격권으로 보는 견해 .....	15
III. 판례 .....	16
IV. 검토 .....	16
<b>제4절 각국 개인정보법의 입법방향 .....</b>	<b>17</b>
I. 개인의 권리보호를 강조하는 입법 유형 .....	18
II. 개인정보의 유용성을 고려한 입법 유형 .....	18
III. 우리나라의 경우 .....	18
<b>제5절 개인정보의 유형 및 개인정보의 분류 .....</b>	<b>19</b>
I. 개인정보의 유형 .....	19
II. 개인정보의 분류 방식 .....	21
1. 민감성에 따른 분류 .....	21
2. 식별가능성에 따른 분류 .....	21
3. 민감성과 식별가능성을 종합하여 개인정보를 분류하는 견해 .....	22
4. 검토 .....	23
<b>제3장 개인정보의 유출 .....</b>	<b>24</b>
<b>제1절 개인정보 유출의 의미 .....</b>	<b>24</b>
I. 서설 .....	24
II. 학설 .....	24
III. 판례의 태도 .....	25
IV. 검토 .....	26
<b>제2절 개인정보의 유출로 인한 기업의 책임 .....</b>	<b>27</b>
I. 형사책임 .....	27
II. 행정상의 책임 .....	28
1. 개인정보보호법 상 과징금의 부과 .....	28

가. 과징금 부과 원칙 .....	28
나. 과징금의 산정 방식 .....	29
(1) 1단계 .....	29
(2) 2단계 .....	29
(3) 3단계 .....	30
(4) 4단계 .....	30
다. 검토 .....	30
2. 정보통신망법 상 과징금의 부과 .....	30
가. 과징금 부과 원칙 .....	30
나. 과징금의 산정 방식 .....	31
3. 검토 .....	32
Ⅲ. 손해배상책임 .....	33
<b>제3절 개인정보 유출사고 사례 .....</b>	<b>33</b>
I. 손해배상책임 인정 사례 .....	33
1. 리니지Ⅱ 사건 .....	34
2. 국민은행 사건 .....	35
3. LG전자 사건 .....	35
4. SK브로드밴드 사건 .....	36
5. KT 사건 .....	37
6. SK커뮤니케이션즈 사건 .....	38
(1) 인정 판례 .....	38
(2) 부정 판례 .....	38
II. 손해배상책임 부정 사례 .....	39
1. LG텔레콤 사건 .....	39
2. 다음 사건 .....	40
3. 옥션 사건 .....	41
4. GS칼텍스 사건 .....	42
III. 검토 .....	42
<b>제4절 개인정보 유출사고의 유형화 .....</b>	<b>44</b>
I. 서설 .....	44
II. 유출사고의 5가지 유형 .....	44



1. 분류 방법 .....	44
2. 분류 근거 .....	45
III. 실제 사례 적용 .....	46
<b>제4장 개인정보 유출로 인한 기업의 손해배상책임</b>	<b>47</b>
<b>제1절 총설</b> .....	<b>47</b>
<b>제2절 개인정보의 침해와 손해의 구별</b> .....	<b>48</b>
I. 서설 .....	48
II. 학설 .....	48
1. 국내에서의 논의 .....	48
2. 해외에서의 논의 .....	49
III. 판례 .....	50
1. 우리 판례의 경향 .....	50
2. 미국 판례의 경향 .....	51
3. 영국 판례의 경향 .....	52
4. 캐나다 판례의 경향 .....	53
IV. 검토 .....	54
<b>제3절 개인정보 유출로 인한 손해의 종류</b> .....	<b>55</b>
I. 서설 .....	55
II. 재산적 손해와 정신적 손해 .....	55
III. 통상손해와 특별손해 .....	56
IV. 검토 .....	56
<b>제4절 개인정보 유출로 인한 손해배상책임의 발생</b> .....	<b>57</b>
I. 손해배상청구권의 성립요건 .....	58
1. 서설 .....	58
2. 입증책임의 전환 .....	58
3. 개인정보처리자의 주의의무 .....	59
가. 서설 .....	59
나. 주의의무의 발생근거 .....	60
다. 주의의무 판단의 전제 - 합리적 기대가능성 .....	60

4. 법령에 따른 고려요소 .....	61
가. 안전조치의무 .....	61
나. 사후조치의무 .....	63
5. 세부적 고려요소 .....	64
가. 개관 .....	64
나. 정보 자체와 관련된 고려 요소 .....	64
(1) 정보의 민감성과 위험성 .....	64
(2) 정보의 양 .....	65
다. 개인정보처리자와 관련한 고려 요소 .....	65
(1) 개인정보처리자의 영업내용 .....	65
(2) 유출 개인정보수집 및 보관의 필요성 .....	66
(3) 개인정보처리자와 해커의 관계 .....	67
라. 외부적 고려요소 .....	67
(1) 해커의 기술 수준 .....	68
(2) 개인정보처리자의 기술적 보호조치 수준 .....	68
마. 사후조치 .....	69
(1) 사후조치를 취한 시점 .....	70
(2) 사후조치를 취하게 된 경위와 사후조치의 내용 .....	70
바. 정리 .....	70
6. 검토 .....	71
II. 재산적 손해에 대한 손해배상책임 .....	71
1. 재산적 손해의 의미 .....	72
가. 재산적 손해의 형태 .....	72
나. 재산적 손해의 성질 .....	72
다. 재산적 손해에 대한 판례의 태도 .....	72
(1) 판시 내용 .....	72
(2) 판례의 태도에 대한 비판적 검토 .....	73
2. 재산적 손해의 범위 .....	74
3. 재산적 손해의 범위에 대한 판례 .....	74
가. 판시 내용 .....	74
나. 판례에 대한 검토 .....	75

4. 개인정보의 객관적인 재산적 가치 평가에 대한 문제	76
Ⅲ. 정신적 손해의 발생	77
1. 정신적 손해배상의 의의	77
2. 정신적 손해의 특성	78
가. 객관적 측정의 곤란성	78
나. 개인에 따른 차이	78
다. 검토	79
3. 정신적 손해배상의 기능	80
가. 손해배상의 기능	80
나. 위자료의 기본적 기능	80
다. 위자료의 보완적 기능	81
Ⅳ. 정신적 손해배상의 범위	82
1. 우리 민법상 기준	82
2. 개인정보 유출로 인한 위자료에 대한 우리 판례의 태도	83
3. 비교법적 정신적 손해 산정의 원칙	84
가. 미국에서의 논의	85
나. 캐나다에서의 논의	85
다. 일본에서의 논의	86
(1) 위자료에 대한 일반적 논의	86
(2) 명예훼손으로 인한 위자료 산출에 대한 논의	86
4. 검토	88
Ⅴ. 정신적 손해배상액 산출의 참작요소	89
1. 개인정보자체와 관련한 요소	89
가. 개인정보의 종류 및 성격	90
(1) 침해정보의 민감성	90
(2) 침해정보의 식별가능성	91
(3) 검토	92
나. 침해된 정보의 양	93
다. 침해의 기간	93
라. 침해 빈도	94
마. 유출된 정보의 확산 범위 및 전파 가능성	94

2. 피해자 측 고려 요소 .....	95
가. 사회생활상의 불이익 .....	95
나. 후속손해의 발생 .....	96
다. 피해자의 과실 .....	97
3. 가해자 측 고려 요소 .....	99
가. 개인정보의 수집 동기, 목적 .....	99
나. 개인정보 유출 사고의 태양 .....	99
다. 침해의 동기·목적 .....	100
라. 침해행위를 통해 얻은 이익 .....	100
마. 가해자의 사회적 책임 .....	101
바. 가해자의 재산상태 .....	102
사. 개인정보 영향평가의 실시 여부 .....	104
아. 사후조치의 신속성, 적절성, 보완성 .....	105
자. 피해자에 대한 안내 및 피해회복조치 이행 여부 .....	106
4. 정리 .....	107
<b>제5절 개인정보 유출로 인한 손해배상액 산정방식 .....</b>	<b>108</b>
I. 기존의 손해배상액 산정 모델 .....	108
1. JNAS JO 모델의 산정방식(제1모델) .....	108
2. CVM(조건부 가치추정법)을 이용한 산정방식(제2모델) .....	111
3. 피해자 측과 가해자 측을 고려한 산정방식(제3모델) .....	112
4. 항목별 피해등급을 5단계로 구분하는 산정방식(제4모델) .....	114
5. 기존 모델에 대한 검토 .....	116
II. 통합적 손해배상액 산출모델의 제안 .....	117
1. 서설 .....	117
2. 구체적인 손해배상액 산출 과정 .....	118
가. 1단계 - 재산적 손해와 정신적 손해의 구분 단계 .....	118
나. 2단계 - 유출정보에 대한 객관적 평가단계 .....	118
(1) 유출 개인정보의 기초 가치산정 .....	119
(2) 개인정보 유출의 태양 .....	119
(3) 유출된 개인정보의 양 .....	120
다. 3단계 - 유출 사고에 대한 객관적 평가 단계 .....	121

라. 4단계 - 피해자와 가해자에 대한 주관적 평가단계 .....	122
(1) 피해자 측 참작요소 반영 .....	122
(2) 가해자 측 참작요소 반영 .....	123
3. 결어 .....	124
제5장   결   론 .....	125
참 고 문 헌 .....	127
Abstract .....	131

## 표 목 차

[표 1]	.....	1
[표 2]	.....	2
[표 3]	.....	23
[표 4]	.....	43
[표 5]	.....	46
[표 6]	.....	62
[표 7]	.....	71
[표 8]	.....	87
[표 9]	.....	93
[표 10]	.....	107
[표 11]	.....	112
[표 12]	.....	113
[표 13]	.....	114
[표 14]	.....	115
[표 15]	.....	120
[표 16]	.....	122
[표 17]	.....	123
[표 18]	.....	124

# 제1장 서론

## 제1절 개인정보의 관리 및 보호 현황

### I. 정보화 사회와 개인정보

#### 1. 개인정보의 필요성

정보화 사회가 진전함에 따라 사회·경제·문화 등 사회의 전 영역에서 개인정보를 활용한 서비스의 제공활동이 증대하였다. 개인정보의 활용은 이노베이션을 촉진시키는 중요한 기능을 하고,<sup>1)</sup> 이를 통해 사회와 경제에 도움이 되는 다른 다양한 기능이 제공될 수 있다.

정보통신기술을 활용한 서비스의 제공과정에서 개인을 특정하는 것이 필수적인데, 개인을 특정하기 위해서는 개인정보의 제공이 불가피하기 때문에,<sup>2)</sup> 이러한 오늘날의 인터넷과 무선통신 등의 정보통신기술은 개인정보의 적극적인 활용을 전제조건으로 발전하고 있다.

이에 따라 정보통신 등 서비스 제공자는 방대한 양의 개인정보를 수집·관리하게 되었고, 그 과정에서 개인정보가 침해될 위험이 증가하였다. 일찍이 울리히 벡이 표현한 것의 연장선상에서, 고도화된 정보통신기술의 발달로 인하여 이른바 개인정보의 위험사회<sup>3)</sup>가 도

---

1) 고태수, "개인정보보호의 법, 경제 및 이노베이션", 경제규제와 법(Journal of Law & Economic Regulation) 제5권 제2호 (통권 제10호) (Vol. 5. No. 2 (Serial No. 10), 2012. 11. 148면.

2) 이원우, "개인정보보호를 위한 공법적 규제와 손해배상책임, 개인정보누출을 중심으로", 사단법인 행정법이론실무학회 (행정법연구 제30호 2011. 8.), 239면.

래하게 된 것이다.

## 2. 개인정보의 양면성

개인정보의 수집과 활용의 순기능은 정보의 가치를 극대화시키고 이를 통해 개인 및 사회가 부담하는 비용을 감소시킨다는 것이나, 그 과정에서 개인정보자기결정권 또는 프라이버시권 등 인격권의 침해우려가 높아지고, 무단으로 수집·가공·유통되는 개인정보가 범 죄에 제공되거나 활용될 위험성도 함께 증대되었다.<sup>4)</sup>

이러한 개인정보의 양면성을 다시 표현하면, 개인정보는 정보주체에게는 인격권에 의해 보호되어야 할 대상이지만, 다른 측면으로는 기업의 영업자산 혹은 공공기관의 공공기록물로서의 의미를 지니고,<sup>5)</sup> 서비스제공자에게는 재산권의 대상이라는 이중적인 성격을 갖는다고 할 수 있다.<sup>6)</sup>

## 3. 개인정보의 활용성

정보통신기술 기업 특히 전자상거래를 기반으로 하는 기업들에게는 고객들의 인적 사항 등 기본적인 정보와 고객의 거래정보, 웹 서핑 정보 및 이를 분석하여 도출되는 구매성향, 취향 등 2차적 정보 등 고객의 개인정보가 집약된 데이터베이스는 고도의 경제적 가치를 갖는 중요 무형자산이다.<sup>7)</sup> 빅데이터의 경제적 가치가 새롭게 조명되고 있는 최근의 현상도 이러한 관점에서 생각할 수 있다.<sup>8)</sup>

---

3) 백(U. Beck), 홍성태 옮김, 위험사회, 새물결, 1997.

4) 정상조, 권영준, “개인정보의 보호와 민사적 구제수단”, 법제 58권 3호 통권 630호 (2009. 3.), 7면.

5) 이창범, 『개인정보 보호법』, 법문사, 2012.1. 3면

6) 임종인, 이숙연, “개인정보관련분쟁의 사례분석과 대안의 모색”, 정보법학 제12권 제2호, 2008. 12. 219면.

7) 임종인, 이숙연, 전개 논문, 214면 내지 214면.



따라서 이와 같이 개인정보의 경제적 가치를 인식하게 된 해커들 또는 기업의 내·외부관계자에 의하여 제3자에 대한 판매를 목적으로 한 개인정보 유출사고가 지속적으로 발생하고 있다.

따라서 개인정보의 이용을 활성화하면서도 한편으로는 그에 수반되는 잠재적 위험성을 파악하여 개인정보에 대한 자율적이고 효율적인 규제방안을 모색하는 것이 오늘의 과제라고 할 것이다.<sup>9)</sup>

#### 4. 개인정보의 위협사회

개인정보 서버에 대한 해킹 또는 개인정보의 위탁 과정에서의 범죄 등으로 인하여 개인정보 유출사고가 빈번하게 발생한 결과, 근래 5년간 총 2억 5,000만 여건(중복유출 포함)에 달하는 개인정보가 해킹이나 기업 내부 공모자에 의해 빠져나간 것으로 분석되었다.<sup>10)</sup>

최근 개인정보 유출사고는 사고발생 시 유출되는 정보의 양과 피해의 범위가 매우 확대되어 되어,<sup>11)</sup> 일단 사고가 발생하면 매우 많은 수의 피해자가 발생하고 그 피해로 인한 경제적 규모 또한 가히 추측하기 어렵다. 반면 대규모의 피해자가 발생하는 것에 반하여 피해의 구제는 거의 이루어지고 있지 못하고,<sup>12)</sup> 개인정보 침해 방지를 위하여 정부가 내어놓은 각종 정책에도 불구하고 대규모 개인정보 유출사고가 연이어 발생하여 그 실효성에 의문이 제기되고 있다.

---

8) 한국정보화진흥원. 새로운 미래를 여는 빅데이터 시대, 2013.

9) 서울대학교 기술과 법센터, 개인정보의 보호에 관한 입법론 (SNU CLT Working Paper 2006-3, 연구진: 정상조, 권건보, 박재우), 제71면.

10) 헤럴드경제, “개인정보는 없다’ 최근 5년간 개인정보 2억5000만여 건 유출”, 2014. 4. 5. [http://news.heraldcorp.com/view.php?ud=20140404001104&md=20140407003610\\_BK](http://news.heraldcorp.com/view.php?ud=20140404001104&md=20140407003610_BK)

11) 손형섭, “연예인의 프라이버시권 범위”, 법조 통권 제635호, 2009, 26면.

12) 윤주희, “개인정보 침해현황과 이용자보호”, 법학논총(제33권 제1호), 2013. 4. 19, 328면.

정보통신윤리위원회가 2006년 실시한 한 조사에 의하면 인터넷 사용자의 95.4%가 프라이버시 침해나 개인정보유출 가능성에 대해 불안감을 지니고 있는 것으로 나타났는데,<sup>13)</sup> 이 조사에 따르면 인터넷의 사용자는 그 편리함 때문에 인터넷을 사용하지만, 인터넷의 사용과 동시에 개인정보침해에 대한 위험에 상시 노출되어 있다는 생각을 가져야 하는 실로 개인정보의 위험사회를 살고 있는 셈이다.

## II. 개인정보보호 관련법규의 개정

### 1. 개편의 필요성

개인정보에 관한 사회적 이슈는 주로 정보통신망상에서 발생하였기 때문에 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’(이하 ‘정보통신망법’)을 통해서 온라인사업자가 수집하여 이용하는 개인정보에 대한 보호의무가 규정되었고, 공공분야에서는 ‘공공기관의 개인정보보호에 관한 법률’이 개인정보보호에 관하여 규정하고 있었다.<sup>14)</sup> 그런데 개인정보의 오·남용 및 불법유출이 사회적인 문제로 부각되면서 정보통신망법의 개정이 계속되었고, 나아가 오프라인에서의 개인정보보호까지 포섭하기 위하여,<sup>15)</sup> ‘공공기관의 개인정보보호에 관한 법률’을 폐지하고 ‘개인정보보호법’이 제정되기에 이르렀다.

### 2. 개인정보보호법의 제정

개인정보보호법은 2011. 3. 29. 공포되었으며, 2011. 9. 30.부터 개인정보보호법이 시행되게 되었는데, 개인정보보호법의 제정 이유에 의

---

13) 정보통신 윤리위원회, “인터넷 개인정보 침해 대응방안 연구”, 2006.

14) 윤주희, 전제 논문, 제327면.

15) 김일환, 김민호, 지성우, “개인정보보호 법규 위반에 대한 징벌적 과징금의 성격 및 합리적 처분 기준 연구”, 방송통신위원회, 2011. 11. 49면.

하면 ① 공공부문과 민간부분을 망라하여 국제 수준에 부합하는 개인정보 처리원칙을 규정, ② 개인정보 침해로 인한 국민의 피해구제를 강화하여 국민의 사생활의 비밀을 보호, ③ 개인정보에 대한 권리와 이익을 보장하려는 목적을 가지고 있음이 명시되어 있는바,<sup>16)</sup> 우리의 개인정보보호법은 정보주체에 대한 충실한 보호를 기본원칙으로 하여 제정된 것으로 보인다.

### 3. 개인정보보호법의 개정

개인정보보호법 제정 이후에도 대량의 주민등록번호 유출 사고가 빈번하게 발생하는 등 문제점이 지적되어,<sup>17)</sup> 2014. 8. 7. 시행된 개인정보보호법(법률 제11990호, 2013. 8. 6. 개정된 것)에서는 모든 개인정보처리자에 대하여 원칙적으로 주민등록번호의 처리를 금지하고(제24조의2), 주민등록번호가 분실·도난·유출·변조·훼손된 경우 5억 원 이하의 과징금을 부과·징수할 수 있도록 하며(제34조의2), 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 대표자 또는 책임 있는 임원을 징계할 것을 권고할 수 있다는 규정(제65조 제2항)이 추가되었다.

### 4. 정보통신망법의 개정

정보통신망을 통한 개인정보 유출 사고의 방지를 위하여 법상 의무를 위반한 정보통신서비스 제공자의 처벌을 엄격히 한다는 차원에서,<sup>18)</sup> 정보통신서비스 제공자가 관리하는 개인정보가 분실·도난·누출된 경우에 정보주체가 300만원 이하의 법정손해배상을 청구할 수 있도록 개정하고(제32조의2), 정보통신서비스 제공자는 개인정보의

---

16) 법제처, 개인정보보호법 제정 이유.

17) 법제처, 개인정보보호법 개정 이유.

18) 법제처, 정보통신망법 개정 이유.

누출 등 사실을 안 때로부터 정당한 사유가 없는 이상 24시간 이내에 사고 사실을 통지·신고해야 하는 것으로 개정되었다.

## 5. 검토

기존의 개인정보유출로 인한 손해배상액은 10만원 내외의 비교적 적은 손해배상에 머물렀다. 그러나 개인정보보호법 제정으로 개인정보에 대한 입법자의 강력한 보호의지가 천명되었고, 특히 최근 개인정보보호법 개정으로 주민등록번호의 처리가 원칙적으로 제한되면서, 향후 주민등록번호 유출로 인한 개인정보처리자의 손해배상책임 판단 시에 손해배상액수가 증액될 가능성이 다분하다.

더군다나 정보통신망법이 새롭게 300만원이라는 법정의 손해배상액을 규정한 이상,<sup>19)</sup> 기존과 같이 10만원 내외의 위자료만을 개인정보 침해로 인한 손해배상액으로 인정하는 법원의 태도는 더 이상 유지되기 어려울 것으로 보인다. 따라서 300만원이라는 새로운 상한선 규정의 도입에 발맞추어 개인정보의 유출·노출 사고로 인한 손해배상액의 산정기준을 더욱 구체화, 세부화 하는 연구의 필요성이 대두되었다.

## 제2절 연구의 목적·범위

본 논문은 크게 세 부분으로 나뉜다. 2장에서는 개인정보 자체에 대한 다각적인 분석을 통하여 개인정보의 유출로 인한 손해배상책임

---

19) 2014. 7. 11. 이찬열 위 9인에 의하여 발의된 ‘개인정보보호법 일부 개정법률안’에 의하면 개정 정보통신망법과 동일한 300만원을 상한으로 하는 법정손해배상 규정은 물론, 발생한 손해의 3배 이내의 범위에서 배상책임이 부과된다는 징벌적 손해배상 규정까지 입법이 제안되어 있다(출처: 국회 의안정보시스템).

[http://likms.assembly.go.kr/bill.jsp?BillDetail.jsp?bill\\_id=PRC\\_B1N4Q0S7Q1K1V1P6G1R9G3E6D1V8S9](http://likms.assembly.go.kr/bill.jsp?BillDetail.jsp?bill_id=PRC_B1N4Q0S7Q1K1V1P6G1R9G3E6D1V8S9)

과 관련한 논의의 전제를 마련한다. 3장에서는 개인정보 유출 사고의 구체적인 유형을 제시하고 이를 5가지 유형으로 분류하였다. 제4장에서는 위 제2장, 제3장의 논의를 바탕으로 개인정보의 유출로 인한 정형화된 손해배상액 산정의 기준을 제시하려고 하였다.

이를 분설하면, 제2장에서는 개인정보의 의의 및 인정범위에 대한 국내·외의 논의를 검토하고, 개인정보 보호범위의 법률적 근거를 재산권으로 보는 견해와 인격권으로 보는 견해를 비교하였다. 이를 토대로 각국의 개인정보법이 어떠한 방향으로 입법되어 있는지를 확인하였고, 개인정보를 민감성과 식별가능성을 기준으로 분류하는 관점을 소개하였다.

3장에서는 개인정보 유출의 개념적 요소들을 검토하고, 개인정보의 유출사고로 인하여 기업에게 발생하는 형사책임, 행정상의 책임, 손해배상책임의 요건 및 효과를 확인하였다. 특히 행정상의 책임 중 과징금의 산정방식을 상세히 검토하여 손해배상금 산정과정에 참작하고자 하였다. 다음으로 국내의 대표적인 개인정보 유출사례들을 상세히 분석하고, 해당 사건들을 5가지 유형으로 분류하였다.

4장에서는 개인정보에 대한 침해 및 손해에 대한 개념적인 구별을 전제로, 개인정보의 유출로 인하여 정보주체에게 어떠한 손해가 발생하는지를 확인하였다. 이를 토대로 개인정보 유출로 인한 손해배상청구권의 성립요건으로서 개인정보처리자의 주의의무를 분석하였고, 개인정보 유출로 인한 재산적 손해에 대해 상세히 검토하였다.

정신적 손해와 관련해서는 손해배상의 산정기준이 되는 참작요소들을 유형별로 세부적으로 검토하여 정형화된 위자료 판단을 도모하고자 하였다. 특히 기존 연구들과는 다소 다른 관점에서 개인정보 자체와 관련된 요소들을 분리하여 별도로 검토하였고, 가해자인 기

업 측이 손해배상책임의 감경을 위해 제출할 수 있는 각종 참작요소들에 대해서도 상세히 검토하였다. 특히 가해자의 현실적 배상가능성과 관련하여 가해자의 재산상태가 참작될 수 있는지 여부도 자세히 논의하였다.

마지막으로는 기존의 연구들에서 제안된 손해배상액 산출방식을 종합적이고 발전적인 방식으로 결합한 통합적 손해배상액 산출모델을 제안하였다. 위 모델은 1단계로 재산적 손해와 정신적 손해를 구분하고, 2단계에서는 유출된 개인정보에 대한 객관적 평가를 하였다. 3단계에서는 유출사고의 유형별로 2단계에서 산출된 액수에 가중치를 부여하였고, 마지막으로 4단계에서는 주관적 요소로써 가해자 측의 참작요소와 피해자 측의 참작요소 각각에 대한 세부적인 가중치를 제시하여 최종적인 손해배상금액을 산출하고자 하였다.

## 제2장 개인정보 보호체계

### 제1절 개인정보의 의의 및 인정범위

#### I. 개인정보에 대한 정의

OECD 이사회가 1980. 9. 23. 채택한 프라이버시보호 및 개인정보의 국제유통에 관한 가이드라인<sup>20)</sup>에 의하면, 개인정보란 “식별된 또는 식별될 수 있는 개인에 관한 모든 정보(any information relating to identified or identifiable individual)”라고 규정되어 있고, EU가

---

20) “Guidelines on the Protection of Privacy and Trans-border Flows of Personal Information”

1995. 10. 24. 공표한 개인정보보호지침<sup>21)</sup>에 의하면 개인정보는 “자연인을 식별하거나 식별할 수 있는 모든 정보”라고 규정되어 있다.<sup>22)</sup>

우리의 개인정보보호법 제2조 제1항에서는 개인정보를 “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)”라고 규정하고 있고, 정보통신망법 제2조 제6호에서는 개인정보를 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)”라고 규정하여 개인정보보호법보다 다소 구체적으로 규정하고 있다.

즉 우리 개인정보보호법 제2조 제1항 및 정보통신망법 제2조 제6호에서 도출되는 개인정보의 구성요소는 일반적으로 ① 정보의 임의성, ② 살아 있는 개인에 대한 정보, ③ 특정 개인과의 관련성, ④ 개인의 식별 가능성 등으로 요약된다.<sup>23)</sup>

위 각 개념을 상술하면 ① 정보의 임의성과 관련하여서는 개인을 알아볼 수 있는 정보면 충분하여 정보의 성격, 내용, 형식 등에 대해서는 특별한 제한이 없다. ② 살아 있는 개인에 관한 정보만 개인정보의 개념에 포함되는 것이고, ③ 해당 정보와 특정 개인 사이에 일정한 관련성이 존재하여야 한다. 나아가 ④ 해당 정보를 통하여

---

21) “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”

22) 임종인, 이숙연, 전개 논문, 217면.

23) 이창범, 전개서, 15면.

개인을 알아볼 수 있는 식별가능성이 있는 정보에 해당해야지만<sup>24)</sup> 비로소 개인정보보호법 및 정보통신망법상의 보호대상인 “개인정보”에 해당하게 된다.

## II. 개인정보의 인정범위

### 1. 학설

개인정보보호법 제2조 제1항 및 정보통신망법 제2조 제6항 후단은 개인정보에 대하여 “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.”라고 규정하고 있다.

이에 대하여 위 규정이 문제라고 지적하면서 다른 정보와 결합해야만 특정 개인을 알아볼 수 있게 되는 정보는 진정한 개인정보가 아니고, 개인정보보호법 위반 시 형사처벌 규정까지 두고 있는 우리 법제 상 개인정보를 지나치게 넓게 정의할 경우 자칫 많은 부작용을 가져올 수 있다면서 위 조항의 규정 방식을 비판하는 견해가 있다.<sup>25)</sup>

반면 인터넷기술의 발전에 따라 사업자들이 수집하는 정보가 다양해지고 광고기술의 발전으로 다양한 정보가 소비자들의 시각과 청각, 시간을 지배하게 됨에 따라 개인정보의 범위가 어느 정도 넓게 해석될 필요가 있다는 견해도 존재한다.<sup>26)</sup>

### 2. 우리나라의 판례

---

24) 이창범, 진게서, 제15면 내지 제20면.

25) 구태언, “개인정보 보호법의 제문제”, 법학평론 제3권 (2012. 12.), 71면.

26) 정상조, “광고기술의 발전과 개인정보의 보호”, 저스티스 통권 제106호, 603면.



우리의 판례는 이메일 주소에 대해 “이메일 주소는 당해 정보만으로는 특정 개인을 알아볼 수 없을지라도 다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보라 할 것이므로 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제6호에서 정한 ‘개인정보’에 해당한다.”라고 판시하여,<sup>27)</sup> 이메일 주소를 개인정보로 분류하였음은 물론, 일반적인 관점에서도 “반드시 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.”라고 판시하여,<sup>28)</sup> 개인정보의 범위를 해석이 가능한 가장 넓은 범위로 확대하고 있다.

### 3. 미국의 판례

미국의 경우도 개인정보의 범위에 대하여는 우리 판례와 유사한 태도를 취하고 있는 것으로 보인다. 메사추세츠 지방법원은 *Melissa Tyler v. Michaels Stores, Inc* 사건<sup>29)</sup>에서 “신용카드 결제 시 요구하는 우편번호는 체크카드 결제 시의 개인식별번호인 PIN번호에 상응하는 것이며, 이 때 우편번호가 다른 정보와 결합하여 특정 개인을 식별할 수 있게 되므로, 우편번호를 신용카드번호 및 이름과 결합하여 신용카드단말기에 입력하도록 한 피고의 운영 방법은 신용카드결제양식에서 개인식별정보의 기재를 금지하고 있는 메사추세츠 주법 제105조(a)<sup>30)</sup>의 위반에 해당한다.”라고 판결하였다.

27) 서울중앙지방법원 2007.02.08. 선고 2006가합33062 판결.

28) 대법원 2014.07.24. 선고 2012다49933 판결.

29) MELISSA TYLER vs. MICHAELS STORES, INC.  
<http://masscases.com/cases/sjc/464/464mass492.html>

30) 메사추세츠 주법 제105조(a)항

결제를 위해 신용카드를 받는 개인, 회사, 제휴사, 기업 등은 신용카드 발행자가 요구하지 아니한 개인식별정보를 요청하거나 이를 기재하도록 하여서는 아니된다. 개인식별정보는

## 4. 검토

정보통신기술의 발달로 개인의 식별을 가능하게 하는 수많은 방법들이 개발됨에 따라 개인정보의 범위는 무한히 넓어지고 있다. 예컨대 개인의 위치정보의 경우 과거에는 그 자체만으로 개인에 대한 식별성을 가지지 않았을 것이나, 휴대용 스마트기기의 아이디와 결합한 개인의 위치정보는 개인에 대한 식별가능성 이상의 의미를 갖게 되었다. 컴퓨터에 남겨지는 검색기록 및 쿠키정보나, 수많은 영상장비들에 의하여 수집된 정보도 마찬가지이다.

따라서 개인정보의 인정 범위는 최대한으로 넓게 설정하여 개인의 권익보호를 최대한으로 보장할 수 있도록 하되, 개인정보의 침해 여부를 결정하는 단계에서 개인정보 활용의 필요성, 해당 개인정보에 대한 보호정도, 보호가치 등을 다각적으로 고려하여 보호가 필요한 개인정보에 해당하는지 여부를 검토할 필요가 있다.

예컨대 개인정보의 침해로 인한 손해배상액을 산정하는 단계에서 개인정보 중 민감한 정보, 식별정보와 그렇지 않은 정보를 구별하여 각 정보에 대한 침해로 인한 손해배상액을 산정함에 있어 차등을 두거나 손해발생 여부를 달리 판단하는 방법이 있을 수 있다.

## 제2절 개인정보보호의 법적근거

### I. 헌법적 근거

개인정보보호의 이론적·실정법적 근거에 관하여는 이를 헌법상 사생

---

주소, 전화번호에 한정되지 아니한다.

활의 자유 및 그로부터 유래한 자기정보통제권에서 찾는 것이 일반적이다.

대법원도 보안사의 민간인 사찰에 대한 국가배상소송에서 “헌법 제 10조는 ‘모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 가진다.’라고 규정하고, 헌법 제17조는 ‘모든 국민은 사생활의 비밀과 자유를 침해받지 아니하며, 이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다.”라고 판시하여,<sup>31)</sup> 정보주체의 자기정보통제권을 헌법상 기본권의 하나로 인정하였다.<sup>32)</sup>

헌법재판소 또한 “그러한 헌법 조항들을 적어도 이념적 기초로 삼아 헌법에 명시되지 아니한 기본권으로서 ‘개인정보 자기결정권’을 도출할 수 있다.”라고 실시하여<sup>33)</sup> 개인정보 자기결정권을 헌법에 명시되지 아니한 기본권의 하나라고 판시한 바 있다.

개인정보에 관한 권리가 헌법에 직접 명시되었는지 여부에 관하여는 대법원과 헌법재판소의 판단에 다소 차이가 있지만, 헌법이 보장하는 사생활의 비밀과 자유, 즉 프라이버시의 보장과 개인정보에 관한 권리가 상호 밀접한 관련이 있다는 점에 대하여는 서로 시각이 일치한다고 볼 수 있을 것이다.

---

31) 대법원 1998.7.24. 선고 96다42789 판결.

32) 정상조, 권영준, 전계 논문, 12면.

33) 헌법재판소 2005. 5. 26. 자 99헌마513, 2004헌마190(병합) 결정.

## II. 법률적 근거

### 1. 간접 적용설

위와 같은 헌법의 원칙은 이를 구체화한 법률의 규정에 의해 또는 명문의 규정이 없더라도 사법상의 일반원칙 조항들을 통하여 간접적으로 사인(私人)간에도 적용된다.<sup>34)</sup>

### 2. 민법상 채무불이행책임과 불법행위

우선 거래당사자 사이의 약관 또는 사업자의 개인정보보호정책에 기하여 개인정보보호의무가 인정될 수 있고, 그 위반에 대하여는 채무불이행책임 또는 불법행위책임을 추궁하여 손해배상청구가 가능하다.<sup>35)</sup>

### 3. 개인정보보호법 및 정보통신망법

개인정보보호법은 제4장 및 제5장에서 개인정보처리자에 대한 개인정보의 안전한 관리의무 및 동법 위반행위로 인한 손해배상청구권을 규정하고 있고, 정보통신망법은 제4장에서 정보통신서비스제공자에 대하여 구체적인 개인정보보호의무 및 동법 개인정보보호법과 동일한 손해배상청구권 규정을 명문으로 두고 있으므로, 간접적용설을 따르지 않더라도 개인정보에 대한 보호의무는 현행법 상 사인간에도 당연히 적용이 된다고 할 것이다.<sup>36)</sup>

## 제3절 개인정보의 보호범위

34) 권영성, 『헌법학원론(개정판)』, 법문사, 2008, 329면.

35) 임종인, “개인정보 유출로 인한 기업의 책임”, 상장협연구 제59호 2009. 4., 164면.

36) 임종인, 전제 논문, 164면.

## I. 재산권으로 보는 견해

수집되어 집적·가공된 개인정보는 마케팅의 기초자료로서 기업의 중요한 무형자산으로 됨에 따라, 개인정보 데이터베이스의 재산적 가치가 증대하고 합법이든 불법이든 개인정보의 유통과 활용이 증가하면서, 프라이버시가 획득하게 되는 경제적 가치만을 주목하여 이를 재산권으로 파악하고 재산권에 의한 보호를 적용해야 한다는 견해가 있다.<sup>37)</sup> 이 견해에 따르면 프라이버시를 일종의 재산권의 목적으로 보고, 이를 취득하려는 자는 우선 정보 주체에 대한 청약을 의무적으로 하여야 하고 그 가격은 협상을 통하여 정해질 것이라고 한다.

미국에서는 개인정보에 재산권성을 인정할 수 있다고 하는 것이 일반적이다. 이러한 견해에 따르면 개인정보에 대한 권리는 전통적으로 소극적 의미를 갖는 프라이버시와는 달리, 개인정보를 처분하고 서비스 등 이익을 누릴 수 있는 적극적인 권리에 해당하여 소유권과 유사한 재산권의 일종이라고 설명한다.<sup>38)</sup>

이러한 견해는 개인정보의 수집 등에 이용자의 동의를 요구하는 거래 현실에 부합하고, 정부의 개입보다 시장의 자율적인 규제를 선호하는 영미의 입법정책에도 부합되며, 기존의 물권법과 계약법이론을 적용함으로써 복잡한 입법이나 법리구성 내지 정부의 개입이 불필요하게 된다는 장점이 있다고 한다.<sup>39)</sup>

## II. 인격권으로 보는 견해

---

37) 윤중수, “개인정보보호법제개관”, 정보보호법학회 2008. 9. 27. 세미나 발표논문, 6면.

38) Lawrence Lessig, Code (Basic Books, 1999), p. 160.

39) 정상조, 권영준, 전개 논문, 17면 내지 18면.

우리나라에서는 개인정보를 재산권의 대상으로 파악하는 것이 부적절하다는 것이 일반적이다. 즉 개인정보가 상업적으로 이용된다고 하여 수집되기 전 상태의 개인정보가 재산이라고 하는 것은 논리적 비약이라고 한다.<sup>40)</sup> 또한 개인정보는 해당 정보주체와 불가분의 관계에 있고,<sup>41)</sup> 개인정보는 누군가가 창조한 객체라기보다는 정보주체인 개인의 인격적 표상의 성격이 강하기 때문에,<sup>42)</sup> 재산권이 아닌 인격권으로 새길 수밖에 없다는 것이다. 따라서 이와 같은 정보주체의 자기정보통제권도 인격권에 속한다고 보는 것이 통례이다.<sup>43)</sup>

### III. 판례

국내에서 개인정보의 침해에 관한 소송의 내용을 보면 원고는 대부분 정신적 손해의 배상을 구하고 법원도 이러한 원고의 청구를 인정하는 경우 손해배상으로서 위자료의 지급을 명하고 있다.<sup>44)</sup> 따라서 우리나라의 판례는 개인정보에 대한 권리에 대해 인격적 이익을 그 주된 보호법익으로 삼고 있는 것으로 보인다.<sup>45)</sup>

### IV. 검토

개인의 의사에 반하여 개인정보를 함부로 수집, 유통당하지 아니할 소극적 자유는 인격권을 그 보호법익으로 하여 ‘방해받지 아니할 권리(the right to be let alone)’의 일종으로 파악되어 왔으나,<sup>46)</sup> 컴퓨터

---

40) 정상조, 권영준, 전계 논문, 18면.

41) 임건면, “개인정보의 의의와 귀속관계”, 『중앙법학』, 중앙법학회, 2005. 12, 233면.

42) 정상조, 권영준, 전계 논문, 18면.

43) 임종인, 이숙연, 전계 논문, 218면.

44) 예컨대 대법원 2011. 9. 2. 선고 2008다42430 전원합의체 판결. 위 판결은 변호사 정보 제공 웹사이트 운영자가 변호사들의 개인신상정보를 기반으로 변호사들의 ‘인맥지수’를 산출하여 공개하는 서비스를 제공한 사안에서, 위 인맥지수 서비스 제공행위가 변호사들의 개인정보에 관한 인격권을 침해하는 위법한 것이라고 판시하였다.

45) 정상조, 권영준, 전계 논문, 19면.

터와 정보통신기술의 발달로 비대면 방식의 전자상거래가 활발해짐에 따라 사이버공간에서의 식별을 위하여 정보주체들은 서비스제공자에게 자신의 개인정보를 자발적으로 제공하고 그 반대급부로서 각종 편의 및 맞춤형 서비스를 누릴 수 있게 되었다.

즉 개인정보가 경제적으로 유통, 이용되는 현실을 도외시 할 수 없으므로, 개인정보자기결정권은 순수하게 인격적 이익만 보호한다기 보다는 자신의 개인정보가 영리 목적으로 무단활용 되지 않도록 제어한다는 의미에서 재산적 이익도 부수적으로 보호하는 특수한 형태의 인격권이라고 하는 견해가<sup>47)</sup> 좀 더 현대 정보화 사회의 현실에 부합한다. 다만 위 견해에서도 인격권이 양도의 대상이 될 수 없는 것처럼, 개인정보에 대한 권리도 영원히 양도할 수는 없고 오직 그 사용을 허락할 수 있을 뿐이라고 하는 바,<sup>48)</sup> 위 견해 또한 개인정보자기결정권의 특성을 파악함에 있어서는 인격적 관점을 기초로 하고 있는 것으로 보인다. 따라서 위 견해는 개인정보에 대한 보호범위를 인격권으로 파악하는 연장선상에서 재산적 관점을 참작한 입장으로 평가할 수 있을 것이다.

## 제4절 각국 개인정보법의 입법방향

일반적으로 정보주체는 자신의 개인정보를 인격적인 것으로 인식하는 반면, 개인정보처리자는 개인정보의 인격적 특성과 재산적 특성을 다 함께 고려할 것이다. 개인정보의 어떠한 특성을 우선시하느냐 즉 정보주체에 대한 보호 또는 개인정보에 대한 개인정보처리자의 활용 중 어느 가치를 우선하느냐에 따라 각국의 개인정보에 대한 입장도 달라진다.<sup>49)</sup>

---

46) Samuel D.Warren과 Louis D.Brandeis가 1890년에 발표한 “The Right to Privacy”에서 이와 같이 정의되었다.

47) 정상조, 전계 논문, 607면.

48) 정상조, 전계 논문, 608면.

## I. 개인의 권리보호를 강조하는 입법 유형

호주, 이탈리아 독일 등은 개인정보보호법의 목적을 개인의 프라이버시 및 자유 등의 권리 보호에 두고 법률의 명칭도 ‘프라이버시법’ 또는 ‘데이터보호법’으로 하고 있다. 독일 ‘연방 개인정보 보호법’ 제 1조 제1항도 법의 목적을 “개인정보의 처리 과정에서 개인의 프라이버시 침해를 방지하는 데 있다.”라고 하여 기본적으로 프라이버시 보호를 강조하고 있는 입장이다.<sup>50)</sup>

## II. 개인정보의 유용성을 고려한 입법 유형

OECD, EU, 캐나다, 일본 등에서는 개인정보 보호법의 목적을 개인의 프라이버시, 자유 등과 같은 정보주체의 권리 보호에 한정하지 않고 개인정보 처리가 경제·사회의 발전에 미치는 기여도 함께 고려하도록 요구하고 있다.<sup>51)</sup>

미국도 사적자치의 원칙을 중시하여 정부의 간섭을 최소화한 자유로운 시장경제질서의 유지를 바라는 경제적 관점을 중시하고 있다. 즉, 기업이 자율적으로 개인정보의 보호를 위한 제도를 마련하도록 유도하는 것이 정부가 담당해야 하는 부분으로 생각하고 ‘자율규제 (Self Regulation)’의 방식으로 접근하고자 한다.<sup>52)</sup>

## III. 우리나라의 경우

---

49) 최진혁, 박준석, “개인정보 유출 최소화를 위한 통합 접근통제 모델 연구”, 한국공안행정학회보 제38호(2010), 327면.

50) 이창범, 전게서, 6면.

51) 이창범, 전게서, 7면 내지 9면.

52) 남길현, “국내외 개인정보보호법 동향과 기업의 대응전략,” 정보보호학회지 (2011. 12), 64면.



우리나라의 개인정보보호법의 경우 정보주체의 개인정보에 대한 권리를 보호하는 입법유형 중 가장 진보된 형태로 평가되고 있다. 다만 이러한 규제의 방향이 세계적인 추세에 부합한다고 할 수 있을 것인지는 의문이고, 개인정보의 활용원칙에 대한 논의 또한 향후 개인정보보호법의 개정 과정에서 적극적으로 참작되어야 할 필요성이 있다.

## 제5절 개인정보의 유형 및 개인정보의 분류

### I. 개인정보의 유형

개인정보는 개인의 일반적인 인적사항에서부터 생체·의료, 재산, 고용, 정치적 성향, 교육, 사회참여, 문화생활 등에 이르기까지 매우 다양한 바, 개인정보의 구체적 예를 살펴보면 다음 [표 1]과 같다.

[표 1] 개인정보의 유형 및 구체적 예<sup>53)</sup>

구 분		구체적 예
일반 정보	일반정보	이름, 주민등록번호, 주소, 전화번호, 생년월일, 출생지, 이메일주소, ID·PW, 가족관계 및 가족구성원의 정보, IP주소 등
신체적 정보	신체정보	얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등
	의료·건강 정보	건강상태, 진료기록, 신체장애, 장애등급 등
정신적 정보	기호·성향 정보	도서·비디오 대여기록, 잡지구독정보, 여행 등 활동내역, 식료품 등 물품구매내역, 인터넷 웹사이트 검색내역 등
	신념·사상 정보	종교 및 활동내역, 정당·노조 가입여부 및 활동내역 등
재산적 정보	개인금융 정보	소득정보, 신용카드번호 및 비밀번호, 통장계좌번호 및 비밀번호, 동산·부동산 보유내역, 저축 내역 등

53) 표 출처: 이창범, 김본미, “개인정보 피해구제 및 배상기준에 관한 연구”, 개인정보분쟁조정위원회, 2004, 제25면.

	신용정보	개인신용평가정보, 대출 또는 당보설정 내역, 신용카드 사용액 등
사회적 정보	교육정보	학력, 성적, 출석상황, 자격증 보유내역, 상벌기록, 생활기록부 등
	법적정보	전과·범죄기록, 재판 기록, 과태료 납부내역 등
	근로정보	직장, 고용주, 근무처, 근로경력, 상벌기록, 직무평가기록 등
기타	통신정보	전화통화내역, 인터넷 웹사이트 접속내역, 이메일이나 전화메시지 등
	위치정보	IP주소, GPS 등에 의한 개인위치정보
	병역정보	병역여부, 군번, 계급, 근무부대 등

그리고 최근 몇 년간 기업의 대규모 개인정보 유출사고에서 주로 문제되고 있는 개인정보의 종류를 예시하면 아래 [표 2]와 같다.

[표 2] 최근 개인정보 유출 사고에서 유출된 개인정보

KT 개인정보 유출사고 <sup>54)</sup> (2014. 3.)	이름, 주소, 주민등록번호, 전화번호, 이메일, 신용카드번호, 카드유효기간, 은행계좌번호, 고객관리번호, 유심카드번호, 서비스가입정보, 요금제 관련정보 <sup>55)</sup>
농협, 국민, 롯데카드 개인정보 유출사고 (2014. 1.)	성명, 이메일, 휴대전화, 직장전화, 자택전화, 주민번호, 직장주소, 자택주소, 직장정보, 이용실적금액, 결제계좌, 결제일, 신용한도금액, 신용등급 <sup>56)</sup>
한국 SC은행 개인정보 유출 사고 (2012. 2.)	성명, 주민등록번호, 휴대폰 번호, 유선전화 번호, 이메일, 직장 정보, 연간 소득, 회사 등급, 제2금융권 활성 대출 건수, 최근 3개월 연체카드 수, 최근 연체시작일로부터의 기간, 연체 정보, 최근 6개월 총 조회 건수 <sup>57)</sup>

54) 다만 KT 개인정보 유출 사건의 경우 방송통신위원회가 발표한 위 12개의 개인정보 외에도 “잔여가입비, 핸드폰대금, 보험정보, 할인정보, 주민등록번호, 고객등급, 요금제, 가입 대리점, 최초가입일, 사용하고 있는 서비스, 가입요금제” 등 더욱 광범위한 개인정보가 유출되었다는 반론이 일고 있다.

55) 조선비즈, “KT, 3월 980만명 개인정보 유출에 ‘무혐의’ 처분받아”, 2014. 11. 9.  
[http://biz.chosun.com/site-data/html\\_dir/2014/11/09/2014110901169.html](http://biz.chosun.com/site-data/html_dir/2014/11/09/2014110901169.html)

56) TV 리포트, “국민카드·농협카드·롯데카드, 개인정보유출 어디까지?”, 2014. 1. 18.  
<http://www.tvreport.co.kr/?c=news&m=newsview&idx=451966>

57) 스포츠조선, “한국SC은행, ‘엮힌 데 덮친 격’ 고객정보 또 유출”, 2014. 6. 10.

## II. 개인정보의 분류 방식

### 1. 민감성에 따른 분류

대부분의 개인정보보호 법제들은 민감한 개인정보를 다른 개인정보와 구분하여 다루고 있으므로, 민감한 정보와 그렇지 않은 정보를 구분할 필요가 있다.<sup>58)</sup>

민감한 정보란 예컨대 사상, 종교, 정치적 신념 등의 내면적 정보나 성생활, 전과 등의 개인적·사회적 정보로서 유출로 인해 다른 기본적인 인권 등이 침해될 가능성이 많은 개인정보이다. 개인정보보호법 및 정보통신망법은 이와 같이 개인의 권리, 이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보는 원칙적으로 그 수집을 금지하고 있다(개인정보보호법 제23조 제1항, 정보통신망법 제23조 제1항). 미국에서는 종교, 인종, 정치, 성 관심, 건강, Trade Union Member 등을 민감한 정보로 분류하고 있다.<sup>59)</sup>

### 2. 식별가능성에 따른 분류

개인정보는 개인에 대한 식별자로서 기능하는 정보와 그 식별자에 의하여 당해 개인에 대한 것으로 식별되는 정보로 나누어진다.<sup>60)</sup> 식별 가능한 개인정보는 내용상으로 볼 때, 성명, 주민등록번호, 주소, 가족관계 등의 신분관계정보, 학력, 직업, 전과 등의 사회관계정보, 신용정보, 상거래내역, 소득, 보유재산 등의 경제관계정보, 신장,

---

<http://sports.chosun.com/news-ntype.htm?id=201406120100112350007575&servicedate=20140611>

58) 임종인, 이숙연, 전개 논문, 217면.

59) 전은정, 김학범, 염홍열, “미국의 개인정보보호 법·제도 동향” 정보보호학회지, 제22 권 제1 호, 2012. 2, 49면.

60) 임종인, 이숙연, 전개 논문, 217면.

체중, 병력, 장애, 지문, DNA 등의 심신관계정보, 사상, 종교, 가치관, 정치적 성향 등의 내면관계정보 등으로 구분된다.<sup>61)</sup>

이메일 주소도 “다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보”라고 한 판결<sup>62)</sup>과, 게임사이트의 아이디와 비밀번호에 대하여, “가상공간에서 그 행위자의 인격을 표상한다고 할 것이므로, 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 정보”라고 판시한 판결<sup>63)</sup>이 있고, 정보통신기술의 발달로 개인의 식별을 가능하게 하는 수많은 방법들이 개발됨에 따라 개인정보의 범위는 무한히 넓어지고 있으므로 식별가능정보의 개념 범위는 앞으로도 더욱 넓어지게 될 것으로 보인다.

### 3. 민감성과 식별가능성을 종합하여 개인정보를 분류하는 견해

이와 같이 개인정보의 민감도 및 식별력에 따라 개인정보의 중요도를 평가함에 있어서 참작이 가능한 연구로써 개인정보를 크게 민감정보, 활동정보, 속성정보로 분류하고 유출 시 개인정보의 피해 정도에 따라 개인정보의 중요도에 따른 등급 분류 기준을 3등급으로 분류하는 견해가 있다.<sup>64)</sup>

이 견해에 의하면 우선, 사상, 신조, 성생활과 같이 개인정보 유출 시 헌법상 보장된 기본권을 심각하게 침해 받을 수 있는 개인정보는 중요도 1등급으로 분류된다. 다음으로, 속성정보가 포함된 활동정보와 고유식별정보는 중요도 2등급으로 분류된다. 마지막으로, 속성정보가 없는 민감정보, 활동정보, 가변정보, 비식별정보 등이 중요

---

61) 윤중수, 전제 논문, 2면 내지 3면.

62) 서울중앙지법 2007. 2. 8. 선고 2006가합33062, 53332 판결.

63) 대법원 2005.11.25. 선고 2005도870 판결.

64) 차건상, “개인정보 유출에 따른 손해배상액 산정기준에 관한 연구”, 숭실대학교 박사학위논문, 2012. 13면.

도 3등급으로 분류된다. 다만 민감정보와 속성정보가 연계될 경우 민감도는 높은 등급으로 조정된다고 한다.<sup>65)</sup> 이를 정리하면 아래 [표 3]와 같다.

[표 3] 개인정보의 중요도에 따른 분류방식<sup>66)</sup>

중요도	정보 구분	예 시
1등급 (높음)	속성정보가 포함된 민감정보	(주민등록번호, 이름 + 신조), (주민등록번호, 이름 + 건강정보), (이름, 주소, 연령 + 성생활), (주민등록번호, 이름 + 범죄정보) 등
2등급 (보통)	속성정보가 포함된 활동정보	(주민등록번호, 이름 + 신용상태), (이름, 회사명 + 근무평가기록), (이름, 출신학교, 학번 + 성적), (주민등록번호, 이름 + 출입국내역), (주민등록번호, 이름 + 납세내역)
	속성정보(고유 식별정보 포함)	주민등록번호, 이름, 주소, 고향, 출신학교 등
3등급 (낮음)	속성정보가 없는 민감정보, 활동정보 등	신조, 건강정보, 성생활 정보 등
	가변정보, 비식별정보	나이, 성별, 혈액형, 체중 등

#### 4. 검토

이러한 개인정보의 분류의 의미는 민감도, 식별성이 높은 개인정보의 침해는 필연적으로 높은 손해배상으로 연결된다는 점에 있을 것이다. 본 논문에서는 개인정보 자체를 재산적 가치가 내포된 특별한 인격권으로 접근하는 입장에서, 유출된 개인정보에 대한 가치평가를 개인정보의 유출로 인한 손해배상액 산정의 출발점으로 삼았다.

65) 차건상, 전계논문, 13면.

66) 표 출처: 차건상, 전계논문, 14면.

## 제3장 개인정보의 유출

### 제1절 개인정보 유출의 의미

#### I. 서설

개인정보보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 하여 개인정보처리자의 안전조치의무를 부과하고 있다. 한편 개인정보보호법 제39조는 “정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다”라고 하여 안전조치의무 위반으로 인하여 손해를 입은 정보주체는 개인정보처리자에 대하여 손해배상을 청구할 수 있다.

그런데 안전조치의무 위반으로 인하여 개인정보가 분실·도난·유출·변조 또는 훼손되는 경우 언제나 손해배상책임이 인정되는지에 대해서는 의문의 여지가 있다. 특히 문제가 되는 것이 개인정보의 유출이다. 보호조치의무 위반으로 개인정보가 유출되더라도 그것으로 인하여 반드시 손해가 발생하는 것은 아니며, 근본적으로 과연 어떤 상태를 유출로 규정할 것인지에 대해 논란이 있기 때문이다.<sup>67)</sup>

#### II. 학설

유출 또는 누출에 관하여 확립된 개념정의가 존재하지는 않으나, 정

---

67) 이원우, 전제 논문, 239면.

보통신망법 제28조의2의 누설과 구별되는 유출은 제3자에 의한 열람가능성 내지 이용가능성이라는 위험을 야기하거나 위험을 증대시키는 행위이지 그 자체로서 정보주체에게 어떠한 손해를 야기하는 것은 아니다. 누설이란 제3자가 이를 인식하도록 하는 결과까지를 포함하지만, 유출은 그러한 결과를 요하지 않기 때문이다. 따라서 유출은 그 자체만으로는 손해배상책임의 원인행위로 인정될 수 없으며, 유출로 인하여 현실적인 손해가 발생한 경우에만 손해배상책임이 문제될 수 있다는 견해가 있다.<sup>68)</sup>

### III. 판례의 태도

리니지Ⅱ 사건의 항소심 판결<sup>69)</sup>에서 정보통신망법 제28조의 “누출”의 의미가 실시된 이후 다수의 판결에서 누출 또는 유출의 의미를 동일하게 파악하고 있다.<sup>70)</sup> 위 판결에 의하면 “누출이라 함은 일반적으로 ‘액체나 기체 따위가 밖으로 새어 나오는 것 또는 그렇게 하는 것’, ‘비밀이나 정보 따위가 밖으로 새어 나가는 것’을 말하는 점과 정보통신망법이 누출을 침해, 누설, 도용과 구분하여 규정하고 있는 취지에 비추어 보면, 개인정보가 정보통신서비스제공자 및 이용자의 개인정보 관리·통제권의 범위를 벗어나 당해 개인정보를 모르는 제3자가 그 내용을 알 수 있는 상태를 이르는 것을 의미한다고 봄이 상당하고, 나아가 침해, 누설, 도용의 경우처럼 당해 개인정보를 모르는 제3자가 현실적으로 그 내용을 알게 되었다거나 적어도 이와 동일시할 수 있는 정도의 구체적이고 현실적인 고도의 위험이 발생할 것 또는 당해 개인정보를 모르는 제3자에게 그 내용을 알릴 것 또는 이를 도용할 것까지 요구하는 것은 아니라고 볼 것이다.”라고 한다.

---

68) 이원우, 전제 논문, 246면.

69) 서울중앙지방법원 2007. 1. 26. 선고 2006나12182 판결.

70) 서울중앙지법 2006가단378591, 서울중앙지법 2008가합75268, 서울고등법원 2009나119131 판결 등.

위 판결에서는 이러한 전제하에서 원고들을 불특정 다수가 사용할 수 있는 피시방 컴퓨터를 사용한 원고들과, 가정용 PC를 사용한 원고들로 구분하고 ① 피시방 컴퓨터를 이용한 원고의 경우 원고들의 아이디 및 비밀번호가 담긴 로그파일이 저장됨으로써 컴퓨터에 관한 일정 수준의 지식이 있는 제3자라면 누구라도 로그파일에 접근하여 위 원고들의 아이디 및 비밀번호를 알 수 있는 상태에 이르렀으므로, 위 원고들의 개인정보는 누출되었다고 봄이 상당하다고 판단하였으나, ② 집에서 사용하는 개인용 컴퓨터를 이용한 원고들의 경우 개인정보 관리·통제권의 범위를 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르렀다고 보기 어려우므로, 위 원고들의 개인정보는 누출되지 않았다고 봄이 상당하다고 판단하였다.

또한 LGT사건의 상고심<sup>71)</sup>에서 대법원은 “어느 개인정보가 정보통신서비스 제공자의 관리·통제 하에 있고 그 개인정보가 제3자에게 실제 열람되거나 접근되지 아니한 상태라면, 정보통신서비스 제공자의 기술적·관리적 보호조치에 미흡한 점이 있어서 제3자가 인터넷상 특정 사이트를 통해 정보통신서비스 제공자가 보관하고 있는 개인정보에 접근할 수 있는 상태에 놓여 있었다고 하더라도 그것만으로 바로 개인정보가 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 되었다고 할 수는 없다.”라고 하여, 개인정보가 개인정보처리자의 서버에 그대로 보관되어 있고, 원고들의 휴대폰번호가 해당 서버에 입력되었는지 여부가 확인되지 않은 이상, 개인정보가 유출된 것이 아니라고 판시하였다.

#### IV. 검토

판례의 태도는 분명하지는 않으나, 개인정보가 개인정보처리자인 서

---

71) 대법원 2014.5.16. 선고 2011다24555,24562 판결.



비스제공자의 관리·통제 하에 있었던 경우에는 개인정보의 유출 자체를 인정하지 않았고, 개인정보가 서비스제공자의 영역을 벗어나서 불특정다수인이 열람할 수 있는 영역으로 진입한 경우에는 유출을 인정한 것으로 분석된다. 반면 개인정보가 서비스제공자의 영역을 벗어났지만 여전히 개인정보주체의 관리·통제 하에 있었던 경우는 유출이 인정되지 않는다고 판단하였다.

즉 판례는 개인정보 사고 발생으로 인하여 개인정보의 제3자에 의한 열람가능성 내지 이용가능성이라는 위험이 실질적인 정도로 입증되는 경우에만 개인정보의 유출을 인정하는 것으로 보인다. 이러한 판례의 태도는 손해발생 여부 판단에 선행하여 유출 여부를 판단을 실시하였다는 점에서 논리적으로 타당하다.

## 제2절 개인정보의 유출로 인한 기업의 책임

### I. 형사책임

개인정보보호법 제29조는 개인정보처리자에 대하여 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하면서, 이를 위반한 경우에 대해 제73조 제1호에서 2년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하였다. 정보통신망법 제28조에서도 정보통신서비스제공자 등으로 하여금 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 기술적·관리적 조치를 하여야 한다고 규정하고 있으며, 마찬가지로 이를 위반한 경우에 대하여 제73조 제1호에서 2년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하였다.

그러나 이러한 형벌규정에 따른 실제 형사처벌은 미미한 수준에 그치므로 수백만, 수천만 개인정보의 유출사고 앞에서 이 규정은 그다지 큰 힘을 발휘하지 못한다. 또한 기술이 발전하고 시장이 변화하는데 처벌법규는 죄형법정주의 원칙에 따라서 확대 내지 응용될 수 없기 때문에 예상하지 못한 개인정보침해 행위 유형은 처벌될 수 없다고 하는 한계도 존재한다.<sup>72)</sup>

## II. 행정상의 책임

### 1. 개인정보보호법 상 과징금의 부과

#### 가. 과징금 부과 원칙

개인정보보호법 제34조의2는 “안전행정부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·변조 또는 훼손된 경우에는 5억 원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.”라고 규정하여 개인정보 중 주민등록번호가 유출된 경우에 한하여 과징금을 부과하는 규정을 두고 있다.

다만 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조 제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 과징금을 부과하지 아니하고, 과징금을 부과하는 경우에는 ① 제24조 제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도, ② 분실·도난·유출·변조 또는 훼손된 주민등록번호의 정도, ③ 피해확산 방지를 위한 후속조치 이행 여부를 고려할 수 있도록 하고 있다.

---

72) 정상조, 전게 논문, 618면.

## 나. 과징금의 산정 방식<sup>73)</sup>

### (1) 1단계

개인정보보호법 시행령 별표1의2는 주민등록번호의 유출사고를 매우 중대한 위반행위, 중대한 위반행위, 일반 위반행위의 3가지로 분류하고, ① 고의 또는 중과실로 인하여 10만 건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손된 경우인 “매우 중대한 위반행위”에 대해서는 과징금의 기본액을 3억 5천만원으로 하고, ② 고의 또는 중과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우 및 경과실로 인하여 10만 건 이상의 주민등록번호가 분실 등이 된 경우인 “중대한 위반행위”에 대해서는 산정기준액을 2억 3천만원으로 하고 있으며, ③ 경과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우인 “일반 위반행위”에 대하여는 1억 원을 산정기준액으로 규정하고 있다.

### (2) 2단계

나아가 과징금에 대한 1차 조정과정에서는 개인정보보호법 제24조 제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도, 피해를 최소화하기 위한 대책 마련 등 피해확산 방지를 위한 후속조치 이행 여부를 고려하여 산정기준액의 100분의 50의 범위에서 가중하거나 감경한다.

---

73) 공정거래위원회 과징금 부과 세부기준 등에 관한 고시(개정 2014. 5. 30. 공정거래위원회 고시 제2014- 7호)에 의하면 과징금 부과 시에는 다음의 절차를 거친다. 이 중 일정요소는 개인정보보호의무 위반으로 인한 과징금 산출 시에도 참작이 가능할 것이다.

1. 위반행위 유형에 따른 기본 산정기준, 2. 위반행위의 기간 및 횟수 등에 따른 조정, 3. 위반사업자의 고의·고실 등에 따른 조정, 4. 부과과징금, 5. 관련매출액, 6. 위반기간, 7. 평균매출액(영 제9조 관련), 8. 위반액, 9. 사업자단체 연간예산액, 10. 부당이익

### (3) 3단계

2차 조정과정에서는 위반행위의 기간 및 횟수, 위반 행위에 대한 조사 협조 여부, 위반행위에 따른 추가적 피해 발생 여부, 평소 개인 정보 보호를 위한 노력 정도 등을 종합적으로 고려하여 1차 조정된 금액의 100분의 50의 범위에서 가중하거나 감경한다.

### (4) 4단계

개인정보처리자의 현실적 부담능력이나 그 위반행위가 미치는 효과, 위반행위로 인하여 취득한 이익의 규모 등을 고려하여 볼 때 과중하다고 인정되는 경우에는 2차 조정된 금액의 100분의 50의 범위에서 감액하여 부과과징금으로 정할 수 있다.

## 다. 검토

이상의 규정은 주민등록번호의 분실 등에 한정되어 적용될 것을 예정하고 있으나, 개인정보보호법은 개인정보보호에 위험이 발생하게 한 경우에 대하여 개인정보처리자에 대한 법적 책임 추궁과정에서 위와 같은 논리적 단계를 거쳐 책임의 크기를 산출하였음을 알 수 있다.

## 2. 정보통신망법 상 과징금의 부과

### 가. 과징금 부과 원칙

정보통신망법은 개인정보보호의무 미이행에 대해 방송통신위원회로 하여금 기업들에게 과징금을 부과할 수 있도록 하고 있는데, 정보통신망법 제64조의3(과징금의 부과 등)에서는 각 호의 어느 하나에 해

당하는 행위가 있는 경우에는 방송통신위원회가 해당 전기통신사업자에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있도록 하고 있다.

## 나. 과징금의 산정 방식

정보통신망법은 방송통신위원회가 제1항에 따른 과징금을 부과할 때 ① 위반행위의 내용 및 정도, ② 위반행위의 기간 및 횟수, ③ 위반행위로 인하여 취득한 이익의 규모 등을 종합적으로 고려하도록 규정하고 있다. 즉, 기업들의 위반행위가 과중하거나 반복적으로 위반했을 경우, 또한 위반행위로 인한 경제적 이익이 클수록 더 많은 과징금을 부과하도록 하고 있다.<sup>74)</sup>

과징금의 구체적인 산출방식은 우선 ① 관련 매출액<sup>75)</sup>을 산정하고, ② 그 금액에 일정한 부과기준율을 곱하여 기준금액을 산정한 후, ③ 필수적 가중 및 추가적 가중·감경 단계를 거쳐 ④ 최종 부과 과징금을 산정하는 방식을 취하고 있다.

기본과징금은 대상 사업자의 관련매출액과 위반행위의 중대성에 따라 0.5% ~ 0.9%의 부과기준율을 곱해 산정하는데 위반행위의 중대성은 일반 위반행위, 중대한 위반행위, 매우 중대한 위반행위 3가지로 구분하고, 그 판단은 원인과 결과를 단계별로 고려하는 방식을 적용한다.<sup>76)</sup>

과징금 위반 기간 및 횟수에 따라 50% 범위에서 기본과징금을 가

74) 임종인, 전계 논문, 175면.

75) 정보통신망법은 과징금 부과 시 전기통신사업자가 매출액 산정자료의 제출을 거부하거나 거짓 자료를 제출한 경우에는 해당 전기통신사업자와 비슷한 규모의 전기통신사업자의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있도록 하고 있다.

76) 김일환, 김민호, 지성우, 전계 논문, 129면.

중·감정하는 의무조정방식을 운영한다. 이에 따라 최초 법규 위반행위자는 50% 감경해주고, 위반기간에 따라 1~2년은 20%, 2년 초과기간은 50%로 과징금을 가산한다.<sup>77)</sup>

이와 함께 방송통신위원회는 50% 범위에서 의무적 조정과징금을 가중·감경 할 수 있는 재량권도 가지고 있으므로, 방송통신위원회가 인정하는 개인정보보호인증을 받은 경우에는 50% 이내, 개인정보위반 관련조사에 적극 협력한 경우에는 30% 이내에서 과징금을 감액할 수 있다. 반면에 자료제출 거부 등 조사를 방해하거나 또는 이용자에게 허위진술을 요청한 경우, 다수 사업자가 관련된 위반행위를 주도하거나 선도한 경우에는 각각 30%, 20% 내로 과징금이 증액될 수 있다.<sup>78)</sup>

### 3. 검토

방송통신위원회의 ‘최근 4년간 주요 개인정보 유출사고 현황’에 의하면 방송통신위원회 소관 민간기업의 개인정보 유출은 최근 4년간 1억 620만건이었지만, 부과된 과징금은 177억 7,300만원에 불과했다.<sup>79)</sup> 이는 개인정보 유출이 국민 1인당 2.1회, 1건당 과징금 166원에 불과하다는 결론이 된다. 이와 같은 현실에서 볼 수 있듯이, 개인정보유출에 대한 과징금 부과 등 행정처분은 개인정보 유출사고의 대형화 경향에 비하여 여전히 소극적 수준에 머무르고 있으며,<sup>80)</sup> 더군다나 과징금은 정보주체에 대하여는 아무런 경제적 보상을 제공하지 않는다는 점에서 기능적 한계가 있다.

---

77) 김일환, 김민호, 지성우, 전계 논문, 129면.

78) 김일환, 김민호, 지성우, 전계 논문, 129면.

79) 국민일보, “1억620만건 개인정보 유출에 과징금은 177억에 불과, 166원 하는 개인정보”, 2014. 10. 14. 자 기사.

<http://news.kmib.co.kr/article/view.asp?arcid=0008760647&code=61121111&cp=nv>

80) 윤주희, 전계 논문, 348면

### Ⅲ. 손해배상책임

개인정보의 유출이나 도용 등의 위법한 행위로 인하여 제3자에게 손해를 입힌 경우에는 불법행위로 인한 손해배상책임을 부담할 수 있다. 개인정보보호법을 비롯한 개인정보에 관한 대부분의 현행법은 개인정보처리자에게 범위반으로 인한 손해배상의무를 규정하고 있을 뿐만 아니라, 사업자가 고의 및 과실이 없었다는 점을 입증하지 않는 한 배상책임을 진다고 하는 입증책임의 전환에 관한 규정까지 두고 있다. 손해배상책임과 관련하여서는 제4장에서 상세히 설명하기로 한다.

### 제3절 개인정보 유출사고 사례

인터넷 이용자의 폭발적 증가와 인터넷 환경의 급속한 발달에 따라 개인정보에 대한 집중 관리와 대량 통제가 용이하게 된 반면, 그에 따른 대규모 개인정보 유출 사례가 국내·외를 막론하고 빈번하게 발생하고 있다.

특히 개인정보를 취급하는 기업이나 조직의 개인정보 유·노출 등의 침해사고가 빈번해지고 있고, 근래에는 수천만명 단위의 대규모 개인정보 유·노출 사고가 연이어 발생하는 등 사회적 손실과 더불어 개인의 피해범위가 확대가 문제되고 있다.<sup>81)</sup>

이하에서는 최근 수년간 발생한 국내 주요 개인정보 유출사례들을 간략히 정리하였다.

#### I. 손해배상책임 인정 사례

---

81) 권홍 외 3, “CVM을 이용한 국내 개인정보 침해사고의 위자료 산정”, 정보보호학회논문지 제22권 제2호, 2012. 4. 368면.

## 1. 리니지Ⅱ 사건<sup>82)</sup>

① 2005. 5. 11. 피고 엔씨소프트의 직원이 리니지Ⅱ 게임의 네트워크 정기점검 작업을 하는 과정에서 이용자들의 게임 아이디와 비밀번호가 이용자들이 사용하는 컴퓨터의 하드디스크 로그파일에 기록 되도록 하는 실수를 하였고, 엔씨소프트는 2005. 5. 16. 12:00 경에서야 그와 같은 사고가 발생한 사실을 인식하고 더 이상 이용자의 아이디와 비밀번호가 기록되지 않도록 하는 조치를 취한 사건이다.

② 아이디와 패스워드의 노출로 인해 원고들에게 현실적으로 발생한 경제적 손해는 확인되지 않았고, 원고들은 정신적 손해의 배상을 구하였다.<sup>83)</sup>

③ 법원은 아이디와 비밀번호는 가상공간에서 그 행위자의 인격을 표상한다고 할 수 있으므로 당해 개인을 알아볼 수 있는 개인에 관한 정보에 해당하고 피고 회사는 원고들의 개인정보가 누출되지 않도록 하여야 할 주의의무를 위반한 결과 원고들의 기본권인 자신들의 의사에 반하여 개인정보가 함부로 공개되지 아니할 권리를 침해하였으므로 원고들에게 위자료를 지급할 의무가 있다고 판결하였다.<sup>84)</sup>

④ 원고들 중 PC방과 같이 일반 다중이 이용할 수 있는 컴퓨터가 아닌 개인용 컴퓨터를 이용해서 게임에 접속했던 원고들에 대해서는 원고들의 개인정보가 원고들의 개인정보 관리·통제권의 범위를 벗어나서 제3자가 그 내용을 알 수 있는 상태에 이르렀다고 보기

---

82) 또는 엔씨소프트 사건, 대법원 2008. 8. 21. 선고 2007다17888 판결.

83) <http://cafe.naver.com/cardleak/150>

84) 윤주희, 전제 논문, 330면



어려우므로 원고들의 개인정보는 누출되지 않았다고 판단하였고, PC방을 사용하여 개인정보의 누출이 인정되는 다른 원고들에 대해서 10만원의 위자료를 인정하였다.

## 2. 국민은행 사건<sup>85)</sup>

① 피고 국민은행 직원이 복권서비스 이용계약을 체결한 가입회원들에게 서비스 안내 메일을 발송하는 과정에서 2006년 3월 15일 회원 32,377명의 성명, 주민등록번호, 이메일 주소 등이 수록된 텍스트 파일을 이메일 첨부파일로 전송한 사고로서 해당 직원은 이메일 전송 후 회원정보가 이메일에 첨부된 사실을 알고, 이메일 전송을 강제 중단하였으나 이미 3,723명의 회원들에게 이메일 발송이 완료된 사건이다.<sup>86)</sup>

② 법원은 피고 국민은행이 고객들의 개인정보가 누출되지 않도록 필요한 관리적 조치를 다하여야 할 주의의무를 위반하여 이용자들의 권리가 침해되었기 때문에 정신적 고통에 대한 손해를 배상할 의무가 있다고 판결하였다. 이에 따라 성명, 주민등록번호, 이메일주소의 정보가 누출된 원고들에게는 20만원을, 성명과 이메일 주소가 누출된 원고들에게는 10만원의 위자료를 지급하도록 하였다.

## 3. LG전자 사건<sup>87)</sup>

① 피고 LG전자가 2006년 9월 3일 2006년도 하반기 신입사원 채용 공고를 하고, 2006년 9월 4일부터 2006년 9월 19일까지 채용사이트를 통하여 인터넷으로 신입사원 지원을 받았는데, 입사지원자들은

---

85) 서울고등법원 2007. 11. 27. 선고 2007나33059 판결.

86) 윤주희, 전계 논문, 331면.

87) 서울고등법원 2008. 11. 25. 선고 2008나25888 판결.

채용사이트에 입사지원서를 작성하여 제출하였다.

② 채용심사과정에서 서류전형에 불합격통지를 받은 지원자 중 한 명이 포털사이트 다음의 취업정보 공유카페 게시판에 LG전자의 모든 지원자에 대하여 조회가 가능한 링크파일을 첨부하여 게시하였는데 이 주소에 접속하면 입사지원자들의 사진이 나타나고 사진을 클릭하면 기본인적사항(성명, 주민등록번호 등)과 상세인적사항(학력, 학점 등), 자기소개, 경력, 연구실적 등의 하부메뉴가 있는 페이지가 나타났다. 이 글의 조회수가 3,056회에 달하게 되어 결국 3천여 명의 입사지원자의 개인정보가 누출된 사건이다.<sup>88)</sup>

③ 이에 피해자들이 제기한 소송에서 법원은 LG전자는 입사지원자들의 개인정보에 대하여 유출되거나 훼손되지 않도록 당시의 기술 수준에 부합하는 보안조치를 취하여야 할 주의의무가 있음에도 이를 위반하였다고 판단하였으나, 입사지원을 위한 등록정보를 실제로 열람당한 원고들에게 30만원의 위자료를 인정하고, 단순히 열람당할 가능성이 있었던 다른 원고들의 경우에는 위자료 지급을 인정하지 않았다.

#### 4. SK브로드밴드 사건<sup>89)</sup>

① 피고 하나로텔레콤이 자사 서비스에 가입하거나 이미 계약을 해지한 고객 600여만 명의 개인정보 8500만여 건을 텔레마케팅 업체, 금융기관 등에 제공한 사건이다. 하나로텔레콤은 SC제일은행과 신용카드 회원모집제휴계약을 맺은 뒤 통신상품 가입고객의 개인정보 96만건을 신용카드 회원을 모집하는 판촉업체에게 제공하였고, 자회사인 하나로텔레세일즈를 통해 회사 차원에서 고객정보를 불법적으

---

88) 윤주희, 전계 논문, 332면.

89) 또는 하나로텔레콤 사건, 서울고등법원 2013. 2. 7.선고 2011나83747 판결 등.

로 관리한 것으로 밝혀졌다.<sup>90)</sup>

② 법원은 1심과 항고심에서 모두 하나로텔레콤에 대해 개인정보자기결정권은 자신의 의사에 반해 개인정보가 함부로 공개되거나 사용되지 않도록 하는데 그 본질이 있으므로 SK브로드밴드는 이용자들의 동의를 얻지 않고 텔레마케팅업체에게 개인정보를 제공해 이용자들의 개인정보자기결정권을 침해하였다고 판단했다. 그리고 SK브로드밴드가 제공한 개인정보를 토대로 위탁업체가 텔레마케팅을 실시해 이용자인 원고들이 정신적 고통을 당한 것이 인정되므로 동의 없이 개인정보가 제공된 경우 20만원, 동의했지만 동의 범위 외의 외부업체에게 개인정보가 제공된 경우 10만원의 손해배상을 하도록 판결하였다.

## 5. KT 사건<sup>91)</sup>

① 해커 두 명이 피고 KT 고객정보 조회시스템을 해킹하는 프로그램을 제작해 KT고객 영업시스템에 무단으로 접속하여 870만명의 고객정보를 빼낸 사건이다. 이들은 2011년 8월부터 2012년 4월까지 KT고객들의 주민등록번호, 휴대폰번호, 고객명, 기기모델명, 요금제, 매월 사용료 등의 개인정보를 빼내었고, 유출시킨 개인정보를 휴대폰 텔레마케팅 사업자 등에게 매도한 사건이다.<sup>92)</sup>

② 1심 법원은 정보유출자들이 사용한 해킹의 수법, 해킹방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도, 개인정보 유출로 인해 이용자가 입게 되는 피해의 정도 등을 종합하면, 피고는 정보통신서비스 제공자로서 이 사건 정보유출사고로 원고들의 개인정보가 누

---

90) 윤주희, 전계 논문, 333면.

91) 서울중앙지방법원 2014. 8. 22. 선고 2012가합81628 판결.

92) 윤주희, 전계 논문, 336면.

출되는 것을 방지하기 위한 선량한 관리자로서의 주의의무를 다하지 못하였다고 평가한 후 원고들에 대하여 10만원의 위자료 지급의 무가 있다고 판단하였다.

## 6. SK커뮤니케이션즈 사건

2011년 7월 28일 네이트와 싸이월드 회원정보가 저장된 데이터베이스가 해킹당하면서 3,500만명에 달하는 개인정보가 유출된 사건이다. 이 사건에 대해서는 피고 SK커뮤니케이션즈에 대해 손해배상책임을 인정한 판례와 부정한 하급심 판례가 동시에 존재한다.

### (1) 인정 판례<sup>93)</sup>

서울서부지방법원은 개인정보 3500만 여 건이 여러 단계를 거쳐 외부로 유출되었는데도 SK커뮤니케이션즈 탐지 시스템이 전혀 감지하지 못했으며, 기업형 알집보다 보안상 취약한 공개용 알집을 사용해 해킹이 더 쉽게 이뤄지도록 했고 담당 직원이 로그아웃하지 않고 새벽까지 컴퓨터를 켜둬 해커가 쉽게 서버에 접근할 수 있도록 하는 등 개인정보 보호업무를 소홀히 해 생긴 손해로 20만원을 배상해야 한다고 판결하였다.<sup>94)</sup>

### (2) 부정 판례<sup>95)</sup>

반면 서울중앙지방법원은 SK커뮤니케이션즈 직원의 무료 공개용 프로그램 이용과 이 사건 해킹 사고·손해발생 사이에 인과관계가 존재하지 않고, 백신소프트웨어 운용, 불법 접근 탐지·방지를 위한 시스

---

93) 서울서부지방법원 2013. 2. 15. 2011가합11733 판결.

94) 윤주희, 전계 논문, 335면.

95) 서울중앙지방법원 2012. 11. 23. 선고 2011가합90267 판결.

템 설치 및 운용, 망 분리 조치, 공인인증서 등 추가적인 인증수단 적용 조치 등과 관련하여 SK커뮤니케이션즈가 정보통신망법 등 관련 법령에서 요구하는 기술적·관리적 보호조치를 이행하지 않았다고 보기는 어려우며, 피고 SK컴즈가 사용한 MD5 방식이 구식이어서 상대적으로 해독 가능성이 크더라도 이러한 사정만으로 암호화 기술사용 관련 기술적·관리적 보호조치를 위반한 것으로 보기 어렵다고 판결하였다.

## II. 손해배상책임 부정 사례

### 1. LG텔레콤 사건<sup>96)</sup>

① 벨소리 다운로드 서비스사이트인 엠샵에서 피고 LG텔레콤 가입자의 전화번호를 입력할 경우, 핸드폰의 지원가능컬러나 액정사이즈 등의 정보만 제공되어야 하는데 상태표시줄에 해당 번호의 주민등록번호와 핸드폰기종, 핸드폰가입일 등 중요한 개인정보가 노출된 사건이다.<sup>97)</sup>

② 1심 법원은 LG텔레콤이 수많은 가입자의 개인정보를 수집·이용하고 있음에도 보안이 취약한 시스템을 운영하는 등 주의의무를 위반하였으므로 원고 1인당 5만원의 위자료를 지급할 의무가 있다고 판단하였으나, 항소심에서는 LG텔레콤이 개인정보가 유출될 수 있다는 사실을 알고 즉각 개인정보 조회가 가능한 홈페이지를 차단하는 등 필요한 조치를 취했고 원고가 입은 정신적인 피해가 없는 이상 손해배상청구는 받아들일 수 없고 CP사의 사용자 인증과정에서 이미 주민등록번호를 제공하는 것에 동의했다고 볼 수 있으며 LG텔레콤이 부주의나 소홀로 원고의 개인정보가 제공되었다고 볼 수도

---

96) 대법원 2014.5.16. 선고 2011다24555,24562 판결.

97) 윤주희, 전계 논문, 332면.

없다고 판결하였다.<sup>98)</sup>

③ 대법원에서는 웹사이트의 폰정보 조회 페이지에 휴대폰번호를 입력하기 전에는 개인정보는 서버에 그대로 보관된 채 아무런 접근이 이루어지지 않으며 회사가 관리·통제권을 행사하여 위 웹사이트와 서버가 더 이상 연동하지 않도록 함으로써 개인정보에 대한 접근과 전송 가능성을 없앨 수 있었던 상태에 있었으므로, 휴대폰번호가 위 웹사이트의 폰정보 조회 페이지에 입력되었는지가 확인되지 않은 상황에서 위 웹사이트와 서버가 연동하고 있었다 하더라도 개인정보가 회사의 관리·통제권을 벗어나 제3자가 내용을 알 수 있는 상태에 이르게 되었다고 볼 수 없다고 판단한 후, 개인정보의 유출 자체를 인정할 수 없다고 판결하였다.<sup>99)</sup>

## 2. 다음 사건<sup>100)</sup>

① 피고 다음은 2008년 7월 22일 한메일 서비스의 보안기능을 개선하는 작업으로서 다음에 접속하면 본인의 마지막 로그인 기록을 보여주는 기능을 추가한 프로그램을 개발해 이용자들에게 배포했다. 그런데 프로그램에 오류가 발생해 동시간대에 다음 서버에 접속한 이용자들이 어떤 서비스를 요청한 경우 마지막에 서비스를 요청한 이용자들의 이메일 정보가 동시에 접속한 다른 이용자들에게 노출된 사건이다.<sup>101)</sup>

② 법원은 2010년 8월 11일 접속기록 등에 의하면 원고들은 당시 사고로 자신의 메일 내용이 공개되거나 자신의 메일에 첨부된 파일을 다른 사람이 다운로드한 경우에 해당하지 않는다면 손해가 발생

---

98) 서울고법 2011. 2. 10. 선고 2009나119131, 119148 판결.

99) 대법원 2014.5.16. 선고 2011다24555,24562 판결.

100) 서울중앙지방법원 2010. 8. 11. 선고 2008가단407653 판결, 불항소로 1심 확정.

101) 윤주희, 전계 논문, 332면.

했다는 사실을 인정할 증거가 없고, 프로그램의 제작, 배포과정 및 그 후 사고수습 과정에서 주의의무를 위반했음을 인정하기에 부족하며, 이 사고에 대해서 사업자가 개인정보보호를 태만히 해 발생한 것으로 볼 수 없고, 현재의 기술 수준과 경제성에 비쳐 프로그램 개발 과정에서 버그발생 가능성을 완전히 배제하는 것은 거의 불가능하다는 것을 이유로 원고의 청구를 기각하였다.

### 3. 옥션 사건<sup>102)</sup>

① 중국인 해커로 추정되는 자가 피고 옥션의 데이터베이스 서버에 2008년 1월 4일부터 2008년 1월 9일까지 침입하여 이 서버에 저장되어 있던 옥션회원 약 1천 800만명의 성명, 주민등록번호, 주소, 전화번호, 아이디 등 개인정보를 해킹한 사건이다.<sup>103)</sup>

② 법원은 정보통신서비스제공자가 이용자로부터 수집한 개인정보를 해킹으로 인해 도난당하지 않기 위하여 선량한 관리자로서 취해야 할 기술적·관리적 조치의무를 준수하여야 하고 이러한 조치를 취한 옥션에 대해서는 손해배상책임을 물을 수 없다고 판결하였다.

③ 즉 옥션이 관련법에 정해진 기준을 어겼다고 볼 근거가 없고 옥션이 방화벽을 설치하지 않았다는 원고 측 주장에 대해서 법이 정한 의무사항이 아니며 당시 다수 업체가 방화벽을 신뢰하지 않아 이용하지 않은 점을 고려하면 잘못이라고 보기 어렵다고 하면서 옥션이 해킹을 막지 못한 아쉬움이 있더라도 해킹 기술 발전과 사건 당시 옥션의 보안조치 내용들을 종합적으로 따져볼 때 옥션에 민법상 불법행위에 해당하는 과실이 있다고 보기 어렵다고 판단하였다.

---

102) 서울고등법원 2013. 5. 2. 2010나31510 (1심 서울중앙지방법원 2008가합31411), 대법원  
계류 중.

103) 윤주희, 전계 논문, 334면.

#### 4. GS칼텍스 사건<sup>104)</sup>

① 피고 GS칼텍스의 이용실적에 따라 포인트가 적립되는 GS포인트 카드 회원으로 가입한 고객들의 개인정보에 대한 데이터베이스에 접근할 권한이 있는 자회사 직원이 해당권한을 이용하여 고객정보를 빼낸 후 이를 시중에 판매하거나 집단 소송을 의뢰받은 변호사에게 판매하는 방법 등으로 금원을 취득하기로 모의한 후, 2008년 7월 8일부터 7월 20일까지 데이터베이스 서버에 접속하여 회원 1100만여명의 성명, 주민등록번호, 주소, 전화번호, 이메일 주소 등 개인정보를 자신의 사무용 컴퓨터로 전송받아 “쓰레기 더미에서 GS칼텍스 고객정보가 담긴 DVD를 주웠다”고 기자들에게 알리면서 개인정보의 유출사고가 알려진 사건이다.<sup>105)</sup>

③ 법원은 비록 개인정보가 외부로 누출됨으로써 불특정 다수에게 공개되어 이를 열람할 수 있는 상태 또는 원고들의 의사에 반하여 개인정보가 수집·이용될 수 있는 상태에 이르렀지만 이 유출된 개인정보를 수록한 저장매체가 모두 조기에 수사기관에 제출되어 폐기된 점 등을 비추어 보면, 피해자들의 개인정보가 불특정 다수에게 공개되어 이를 열람할 수 있는 상태 또는 원고의 의사에 반하여 개인정보가 수집·이용될 수 있는 상태에 이르러 원고들의 개인정보자기결정권이 침해되었거나 침해될 상당한 위험이 발생하여 원고들에게 정신적 손해가 발생하였다는 점을 인정하기 어렵다고 판단하였다.

### III. 검토

---

104) 대법원 2012. 12. 26. 선고 2011다59834 판결.(1심 2008고단58777, 2심 2010나11478).

105) 윤주희, 전계 논문, 336면 내지 337면.



이상의 소송에 대한 핵심적인 내용을 정리하면 다음과 같다.

[표 4] 개인정보 유출사고 사례의 결과<sup>106)</sup>

책임 인정 사례		
엔씨소프트 사건 리니지Ⅱ 사건	누출 인정, 주의의무위반 인정	PC방 이용자 10만원 배상
	누출 불인정	가정용 PC 이용자 기각
국민은행 사건	관리적 조치를 하여야 할 주의의무 위반	주민번호포함 원고 20만원
		주민번호불포함 원고 10만원
LG전자 사건	당시 기술수준에 부합하여야 하는 보안조치를 취하여야 할 의무 위반	실제 유출 원고 30만원
		실제 유출 없는 원고 기각
SK브로드밴드 사건	동의 없는 개인정보 제공은 개인정보자기결정권을 침해	동의 없이 제공한 경우 20만원
		동의 있었으나 동의 범위 외로 제공한 경우 10만원
KT 사건	관리자로서의 주의의무 위반 인정	10만원
SK커뮤니케이션 즈 사건	개인정보보호업무를 소홀히 한 책임을 인정	20만원
	기술적·관리적 보호조치를 이행하지 않았다고 보기 어렵다	기각
책임 부정 사례		
LG텔레콤 사건	개인정보의 누출이 없었다고 판단	기각 (1심은 5만원 인정)
다음 사건	당시의 기술수준으로 주의의무를 위반했음을 인정하기 어렵고, 손해발생 사실 인정할 근거가 없음	기각
옥션 사건	해킹 기술발전과 사건 당시 옥션의 보안조치내용을 볼 때 과실인정 어려움	기각
GS칼텍스 사건	유출사고 후 불법적인	기각

106) 표 출처: 윤주희, 전제 논문, 337면 내지 338면의 표를 추가 및 재구성.

	사용없이 바로 폐기되어 손해를 입었다고 인정하기 어려움	
--	--------------------------------------	--

## 제4절 개인정보 유출사고의 유형화

### I. 서설

개인정보처리자가 개인정보의 유출로 인하여 민사상 손해배상책임을 부담하는 유형을 다음과 같이 5가지로 분류하면서, 유형에 따라 개인정보처리자가 책임을 부담하는 근거를 달리 설명하는 견해가 있다.

### II. 유출사고의 5가지 유형

#### 1. 분류 방법

제①유형: 개인정보처리자(그 피용자와 그로부터 개인정보 취급위탁을 받은 자(수탁자)를 포함한다)의 과실로 개인정보가 유출된 경우

제②유형: 개인정보처리자의 과실과 제3자(해커 등)의 고의로 인한 불법행위가 경합하여 개인정보가 유출된 경우

제③유형: 개인정보처리자의 피용자, 수탁자가 고의로 개인정보를 유출한 경우

제④유형: 개인정보처리자가 동의를 받지 아니하고 개인정보를 제3자에게 제공하거나 이전한 경우

제⑤유형: 개인정보처리자가 동의 없이 정보를 수집하거나, 동의 받은 목적과 달리 사용하거나, 이용자의 동의철회, 열람, 정정 등 요구를 받고도 이행하지 아니하는 경우<sup>107)</sup>

107) 임종인, 이숙연, 전계 논문, 224면 내지 225면.

위 견해에 따르면 종래에는 제①유형의 사건이 지배적이었지만(국민은행 사건과 리니지 사건이 이 유형에 속함), LG전자 사건과 옥션 사건은 개인정보처리자의 보안조치 상의 과실이 인정될 경우 제②유형에 속하게 될 것이고, 하나로텔레콤 사건은 제④유형인지 여부가 다투질 것으로 보이며, GS칼텍스 사건은 제③유형에 해당하는 사례가 될 것이다.<sup>108)</sup>

## 2. 분류 근거

위 제①, ③유형에 대해서는 민법 제750조 불법행위책임 또는 제756조의 사용자책임을 물을 수 있는데, 이에 대한 특칙이라 할 수 있는 개인정보보호법 제39조 및 정보통신망법 제32조는 정보주체의 보호를 강화한 특칙으로서 개인정보처리자 및 정보통신서비스 제공자 등에 대하여 적용되며 입증책임의 전환 법리에 의하여 정보주체의 입증부담을 경감시키고 있다.<sup>109)</sup>

한편 위 제②유형은 개인정보처리자의 과실과 제3자의 고의가 결합되어 개인정보침해라는 결과가 발생한다는 측면에서 민법 제760조 제1항의 공동불법행위책임에 해당하는지가 여부가 문제된다. 그런데 공동불법행위를 인정하기 위해서는 행위자 각자가 독립하여 일반불법행위의 요건을 갖추어야 하나, 각 행위자 사이의 ‘주관적 공동관계(공모 내지 공동의 인식)’를 요하지 아니하며, ‘객관적 공동관계(행위의 관련, 공동성)’만 인정되면 족하다는 것이 판례와 다수설의 입장이고, 고의가 있는 자와 과실이 있는 자 사이에서도 공동불법행위가 성립할 수 있으므로,<sup>110)</sup> 개인정보처리자의 개인정보보호 주의의

108) 임종인, 이숙연, 전계 논문, 225면.

109) 임종인, 이숙연, 전계 논문, 225면.

110) 임종인, 이숙연, 전계 논문, 225면.

무 위반과 제3자의 행위의 사이에 관련공동성이 인정될 경우에는 제3자(해커)와 함께 손해 전체에 대한 부진정 연대책임을 부담하도록 하는 것이 가능하다고 해석할 것이다.<sup>111)</sup>

한편 관련공동성이 인정되지 않는 경우라도 수인이 독립된 행위에 의하여 동일한 결과에 대해서 각각의 원인을 제공한 경우라면 각자는 발생한 결과 전부에 대하여 배상책임을 부담하여야 할 것이므로<sup>112)</sup> 결과적으로는 큰 차이가 없다고 한다.<sup>113)</sup>

### Ⅲ. 실제 사례 적용

위의 분류기준을 근거로 대표적인 앞의 제2절에서 검토한 대표적인 개인정보유출 사고를 분류하면 다음 [표 5]와 같다.<sup>114)</sup>

[표 5] 개인정보 유출 사례 유형에 따른 소송 결과

침해유형	예시	결과
① 유형	리니지Ⅱ 사건	10만원 or 기각
	LG전자 사건	30만원 or 기각
	LG텔레콤 사건	기각
	다음 사건	기각
	국민은행 사건	20만원 or 10만원
② 유형	KT 사건	10만원

111) 한편 위 견해는 제②유형의 행위를 공동불법행위로 구성할 경우, 개인정보처리자의 과실에 비해 제3자(해커)의 불법이 현저하게 크더라도, 개인정보처리자는 제3자에 대하여 내부 분담비율에 따라 구상권을 행사하는 것은 몰라도, 피해자에 대하여 자신의 부담부분에 대하여만 배상책임을 있음을 주장할 수 없고 제3자와 연대하여 전체 손해를 배상하여야 하므로 가혹한 결과에 이를 수 있다고 한다.

112) 정태윤, “민법 제760조”, 민법주해(XIX), 박영사, 187~190면, 위 저자는 이와 같은 유형의 불법행위를 경합불법행위(Nebentaterschaft)로 분류한다.

113) 임종인, 이숙연, 전제 논문, 225면.

114) 표본이 매우 제한적이므로 현 상황에서는 손해배상금액으로 산출된 액수에 대해 유형별로 유의미한 차이가 없는 것으로 보인다. 향후 관련 판례가 누적되어야 유형별로 유의미한 차이를 발견할 수 있을 것으로 생각된다.

	SK커뮤니케이션즈 사건	20만원 or 기각
	옥션 사건	기각
③ 유형	GS칼텍스 사건	기각
④ 유형	SK브로드밴드 사건	20만원 or 10만원

## 제4장 개인정보 유출로 인한 기업의 손해배상책임

### 제1절 총설

손해배상청구권이 인정되려면 손해가 실제로 발생해야 한다. 손해발생에 대한 위험만이 존재할 경우 그러한 추정적 손해는 배상의 대상이 되지 않는다.<sup>115)</sup> 따라서 손해배상청구를 하는 원고로서는 스스로 구체적 손해의 발생에 대한 입증책임을 부담함이 원칙이다.

그러나 손해는 법적 개념이고, 사실상의 모든 불이익을 전부 손해로 포섭시킬 수는 없다. 따라서 불법행위로 인한 손해배상청구권은 법률상 보호받아야 마땅한 이익에 관하여 현실적으로 손해가 발생한 때 비로소 성립하는 것이다.<sup>116)</sup> 이때 현실적으로 손해가 발생하였는지 여부는 사회통념에 비추어 객관적이고 합리적으로 판단하여야 할 것이다.<sup>117)</sup> 그리고 이러한 판단에 있어서는 손해의 직접성, 구체성, 특정성, 법익과의 거리, 법익에 야기된 불이익에 대한 법적 가치 판단 등 여러 가지 요소들에 대한 고려가 필요하다.<sup>118)</sup>

115) 정상조, 권영준, 전계 논문, 29면.

116) 정상조, 권영준, 전계 논문, 29면.

117) 대법원 2004. 11. 26. 선고 2003다58959 판결.

118) 정상조, 권영준, 전계 논문, 29면.

이하에서는 침해와 손해의 구별 논의를 전제로 하여 어떠한 경우에 개인정보처리자의 주의의무위반 및 손해배상책임이 인정될 수 있는지 및 손해배상액은 어떻게 산정할 것인지 등에 대한 구체적이고 세부적인 판단기준을 제시한다.

## 제2절 개인정보의 침해와 손해의 구별

### I. 서설

대부분의 개인정보에 관한 민사소송은 인격권의 일종인 개인정보자기결정권 침해를 이유로 정신적 손해배상을 청구하는 내용이다. 즉 개인정보의 유출로 인한 개인정보처리자의 손해배상책임을 논하기 위한 전제로써 우선 검토해야 하는 것이 인격권에 대한 침해와 손해의 구별이라고 할 것이다.<sup>119)</sup>

### II. 학설

#### 1. 국내에서의 논의

개인정보의 침해와 손해를 구별하는 견해는 인격권의 침해와 이로 인한 손해는 구별되므로, 인격권의 일종인 개인정보 자기결정권이 침해되었다고 하여 논리필연적으로 정신적 손해가 곧바로 발생하는 것은 아니라고 한다. 즉 개인정보의 침해가 정신적 손해를 발생시킬 개연성은 크지만, 개인정보권의 침해가 있었어도 정신적 손해가 발생되지 않을 가능성이 있으므로, 개념적으로나 실제적으로도 침해와 손해를 구분할 실익이 있다는 것이다.<sup>120)</sup>

---

119) 정상조, 권영준, 전계 논문, 31면.

120) 정상조, 권영준, 전계 논문, 32면.

반면, 개인정보가 한정된 범위에서 유출된 경우에 과연 피해자들의 정신적 손해 자체가 아예 발생하지 않았다고 볼 수 있는지에 대한 의문을 제기하면서, 일단 침해가 있었다면 손해 자체를 부정하는 방법으로 해결하기보다는 손해억지의무 또는 손해경감의무를 이행했다고 보아 손해배상책임을 감경 또는 면제하는 방법으로 검토해야 한다는 견해가 있다.<sup>121)</sup>

## 2. 해외에서의 논의

독일의 학설은 인격권의 침해가 있더라도 그 침해의 정도가 중할 때 비로소 손해배상이 인정된다고 한다.<sup>122)</sup> 독일 판례는<sup>123)</sup> 더 나아가 고의 내지 중과실, 다른 보상가능성의 결여 등의 요건이 충족된 경우에 한하여 보충적으로 인격권침해에 대한 위자료를 인정하고 있다.<sup>124)</sup>

미국에서는 개인정보에 관한 권리는 프라이버시의 문제로 다루어진다. 개인정보침해는 프라이버시의 노출(Disclosure of Private Fact)의 일종인데 프라이버시의 노출이 인정되려면, ① 노출된 사적 사실이 합리적 사람에게 매우 불쾌한(highly offensive) 것이어야 하고,<sup>125)</sup> ② 그 정보가 상당한 수의 사람들에게 알려져서 공개된 지식(public knowledge)에 이를 것이 확실하여야 한다.<sup>126)127)</sup>

---

121) 김재형, “2012년 분야별 중요판례분석 - 민법(하)”, 법률신문 2013. 2. 28.자 13면.

122) Rixecker in Münchener Kommentar zum Bürgerlichen Gesetzbuch für das Deutsche Reich, 5. Aufl. 2006, Anhang zu § 12, Das Allgemeine Persönliche, Rn. 221.

123) BVerGE 34, 269; Wenzel, Das Recht der Wort- und Bildberichterstattung, Handbuch des Äußerungsrechts, 4. Aufl. 1994, S. 758 ff.

124) 정상조, 권영준, 전계 논문, 35면 내지 36면.

125) Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1353 (Ill. App. Ct.1995).

126) Restatement(Second) of Torts §652D.

127) 정상조, 권영준, 전계 논문, 36면.

즉 미국에서는 개인정보침해의 범위 자체가 우리나라나 독일에 비하여 좁게 해석되고 있고, 나아가 침해가 성립하였더라도 이를 이유로 손해배상을 받으려면 실제의 손해(actual damage)의 입증에 성공하여야 한다.<sup>128)129)</sup>

반면 우리나라와 일본에서는 독일이나 미국에 비하여 위자료 즉 정신적 손해배상책임을 폭넓게 인정하는 경향을 보인다. 위자료 인정에 관하여 특별한 입법적인 제약을 두고 있지 않기 때문이다.<sup>130)</sup>

### III. 판례

#### 1. 우리 판례의 경향

이와 관련한 명시적인 대법원 판례는 없으나, 인격권과 유사한 절대성을 가진 소유권에 대한 판례에서 대법원은 소유권의 방해와 손해가 구별되는 개념임을 전제하고 있다.<sup>131)</sup> 이러한 구분은 권리에 대한 침해자가 필연적으로 손해배상책임을 부담하는 것은 아니라는 것을 의미한다.<sup>132)</sup>

하급심 판례 중에는 개인정보자기결정권 침해를 인정하면서도 정신적 손해발생은 부정하는 것이 있다. 서울중앙지방법원은 변호사 관련 정보를 제공하는 웹사이트를 운영하는 회사가 변호사들의 개인신상 정보를 재처리하여 법조인의 인맥 지수 서비스를 제공하고, 대법원

---

128) Vincent R. Johnson, "Cybersecurity, Identity Theft, and the Limits of Tort Liability", 57 S.C.L.Rev. 255, 305 (2005).

129) 정상조, 권영준, 전계 논문, 37면.

130) 정상조, 권영준, 전계 논문, 38면.

131) 대법원 2003. 3. 28. 선고 2003다5917 판결은 방해와 손해를 구별하는 기준으로 지속성을 제시하는데, 즉 현재 지속되는 침해상태는 방해로, 이미 종결되어 그 결과제거만 문제되는 상태는 손해로 본다라는 것이다.

132) 정상조, 권영준, 전계 논문 40면.



홈페이지 나의사건검색 서비스를 통해 수집한 소송정보를 기초로 변호사들의 승소율, 전문성 지수 등도 제공한 사건에서, 변호사들의 승소율과 전문성 지수 등에 대한 서비스 제공은 변호사들의 자기정보통제권을 침해하는 것이라고 판단하면서도, 이로 인하여 원고들 개인에게 정신적 손해가 발생하였다고 보기 어렵다는 이유로 손해배상청구는 기각하였다.<sup>133)</sup>

대법원은 고객의 개인정보 데이터베이스가 들어있는 DVD가 유출되어 사건관련자와 언론관계자들에게만 그 일부가 열람된 사건에서 개인정보의 유출 사실을 인정하면서도, 제반 사정에 비추어 볼 때, 개인정보의 유출로 인하여 원고에게 위자료로 배상할 만한 정신적 손해가 발생하였다고 보기는 어렵다고 판시하였는바,<sup>134)</sup> 이는 개인정보에 대한 침해와 손해의 개념적 구별을 전제로 한 최초의 대법원 판례로 평가할 수 있을 것이다.

## 2. 미국 판례의 경향

미국 법원은 손해배상에 이를 수 있는 실제의 손해에 대한 발생의 입증을 매우 엄격하게 요구하여<sup>135)</sup> 개인정보의 침해로 인하여 손해배상책임을 인정한 미국 연방대법원의 판례는 찾기 어렵고, 해킹, 도난 등으로 개인정보가 제3자에 의하여 무단취득된 다수 사례에서 “개인정보가 실제 손해를 야기하는 행위에 사용되지 않은 이상, 단지 위험성이 증가하였다는 점만으로는 실제 손해가 발생하였다고 볼 수 없다.”라고 판시하면서 원고의 청구를 각하 또는 기각하는 판결을 하고 있다.<sup>136)</sup>

---

133) 서울중앙지방법원 2007. 7. 6. 선고 2006가합22413 판결.

134) 대법원 2012.12.26. 선고 2011다59834 판결.

135) 정상조, 권영준, 전계 논문, 37면.

136) 이원우, 전계 논문, 250면.

최근 미국 연방대법원의 판결 중에는 개인정보주체의 사전 동의 없이 실시한 연방정부부처간의 개인정보공유는 프라이버시보호법(the Privacy Act of 1974)을 침해한 행위에 해당하기는 하지만, 이 사건에서는 단지 감정적 손해(emotional damages)만이 발생하였고 금전적 손해(pecuniary damages)는 발생하지 않았으므로 실제손해가 없었다고 보아 원고의 청구를 기각한 사건이 있었다.<sup>137)</sup> 즉 미국 판례 또한 개인정보에 대한 침해와 손해의 발생을 전제로 판단하고 있는 것으로 보인다.

### 3. 영국 판례의 경향

영국에서는 SBC(Scottish Borders Council)의 직원들의 성명, 주소, 생년월일, 사회보장번호, 급여 등에 관한 개인정보가 포함된 연금관련 서류파일이 담긴 CD가 쓰레기통에서 발견된 사건에 대해, ICO는 정보처리자인 SBC의 정보보호원칙 위반행위로 실질적인 피해(substantial damage)가 발생할 가능성이 있고, 개인정보가 포함된 서류파일을 제3자가 발견한 것 자체가 실질적 피해에 해당한다고 판단하여 벌금 250,000 파운드를 부과하였다.<sup>138)</sup> 그러나 이에 대해 영국의 제1심 법원(First Tier Tribunal)은 직원들의 연금관련 정보가 저장된 CD가 쓰레기통에서 발견된 것에 대하여 SBC의 행위는 정보보호원칙 위반에 해당하지만, 위반행위가 직원들에게 심각한 피해를 야기할 가능성이 없기 때문에 ICO가 벌금 250,000 파운드를 부과한 것은 적절하지 않다고 결정하였다.<sup>139)</sup>

---

137) FAA v. Cooper, 132 S.Ct. 1441, 1446 (2012).

<http://www.supremecourt.gov/opinions/11pdf/10-1024.pdf>

138) Mayer Brown Legal Update, "ICO fines for breach of data protection legislation"

<http://www.mayerbrown.com/ICO-fines-for-breach-of-data-protection-legislation-09-11-2013>

139) Scottish Borders Council v. The Information Commissioner (21 August 2013)

[http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20\(210813\)%20Preliminary%20Decision.pdf](http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20(210813)%20Preliminary%20Decision.pdf)

이는 민사상 손해배상에 대한 판결은 아니지만, 개인정보 유출로 인한 실질적 피해(substantial damage)의 개념에 대한 영국법원의 태도를 추론할 수 있는 사례로 보인다.

#### 4. 캐나다 판례의 경향

피고 Sun Life의 직원이 실수로 원고 Townsend의 우편주소를 잘못 입력하여 두 번의 우편물이 틀린 주소로 발송되었는데, 한 번은 원고가 직접 수령하였고, 또 한 번은 피고로 반송되었으며, 피고 고객센터가 실수로 원고의 질의에 대한 회신서를 원고의 보험설계사에게 송부하였는데, 그 회신서에는 민감한 의료정보가 포함되어 있었던 사건에서, 자신의 개인정보에 대한 안전조치를 취하지 않았으며, 자신의 동의 없이 제3자인 보험설계사에게 자신의 개인정보를 제공하였다고 주장하며 원고가 PIPEDA(Personal Information Protection and Electronic Documents Act) 위반을 근거로 피고에게 25,000 달러의 손해배상을 청구한 것에 대하여, 캐나다 연방법원은 다음과 같이 판시하였다.<sup>140)</sup>

피고 Sun Life가 틀린 주소로 우편을 발송하였지만, 첫 번째 편지는 원고가 직접 수령하였고, 두 번째 편지는 반송되었으므로 어떤 개인정보 유출도 없었다. 한편 민감정보를 포함한 우편물을 정보주체의 동의 없이 제3자에게 발송한 것은 위 법 위반사항이 분명하나, 손해배상액을 산정할 때에는 ① 손해배상이 법에서 추구하는 일반적인 목적에 부합하는지, ② 개인정보유출 예방을 위해 필요한지, ③ 유출의 심각성 등을 종합적으로 고려해야 한다. 특히 유출의 심각성

---

140) Townsend v. Sun Life Financial, 2012 FC 550 (CanLII)

<http://www.canlii.org/en/ca/fct/doc/2012/2012fc550/2012fc550.html>

여부는 유출이 정보주체의 건강, 안녕, 거래 및 경제 활동에 미치는 영향, 유출한 자의 유출 전후 행위, 법 위반자가 유출로 인해 이득을 얻었는지 여부에 따라 결정된다.

그런데 이 사건에서 원고의 개인정보는 보험설계사에게만 유출되었고, 피고는 보험설계사가 즉시 편지를 파기하도록 조치하였으며, 피고가 고의적·악의적으로 행위한 것이 아니고, 유출로 인한 어떤 이득도 취하지 않았으며, 같은 실수가 반복되지 않도록 즉각적이고 효율적인 보안조치를 취하였다. 반면 원고는 손해에 대한 어떤 증거도 제시하지 못했고, 피고의 위반행위로 인해 겪은 모욕도 구체적으로 입증하지 못하였다. 따라서 설령 피고가 고의 또는 악의가 있었음이 증명되었다 하더라도 원고의 개인정보 유출정도 및 피고의 범위가 아주 경미하여 이러한 개인정보의 유출로 인하여 원고에게 피해가 없거나 피해가 있더라도 1달러 미만의 명목손해(nominal damage)에 불과하다.

즉 캐나다 연방법원의 위 판결에서도 PIPEDA법 위반 즉, 개인정보의 일정한 침해를 인정하면서도, 손해의 발생여부 판단에 있어서는 ① 손해배상이 법에서 추구하는 일반적인 목적에 부합하는지, ② 개인정보유출 예방을 위해 필요한지, ③ 유출의 심각성 등을 부가적으로 고려하였는바, 매우 경미한 침해에 대해서는 곧바로 손해배상책임이 인정되지 않는다고 판시하여 침해와 손해를 구별한 전제하에 있는 것으로 보인다.

#### IV. 검토

개인정보권이 침해된 구체적인 사안에 따라 그리고 개인정보에 대한 관점에 따라서 손해발생의 여부와 손해의 범위 또는 손해액에 관한 판단은 달라지므로, 개인정보에 대한 정보주체의 권리가 침해

되었다고 항상 정신적 손해가 발생한다고 획일적으로 말할 수는 없다.<sup>141)</sup> 대륙법계인 독일에서는 개념적으로 이러한 구분을 인정한다고 할 수 있고, 미국, 영국 또는 캐나다 등 영미법계에서는 판례법상 침해와 손해의 구분을 명확히 하고 있는 것으로 보인다.

따라서 개인정보권이 침해되었다는 사실만으로 손해배상의무가 발생하는 것은 아닐 것이고, 침해대상인 개인정보의 가치 및 가해자와 피해자의 각 영역에 대한 다양한 참작사유를 고려하여 손해발생의 여부를 판단하는 것이 타당하다.

### 제3절 개인정보 유출로 인한 손해의 종류

#### I. 서설

개인정보의 유출로 인한 손해의 유형을 분류하여 검토하기 위한 전제로서 재산적 손해와 정신적 손해 및 통상손해와 특별손해의 개념을 검토하도록 한다.

#### II. 재산적 손해와 정신적 손해

재산적 손해는 직접 재산권이 침해된 경우와 인격권 또는 인격적 이익이 침해된 경우(신체, 자유, 명예, 생명, 정조, 신용, 성명, 초상 등의 침해)에 발생한다. 일반적으로 재산적 손해라 함은 가해행위에 의하여 손해를 받은 자가 가해행위가 없었더라면 가지고 있어야 할 재산과 그 자의 침해받은 후의 현재의 재산과의 차액을 의미한다.<sup>142)</sup>

---

141) 정상조, 박준석, 전제 논문, 33면.

142) 박준서, 주식 민법 {채권각칙(6)} 2000. 3. (제3판), 219면.

한편 민법 제751조 제1항에 규정된 ‘재산 이외의 손해’란 금전으로 평가할 수 없는 손해로서 정신적 손해를 의미한다. 정신적 손해는 정신적 고통을 의미하는 것으로 이해되고 있고, 민법 제751조 제1항 역시 “기타 정신적 고통을 가한 자”라는 표현을 사용하고 있다. 정신적 손해에 대한 배상금은 위자료라고 부른다.<sup>143)</sup>

### Ⅲ. 통상손해와 특별손해

불법행위로 인한 손해배상은 통상의 손해를 그 한도로 한다(민법 393조 제1항, 제763조). 통상의 손해는 그와 같은 불법행위가 있으면 사회일반의 관념에 따라 통상 발생하는 것으로 생각되는 범위의 손해를 말한다. 통상의 손해에 대하여서는 가해자가 알았거나 알 수 있었을 것을 필요로 하지 않는다. 불법행위 손해배상청구권자는 불법행위 및 통상의 손해액을 주장·입증하면 된다.<sup>144)</sup>

반면 특별한 사정으로 인한 손해는 불법행위자가 불법행위 당시에 그 사정을 알았거나 선량한 관리자로서 주의를 하였더라면 알 수 있었을 때에 한하여 배상책임이 있다(민법 제393조 제1항, 제763조).<sup>145)</sup>

### Ⅳ. 검토

개인정보가 유출 사고의 경우 개인정보가 유출되는 단계에서의 피해는 정신적 손해로 인정되는 경우가 대부분일 것이며, 이후 누출된 개인정보가 타인에 의해 이용되어 정보주체에게 서비스 이용료나 신용카드 사용대금 등이 청구되는 단계에서 현실적인 재산적 손해

---

143) 박준서, 주식 민법 {채권각칙(8)} 2000. 2. (제3판), 269면.

144) 박준서, 주식 민법 {채권각칙(6)} 2000. 3. (제3판), 173면.

145) 박준서, 주식 민법 {채권각칙(6)} 2000. 3. (제3판), 183면.

가 발생한다.

법원은 은행직원이 신용카드 절도범에게 비밀번호를 누출하여 410만원에 이르는 현금이 절도범에 의해 인출된 사건에서 은행직원의 행위와 현금인출과의 상당인과관계를 인정하여 은행에 대해 인출액 전액에 대한 손해배상과 위자료까지 지급하라고 판결한 반면<sup>146)</sup><sup>147)</sup>, 이동통신회사직원이 본인확인을 소홀히 하여 피해자의 처에게 피해자의 통화내역을 발급하여 주어 이혼에 이르게 된 사건에서는 이동통신회사의 과실은 인정되나 그로 인한 이혼은 특별손해에 해당하므로 이동통신회사의 직원이 알았다는 증거가 없는 한 이혼에 대한 책임을 물을 수 없다고 판시하여 이혼위자료와 처와 별거한 기간 동안의 파출부 비용, 통화내역 누출로 인한 위자료 등에 대한 1억 5천여만원의 손해배상 청구를 기각하였다.<sup>148)</sup>

따라서 개인정보 침해로 인한 손해배상도 불법행위로 인한 손해배상이므로 통상손해와 특별손해의 구별은 필수적이다. 개인정보가 타인에게 누출됨으로써 발생하는 불안감은 통상의 정신적 손해가 될 것이고, 이용자의 동의 없이 가입된 서비스의 이용료나 이용자의 개인정보를 도용하여 구입한 재화의 대금 등은 통상의 재산적 손해가 될 것이다. 다만 통상손해를 넘어서는 손해는 가해자에게 예견가능성이 인정되는 경우에 한하여만 손해배상책임이 인정될 수 있을 것이다.

## 제4절 개인정보 유출로 인한 손해배상책임의 발생

---

146) YTN 2003. 6. 20 자 기사.

147) 대법원 93다19115판결에서 보듯 재산적 손해가 전보되면 정신적 손해는 회복된다고 보는 관례의 입장을 감안할 때 법원이 이 사건에서 인출액 이외에 별도의 위자료를 인정한 것은 개인정보 침해의 경우도 생명침해로 인한 불법행위처럼 재산적 손해배상과 함께 위자료를 인정하는 것으로 보아야 한다는 견해도 있다. 이창범, 김본미 전계 논문, 106면.

148) 한겨레 2004. 4. 23. 자 기사.

## I. 손해배상청구권의 성립요건

### 1. 서설

손해배상책임의 발생원인은 계약관계가 있는 자에 의한 침해일 경우 채무불이행과 불법행위가 병존할 수 있지만, 이러한 계약관계가 없는 자에 의한 침해일 경우 불법행위만이 문제된다. 따라서 개인정보처리자는 민법 제750조에 따른 불법행위성립요건이 인정될 때에 한하여 비로소 책임을 부담하게 된다. 개인정보보호법 제39조는 정보주체의 손해배상청구권에 관하여 규정하고 있고, 위 조항은 민법상 일반 불법행위의 특칙 규정에 해당한다.<sup>149)</sup>

개인정보보호법 제39조에 따른 손해배상청구권이 발생하기 위해서는 개인정보처리자에게 이 법을 위반한 사실(침해행위)이 있어야 한다. 통상적으로는 개인정보보호법을 위반한 경우라면 일단 위법한 것으로 판단되고, 그 위반행위가 법질서 전체의 입장과 객관적으로 모순·충돌하는 경우, 즉 위법성이 인정되는 경우에 한하여 개인정보처리자의 손해배상책임이 발생한다.<sup>150)</sup> 나아가 이 법 위반행위와 손해 사이에 상당인과관계 및 개인정보처리자의 고의 또는 과실과 책임능력이 인정되어야 한다.

### 2. 입증책임의 전환

그러나 개인정보처리자의 고의 또는 과실을 입증하는 것은 쉬운 문제가 아니기 때문에 피해를 입었다고 하더라도 입증에 성공하지 못하여 손해배상을 받지 못하게 되는 결과가 발생할 수 있다.<sup>151)</sup> 이러

---

149) 권영준, 전계 논문, 40면.

150) 이창범, 전계서, 제349면.



한 점을 감안하여 정보통신망법에서는 고의 또는 과실에 대한 입증 책임을 전환하여 개인정보처리자가 고의 또는 과실이 없음을 입증하지 못한 경우에 이로 인한 책임을 면하지 못하도록 규정하였고(정보통신망법 제32조). 개인정보보호법 또한 손해배상책임에 대하여 입증 책임을 전환하고 있다(정보통신망법 제39조 제1항).<sup>152)</sup>

이에 따라 정보주체로서는 이 법 위반행위가 존재한다는 사실과 그로 인한 손해가 발생하였다는 사실을 주장·입증하기만 하면, 개인정보처리자가 개인정보 유출에 대하여 자신의 고의 또는 과실이 없었는지를 주장·입증하여야 한다. 따라서 법원은 원칙적으로 위 제39조 제1항의 논리적인 순서대로라면 정보주체에게 손해가 발생하였는지 여부를 우선 판단한 후, 개인정보처리자에게 고의·과실이 인정되는지 여부에 대한 판단으로 나가서 개인정보처리자의 책임이 해제되는지 여부를 검토하여야 할 것이다.

### 3. 개인정보처리자의 주의의무

#### 가. 서설

손해발생 여부 및 그 범위 판단의 전제로써 개인정보의 유출과 관련하여 개인정보처리자에게 요구되고 있는 법령 및 신의칙상 과실 판단의 기준에 대해 우선적으로 검토할 필요성이 있다. 그런데 과실이 인정되는지 여부에 대한 판단은 사안 중심적 성격이 강하여 상당한 정도로 법관의 재량에 따를 것이기 때문에 법관의 판단재량을 부당하게 제약하지 않는 한도 내에서 과실의 판단기준을 구체화할 필요성이 있다.<sup>153)</sup>

---

151) 고형석, "개인정보침해와 피해구제에 관한 연구", 법조 제60권 제10호, 2011. 277면.

152) 이창범, 전거서, 352면.

153) 권영준, 전계 논문, 36면.

## 나. 주의의무의 발생근거

개인정보처리자의 주의의무 역시 주로 법령과 계약에 따라 결정될 것이다. 우리의 개인정보보호법과 하위 규범들은 매우 포괄적이고 체계적인 방식으로 개인정보처리자의 주의의무를 정하고 있다.<sup>154)</sup>

## 다. 주의의무 판단의 전제 - 합리적 기대가능성

주의의무는 합리적 기대가능성이라는 범주 안에서 인정된다. 법은 합리적으로 기대할 수 없는 행위를 강제할 수 없기 때문이다. 가령 개인정보처리자가 어떠한 보안조치를 취하지 않았다는 것이 문제될 경우 우선 그러한 보안조치를 취하는 것이 합리적으로 기대가능한지 여부를 검토하여야 한다.<sup>155)</sup>

인터넷 보안을 강화하는 것은 한편으로는 개인정보의 유출 가능성을 줄이지만, 다른 한편으로는 인터넷 관련 비용을 증가시켜 사업체에 부담을 줄 수 있고, 이러한 부담은 궁극적으로는 인터넷 이용자에게 전가될 가능성이 크다. 결국 법령에 정해진 주의의무의 외연을 확장하여 나가는 것만이 능사가 아니라 일종의 비용-편익 분석(cost-benefit analysis)의 사고에 기초하여 합리적으로 기대할 수 있는 범위 안에서 주의의무의 외부 경계선을 확정할 필요가 있다.<sup>156)</sup>

---

154) 개인정보보호법, 동법 시행령, 동법 시행규칙 외에도 행정안전부 장관의 표준 개인정보 보호지침(법 제12조 제1항 참조), 개인정보 안전성 확보조치 기준 고시(법 제24조 제3항 및 제29조, 시행령 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실, 도난, 유출, 변조, 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준), 개인정보 영향평가에 관한 고시(시행령 제38조에 따른 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준을 정함)가 마련되어 있다.

155) 권영준, 전계 논문, 52면.

156) 권영준, 전계 논문, 52면.

미국에서 이러한 사고방식이 일반적인 과실판단기준으로 구체화된 것이 핸드 공식(Hand Formula)이다. 핸드 공식은 미국의 Learned Hand 판사가 1947년의 한 판결에서 제시한 과실판단의 공식이다.<sup>157)</sup> 이에 따르면 손해가 발생할 확률을 P(probability), 그 손해를 L(loss), 그 손해를 방지하기 위하여 취하여야 할 조치의 비용을 B(burden)라고 하면, B가  $P \times L$  보다 적을 때 비로소 과실이 인정된다는 것이다.<sup>158)</sup>

핸드 공식에 따르면 주의의무는 사고방지비용이 사고기대손실보다 적은 경우에 성립한다. 따라서 주의의무를 추가로 이행하는 데 들어가는 한계비용<sup>159)</sup>이 이로 인한 한계편익과 일치할 때 주의의무는 가장 효율적 수준이 이른다.<sup>160)</sup> 그러나 법원이 실제로 이러한 한계비용과 한계편익을 정확하게 계산하여 이에 기초하여 과실유무를 판단하는 것은 가능하지 않다. 이러한 이유 때문에 미국에서도 핸드 공식이 명시적으로 사용되는 경우는 드물다고 한다.<sup>161)</sup> 결국 현실적으로는 비용과 편익의 트레이드오프(trade-off)관계를 염두에 두고 주의의무의 내용과 정도를 정하면 충분할 것이다.<sup>162)</sup>

#### 4. 법령에 따른 고려요소

##### 가. 안전조치의무

개인정보보호법 제29조는 안전조치의무라는 표제 하에 “개인정보처

---

157) U.S. v. Carrol Towering Co., 159 F.2d 169(2d Circuit, 1947)

158) 권영준, 전계 논문, 52면.

159) 핸드 공식에서의 비용과 편익 개념은 일반적으로 한계가치로 이해되고 있다. Cooter·Ulen, 한순구 역, 법경제학 (5th ed.), 경문사, 2009, 411면.

160) Cooter·Ulen, 전게서, 412면.

161) 같은 취지로 Richard W. Wright, “Hand, Posner, and Myth of the ”Hand Formula“”, 4 Theoretical Inq. L. 145(2003).

162) 권영준, 전계 논문, 52면.

리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 규정하여, 개인정보처리자의 주의의무를 기술적 조치의무, 관리적 조치의무 및 물리적 조치의무로 구분하고 있다.

이에 따라 개인정보보호법 시행령 제30조 제1항은 개인정보처리자가 취해야 하는 개인정보의 안전성 확보조치로서 “1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치, 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치, 5. 개인정보에 대한 보안프로그램의 설치 및 갱신, 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치” 등을 규정하고 있다. 위 각 내용 중 제1호와 6호는 관리적 조치의무, 제2호 내지 제5호는 기술적 조치의무의 성격을 가진다.<sup>163)</sup>

나아가 같은 조 제3항은 안전성 확보조치의 세부기준을 행정자치부장관이 정하는 고시에 의할 것을 규정하고 있는데, 이에 따라 제정된 안전성 확보조치 기준<sup>164)</sup>은 더욱 세부적인 준수사항을 제시하고 있다. 이를 표로 정리하면 다음과 같다.

[표 6] 개인정보처리자의 안전조치의무<sup>165)</sup>

대분류	소분류	내용의 요지	관련 조항
기술적 조치의무	접근통제	접근권한 제한, 접근 통제 시스템 설치 및	법 제29조 고시 제4, 6조

163) 권영준, 전계 논문, 54면.

164) 행정안전부고시 제2011-43호, 2011.9.30. 제정.

165) 표 출처: 권영준 전계 논문, 54면.

		운영	
	암호화	일정한 정보를 암호화하여 저장	법 제29조 영 제21조, 제30조 제1항 제3호 고시 제7조
	접속기록의 보관 및 위·변조 방지조치	개인정보처리시스템 접속기록을 안정하게 보관·관리	법 제29조 영 제30조 제1항 제4호 고시 제8조
	보안프로그램의 설치와 갱신	백신 소프트웨어 등 보안프로그램 설치와 업데이트	법 제29조 영 제30조 제1항 제5호 고시 제9조
관리적 조치의무	내부관리계획	개인정보의 안전한 처리를 위한 내부관리계획 수립	법 제29조, 영 제30조 제1항 제1호 고시 제3, 5조
	물리적 조치	개인정보의 안전한 보관 및 출입통제절차	법 제29조 영 제30조 제1항 제6호 고시 제10조

## 나. 사후조치의무

개인정보처리자는 개인정보가 유출되지 않도록 안전성을 확보하여야 할 사전적인 조치의무를 부담하는 이외에도 개인정보보호법 제34조에 따라 일단 개인정보가 유출된 후에도 사후적인 조치의무를 부담한다.<sup>166)</sup> 즉 개인정보처리자는 개인정보 유출 후 지체 없이 해당 정보주체에게 그 사실을 알리고, 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 하며, 일정 규모 이상<sup>167)</sup>의 개인정보 유출 시에는 제1, 2항에 따른 통지 및 조치결과를 지체 없이 대통령령이 정하는 전문기관에 신고하여야 한다.

166) 권영준 전계 논문, 55면.

167) 개인정보보호법 시행령 제39조 제1항은 1만 명 이상의 개인정보 유출사고 발생 시 신고의무를 부과하고 있다.

## 5. 세부적 고려요소

### 가. 개관

앞서와 같이 법령상 주의의무의 내용을 확정하였다고 하더라도 구체적인 사안에서 주의의무 위반 여부를 판단하는 것은 결코 용이하지 않으며, 법원은 주의의무의 틀 안에서 여러 가지 세부요소들을 고려하여 규범적·총체적인 관점에서 과실판단을 하게 된다.<sup>168)</sup>

한편 법원은 과실판단에 있어서 고려해야 하는 주의의무의 요소들에 대하여는 옥션 사건<sup>169)</sup>에서 다음과 같이 판시하였다. “정보통신서비스 제공자가 해킹사고 방지를 위해 취해야 할 선량한 관리자로서의 주의의무를 위반하였는지 여부는 ① 관련 법령이 정보통신서비스 제공자에게 요구하고 있는 기술적·관리적 보안 조치의 내용, ② 해킹 당시 당해 정보통신서비스 제공자가 취하고 있던 보안 조치의 내용, ③ 해킹방지 기술의 발전 정도, ④ 해킹 방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도, ⑤ 해커가 사용한 해킹기술의 수준, ⑥ 개인정보 유출로 인하여 이용자가 입게 되는 피해의 정도 등을 종합적으로 고려하여 판단하여야 한다.”

### 나. 정보 자체와 관련된 고려 요소

개인정보 자체의 성격에 따라 정보주체의 피해의 여부 또는 정도가 달라질 수 있다.

#### (1) 정보의 민감성과 위험성

---

168) 권영준 전계 논문, 56면.

169) 서울고등법원 2013. 5. 2. 선고 2010나31510 판결.

개인정보보호법이 강화된 안전조치의무를 요구하고 있는 민감정보는 그에 대한 주의의무수준 또한 높다. 또한 유출되었을 경우 정보주체의 권리가 침해받을 가능성이 높아지는 정도 예컨대 고유식별정보를 비롯하여 신용카드 비밀번호 등은 상대적으로 위험성이 높다.<sup>170)</sup> 위와 같이 개인정보 유출로 위험성이 높아지면 주의의무도 제고되어야 한다.<sup>171)</sup>

## (2) 정보의 양

개인정보보호법 제33조 제2항 제1호는 개인정보 영향평가를 할 때 ‘처리하는 개인정보의 수’를 고려하도록 하고 있고, 시행령 제35조에서는 개인정보의 양<sup>172)</sup>에 따라 개인정보 영향평가 대상이 되는 개인정보파일에 해당하는지 여부를 정하고 있는데. 이는 개인정보의 양과 안전조치의무의 상호관계를 감안한 조항이다. 즉 대량의 개인정보를 취급하는 개인정보처리자가 적은 개인정보를 취급하는 개인정보처리자보다는 더욱 강한 주의의무를 부담하는 결과가 된다.<sup>173)</sup>

## 다. 개인정보처리자와 관련한 고려 요소

### (1) 개인정보처리자의 영업내용

170) 권영준, 전계 논문, 58면.

171) 결과발생의 위험성이 커지면 주의의무의 정도도 높아진다는 취지로, 박동진, “불법행위 법상 주의의무의 기능”, 고시계 45권 11호(2000.11), 38면.

172) 개인정보보호법 시행령 제35조는 개인정보 영향평가의 대상이 되는 개인정보의 양을 다음과 같이 규정하고 있다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 “민감정보”라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만 명 이상의 정보주체에 관한 개인정보파일

173) 권영준, 전계 논문, 58면.

우선 개인정보의 수집과 보관 그 자체가 영업의 주요한 내용을 구성하는 정부기관이나 신용정보기관 등 개인정보처리자의 경우에는 단순히 본래의 영업을 수행하는 과정에서 개인정보를 부수적으로 취득하게 되는 개인정보처리자보다 더욱 강한 주의의무를 부담한다. 그리고 개인정보처리자가 영리적 목적<sup>174)</sup>으로 개인정보를 수집하거나 보관할 경우에는 그렇지 않은 경우보다 더욱 강한 주의의무를 부담한다.<sup>175)</sup>

## (2) 유출 개인정보수집 및 보관의 필요성

법령상 특정한 서비스를 제공하기 위해 개인정보 수집이 의무화 되어 있다면 정보의 수집과 보관은 필수적이거나, 반면 개인정보처리자의 업무수행에 꼭 필요하지 않으면서 사적인 영리추구 등을 위해 개인정보를 수집하는 경우에는 그와 반대이다. 즉 수집이 필수적이지 않은 정보를 수집하거나 보관할 경우 그 관리에 소요되는 인력, 시간, 비용 등이 늘어나고 이는 안전조치의무의 이행을 더욱 어렵게 한다. 따라서 이러한 상황에서 해킹사고가 발생할 경우 주의의무 위반을 더욱 용이하게 인정할 수 있게 된다.<sup>176)</sup> 그러므로 개인정보처리자가 개인정보를 최소한의 범위에서 수집하였는지, 적법하고 정당

---

174) 판례 또한 제3자가 타인의 명의를 도용하여 온라인 게임 서비스에 회원가입을 하였던 사건에서 “온라인 서비스 제공자가 실명정보의 확인의무를 위반하였는지는 (중략) 관련 인터넷기술의 발전 수준, 해당 게임의 특성, 운영 주체로서의 서비스 제공자의 영리적 성격·규모, 기술적 수단의 도입에 따른 일반 이용자에 대한 이익과 불이익 및 이에 따른 경제적 비용, 명의도용행위로 인한 피해의 정도, 가해자와 피해자의 관계 등을 종합하여 판단하여야 한다.”라고 판시하여, 개인정보처리자의 영리적 성격을 고려해야 한다고 판시하였고(대법원 2009. 5. 14. 선고 2008다75676 판결), 고객 정보통신서비스제공자가 고객 600만 명의 개인정보 8,500만 건을 텔레마케팅 업체, 금융기관 등에 제공한 사건에서 개인정보를 제공받은 개인정보처리자가 정보통신서비스제공자였던 경우 개인정보 보호에 대한 고도의 신뢰관계가 형성된 것이므로 그에 따른 주의의무가 인정되어야 한다.“라고 같은 취지로 판시하였다(서울고등법원 2013. 2. 7. 선고 2011나83747 판결).

175) 권영준, 전계 논문, 58면.

176) 권영준, 전계 논문, 57면 내지 58면.



하게 수집하였는지 및 보유기간을 경과하여 보관하고 있지 않았는지 여부 또한 주의의무위반 여부 판단의 고려요소가 된다.

### (3) 개인정보처리자와 해커의 관계

해킹이 내부자에 의해 행하여졌다거나 내부자의 조력을 받아 행하여졌다면 개인정보처리자가 관리적 조치의무를 위반하였다는 판단을 더욱 용이해진다. 개인정보처리자로부터 업무위탁을 받아 개인정보를 관리하는 업체의 내부자가 관여한 경우도 주의의무 위반의 여지가 높아진다.<sup>177)</sup>

#### 라. 외부적 고려요소

최근 선고된 KT 사건의 1심 법원<sup>178)</sup>에서는 정보통신서비스 제공자가 해킹 사고 방지를 위해 취해야 할 선량한 관리자로서의 주의의무를 위반하였는지 여부에 대하여 “자신의 이익을 위하여 이용자의 개인정보를 수집·관리하는 자로서는 시스템 운영체제 또는 서버 프로그램을 구축한 이후에도 기술의 발달 속도에 맞추어 시스템의 보안 수준을 보완하고 기술 개선을 해나가는 등 해킹 당시의 해킹 기술 및 보안 기술의 수준에 비추어 기대가능성 있는 주의의무를 기울여야 한다.”고 전제한 후 주의의무 판단의 기준으로서 “① 관련 법령이 정보통신서비스 제공자에게 요구하고 있는 기술적·관리적 보안 조치의 내용, ② 해킹 당시 당해 정보통신서비스 제공자가 취하고 있던 보안 조치의 내용, ③ 해킹 방지 기술의 발전 정도, ④ 해킹 방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도, ⑤ 해커가 사용한 해킹 기술의 수준, ⑥ 개인정보 유출로 인해 이용자가 입게 되는 피해의 정도 등을 종합적으로 고려하여 판단하여야 할

177) 권영준, 전제 논문, 58면.

178) 서울중앙지방법원 2014. 8. 22. 선고 2012가합81628 판결.

것이다.”라고 상세히 실시하였다.

따라서 해커가 사용한 기술과 대비하였을 때, 정보처리자가 사용하고 있던 기술적 보호조치가 얼마나 적절하고 효율적이었는지 여부가 주의의무의 판단기준이 될 것이다. 따라서 기술적 보호조치의 적합성 판단을 위해 해커가 사용한 기술과 정보처리자가 적용한 기술의 수준의 정도를 나누어 비교할 필요가 있다.

### (1) 해커의 기술 수준

해커가 사용한 기술의 수준이 어느 정도인지가 확정되어야 한다. 인터넷을 통한 해킹은 지역에 제한을 두지 않고 발생한다. 최근 발생한 대형 해킹 사고들 역시 해킹이 이루어진 장소는 중국 또는 해외의 제3국으로 밝혀지는 경우가 많다. 따라서 이러한 해커의 기술 수준은 국내외에 존재하는 모든 해커들의 평균적인 기술수준을 의미하는 것이라고 해야 할 것이며, 해커가 해당 기술을 만들어 내기 위하여 어느 정도의 시간이 소요되었는지, 어떤 과정을 거쳐서 해킹에 성공하였는지, 얼마나 해킹에 숙달되어 있는지 여부<sup>179)</sup> 등을 종합적으로 판단하여 해커의 기술 수준이 보편적인 해킹 기술을 초과하고 있는지 여부를 확정해야 할 것이다.

### (2) 개인정보처리자의 기술적 보호조치 수준

---

179) 위 KT 사건에서도 ① 해커가 10년가량 컴퓨터 프로그램 제작 관련 업무에 종사하기는 하였으나 해킹을 전문적으로 해온 것은 아니라는 점, ② 해커가 피고의 N-STEP 서버가 한 번 사용한 세션 정보에 대해 유효성을 체크하지 않고 계속 사용할 수 있다는 점을 파악한 것에 관하여 이를 미리 구상하지는 않았고, 시도를 하다 보니 알게 된 것이며 일반적으로 프로그램 개발을 하는 사람은 당연히 한 번 쯤 해볼 수 있는 시도였었다는 점, ③ 이 사건 해킹프로그램에 계속 매달려서 개발을 한 것은 아니며 시간이 날 때마다 연구를 하였는데 프로그램의 개발에 3개월 정도가 걸렸다는 점 등 해커가 사용한 기술수준이 높지 않다는 점에 비추어 개인정보처리자의 주의의무위반을 인정할 수 있다고 판시하였다(서울중앙지방법원 2012가합81628 판결).

개인정보처리자의 충분한 기술적 보호조치가 강구되었는지 여부를 판단하기 위해서는 우선적으로는 관련 법령이 정보통신서비스 제공자에게 요구하고 있는 기술적·관리적 보안 조치의 내용이 얼마만큼 준수되었는지 여부가 판단되어야 할 것인데, 이 경우 해킹사고가 발생한 당시의 보편적 기술수준<sup>180)</sup>을 고려해야 한다.<sup>181)</sup>

즉 해킹 당시의 보편적인 기술수준과 개인정보처리자가 실제로 취하였던 조치를 비교한 뒤 후자가 전자에 미치지 못하면 과실인정으로 연결될 수 있다. 반면에 해커가 실제 사용한 해킹 기술에 대처하거나 탐지할 수 있는 기술이 이론적으로 존재하였더라도 그 해킹 기술이 보편적인 기술수준에 비추어서는 막을 수 없는 것이었다면 해킹사고가 발생하였다는 것만으로 과실을 인정할 수 없다. 이와 관련하여 보편적인 기술수준의 준거집단을 어떤 범위로 확정하는가가 중요하다. 이는 국내외에 존재하는 모든 개인정보처리자들의 평균적인 기술수준을 의미하는 것이라고 할 것이 아니라, 적절한 기준에 따라 구획된 동종 집단에 속한 개인정보처리자들의 평균적인 기술수준을 의미한다고 보아야 한다.<sup>182)</sup>

#### 마. 사후조치

해킹이 일어난 이후 사후조치를 취한 시점과 경위, 내용과 방법, 정보주체의 정보통제가능성 등 구체적인 정황을 고려하여야 한다.<sup>183)</sup>

---

180) 보편적 기술수준에 대한 판단과 관련하여 의료판례를 참조할 수 있다. 판례에 의하면 “의사의 주의의무는 의료행위를 할 당시 의료기관 등 임상의학분야에서 실천되고 있는 의료행위의 수준을 기준으로 판단하여야 한다.”라고 판시한다(대법원 1994. 4. 26. 선고 93다59304 판결). 즉 의사가 도달해야 할 의료수준은 객관적·규범적으로 정해지므로 당해 의사나 의료기관의 구체적 상황에 따라 달라져서는 안 된다는 것이다. 이러한 법리는 과실의 객관성 내지 규범성에 비추어 당연한 것으로 개인정보처리자에게도 동일하게 적용된다.

181) 권영준, 전계 논문, 61면

182) 권영준, 전계 논문, 62면.

183) 권영준, 전계 논문, 60면.

## (1) 사후조치를 취한 시점

개인정보보호법 제34조 제1항은 “개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.”라고 규정하고 있다. 따라서 ① 개인정보처리자가 개인정보의 유출사실을 안 때가 언제인지, ② 위 사실을 고지한 시점이 언제인지는 주의의무 위반여부의 중요한 요소가 된다. 위 “지체 없이”의 기준에 대해 표준개인정보보호지침<sup>184)</sup> 제27조는 5일 이내라고 규정하고 있으나, 구체적인 사안에서는 유출의 원인과 규모, 이를 파악하는데 소요되는 시간, 통지에 소요되는 기술적 시간 등에 비추어 개별적으로 판단해야 할 것이다.<sup>185)</sup>

## (2) 사후조치를 취하게 된 경위와 사후조치의 내용

사후조치를 자발적으로 취하게 되었는지 여부, 개인정보 유출로 인한 피해를 최소화 할 수 있는 적절한 대응조치가 마련되었는지 여부, 개인정보 유출 통지가 내용적으로 충분하였는지, 그 방법이 적절하고 효과적이었는지 여부도 주의의무 위반의 고려요소가 되어야 한다.<sup>186)</sup>

### 바. 정리

위에서 검토한 주의의무 판단의 세부적 요소들을 표로 정리하면 다음과 같다.

---

184) 행정안전부고시 제2011-45호, 2011.9.30 제정.

185) 권영준, 전계 논문, 60면.

186) 권영준, 전계 논문, 60면.

[표 7] 주의의무 판단의 세부적 고려요소<sup>187)</sup>

대분류	고려요소	주의의무 판단에 미치는 영향
정보자체	정보의 민감성과 위험성	민감정보 + 위험정보 +
	정보의 양	대량정보 +
개인정보 처리자	개인정보처리자의 영업내용	개인정보처리 자체가 주된 업무내용 인 기관 ++
	정보의 필요성	불필요하거나 필요성이 적은 정보의 수집 +
	해커와의 관계	내부자인 해커 ++ 내부자의 조력을 받은 해커 +
외부적요소	해커의 기술수준	전문해커가 아닌 경우 + 해킹성공에 적은 시간 소요 + 난이도가 적은 일반적 해킹 +
	개인정보처리자의 보호조치수준	보편적인 기술수준 미달 +
사후조치	사후조치의 시점	지연된 사후조치 +
	사후조치의 경위 및 내용	비자발적 사후조치 + 적절한 대응조치의 미이행 +

## 6. 검토

기술수준을 법으로 정하는 것은 오히려 더 많은 문제를 발생시킬 수 있다. 반면 법원의 판결은 이를 보충하고 사업자로 하여금 보다 강력한 안정조치를 취하도록 함으로서 이에 준하는 주의를 기울이도록 할 수 있다.<sup>188)</sup> 그러므로 사업자가 관련 법 규정을 준수하였는지 여부뿐만 아니라 앞서 제시한 주의의무에 대한 모든 판단기준을 준수하였는지 여부를 종합적으로 고려하는 경우에만 비로소 그의 주의의무위반 여부를 판단할 수 있는 것이다.

## II. 재산적 손해에 대한 손해배상책임

187) 표 출처: 권영준, 전계 논문, 66면.

188) 윤주희, 전계 논문, 351면.

## 1. 재산적 손해의 의의

### 가. 재산적 손해의 형태

개인정보의 침해로 인한 재산적 피해는 서비스 제공자가 청구한 서비스 이용료의 형태<sup>189)</sup> 또는 유출된 개인정보의 오·남용으로 인하여 발생하는 형태 예컨대 신용카드 정보를 이용한 결제사고, 예금의 인출을 받는 경우의 형태 등으로 나타난다.

### 나. 재산적 손해의 성질

개인정보의 유출로 인하여 발생하는 재산적 손해는 일반적인 불법행위로 인한 재산적 손해와는 그 성격이 다르다. 일반적인 불법행위로 인한 재산적 손해가 일차적으로 발생하지만, 개인정보의 유출로 인하여 발생하는 일차적인 손해는 정보주체의 인격권 침해 즉, 정신적 손해이다. 반면 재산적 손해는 유출된 개인정보가 오·남용되어 발생하는 후속손해에 해당한다.

### 다. 재산적 손해에 대한 판례의 태도

#### (1) 판시 내용

개인정보의 유출로 인한 재산적 손해를 판단한 한 하급심은,<sup>190)</sup> “일반적으로 타인의 불법행위로 인하여 재산권이 침해된 경우에 특별한 사정이 없는 한 그 재산적 손해의 배상에 의하여 정신적 고통도

---

189) 이승길, “정보화 사회에서의 개인정보권의 침해와 그 구제”, 중앙법학 제11집 제1호, 74면.

190) 서울중앙지방법원 2011. 11. 11. 선고 2010가합118427 판결.

회복된다고 보아야 할 것이고, 재산적 손해의 배상만으로는 회복할 수 없는 정신적 손해가 있다면 그 위자료를 인정할 수 있다(대법원 2003. 7. 25. 선고 2003다22912 판결 참조).”는 점을 전제로 하여 원고에게 영업이익 감소 이외에 재산적 손해의 배상만으로 회복될 수 없는 정신적 손해가 발생하였다는 점을 인정할 만한 자료가 없다는 이유로 원고의 정신적 손해에 대한 청구를 기각하였다.

## (2) 판례의 태도에 대한 비판적 검토

해당 판결은, 개인정보의 유출로 인한 손해를 타인의 불법행위로 인하여 “재산권”이 침해된 경우로 전제한 후, 재산적 손해가 배상된 경우에는 특별한 경우가 아닌 이상 정신적 손해를 인정할 필요가 없다고 판단한 것으로 보인다.

그런데, 아직까지의 우리 판례는 일관되게 개인정보의 유출로 인한 피해를 인격권인 개인정보자기결정권에 의한 피해로 파악하고 있고, 개인정보자기결정권을 재산권으로 판단한 선례는 존재하지 않는다. 따라서 위 판례는 우선 개인정보 유출 사고를 재산권의 침해로 전제하였다는 점에서 논리 상 오류를 범하고 있다.

물론 개인정보의 유출로 인한 후속의 재산적 손해가 인정되었다는 사실만으로, 정신적 손해의 발생이 항상 인정되어야 하는 것은 아니다. 정신적 손해의 발생 여부에 대해서는 유출된 개인정보 성격, 가해자 및 피해자의 여러 가지 참작 요소, 전후사정 등이 다양하게 고려되어야 할 것인데, 후속의 재산적 손해가 발생하였다는 사실만으로 위의 모든 요소들이 충족되었다고는 할 수 없기 때문이다.

그러나 위 판례는 정신적 손해의 발생에 대하여 이러한 참작요소들에 대하여 전혀 판단을 하지 않고, 개인정보의 침해를 재산권의 침

해와 동일한 것으로 전제하여 재산적 손해의 배상이 이루어지면 특별한 사정이 없는 한 정신적 고통이 회복되었다고 판단한 것인 바, 위 판결에는 개인정보의 인격적 특성에 대한 판단을 그르친 잘못이 있다고 볼 것이다.

## 2. 재산적 손해의 범위

개인정보의 유출로 인하여 발생한 재산상 손해는 침해 행위와 상당인과관계가 있는 통상의 손해를 기본적인 배상범위로 할 것이고 특별한 손해에 대하여는 예견가능성이 인정되는 경우에만 손해배상책임이 인정되어야 한다.<sup>191)</sup>

구체적인 재산상 손해의 사례를 보면 정보주체가 제공한 개인정보를 사업자 등이 목적 외로 이용하여 정보주체 모르게 서비스에 가입되어 서비스 이용요금이 청구되는 경우, 타인이 정보주체의 개인정보를 도용하여 서비스에 가입하여 정보주체에게 서비스 이용료가 청구되는 경우 등이 있다. 이런 경우 재산적 손해액은 다른 입증이 없으면 영수증이나 청구서 및 통장사본 등 객관적으로 증명되는 피해액을 기준으로 해야 할 것이다. 청구서 등에 의한 정확한 산정이 불가능한 경우에는 합리적으로 피해액을 추정할 수밖에 없다고 한다.<sup>192)</sup>

## 3. 재산적 손해의 범위에 대한 판례

### 가. 판시 내용

위 서울중앙지방법원 사건에서 원고는 피고의 DB유출사고 이후 원

---

191) 이승길, 전계 논문, 74면.

192) 이창범, 김본미, 전계 논문, 108면.



고의 단문 문자메시지 평균 발송건수가 급감하였다는 것을 이유로 문자메시지 감소 해당액인 62,528,625원의 70%인 43,770,037원을 재산상 손해로 청구하였는데, 이러한 원고의 주장에 대해 법원은 문자메시지 발송 감소에 따른 손해 전부가 피고들의 불법행위와 상당인과관계에 있다고 보기 어렵다고 전제한 뒤 다음과 같이 판시하였다.

“불법행위로 인한 손해배상청구소송에서 재산적 손해의 발생 사실은 인정되나 구체적인 손해의 액수를 증명하는 것이 사안의 성질상 곤란한 경우, 법원은 증거조사의 결과와 변론 전체의 취지에 의하여 밝혀진 당사자들 사이의 관계, 불법행위와 그로 인한 재산적 손해가 발생하게 된 경위, 손해의 성격, 손해가 발생한 이후의 여러 정황 등 관련된 모든 간접사실들을 종합하여 손해의 액수를 판단할 수 있다. (중략) 원고는 피고들의 위와 같은 불법행위로 인하여 10,000,000원의 재산적 손해를 입었다고 봄이 상당하다.”<sup>193)</sup>

#### 나. 판례에 대한 검토

위 판결은 개인정보의 유출로 인한 후속 손해 전부를 인용한 것은 아니지만, 후속 손해인 재산적 손해의 일정 부분을 인용하였고, 재산적 손해의 산정이 곤란한 경우는 “당사자들 사이의 관계, 불법행위와 그로 인한 재산적 손해가 발생하게 된 경위, 손해의 성격, 손해가 발생한 이후의 여러 정황” 등 기존에 판례가 실시한 위자료 산정의 제요소들을 참작할 수 있다고 판시한 점에 의의가 있다.

그러나 한편으로는 액수와 상당인과관계를 증명하기 어려운 재산적 손해가 발생한 경우 이를 굳이 무리하게 재산적 손해로 판단할 필요 없이, 위자료의 보완적 기능<sup>194)</sup>을 통하여 위자료의 증액사유로 판단

193) 서울중앙지방법원 2011. 11. 11. 선고 2010가합118427 판결.

194) 대법원 1984. 11. 13. 선고 84다카722 판결은 위자료의 보완적 기능과 관련하여 “재산상

할 수 있었다는 점에서 위 판결에 대한 비판이 가능할 것이다.

#### 4. 개인정보의 객관적인 재산적 가치 평가에 대한 문제

개인정보의 상업적 가치가 인정되면서 개인정보의 재산적 가치측정에 대해서도 사회적으로 많은 관심을 촉발되었다. 그러나 개인정보는 무형의 가치이고 정보주체의 표본을 설정하는 것도 쉽지 않은 문제이기 때문에, 개인정보의 재산적 가치를 현실적으로 측정하기 어려운 것이 사실이다.<sup>195)</sup>

그런데 최근 정보주체들에 대한 설문조사 및 사례분석 등을 통하여 개인정보의 객관적 재산적 가치를 산출한 연구들이 다수 존재한다. 한 연구에서는 정보주체의 개인정보의 재산적 가치는 비보호하에서는 평균값이 16만 9,900원이고, 강보호하에서는 평균값이 12만 3,000원, 약보호하에서는 13만 5,100원이라는 객관적인 수치를 산출하기도 하였다.<sup>196)</sup> 이러한 연구는 개인정보를 시장에서 교환되는 품목으로 보고 개인정보를 시장원리로 해결하려는 경제분석가들의 지지를 받는다고 한다.<sup>197)</sup>

다만 아직까지는 개인정보를 하나의 시장거래품목으로 보아서 그

---

손해의 발생이 인정되는 데 입증곤란 등의 이유로 그 손해액의 확정이 불가능하여 그 배상을 받을 수 없는 경우에 이러한 사정을 위자료의 증액사유로 참작할 수 있다고 할 것이나, 이러한 위자료의 보완적 기능은 재산상 손해의 발생이 인정되는 데도 손해액의 확정이 불가능하여 그 손해 전보를 받을 수 없게 됨으로써 피해회복이 충분히 이루어지지 않는 경우에 이를 참작하여 위자료액을 증액함으로써 손해전보의 불균형을 어느 정도 보완하고자 하는 것이므로 합부로 그 보완적 기능을 확장하여 그 재산상 손해액의 확정이 가능함에도 불구하고 편의한 방법으로 위자료의 명목 아래 사실상 손해의 전보를 꾀하는 것과 같은 일은 허용되어서는 안 될 일이다.”라고 판시하였다.

195) 이창범, 김분미 전계 논문 110면.

196) 정보통신정책연구원, “개인정보보호 제도 시행의 경제·사회적 파급효과 분석연구(2001. 12.)

197) 한국정보보호진흥원, “개인정보의 경제적 가치 산정 연구의 필요성”, 2001. 12. 15면 내지 23면.

경제적 가치를 환산할 만한 교환가격을 산출할 만한 확실한 방법은 확립되어 있지 않다.<sup>198)</sup> 판례도 개인정보에 대한 절대권을 인정하지는 않고 있다. 더군다나 개인정보의 경제적 가치를 추산하여 개인정보의 침해를 재산권의 침해로 보는 이론은 개인정보통제권을 인격권의 일종으로 보는 우리 법제 하에서는 논리적으로 타당성이 부족할 수 있다. 따라서 개인정보 자체를 재산으로 보고 그 가치를 객관적으로 산출하기는 어렵고, 결국 개인정보의 유출은 정신적 손해배상의 문제로 귀결될 수밖에 없는 것이다.<sup>199)</sup>

다만 개인정보의 재산적 가치를 측정하는 이론들이 제시한 개인정보의 가치평가 방식은 정보주체의 개인적인 감각, 즉 심리적 보상 개념에 근거하고 있는 경우가 많은 것으로 보인다. 따라서 개인정보의 재산적 가치를 측정하려는 위 연구들의 본질은 미국에서 말하는 명예 또는 프라이버시 침해로 인한 “추정적 손해”의 일종으로 파악할 수 있고, 이러한 점에서 개인정보의 재산적 가치를 측정하는 연구들이 제시한 개인정보의 객관적 가치는, 개인정보를 유출 당했을 때 정보주체에게 발생하는 정신적 손해의 정도를 평가하는 수단으로 기능할 수 있을 것으로 생각한다.

### Ⅲ. 정신적 손해의 발생

#### 1. 정신적 손해배상의 의의

정신적 손해배상 혹은 위자료는 정신상의 고통을 금전으로 위자하기 위하여 지급되는 금원을 말한다. 그 정신상의 고통은 과거 또는 현재의 것뿐만 아니라 장래의 고통도 보통 기대되는 합리적인 만큼을 포함한다.<sup>200)</sup> 판례는 “위자료는 그 청구권자가 피해 당시 정신상

---

198) 이창범, 김분미, 전계 논문, 105면

199) 이창범, 김분미, 전계 논문, 111면.

고통에 대한 감수성을 갖추고 있지 않다 하더라도 장래 이를 감수할 것임이 현재 합리적으로 기대될 수 있는 경우에 있어서는 역시 청구될 수 있다”라고 한다.<sup>201)</sup> 정신적 고통이라는 비재산적 손해에 대한 배상인 위자료의 성질에 관하여는 학설상 그 본질을 손해배상으로 보는 배상설과 가해자에 대한 제재적 요소를 강조하는 제재설이 대립하고 있다.<sup>202)</sup>

## 2. 정신적 손해의 특성

### 가. 객관적 측정의 곤란성

위자료는 정신적 손해에 대한 배상금이다. 그런데 정신적 손해는 부정형하여 객관적으로 계량화하기 어렵다. 따라서 위자료 산정에 대한 통일적이고 구체적인 기준을 만드는 것은 극히 곤란하다.<sup>203)</sup>

### 나. 개인에 따른 차이

흥미로운 것은 정신적 손해 자체가 이와 같이 부정형한 것뿐 아니라, 개인정보의 유출로 인하여 발생할 수 있는 정신적 손해 즉 심리적 불안의 정도 또한 성별, 이용량, 이용 빈도에 따라 개인별로 차이가 있다는 점이다.

이와 관련하여 한 연구는 ① 내 개인정보가 인터넷상에 떠돌까 불안하다, ② 나는 개인정보를 제시하는 것에 대해서 불안하다, ③ 내 개인정보가 인터넷에 유출될까 불안하다 등의 질문을 남성 178명, 여성 198명에게 하여, 스피이버거(Spielberger)의 상태 불안 척도(State

---

200) 이창범, 김분미 전계 논문 112면.

201) 대법원 1993. 4. 27. 선고 93다4663 판결.

202) 이창범, 김분미 전계 논문 112면.

203) 정상조, 박준석, 전계 논문, 45면.

Anxiety Scale)<sup>204)</sup>를 활용하여 개인정보의 유출 염려로 인한 심리적 불안을 상대적으로 측정하였다.<sup>205)</sup>

위 연구결과에 의하면 개인정보의 유출에 대한 우려로 인한 여성의 심리적 불안도가 3.56으로, 남성의 심리적 불안도인 3.29 보다 높았다. 인터넷 사이트 가입 수에 따른 심리적 불안도 또한 1~10개 미만의 경우가 3.33인 것과 비교하여, 10~20개 미만의 경우는 3.40, 21개 이상의 경우는 3.60으로 가장 높은 수치를 보였다.<sup>206)</sup> 위 연구는 잠재적 개인정보 유출사고에 대한 심리적 불안도의 정도에 관한 것이기는 하나, 이는 곧 개인정보의 유출로 인하여 정보주체가 느끼는 정신적 손해의 정도로 평가할 수 있을 것으로 보인다.

#### 다. 검토

즉 개인이 받는 정신적 손해의 정도를 수치화하여 산정하는 것이 어려운 이유는 정신적 손해가 무정형하여 측정할 수 없기 때문만이 아니고, 동일한 사고에 대해서도 개인마다 느끼는 정신적 손해의 정도가 매우 다르기 때문인 것으로 보인다.

따라서 정신적 손해에 대한 산정이 아무런 기준 없이 법원에 의하여 자의적으로 이루어지는 것은 곤란하다. 이에 정신적 손해 산정에 가급적 자의성을 배제하고, 예측가능성과 검증가능성을 높이기 위하여 정신적 손해 산정에 고려할 요소들을 미리 체계화·유형화 하는 연구가 계속 되어야 하고, 법원 또한 판결문에 이를 가급적 드러내려는 노력을 기울여야 할 것이다.<sup>207)</sup>

---

204) 김정택, “특성불안과 사회성과의 관계: Spielberger의 STAI를 중심으로”, 고려대학교 석사학위논문, 1978.

205) 진성철, 김인경, “인터넷 이용자의 개인정보 유출 가능성에 대한 심리적 불안에 관한 연구: 성별, 이용량, 이용 빈도를 중심으로”, 중앙대학교, 2011. 10. 734면.

206) 진성철, 김인경, 전계 논문, 735면~736면.

207) 정상조, 박준석, 전계 논문, 46면.

### 3. 정신적 손해배상의 기능

#### 가. 손해배상의 기능

불법행위법의 전통적인 목적은 가해자의 잘못으로 인하여 파괴된 원래의 정의로운 상태를 회복하여 주는 것이다. 손해배상제도는 기본적으로 손해전보를 주된 기능으로 하는 제도이다. 그리고 전보되어야 할 손해는 ‘확정적이고 현실적인’ 손해이다. 만약 이러한 요건을 갖추지 못한 덜 익은 불이익에 대하여 자유롭게 손해배상을 명할 수 있게 된다면, 민주적 정당성이 결여된 법원에 의하여 단순한 교정의 범위를 넘어서는 부의 재분배가 초래될 수 있어 타당하지 않다.<sup>208)</sup>

그러나 불법행위법은 사회 구성권들에게 바람직한 행인지침을 제시하고 그러한 행위로 나아갈 인센티브를 부여함으로써 불법행위를 예방하게 하려는 목적도 추구한다. 즉 개인의 행동의 자유를 보장하기 위해서는 무엇이 허용되고 허용되지 않는지에 대해 불법행위법이 개인에게 구체적인 메시지를 발신할 수 있어야 한다. 이를 통해 개인은 불법행위로 인한 외부효과를 내부화하여 행위할 적정한 동기를 가지게 되고, 이러한 불법행위법의 예방적 기능을 통해 불법행위가 사회적으로 적정하게 억제된다. 그러한 점에서 불법행위법의 요건 중 하나인 과실판단에 관한 한 이른바 예방 패러다임이 중요한 기능을 수행하게 된다.<sup>209)</sup>

#### 나. 위자료의 기본적 기능

---

208) 정상조, 권영준, 전계 논문, 43면.

209) 권영준, 전계 논문, 47면.

전통적으로 논의되는 위자료의 기능으로는 손해의 전보 기능과 제재적 기능, 만족적 기능이 있다.<sup>210)</sup> 특히 비재산적 손해배상의 영역에서는 예방이 주도적이지는 않더라도 상당히 의미 있는 기능을 수행한다. 회복기능이 온전히 수행되려면 우선 회복되어야 할 손해액이 정확하게 산정되어야 한다. 그런데 비재산적 손해는 재산적 손해보다 그 범위를 확정하기 어렵다.<sup>211)</sup> 또한 재산적 손해에 대한 재산적 회복에 비하여 비재산적 손해에 대한 재산적 회복이 과연 전보의 기능을 온전히 달성할 수 있는지도 의문이다. 이러한 이유 때문에 위자료 액수를 산정함에 있어서는 예방적, 정책적, 규범적 판단이 개입할 여지가 커진다. 그것이 위자료의 액수를 정하는 실체적인 기준을 제공할 수 있기 때문이다. 인격권침해에 대한 위자료의 만족적·제재적 측면도 이와 같은 예방 패러다임의 작동으로 설명할 수 있다. 따라서 개인정보침해로 인한 위자료 산정에 있어서도 어느 정도의 예방적, 정책적, 규범적 판단이 불가피하다.<sup>212)</sup>

다만 이러한 개인정보침해와 같은 인격권침해의 위자료산정에 있어서 예방적, 정책적, 규범적 판단은 쉽게 규정할 수 없는 회복의 내용을 보충적으로 형성하기 위한 것이지, 회복을 배제하거나 뛰어넘는 것이 아니라는 점을 주지해야 할 것이다.<sup>213)</sup>

#### 다. 위자료의 보완적 기능

오늘날 재산적 손해와의 관련성을 고려하여 새로운 기능이 등장하고 있다. 대법원은 재산상 손해의 발생이 인정되는데도 입증곤란 등의 이유로 그 손해액의 확정이 불가능하여 배상을 받을 수 없게 됨

---

210) Bamberger-RoU, Kommentar zum Bürgerlichen Gesetzbuch. Band 1. ErbbauVO. WFXi, 1.Aufl.(2003), § 253 Rn. 15 21 ; BGHZ 18, 149.

211) 정상조, 권영준, 전계 논문, 49면.

212) 정상조, 권영준, 전계 논문, 50면.

213) 정상조, 권영준, 전계 논문, 51면.

으로써 피해회복이 충분히 이루어지지 않는 경우에는 이를 참작하여 위자료를 증액함으로써 손해전보의 불균형을 어느 정도 보완할 수 있다고 한다.<sup>214)</sup> 그리하여 대법원은 원고가 재산상 손해배상청구권을 모두 포기하고 그 금원을 위자료로서 구하는 경우, 이를 허용하고 있으나,<sup>215)</sup> 한편으로는 함부로 그 보완적 기능을 확장하여 재산상 손해액의 확정이 가능함에도 불구하고 편의한 방법으로 위자료의 명목 아래 사실상 재산상 손해의 전보를 피하는 것은 허용되지 않는다고 한다.<sup>216)</sup> 일반적으로 이를 위자료의 보완적 기능이라고 한다.<sup>217)</sup>

다만 위자료의 속성상 재산적 손해배상에 대한 어느 정도의 보완적 기능을 가지는 것은 불가피하지만<sup>218)</sup> 그 정도를 넘어 만연히 재산적 손해배상의 대체물로 활용되어서는 안 된다고 한다. 특히 손해삼분설에 따라 재산적 손해배상청구와 위자료청구를 엄격하게 구별하는 우리나라에서는 더욱 그러하다.<sup>219)</sup>

#### IV. 정신적 손해배상의 범위

##### 1. 우리 민법상 기준

위자료청구권의 발생 원인으로 명예권, 성명권, 초상권, 사생활의 비밀과 자유, 생명, 신체, 자유, 기타 인격권 등에 대한 침해가 예시되고 있다. 그러나 우리 민법은 위자료의 산정 방법이나 산정 시에 고려하여야 할 요인에 관하여는 아무런 규정을 두지 않고 있다.

---

214) 대법원 1984. 11. 13. 선고 84다카722 판결.

215) 대법원 1980. 11. 11, 선고 80다1924 판결.

216) 이창범, 김분미, 전계 논문, 112면.

217) 서종희, “비재산적 손해배상(위자료)과 ‘정신적 고통’과의 관계 - 법인의 무형손해를 중심으로”, 2011. 5. 동아법학 제51호, 313면.

218) 대법원 1984.11.13 선고 84다카722 판결

219) 정상조, 권영준, 전계 논문, 46면.



판례는 타인의 불법행위로 인하여 입은 정신상의 고통은 금전으로 계량할 수가 없는 무형의 손해로서, 감정기타의 증거방법에 의하여 그 수액을 증명할 수가 없으므로 당사자는 증거에 의하여 이를 증명할 필요가 없고,<sup>220)</sup> 따라서 법원은 위자료액의 결정을 위한 별도의 증거를 필요로 함이 없이 그 직권에 의하여 여러 가지 사정을 참작하여 재량으로 그 액수를 결정하면 되는 것이라고 한다.<sup>221)</sup>

판례에 의하여 제시된 위자료 산정의 구체적인 참작사유로는 피해자의 피해정도, 연령, 성별, 직업, 재산상태, 생활상태, 교육정도, 과실유무 및 과실정도와 가해자의 고의 또는 과실의 정도, 직업, 재산상태 및 배상책임자의 생활상태 등이 있다.

## 2. 개인정보 유출로 인한 위자료에 대한 우리 판례의 태도

최근 개인정보 유출사고와 관련하여 위자료 산정에 있어 판례는 개별적인 사건의 유형에 따라 다양한 위자료의 산정요소를 제시하고 있다.

GS칼텍스 사건<sup>222)</sup>, KT 사건<sup>223)</sup>, SK커뮤니케이션즈 사건<sup>224)</sup>에서 판례는 “개인정보를 처리하는 자가 수집한 개인정보를 그 피용자가 해당 개인정보의 정보주체의 의사에 반하여 유출한 경우, 그로 인하여 그 정보주체에게 위자료로 배상할 만한 정신적 손해가 발생하였는지 여부는, ① 유출된 개인정보의 종류와 성격이 무엇인지, ② 개인정보의 유출로 정보주체를 식별할 가능성이 발생하였는지, ③ 제3자

---

220) 대법원 1959. 8. 27. 선고 4292민상12 판결.

221) 대법원 1976. 2. 10. 선고 75므33 판결.

222) 대법원 2012. 12. 26. 선고 2011다59834, 59858, 59841 판결.

223) 서울중앙지방법원 2014. 8. 22. 선고 2012가합81628 판결.

224) 서울서부지방법원 2013. 2. 15. 2011가합11733 판결.

가 유출된 개인정보를 열람하였는지 또는 제3자의 열람 여부가 밝혀지지 않았다면 제3자의 열람 가능성이 있었거나 앞으로 그 열람 가능성이 있는지, ④ 유출된 개인정보가 어느 범위까지 확산되었는지, ⑤ 개인정보의 유출로 추가적인 범익침해의 가능성이 발생하였는지, ⑥ 개인정보를 처리하는 자가 개인정보를 관리해온 실태와 ⑦ 개인정보가 유출된 구체적인 경위는 어떠한지, ⑧ 개인정보의 유출로 인한 피해의 발생 및 확산을 방지하기 위하여 어떠한 조치가 취하여졌는지 등 여러 사정을 종합적으로 고려하여 구체적 사건에 따라 개별적으로 판단하여야 한다.”라고 판시하였다.

한편 LG전자 사건<sup>225)</sup>에서 판례는 “① 개인정보를 처리하는 자가 취한 사고 당시의 보안조치의 수준, ② 사고발생 후 얼마나 신속하게 사고를 파악하고 적시에 적절한 피해확산방지조치를 취하였는지 여부, ③ 피해자의 자기정보통제권과 관련하여 피해자에 대한 사고발생 안내의 적절성 및 피해접수 내지 확인, 피해회복조치 이행 여부, ④ 유출된 정보의 성격 및 유출된 정보의 양, ⑤ 정보가 유출된 범위 및 유출된 정보의 전파가능성, ⑥ 스팸메일이나 명의도용 등 추가적인 피해 발생 여부, ⑦ 개인정보를 처리하는 자가 개인정보를 수집, 처리함으로써 얻는 이익 등은 그 액수를 산정하는 중요한 요소가 될 것이다.”라고 판시하였다.

이에 따라 우리 판례는 개인정보 자체, 개인정보처리자와 정보주체의 각 사정 및 사고전후의 정황 등 모든 사정을 종합적으로 고려한 후 위자료의 액수를 대략적으로 원고 1인당 5만원에서 30만원 정도 이 금액으로 판단하고 있다.

### 3. 비교법적 정신적 손해 산정의 원칙

---

225) 서울고등법원 2008. 11. 25. 선고 2008나25888 판결.

## 가. 미국에서의 논의

미국에서 별도의 독자적(비재산적) 손해가 없이 정신적 고통만이 있는 경우를 순수한 정신적 고통(pure emotional distress)이라고 한다. 이러한 손해와 관련하여서는 전통적으로 고의에 의한 경우와 과실에 의한 경우가 달리 취급되어왔다.<sup>226)</sup>

고의에 의한 경우에 대한 Restatement (Second) of Torts § 46은 가해자가 ① “고의 또는 현저한 부주의(recklessly)”로 ② “극단적이고 포악한(extreme and outrageous)행동을 하여” 피해자에게 ③ “중대한(severe) 정신적 고통”을 가한 경우에 배상책임을 인정한다.

과실로 정신적 고통을 야기한 경우(negligent infliction of emotional distress; NIED)의 책임요건은 더욱 엄격하다. 보통법은 본래 잘못 부고(訃告)를 전한 경우 외에는 과실로 정신적 고통을 야기하여도 불법행위가 성립한다고 보지 아니하였다. 이러한 경직된 입장은 오늘날 상당 부분 극복되었다고 한다.<sup>227)</sup> 그러나 여전히 다수의 주에서는 과실에 의한 정신적 고통 야기가 불법행위가 되려면 적어도 가해자가 피해자를 물리적으로 충격(physical impact)하여야 한다거나, 정신적 고통이 육체적으로 드러나거나 기타 증상, 가령 진료기록 등으로 확인되어야 한다는 입장을 취하고 있다.<sup>228)</sup>

## 나. 캐나다에서의 논의

캐나다에서는 앞에서 검토한 Townsend v. Sun Life Financial 사건

---

226) 이동진, “미국 불법행위법상 비재산적 손해의 배상과 그 한계”, 민사법학 제 66 호 (2014.3), 286면.

227) 이동진, 전제 논문, 288면.

228) Metro-North Commuter R.R. Co. v. Buckley, 521 U.S. 424 (1997); Keck v. Jackson, 593 P.2d 668 (1979); Reynolds v. Highland Manor, Inc., 954 P.2d 11 (1998)

에서 개인정보유출로 인한 손해배상액의 산출에 대해 ① 손해배상이 법에서 추구하는 일반적인 목적에 부합하는지, ② 개인정보유출 예방을 위해 필요한지, ③ 유출의 심각성 등을 종합적으로 고려해야 한다고 하였다. 특히 유출의 심각성 여부는 유출이 정보주체의 건강, 안녕, 거래 및 경제 활동에 미치는 영향, 유출한 자의 유출 전후 행위, 법 위반자가 유출로 인해 이득을 얻었는지 여부에 따라 결정된다고 판시하였다.<sup>229)</sup>

## 다. 일본에서의 논의

### (1) 위자료에 대한 일반적 논의

일본의 법원실무에서는 동일한 사고로 인하여 발생하는 신체상해를 이유로 재산적 손해와 정신적 손해에 대한 배상을 청구하는 경우에, 재산상의 손해와 정신상의 손해는 원인사실 및 피침해이익이 같은 것이므로 그 배상의 청구권은 1개이고 그 양자의 배상을 소송상 병합하여 청구하는 경우에도 소송물을 1개로 본다. 따라서 일본에서는 재산적 손해와 위자료를 개별적으로 산정하는 것을 단념하고 양자를 전체적으로 산정한다.<sup>230)</sup> 또한 신용훼손에 따른 무형의 손해에 대해서 금전적 평가가 가능하도록 입증하는 것은 지극히 곤란하다고 볼 수 있는데, 이 때 일본 판례는 일본 민사소송법 제248조를 적용하여 산정의 이유나 기준을 명확히 밝히지 않은 채 손해배상액을 인정한다.<sup>231)</sup>

### (2) 명예훼손으로 인한 위자료 산출에 대한 논의

229) *Townsend v. Sun Life Financial* (Ottawa, Ontario, May 8, 2012)

230) 김선석, “위자료의 산정과 그 기준에 관한 제문제.” 재판자료 제21집(법원행정처), 1984. 360면.

231) 일본 민사소송법 제248조는 “손해가 발생한 것이 인정되는 경우에 손해의 성질상 그 액을 입증하는 것이 지극히 곤란한 때에는 법원은 구두변론의 진 취지 및 증거조사의 결과에 의하여 상당한 손해액을 인정할 수 있다.”고 규정하고 있다.

한편 일본에서는 명예훼손 사건에 대해 가해자 측과 피해자 측의 사정을 참작한 위자료 산정기준이 논의되고 있다.<sup>232)</sup> 명예훼손 또한 인격권이나 프라이버시의 침해행위에 대한 평가를 기본적인 기준으로 하고 있다는 점에서 개인정보 침해로 인한 의한 위자료 산정에 참고가 가능할 것으로 생각되어 아래와 같은 기준을 검토한다.

미국의 학설도 개인정보 침해로 인한 정신적 손해를 인정하느냐의 문제는 프라이버시법(The Privacy Act of 1974) 하에서 정신적 피해를 손해로 인정할 수 있느냐의 문제로 귀속된다고 하고 있고,<sup>233)</sup> 미국 판례 또한 Doe v. Chao 사건<sup>234)</sup>에서 프라이버시법 위반으로 인한 피해보상은 명예훼손으로 인한 피해보상과 유사하다고 판시하고 있으므로, 개인정보 유출로 인한 위자료 판단에 대하여 명예훼손의 판단기준을 참작할 필요성이 충분하다.

[표 8] 일본 명예훼손법상 위자료의 산출방식<sup>235)</sup>

		산정요소	가감 기준
가해자 측의 사정	동기·목적	고의	+ 10
		애우 악질	+ 8
		악질	+ 6
		기타	+ 3
	기사내용	부적절한 표현	+ 8
		개인공격적 표현	+ 10
		얼굴사진 게재	+ 10
	진실성	완전결여	+ 10
		결여	+ 8

232) 이창범, 김본미, 전계 논문, 133면.

233) The Privacy Act of 1974 prohibits the government from disclosing private information intentionally, without the individual's consent, and provides for a \$1,000 minimum fine if the individual is "adversely affected." - 미국신문기사

<http://archive.wired.com/politics/security/news/2003/12/61439>

234) Doe v. Chao, 540 U.S. 614 (2004)

235) 출처: 이창범, 김본미, 전계 논문, 134면 내지 136면.

	상당성	공공이해 있음	-4
		공공목적 있음	-4
		오신의 고도의 상당성	-7
		논평의 고도의 상당성	-7
	배포의 방법과 범위	TV, 인터넷	+10
		전국판 신문	+9
		주간지	+8
		단행본	+7
		기타	+5
	배포를 통해 얻은 이익	극대	+10
대		+8	
소		+4	
피해자 측의 사정	사회적 지위	텔런트	+10
		국회의원, 변호사	+8
		기타	+5
		공인	+7
		개인	+8
		법인	+6
	사회적 평가의 저하	대	+10
		중	+7
		소	+5
	영업상의 불이익	대	+10
		중	+7
		소	+5
	사회생활상의 불이익	대	+10
		중	+7
		소	+5
	피해자의 파실	대	-10
		중	-8
		소	-6
	배포 후의 피해회복 조치	양	-6
		불량	+3

#### 4. 검토

우리 판례는 개인정보 유출로 인한 위자료를 산출함에 있어, ① 개인정보 자체와 관련하여, 개인정보의 종류와 성격, 정보주체의 식별 가능성, 유출된 정보의 양, 유출된 개인정보의 확산 범위, 유출된 개인정보의 현실적 열람 여부, 열람가능성이 있는지 여부, 추가 범의

침해가 있는지 여부, ② 정보주체와 관련하여 추가 법익침해 가능성이 있는지 여부, ③ 개인정보처리자와 관련하여, 개인정보의 관리실태, 보안조치의 수준, 개인정보가 유출된 경위, 개인정보를 수집, 처리함으로써 인하여 얻는 이익, ④ 사후조치와 관련하여, 유출로 인한 피해의 발생 및 확산을 방지하기 위한 조치가 적시에 취해졌는지 여부, 피해회복조치가 내용상 적절하였는지 여부 등을 제시하고 있다. 이러한 여러 가지 사정을 참작하여 법원이 재량으로 위자료의 액수를 정하고 있는 것이다.

그러나 법원이 직권에 의하여 이러한 여러 가지 사정을 참작하여 자유재량으로 위자료를 산정한다고 하더라도 법관의 자의가 허용되어서는 안 될 것이고, 그 시대와 사회의 일반적인 법감정에 부합될 수 있는 액수가 산출되어야 한다. 그리고 위자료산정에 있어서 법원에 따라 차이가 생긴다든지 또는 법관에 따라 차이가 생긴다든지 하는 것도 형평과 법적안정성을 위하여 가능한 방지되어야 한다.<sup>236)</sup>

이러한 점에서 개인정보 유출사고와 같이 비교적 동일유형의 사건을 다수 처리하게 되는 경우에는, 위자료에 관한 기준화·유형화 내지 정액화의 방안이 마련되고 활용되어야 하는 것이다. 이에 아래에서는 개인정보 유출로 인한 위자료 인정여부 및 위자료액수 산출시 참작해야 하는 요소에 대하여 크게 ① 개인정보와 관련한 요소, ② 정보주체(피해자)와 관련한 요소, ③ 개인정보처리자(가해자)와 관련한 요소로 나누어 그 하위 고려요소를 세부적으로 검토함으로써 위자료액수 산정에 있어 정형화를 도모하고자 하였다.

## V. 정신적 손해배상액 산출의 참작요소

### 1. 개인정보자체와 관련한 요소

236) 박준서, 주식 민법 {채권각칙(8)}, 2000. 2. (제3판), 751면.

손해발생의 여부 및 손해배상액의 산정에 있어서 고려해야 할 요소가 아주 다양하겠지만 궁극적으로는 침해대상인 개인정보의 가치를 무엇으로 볼 것인가에 의해서 크게 좌우된다.<sup>237)</sup> 즉 개인정보 유출로 인한 손해발생 판단 여부의 첫 단계에서는 어떤 종류의 개인정보가 어떠한 방식으로 노출되었는지가 확정되어야 한다.

## 가. 개인정보의 종류 및 성격

### (1) 침해정보의 민감성

침해된 개인정보에 어떤 종류의 개인정보가 포함되어 있는지를 확인해야 할 것이다. 예컨대 개인의 성생활에 대한 정보가 유출된 경우와 개인의 전화번호 또는 이메일 주소가 노출된 경우를 동일선상에 두고 동일한 정신적 손해가 발생하였다고 할 수는 없다.

일반적으로 성명, 주소, 생년월일, 주민등록번호, 주소, 가족관계 등 인적 동일성을 확인하는 데에 사용되는 기본적인 인적사항보다 건강정보, 사상적 경향, 신용정보, 계좌정보 등 재산정보, 성생활에 관한 정보 등 내부적 특징에 관한 정보가 민감성이 높다고 할 것이다.

특히 개인정보보호법 제23조는 “사상, 신념, 과거의 병력 등 개인의 권리·이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보”에 대해서, 정보통신망법 제23조는 “사상, 신념, 가족 및 친인척관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보”에 대해서 각 수집을 제안하고 있으므로, 개인정보처리자의 주의의무가 가중된 만큼 유출된 개인정보가 사상, 신념, 과거의 병력, 가족 및 친인척관계, 학

---

237) 정상조, 권영준, 전계 논문, 33면.



력, 기타 사회활동 등 개인의 권리·이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보의 유출에 해당하는 경우에는 손해배상책임이 더욱 가중되어야 한다.

법원의 언론의 명예훼손 및 초상권 침해와 관련한 위자료 액수도 성폭력피해, 성형수술 및 기타 의료정보·범죄피의사실 등 민감한 정보를 공표한 경우 비교적 고액의 위자료가 인정되는 경향을 보인다.<sup>238)</sup>

또한 최근 일본 동경지방법원의 판결 중에도 웹사이트를 통한 양케이트 응답 중 응답자의 식별정보와 함께 저장된 응답자가 피부관리 중 관심을 둔 코스이름, 개별 질문에 대한 응답 등의 정보는 일반인의 감수성의 기준에 비춰 보더라도 숨겨져야 할 필요성이 높은 민감한 정보라고 실시한 것이 있다.<sup>239)</sup>

## (2) 침해정보의 식별가능성

침해정보를 통하여 정보주체의 식별이 가능한 경우 프라이버시의 침해가 크고 정보주체의 정신적 고통도 가중되므로, 개인정보의 식별가능성은 손해배상책임의 가중 사유가 된다.

특히 주민등록번호는 우리나라 국민이 공공부문 및 민간부문 모두에서 개인을 식별하는 가장 중요한 정보로서 기능하고 있으며, 대면

---

238) 이창범, 김본미, 전계 논문, 제138면.

239) 동경지방법원 2007. 2. 8. 선고 2002년(와)제27790, 2003년(와)제7975호, 2004년(와)제851호 사건: 이 사건은 피부관리살롱을 경영하는 주식회사(피고)가 자신의 웹사이트에서 실시한 양케이트에 답한 원고들의 성명, 주소, 전화번호, 이메일 주소, 직업, 연령, 성별과, 피부관리 중 관심있는 코스이름, 개별 질문에 대한 응답 등의 정보가 담겨져 있었는데, 피고는 서버 이전 과정에서 위 정보가 담긴 전자파일을 인터넷상에서 제3자가 열람가능한 상태로 두었는데, 실제 제3자가 이에 접근하여 개인정보를 인터넷상의 게시판에 올렸고, 이후 원고들에게 다이렉트 메일이 송신되고 장난전화가 걸려오는 등 2차적 피해까지 발생한 사안이다.

이 불가능한 인터넷상에서 가장 확실한 신원확인 정보이나, 주민등록번호에 대하여 DB암호화, 접근권한관리 등 관리가 미흡하여 유출의 위험성이 크고, 일단 유출되면 불법 도용 등 경제적 효용으로 인하여 확산 범위를 파악하기 어려울 정도로 전파가 빠르며, 정보가 유출되거나 도용을 당하더라도 변경할 수 없다는 데에 큰 문제가 있다.<sup>240)</sup> 이에 개인정보보호법 제24조 또한 다른 개인정보와 구별하여 고유식별정보의 처리를 원칙적으로 제한하고 있고, 최근 개정법의 시행으로 대표적인 식별정보인 주민등록번호의 처리를 매우 강력하게 제한하고 있다(제24조의2 신설). 국민은행 사건<sup>241)</sup>에서도 주민등록번호가 유출된 경우와 그렇지 아니한 경우를 구별하여 위자료를 산정하고 있다. 따라서 주민등록번호가 포함된 경우 손해배상 책임이 가중된다.

### (3) 검토

따라서 침해정보가 민감한 사적인 정보이거나, 정보주체에 대한 식별가능성이 있는 정보에 해당하는 경우에는 통상 개인정보의 유출로 인하여 정보주체에게 그렇지 않은 개인정보가 유출된 것보다 심대한 정신적 손해가 발생할 것이므로, 위자료의 가중사유가 된다.

판례도 입사지원자들의 성명이나 주민등록번호 없이 사진과 학력, 어학성적, 자기소개, 경력사항, 연구실적 등만 유출된 LG전자 사건<sup>242)</sup>에서, 재판부는 “화상”은 가장 오래되고도 확실한 개인 식별수단으로서 성명 및 주민등록번호와 마찬가지로 당해 개인을 식별할 수 있는 정보로서, 개인을 식별할 가능성만 있으면 되는 것이고 정보를 취득한 자가 당해 개인이 누구인지 구체적으로 특정할 것은

240) 임종인, 이숙연, 전계 논문, 223면.

241) 서울고등법원 2007. 11. 27. 선고 2007나33059 판결.

242) 서울고등법원 2008. 11. 25. 선고 2008나25888 판결.

요하지 않으므로, 화상정보의 경우에도 개인의 식별을 가능하게 하는 정보로서 위 정보 등 개인정보의 분실·도난·누출·변조·훼손을 방지하는 데에 필요한 안전성 확보 조치를 강구하여야 할 것이라고 판단하였고, 입사지원자들이 채용 및 인사담당자만 볼 것으로 인사담당자만 볼 것으로 믿고 작성, 제출하였을 개인사나 가족관계, 가치관이나 장래계획 등 사적인 영역의 민감한 정보까지 침범 당하였다는 점을 각 개인정보처리자의 책임을 가중하는 사유로 판단하였다.

#### 나. 침해된 정보의 양

얼마나 많은 개인정보가 침해되었는지도 위자료 산출의 기준이 되어야 할 것이다. 가령 하나의 신용카드 번호가 유출된 경우와 다수의 신용카드 번호가 동시에 유출된 각 경우에 대하여 정보주체의 피해가 동일할 수는 없다. 즉 침해된 정보의 양이 많을수록 정보주체가 받을 통상의 정신적 고통이 증대되므로, 이 또한 위자료 판단에 참작되어야 한다.

#### 다. 침해의 기간

개인정보에 대한 침해 기간이 길수록 정신적 고통의 양 또한 늘어나는 것이 당연하다.<sup>243)</sup> 유사한 사안에 대한 법원의 위자료 액수도 피해기간에 따라 달라지는 경향을 보인다.

[표 9] 침해 기간에 따른 위자료 액수<sup>244)</sup>

판결법원	사건내용	위자료 액수	출처
서울지법	은행에 의해 3년간 신용불량으로 부당하게	2천만원	중앙일보 1999. 4. 29

243) 이창범, 김본미, 전계 논문, 137면.

	등록된 경우		
서울지법	명의도용 피해자에게 카드사용금액 납부를 요구하며 약 6개월간 신용불량자로 등록	3백만원	서울지법 2002. 5. 16. 판결 2001가소 1319518 판결

#### 라. 침해 빈도

침해기간이 짧더라도 침해행위가 빈번하게 이루어졌다면 정보주체가 받는 정신적 고통은 침해기간이 길고 침해행위가 드물게 일어난 경우보다 오히려 클 것이므로, 이 항목은 침해기간과 보완관계에 있다고 할 것이다.<sup>245)</sup> 예를 들어 개인정보를 동의 없이 마케팅에 이용한 경우에는 기간보다 발생빈도가 더 문제될 것인 바, 정신적 손해 배상액 산정 시 침해기간과 침해빈도를 적절히 선택하여 사용할 수 있을 것이다.

#### 마. 유출된 정보의 확산 범위 및 전파 가능성

유출된 정보가 불특정인에게 전파되었거나, 특정인이라도 취득한 정보를 확산하지 않을 것을 기대할 수 없을 만큼 다수의 인원에게 전파된 경우에는 추가확산의 우려가 크므로, 피해는 확대될 수밖에 없고, 유출된 개인정보의 도용에 의한 후속피해의 개연성도 커지게 된다. 따라서 위자료의 액수도 상향되어야 하고, 반면 전파나 확산가능성이 없거나 적은 경우에는 책임이 부정되거나 위자료 감액요소로 작용하기도 한다.<sup>246)</sup>

관례는 리니지Ⅱ 사건<sup>247)</sup>에서 PC방이 아닌 개인용 컴퓨터에서 접속

244) 표 출처: 이창범, 김분미, 전계 논문, 137면.

245) 이창범, 김분미, 전계 논문, 137면.

246) 임종인, 이숙연, 전계 논문, 234면.

247) 또는 엔씨소프트 사건, 대법원 2008. 8. 21. 선고 2007다17888 판결.

한 이용자들의 경우 PC에 자신의 아이디, 비밀번호가 기록된 로그 파일이 저장되더라도 그 정보가 제3자에게 유출되거나 전파될 가능성은 없다는 이유로 해당 원고들의 위자료 청구를 기각하였고, 국민은행 사건<sup>248)</sup>에서는 개인정보파일이 첨부된 이메일을 열람한 사람이 600여명에 이르더라도 자신의 개인정보도 해당 파일에 포함된 경우라면 고의로 위 정보를 수집할 목적이 있는 자가 아니므로 확산가능성은 낮다고 하여 위자료의 감액사유로 판단하였다.

개인정보분쟁조정위원회는 TV프로그램을 통해 속옷에 인쇄된 사진이 방영된 사건에서 언론에 의한 개인정보 침해라는 측면에서 5백만원의 손해를 인정한바 있으며,<sup>249)</sup> 영화를 통해 정보주체의 동의 없이 전화번호가 노출된 경우에는 2백만원이라는 고액의 정신적 피해를 인정한 바 있다.<sup>250)</sup>

## 2. 피해자 측 고려 요소

### 가. 사회생활상의 불이익

대법원은 분쟁 중에 있는 고객을 통보 없이 은행이 일방적으로 신용불량자로 등록한 사건에서 “신용불량자가 사회생활에서 받는 제약과 정신적 고통을 생각할 때 위자료를 지급하는 것이 당연하다”고 판시하고 있는바,<sup>251)</sup> 이러한 태도에 따르면 판례는 사회생활상의 불이익을 일반적인 위자료 산정요소로 보고 있다고 할 것이다.<sup>252)</sup>

예컨대 이메일 주소 또는 핸드폰 번호의 유출로 다수의 스팸메일

---

248) 서울고등법원 2007. 11. 27. 선고 2007나33059 판결.

249) 한국개인정보보호진흥원, 2002 개인정보분쟁조정사례집, 51면.

250) 한국개인정보보호진흥원, 2002 개인정보분쟁조정사례집, 21면.

251) YTN 2004. 10. 14. 자 기사.

252) 이창범, 김분미, 전개 논문, 제141면.

및 스팸문자가 계속해서 들어오고 있는 등의 사정 또는 카드번호 및 비밀번호가 유출되어 카드를 재발급 받을 수밖에 없었던 사정 등은 개인정보의 유출로 인한 사회생활상의 불이익의 일종으로 보아야 할 것이다.

앞에서 본 일본 사례<sup>253)</sup>에서도, 유출사고 이후 스팸메일이나 다이렉트메일이 송신되고 장난전화가 걸려오는 등 2차 피해를 입은 원고들에게는 35,000엔, 그렇지 아니한 원고들에게는 17,000엔(기지급한 3,000엔을 고려한 금액이다)의 위자료가 인정되었다.

#### 나. 후속손해의 발생

침해행위가 단순히 일차적 개인정보 침해로 그치는 것이 아니라 일차적인 개인정보 침해가 이차적 후속손해를 발생시킨 경우에는, 민법 제393조 제2항의 “특별손해”에 해당하게 되는 경우가 대부분이므로 가해자가 “그 사정을 알았거나 알 수 있었을 때”만 배상책임을 지게 된다.<sup>254)</sup> 그러나 설령 가해자의 예견가능성이 없다 하더라도 개인정보 침해로 인하여 후속손해가 발생한 경우 이를 정신적 손해 배상의 산정과정에 감안할 여지는 있다.

후속손해의 예로는 이동통신사의 고객관리요원이 고객 DB에 접근하여 수집한 KT씨의 개인정보를 이용해 K씨의 가족을 스토킹하여 이혼에까지 이르게 한 사건과<sup>255)</sup>, 정보판매상이 스토킹에게 개인정보를 판매함으로써 스토킹 피해자를 사망에 이르게 한 미국의 Amy Boyer Case<sup>256)</sup>를 들 수 있다.

---

253) 동경지방법원 2007. 2. 8. 선고 2002년(와)제27790, 2003년(와)제7975호, 2004년(와)제851호 사건.

254) 이창범, 김분미, 전계 논문, 제143면.

255) 서울지법 2002. 11. 1. 2002가합10832 판결.

256) <http://www.epic.org/privacy/boyer> 참조.

다만 후속 손해로 인한 재산적 손해가 전보됨으로써 정신적 손해 또한 전보된다는 것이 판례의 태도이나<sup>257)</sup>, 개인정보유출사고의 경우에 대해서는 위 판례가 적용됨이 적절하지 않다는 점에 대해서는 앞서 검토하였다.

부언하면, 예컨대 개인정보 유출과 상당인과관계가 인정되는 은행잔고의 이체사고가 발생한 경우 재산적 손해가 발생한 것과 그 손해액은 비교적 명확하다. 그러나 이러한 사고가 발생한 개인정보유출 피해 당사자는 향후 지속적으로 유사한 사고가 발생할 수 있다고 생각하여, 그렇지 않은 피해자에 비하여 더욱 많은 정신적 스트레스를 받을 수 있을 것이다. 나아가 이러한 후속손해가 발생한 피해자의 경우 추가적인 손해의 발생을 막기 위해 기존에 개인정보처리자에 제공한 다양한 개인정보, 예컨대 아이디, 비밀번호 변경 등의 후속조치를 취하여야 할 것이다. 이러한 번거로움을 감수해야 하는 정보주체의 정신적 손해는 그렇지 않은 경우보다 매우 구체적이고 실질적이며 중대하다고 해야 한다. 따라서 후속손해로 재산상 손해가 발생한 경우에는 그 재산상 손해가 전보되는 것 외에도, 동시에 정보주체에게 발생한 위와 같은 사정이 위자료의 증액사유로 참작되어야 할 필요가 있다.

#### 다. 피해자의 과실

불법행위로 인한 손해배상이므로 피해자의 과실 또한 과실상계의 관점에서 참작되어야 할 것이다.<sup>258)</sup> 그런데 판례는 불법행위에서의 과실상계에 대해 “불법행위에 있어서 피해자의 과실을 따지는 과실상계에서의 과실은 가해자의 과실과 달리 사회통념이나 신의성실의

---

257) 대법원 2003. 7. 25. 선고 2003나22912 판결.

258) 이창범, 김본미, 전계 논문, 제139면.

원칙에 따라 공동생활에 있어 요구되는 약한 의미의 부주의를 가리키는 것이다.”라고 판시하였다.<sup>259)</sup> 즉 개인정보처리자에게 과실이 인정되기 위하여 요구되는 주의의무위반의 정도에 비하여 피해자 측의 과실상계에 필요한 과실의 수준은 현저하게 낮다.

즉 정보주체에게 개인정보보호법이나 관계 규정상 요구되는 개인정보주체의 의무사항을 위반한 것에 미치지 아니하고, 사회통념상 요구되는 약한 의미의 부주의만이 있었던 경우에도 과실상계의 적용이 가능할 수 있다. 따라서 개인정보가 유출된 원인에 정보주체가 비밀번호를 단순히 숫자 4자리로 구성하였거나, 비밀번호 설정 시 자신의 주민등록번호나 전화번호를 사용한 경우 또는 이메일에 자신의 인터넷뱅킹 보안카드 스캔본을 올려놓은 경우 등 개인정보 유출에 정보주체의 부주의가 기여한 경우에는 과실상계가 가능할 것이다.

또한 개인정보유출이후의 사후처리 과정에서 정보주체의 협력이 필요한 경우가 있는데, 가령 정보 중 이름이나 주민등록번호, 학력정보, 금융거래내역 등 정보주체조차 바꿀 수 없는 것이 있고 반면 아이디나 비밀번호 또는 비밀번호를 찾는데 사용되는 질문정보처럼 정보주체가 바꿀 수 있는 것이 있다.<sup>260)</sup>

전자에 해당하는 정보는 일단 유출되면 정보주체의 통제가능성이 없지만, 후자에 해당하는 정보는 유출되더라도 정보주체가 사후에 이를 변경함으로써 피해를 막거나 최소화할 가능성이 열려있다. 후자의 경우에 정보주체가 개인정보처리자의 안내에 따라 필요한 사후조치를 취하지 않아 손해가 확대되었다면 이는 과실상계로 고려하여야 할 것이다.<sup>261)</sup>

---

259) 대법원 2000. 8. 22. 선고 2000다29028 판결.

260) 권영준, 전계 논문, 55면.



### 3. 가해자 측 고려 요소

#### 가. 개인정보의 수집 동기, 목적

개인정보를 처리하는 자가 영리목적 사업을 위하여 개인정보를 수집, 처리하였다면 위자료액수를 증액하는 사유가 될 것이다.<sup>262)</sup> LG 전자 사건<sup>263)</sup>에서는 해당 기업이 온라인 입사지원접수를 통하여 비용과 인력을 절감하고 관리의 편의를 얻고는 있으나, 원고들을 대상으로 영리 목적사업을 위하여 개인정보를 수집한 것은 아니라는 점이 참작되었다. 한편 개인정보처리자의 영업에 반드시 필요하지 않은 정보를 수집한 경우에는 개인정보처리자의 관리에 있어서의 주의의무가 가중될 것이므로 책임이 가중된다.<sup>264)</sup>

#### 나. 개인정보 유출 사고의 태양

개인정보가 유출된 경위의 하나로서 개인정보 유출사고가 개인정보처리자의 고의에 의한 유출인지 또는 과실에 의한 유출인지가 위자료 산정의 참작요소가 될 수 있을 것이다. 가해자가 침해의 결과를 인식·의도하면서 행동하는 경우와, 주의의무를 완전하게 이행하지 못하여 행동하는 경우에 가해자의 행위에 대한 비난가능성은 달라질 수밖에 없다. 미국에서도 고의에 의한 정신적 침해의 경우에는 과실에 의한 정신적 침해에서보다 손해의 발생을 넓게 인정하고 있다.<sup>265)</sup>

---

261) 권영준, 전계 논문, 55면.

262) 임종인, 이숙연, 전계 논문, 234면.

263) 서울고등법원 2008. 11. 25. 선고 2008나25888 판결.

264) 권영준, 전계 논문, 57면.

265) 위 Metro-North Commuter R.R. Co. v. Buckley, 521 U.S. 424 (1997); Keck v. Jackson, 593 P.2d 668 (1979); Reynolds v. Highland Manor, Inc., 954 P.2d 11 (1998).

개인정보 유출 사고의 태양과 관련해서는 앞서 검토한 개인정보 유출 사고의 유형 중 어디에 해당하는지를 확인하여, 고의로 개인정보를 침해한 경우에는 중한 책임을, 사용자 책임을 부담하는 경우에는 사용자 책임이 무과실 책임과 동일하게 운용되고 있는 만큼 개인정보 처리자에게 보통의 책임을, 해커의 고의와 개인정보처리자의 과실이 결합된 유형의 경우에는 경한 책임을 부담하게 하는 방법이 있을 수 있다.

#### 다. 침해의 동기·목적

사업자가 고객의 편의를 위해 선의로 한 행동이거나 수사 등 공공 목적을 위한 행위였다 하더라도 적법절차에 따르지 않았다면 개인정보 침해로 인한 손해배상 책임을 면할 수 없다. 그러나 사업자가 악의로 개인정보를 침해한 경우와 이러한 경우를 동일하게 보는 것은 부당하므로 손해배상액을 산정하는데 이러한 사정을 참작할 수는 있을 것이다.<sup>266)</sup>

개인정보분쟁조정위원회의 조정 전 합의 사례를 보면 신청인이 아파트 관리사무소에 취직하기 위해 제공한 이력서를 신청인의 취업을 알선하려는 선의로 학습지 회사에 제공한 사건이 있는데<sup>267)</sup>, 이 경우 아파트 관리사무소의 행위가 비록 선의에서 비롯된 것이기는 하나 정보주체의 동의 없는 제3자 제공인 만큼 개인정보 침해는 있다고 하겠다. 그러나 배상액의 산정에 있어서는 가해자가 선의였음을 감안하여 배상액을 감경할 수는 있을 것이다.

#### 라. 침해행위를 통해 얻은 이익

---

266) 이창범, 김분미, 전계 논문, 제140면.

267) 한국개인정보보호진흥원, 2003 개인정보분쟁조정사례집, 214면.

위법한 행위를 통해 불법행위자가 얻은 이익을 계속 보유하게 하는 것은 사회정의에 반한다. 따라서 각종 형사범에서는 몰수·추징 제도를 갖고 있다. 정신적 손해배상액 산정에서도 침해행위를 통해 가해자가 얻은 이익을 참작할 필요성이 있다. 정보주체에 대한 정신적 손해배상액 산정 시 이런 사실을 감안한다면 개인정보 판매에 대해 제재적 효과를 얻을 수 있을 것이다.<sup>268)</sup>

#### 마. 가해자의 사회적 책임

가해자인 개인정보처리자가 대규모 개인정보를 보유한 정보통신서비스 제공자에 해당하거나, 시장지배력이나 사회적 지위 등으로 인해 개인정보보호를 위해 노력해야 하는 사회적 책임이 강하게 요구되는 경우에는 개인정보 침해행위에 대한 비난가능성이 크다고 할 것이다.<sup>269)</sup> 반면 영세하고 일반적인 업체에 불과하여 충분한 개인정보의 보호조치에 대한 기대가능성이 현저히 적다고 평가되는 경우에는 감경사유로 참작될 수 있을 것이다.

판례<sup>270)</sup> 또한 “원고는 신용사회의 구현을 위하여 노력해야 할 사회적 책임이 있음에도 불구하고 이윤획득에 집착한 나머지 불법영업을 했던 것으로 보이는 점 (중략) 원고가 배상해야 할 위자료 액수는 금 3,000,000원으로 정함이 상당하다.”라고 판시하여 위자료 산정과 관련하여 가해자의 사회적 책임을 고려요소로 직접 언급하였고,<sup>271)</sup> “대규모 개인정보를 수집 및 보유하고 있던 정보통신서비스 제공자로서의 피고의 사회적 책임”을 손해배상책임의 가중사유로 판단한 경우도 있었다.<sup>272)</sup> 즉 가해자의 사회적 위치 즉 시장지배력, 회

268) 이창범, 김분미, 전계 논문, 제139면.

269) 이창범, 김분미, 전계 논문, 제142면.

270) 서울지방법원 2002. 5. 16. 선고 2001가소1319518 판결.

271) 이창범, 김분미, 전계 논문, 제142면.

272) 대구지방법원 2014.02.13. 선고 2012나9865 판결.

사규모, 고객 수 등은 위자료 산정 시 참작요소가 된다.<sup>273)</sup>

## 바. 가해자의 재산상태

원고들의 숫자가 많거나 향후 추가소송이 예견되는 경우 가해자의 자력을 감안한 손해배상액 조정이 타당한지 여부는 위자료의 전보적 기능과 제재적 기능 중 어느 것을 중시할 것인가와 관련이 있다. 전보적 기능만을 강조한다면 가해자의 재산상태가 전보액에 영향을 미치는 것은 받아들이기 어렵다.<sup>274)</sup>

이와 관련하여 민법 제765조를 활용하는 견해가 있다. 민법 제765조는 고의, 중과실에 의하지 않는 불법행위에 있어서 배상으로 인하여 배상자의 생계에 중대한 영향을 미칠 경우 그 배상의무자는 법원에 배상액의 경감을 청구할 수 있게 하고, 법원은 채권자 및 채무자의 경제 상태와 손해의 원인 등을 참작하여 배상액을 경감할 수 있게 한다는 것이다.<sup>275)</sup> 위 견해는 손해배상의 지도 원리를 손해의 공평·타당한 분담으로 이해하는 대법원 판례 태도에 비추어 민법 제765조의 손해배상조정기능을 활용할 수 있다고 한다.

판례는 “위자료를 산정함에 있어 불법행위 자체로 인하여 피해자가 입은 고통의 정도, 가해자가 보인 태도, 가해자와 피해자의 연령, 사회적 지위, 재산 상태는 물론 국민소득수준 및 통화가치 등 여러 사정을 종합적으로 고려하여 사실심 변론종결시를 기준으로 수액이 결정되어야 한다.”라고 하여 위자료 산정에 가해자의 재산상태가 고려되어야 한다고 판시하였다.<sup>276)</sup>

273) 이창범, 김분미, 전계 논문, 제143면.

274) 정상조, 권영준, 전계 논문, 제57면.

275) 정상조, 권영준, 전계 논문, 제58면.

276) 대법원 2011. 7. 21. 선고 2011제다199 전원합의체 판결.

나아가 다수의 사상자가 발생한 항공기 사고로 인한 피해액 산정에 대하여도 “법원이 불법행위로 인한 위자료를 산정함에 있어서는 피해자의 연령, 직업, 사회적 지위, 재산 및 생활상태, 피해로 입은 고통의 정도, 피해자의 과실 정도 등 피해자 측의 사정에 가해자의 고의, 과실의 정도, 가해행위의 동기, 원인, 가해자의 재산상태, 사회적 지위, 연령, 사고 후의 가해자의 태도 등 가해자 측의 사정까지 함께 참작하는 것이 손해의 공평부담이라는 손해배상의 원칙에 부합한다.”라고 판시하여,<sup>277)</sup> 가해자의 재산 상태를 참작하는 것이 손해의 공평부담원칙에 부합하는 결과를 가져올 수 있다고 판시하였다.

따라서 가해자에게 모든 책임을 부과하는 것이 오히려 부정의한 결과를 가져오는 예외적인 사안, 예컨대 개인정보처리자인 기업의 손해배상으로 인하여 기업의 부도 또는 파산을 초래할 것이라는 결과의 발생이 명확하게 예상되는 경우에 한하여 민법 제765조의 손해배상조정기능을 활용해 가해자의 재산 상태를 반영하여 손해배상액을 조정할 수 있을 것이다.<sup>278)</sup>

판례 또한 “피해자가 가해자로부터 당해 사고로 입은 재산상 손해에 대하여 배상을 받을 수 있는지의 여부 및 그 배상액의 다과 등과 같은 사유도 위자료액 산정의 참작 사유가 된다.”라고 하였다.<sup>279)</sup> 따라서 위와 같이 손해배상으로 인하여 개인정보처리자에게 초래할 수 있는 악영향을 공평의 관점에서 고려하는 사고에 기초하면, 단순히 가해자의 현재 재산 상태를 고려하는 것 외에도, 개인정보 유출 사고로 인하여 발생한 피해자의 수 즉, 잠재적인 원고의 인원 수 및 그들에 대한 잠재적인 배상비용 그리고 개인정보처리자에게 부과된 과징금, 개인정보 유출 사고로 인한 가해자의 매출의 감소, 고객의

---

277) 대법원 2009. 12. 24. 선고 2007다77149 판결.

278) 정상조, 권영준, 전계 논문, 59면.

279) 대법원 1984. 11. 13. 선고 84다카722 판결, 대법원 2013. 4. 25. 선고 2012다106508 판결, 대법원 2010. 12. 9. 선고 2007다42907 판결.

감소 등 제반의 요소<sup>280)</sup> 또한 손해배상액 산정의 참작요소로 설정할 수 있을 것으로 본다.

다만 개인정보처리자의 고의에 의하여 개인정보 유출사고가 발생한 경우 침해행위를 자행한 가해자가 위와 같이 민법 제765조를 원용할 수 있도록 하는 것은 공평의 원칙에 부합하지 않는다.<sup>281)</sup> 따라서 개인정보처리자의 위와 같은 사유는 해커의 고의와 개인정보처리자의 과실이 결합된 위 제②유형의 유출사고 또는 개인정보처리자 또는 피용자의 과실로 인하여 개인정보유출 사고가 발생한 제①유형의 유출사고의 경우에 한하여 적용되는 것이 타당하다고 할 것이다.

#### 사. 개인정보 영향평가의 실시 여부

개인정보 영향평가제도는 미리 위험요인을 분석하고 이를 조기에 제거하여 개인정보 유출 및 오·남용 등의 피해를 효과적으로 예방하기 위하여 도입된 제도이다(개인정보보호법 제33조).<sup>282)</sup>

개인정보 영향평가의 대상은 ① 구축·운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일, ② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서

---

280) 개인정보 유출로 인한 기업의 경제적 피해를 산출한 연구에 의하면, 개인정보 유출에 따른 기업의 피해액은 “① 대응인건비, ② IR 대응비용, ③ 수익 손실, ④ 고객에 대한 법정 보상금” 상단에 해당하는 금액이라고 한다(한창희, 채승완, 유병준, 안대환, 박채희, “기업의 개인정보 유출로 인한 경제적 피해규모 산출방법”, 한국전자거래학회지 제16권 제4호, 24면). 따라서 향후 고객에 대하여 예상되는 배상금액은 개인정보유출로 인한 기업의 재무적 손실을 초래할 것인 바, 잠재적인 원고의 인원 수 및 그들에 대한 잠재적인 배상비용은 손해배상액 산정에 참작될 필요성이 있다.

281) 이에 대해서는 판례가 “피해자의 부주의를 이용하여 고의로 불법행위를 저지른 자가 바로 그 피해자의 부주의를 이유로 자신의 책임을 감하여 달라고 주장하는 것이 허용되지 않는다.”라고 판시한 것을 참조할 수 있을 것이다(대법원 2007. 10. 25. 선고 2006다 16758 판결).

282) 김재광, “개인정보보호법에 관한 새로운 법적 문제”, 강원법학 제36권(2012.6), 112면.

구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일, ③ 구축·운용 또는 변경하려는 개인정보파일로서 100만 명 이상의 정보주체에 관한 개인정보파일 등이다(개인정보보호법 시행령 제35조).

따라서 개인정보 영향평가를 실시해야 하는 의무기관이 아닌 이상, 개인정보 영향평가를 실시하지 않음으로 인한 직·간접적인 불이익을 부여할 수는 없다.<sup>283)</sup> 다만, 개인정보 영향평가 대상기관에 해당하는 경우 개인정보보호법이 정한 개인정보 영향평가를 실시하였다는 점은 가해자가 주의의무를 충분히 이행하였다는 유리한 측면으로 참작될 수 있을 것이다.

#### 아. 사후조치의 신속성, 적절성, 보완성

개인정보처리자가 사고발생 후 얼마나 신속하게 사고사실을 파악하고, 적시에 적절하게 피해확산방지를 위한 조치를 취하였느냐와 다양한 효과를 갖는 복수의 조치를 보완적, 중첩적으로 강구하였는지 역시 중요하다. 일단 고의, 과실에 의하여 개인정보 유출의 위험이 발생하더라도 신속한 조치에 의하여 실제 개인정보가 유출되지 않은 경우에는 책임이 발생하지 않거나 손해배상액수 산정 시 감액사유가 될 것이다.<sup>284)</sup>

또한, 사고 발생 이후 사고일지, 신고접수일지의 작성, 네트워크 로그 및 시스템 로그 등 사고의 문서화 및 증거의 확보는 구체적인 사고경위와 책임소재를 밝히고 사후 동일사고의 재발방지를 위하여 필요하며,<sup>285)</sup> 이 또한 위자료 산정 시 유리한 정상으로 참작될 수

---

283) 김재광, 전계 논문, 113면.

284) 임종인, 이숙연, 전계 논문, 232면.

있다.<sup>286)</sup>

직원의 실수로 개인정보가 저장된 파일이 첨부된 이메일이 발송된 국민은행 사건<sup>287)</sup>에서 판례는 사고발생 즉시 강제로 이메일 발송을 중단시키고 이메일을 열람하지 아니한 회원들의 이메일을 회수하였으며, 이메일을 열람한 고객들에게 이메일 삭제를 요청한 것을 위자료액수의 감액하는 사유로 참작하였다.

#### 자. 피해자에 대한 안내 및 피해회복조치 이행 여부

침해행위를 한 사업자 등이 정보주체의 조치요구를 받거나 또는 자체적 인지를 통하여 개인정보 침해로 인한 피해를 줄이려고 노력하였다면 침해행위자의 배상책임이 경감될 것이다. 이와 반대로 정보주체의 개인정보 침해행위 중지요구나 자체 인지가 있는 후에도 이를 무시하고 침해행위를 계속하거나 침해상태를 방치하였다면, 침해행위자에 대한 비난가능성은 커지게 될 것이므로 피해회복조치도 손해배상액의 산정에 영향을 미치는 요인이 된다.<sup>288)</sup>

개인정보가 유출된 회원에게 사과의 이메일을 발송하고, 피해접수센터를 개설하여 정보 유출 여부 조회 및 피해접수 창구를 마련하거나, 개인정보유출 여부를 확인할 수 있는 서비스를 제공하는 것은

285) 이홍섭, 박진섭 공저, 정보보호관리, 생능출판사, 2003, 421면.

286) 개인정보 침해사고의 위자료 산정에 대한 한 연구에서 실시된 설문 중 '개인정보유출기업의 적극적인 사후대처에 따른 책임경감 가능성'에 대한 질문에 응답자들 또한 다음과 같이 응답한 것으로 나타났다(권홍 외 3, 전계 논문, 374).

영향 요인	위자료 경감 용의(N=552)
자발적인 사고공지	408(73.9%)
사후조치의 신속성, 적절성, 보완성	460(83.3%)
사고고지 및 피해회복조치이행	473(85.7%)

287) 서울고등법원 2007. 11. 27. 선고 2007나33059 판결.

288) 이창범, 김본미, 전계 논문, 제141면.



책임을 감경하는 사유가 될 수 있다. 반면, 입사지원기간이 끝나고 합격자 발표가 마무리되어 피해자들이 더는 방문할 것으로 예상되지 않는 입사지원 웹사이트에만 사고발생 사실을 안내하고 피해자들의 정보가 유출된 것인지, 유출된 경우 어떤 정보가 유출된 것인지를 확인할 수 있는 조치를 전혀 취하지 아니한 경우에는 위자료 증액 사유가 될 수 있다.<sup>289)</sup>

#### 4. 정리

이상을 정리하면 다음 표와 같다.

[표 10] 위자료 산정에 있어서 참작 요소<sup>290)</sup>

분 류	참작 요소	참작 내용
개인 정보 자체 관련	침해정보의 민감성	법 제23조의 민감정보인지
	침해정보의 식별가능성	법 제24조의 고유식별정보인지 주민등록번호를 포함하는지
	침해된 정보의 양	침해된 정보의 양이 과도한지
	침해 기간	침해가 지속된 기간이 얼마인지
	침해 빈도	침해 빈도가 높은지(침해기간과 상호평가)
	정보의 확산범위 및 전파가능성	확산된 범위는 어느 정도인지 특정인에게 유출되었는지 또는 불특정 다수에 대한 유출인지
피해자 측 고려 요소	사회생활상 불이익	피해자에게 실제적인 사회생활상 불이익이 발생하였는지
	후속손해	후속의 재산상 손해가 발생하였는지 재산적 손해가 배상되었는지
	피해자의 과실	피해자의 과실이 손해확대에 기여하였는지
가해자 측 고려 요소	개인정보의 수집 동기, 목적	범죄 또는 영리 목적으로 수집한 것인지 필수적인 정보의 수집인지
	개인정보 유출 사고의 태양	유출 사고의 유형이 무엇인지 (1유형 or 2유형or 3,4,5유형)

289) 임종인, 이숙연, 전계 논문, 382면.

침해의 동기·목적	침해의 동기가 선의인지
침해행위를 통해 얻은 이익	침해행위를 통하여 얻은 이익이 있는지
가해자의 사회적 책임	사회적 책임이 큰 기업에 해당하는지 (대규모 개인정보를 수집·관리하고 있는지)
가해자의 재산상태	배상으로 파산의 결과에 이르는지 - 가해자의 재무적 현황이 어떠한지 - 원고의 인원이 과도한지 - 부과 과징금 액이 과도한지 (과실로 인한 유출에 한하여 적용)
개인정보 영향평가	영향평가를 실시하였는지 영향평가에 따른 조치를 취하였는지 (영향평가 대상기관인 경우에 한하여 적용)
사후조치	유출사고에 대한 사후조치가 신속, 적절하였는지
안내조치, 피해회복조치	피해자에 대한 안내조치가 있었는지 피해회복조치가 실시되었는지

## 제5절 개인정보 유출로 인한 손해배상액 산정방식

위와 같은 위자료 산정에 있어서의 참작요소들을 어떠한 방식으로 결합하여 최종적으로 손해배상액을 산출할 것인가가 문제된다. 이하에서는 다양한 위자료 산정방식을 검토한 후 최종적인 손해배상액 산정방식을 제시한다.

### I. 기존의 손해배상액 산정 모델

#### 1. JNAS JO 모델의 산정방식(제1모델)

JNAS(Japan Network Security Association)의 JO모델은 일본 네트워크보안 협회의 보안피해 조사그룹에서 제시한 모델로서<sup>291)</sup> 피해의

290) 표 출처: 정상조, 권영준, 전계 논문, 51면 내지 55면의 표에 내용 추가 및 재구성.

291) JNSA, "2009年 情報セキュリティインシデントに関する 調査報告書", JPO Japan

대상을 각 항목별로 분할하고, 표본조사를 통하여 단위 비용을 추정하고 전체 규모를 산출하는 원단위(Basic Unit) 접근법을 통한 정형화 되어있는 실무적 모델이다. 위 모델은 특히 손해배상액의 산정요소를 체계화적으로 객관화하여, 금액으로 정량화 산출하는 방법론을 제시함에 따라 개인정보를 취급하는 기업 또는 조직에 발생가능한 잠재적 위험을 파악하는데 활용할 수 있다는 점에서 의미가 있다.<sup>292)</sup>

위 모델은 아래의 사례조사, 분석, 산출모델 생성, 검증 등의 절차로 진행된다. JO모델을 통한 추정 손해 배상액 산출은 실제 발생한 사고 분석을 통한 위험 및 대책 효과의 정량화를 목적으로 한다.

첫째, 사례조사는 개인정보 침해사고가 언론 등에 공표된 데이터를 조사하고 동시에 과거 개인정보 침해 또는 명예훼손 판례를 조사한다. 둘째, 분석은 개인정보 유출사고와 관련한 피해자수, 개인정보 유출 유형, 개인정보 유출 원인, 개인정보 유출 경로, 그 밖의 요소 등을 분석한다. 셋째, 산출모델은 개인정보 유출에 따른 가치, 조직의 사회적 책임정도, 조직의 사고 이전에 대한 책임의 평가 등을 포함하는 모델을 개발한다. 넷째 검증은 개인정보 유출사고 중 대표적인 사례를 적용하여 실제 판결에 의한 손해 배상액과 비교한다.<sup>293)</sup>

이에 따라 JO 모델이 제시하는 개인정보 유출에 따른 손해 배상액 산출식은 다음과 같다.

$\begin{aligned} \text{손해배상액} &= \text{유출 개인정보 가치} \times \text{정보 유출 조직의 사회적 책임도} \times \text{사후평가} \\ &= (\text{기본정보 가치} \times \text{정보민감도} \times \text{본인식별 용이도} \times \text{정보 유출 조직의 사회적 책임도} \times \text{사후평가}) \\ &= \text{기본정보 가치}[500엔] \times \text{정보민감도}[\text{산출식}] \times \text{본인식별 용이} \end{aligned}$
--

Network Security Association, September 2010.

292) 권홍 외 3, 전계 논문, 370면.

293) 차진상, 전계 논문, 55면.

$$\text{도}[6 \text{ or } 3 \text{ or } 1] \times [\text{사회적 책임도 } 2 \text{ or } 1] \times \text{사후평가}[2 \text{ or } 1]$$

유출 개인정보 가치 산정 시 “기본정보 가치”는 정보의 종류에 상관 없이 일률적으로 500엔을 부여하고 “정보민감도”는 대상 정보의 단순 EP 다이어그램(x, y)의 위치(레벨 값)를 산출식<sup>294)</sup>에 대입하여 구한다. 유출 정보가 여러 가지라면 모든 정보 중 가장 큰 x 값과 가장 큰 y 값을 채택한다. “본인 식별 용이도”는 유출정보의 유형에 따라 본인 식별 용이도를 6, 3, 1로 부여한다. 개인식별이 되는 성명, 주소 등은 식별 용이도가 6, 비용을 들여 개인을 식별할 수 있는 경우, 예컨대 ‘주소 + 전화번호’ 등의 경우는 식별 용이도가 3, 개인식별이 곤란한 경우는 식별 용이도가 1에 해당한다.<sup>295)</sup>

“정보유출 조직의 사회적 책임도”는 개인정보의 적정한 취급을 확보해야 하는 의료, 금융, 신용, 정보통신 및 공공기관, 지명도가 높은 대기업이 일반보다 높음(2)에 해당하며 기타 일반적인 기업 및 단체 조직이 일반(1)에 해당한다. “사후평가 판정기준”은 개인정보 관련 문제점이 지적되어도 방치하거나 대응이 느린 경우 또는 반복적으로 발생하는 등 부적절한 대응이 (2)에 해당하며, 신속한 대응을 하거나 사고를 공표하고 피해자에게 공지하거나 원인분석을 통한 보안을 향상하고 외부전문가에게 자문 및 감사 등을 실시하는 것이 적절한 대응으로 (1)에 해당한다.<sup>296)</sup>

그러나 해당 모델은 개인정보에 관하여 개인식별성 여부에 대한 가중치만을 적용함으로써 질병, 사상, 범죄경력 등의 민감 개인정보가 유출될 경우 개인의 정신적 피해에 대한 가중치가 반영되지 못하였고, 개인정보 노출범위 기간 등 피해 규모에 대한 항목이 고려되지

294)  $\text{Max}(10^{\max(x)-1} + 5^{\max(y)-1})$

295) 차진상, 전계 논문, 56면 내지 57면.

296) 차진상, 전계 논문, 56면 내지 57면.

않았다는 문제점이 지적되고 있다.<sup>297)</sup>

## 2. CVM(조건부 가치추정법)을 이용한 산정방식(제2모델)

개인정보 침해사고와 관련한 위자료 산정시 조건부가치추정법(Contingent Valuation Methods, CVM)의 DQ-WTA<sup>298)</sup> 방식과 DBDC-WTA<sup>299)</sup> 방식을 사용하여 개인정보 유출시 손해배상에 대한 수용의사금액(Willingness to Accept, WTA)을 보다 현실적인 측면에서 산정하는 방식이다. 개인정보의 중요도를 고려하여 개인정보 유출 항목에 따른 위자료 금액을 다양한 설문 방법을 통해 분석하려 하였다.<sup>300)</sup>

위 연구에서는 총 552명을 대상으로 이중양분선택형 질문형식과 직접질문법을 통해 개인정보 침해 시나리오를 3가지로 가정하여 위자료 수용금액을 조사한다. 이중양분선택형 질문이란 개인정보 침해에 따른 위자료 초기 제시액(X원)을 수용하겠다는가에 대해 질문을 한 후, 이에 동의할 경우는 두 번째 제시액을  $\frac{1}{2}X$ 원으로 제시하여 동의 여부를 질문하고, 비동의할 경우는 두 번째 제시액을 2X원으로 제시하여 동의 여부를 질문한다.<sup>301)</sup>

질문지에서 사용한 3가지 시나리오는 첫째, 이름, 전화번호, 이메일 주소가 유출된 경우이고, 둘째, 이름, 전화번호, 이메일 주소 및 주민등록번호, 아이디 등이 유출된 경우이며, 셋째, 이름, 전화번호, 이메일 주소, 주민등록번호, 아이디 및 계좌번호, 신용카드번호, 구매내역 또는 의료기록, 신체정보, 소득, 직장경력, 사적인 메일 내용이 유출

---

297) 차진상, 전계 논문, 57면.

298) Direct Question Willingness to Accept: 직접질문법을 통한 수용의사금액.

299) Double-bounded Dichotomous Choice: 이중양분선택형을 통한 수용의사금액.

300) 권홍, "CVM을 이용한 개인정보 침해사고의 위자료 산정", 충북대학교 석사학위논문, 2011. 2.

301) 차진상, 전계 논문, 51면.

된 경우로 가정하여 다음과 같은 추정금액을 제시하였다.<sup>302)</sup>

[표 11] 시나리오별 위자료 산정금액<sup>303)</sup>

구분	개인정보내역	판례	JNSA JO	DQ-WTA	DBDC-WTA
시나리오1	이름, 전화번호, 이메일	100	78	314	233
시나리오2	① + 주민등록번호, 아이디	200	234	668	698
시나리오3	② + 계좌번호, 신용카드번호, 구매내역	300	859	3,226	2,595

해당 위자료 산정방식은 정보 중요도를 고려하여 개인정보 유출 항목에 따른 위자료 금액을 다양한 설문 방법을 통해 분석하였다는 점에서 의의가 있다. 그러나 유출된 개인정보의 중요도에 따른 위자료 적용기준이 미흡하고, 유출기간 또는 범위에 따른 피해 규모 등이 고려되지 않았고, 기업의 감정기준에 대해 정량적 기준이 없어서 다양한 개인정보 유출 유형을 적용하기 어렵다는 문제점이 제기되고 있다.<sup>304)</sup>

### 3. 피해자 측과 가해자 측을 고려한 산정방식(제3모델)

정량적인 기준의 제시는 아니나, 위자료 산정 시 피해자 측과 가해자 측에서 고려할 수 있는 항목을 구분하여 제시하는 산정방식이다.

먼저, 위자료 산정시 피해자 측의 고려사항으로 침해단계를 무단수집, 무단이용, 무단유출 등 3단계로 구분하여 제시하고 항목별 증감관계를 표시하였다. 또한 침해범위(좁은 범위, 넓은 범위), 침해대상

302) 차진상, 전계 논문, 52면.

303) 표 출처, 권홍 외3, 전계 논문, 374면.

304) 차진상, 전계 논문, 52면.

(비민감정보, 민감정보), 정보의 정확성(정확한 정보, 부정확한 정보), 정보의 식별가능성(식별가능성이 낮은 정보, 식별가능성이 높은 정보), 악용여부(불특정 또는 다수인에 대한 정보 유출, 불특정 또는 다수인에 대한 정보유출 악용), 재산적 손해(재산적 손해 미발생, 재산적 손해 발생), 피해자의 과실(과실이 있음, 과실이 없음) 등으로 구분하여 위자료 감액과 증액기준을 제시하였다.<sup>305)</sup> 가해자 측의 고려사항으로는 경과실 또는 고의·중과실 등의 침해 양태와 일반기업 또는 공공기관, 정보통신서비스제공자 등 가해자의 지위, 비영리적 또는 영리적 동기, 피해확산방지를 위한 사후적 노력 등의 항목을 고려사항으로 제시하였다.<sup>306)</sup> 이를 표로 정리하면 다음과 같다.

[표 12] 위자료 산정 시 고려해야 할 피해자 측 요소<sup>307)</sup>

분류		위자료	설명
침해 단계	무단 수집	+	밀의 단계로 갈수록 위자료 증액
	무단 이용	++	
	무단 유출	+++	
침해 범위	좁은 범위	+	유출범위가 넓을수록 위자료 증액
	넓은 범위	++	
침해 대상	비민감 정보	+	민감정보일수록 위자료 증액
	민감 정보	++	
정보의 정확성	정확한 정보	+	일반적으로 부정확한 정보일수록 위자료 증액
	부정확한 정보	++	
정보의 식별가능성	식별가능성이 낮은 정보	+	개인식별가능성이 높은 정보일수록 위자료 증액
	식별가능성이 높은 정보	++	
악용 여부	불특정 또는 다수인에 대한 정보 유출	+	신분도용이나 금전인출 등 개인정보의 실제 악용이 일어난 경우에는
	불특정 또는 다수인에	++	

305) 정상조, 권영준, 전계 논문, 45면 내지 55면.

306) 차건상, 전계 논문, 53면.

307) 표 출처: 정상조, 권영준, 전계 논문, 51면.

	대한 정보 악용		위자료 증액
재산적 손해	재산적 손해 미발생	+	신분도용이나 금전인출 등 개인정보의 실제 악용이 일어난 경우에는 위자료 증액
	재산적 손해 발생 (입증 곤란)	++	
피해자의 과실	과실 있음	-	피해자의 과실이 있는 경우에는 위자료 감액

[표 13] 위자료 산정 시 고려해야 할 가해자 측 요소<sup>308)</sup>

분류		위자료	설명
침해 태양	경과실	+	경과실에 의한 침해보다 고의 또는 중과실에 의한 침해의 경우 위자료 증액
	고의 중과실	++	
가해자의 지위	일반적인 경우	0	공공기관이나 정보통신서비스 제공자와 같이 조직적으로 대량의 개인정보를 취급하는 기업에 대해 위자료 증액
	공공기관, 정보통신서비스제공자 등	+	
동기	비영리적인 동기	+	영리적인 동기 또는 범죄 관련 동기의 경우 학술, 언론, 종교 등 그렇지 않은 경우보다 위자료 증액
	영리적인 동기 또는 범죄관련 동기	++	
정보의 필요성	필요성이 높음	+	문제된 개인정보의 필요성이 크지 않음에도 불구하고 굳이 이를 과도하게 수집, 보관하는 과정에서 발생한 사고에 대해서는 위자료 증액
	필요성이 낮음	++	
행위 이후의 사정	피해회복을 위한 적극적인 노력	-	피해회복을 위한 적극적인 노력은 정신적 손해의 폭을 줄일 뿐만 아니라 예방이나 제재의 측면에서도 책임의 폭을 줄일 요인임
	피해회복을 위한 노력을 하지 않음	0	

#### 4. 항목별 피해등급을 5단계로 구분하는 산정방식(제4모델)

308) 표 출처: 정상조, 권영준, 전계 논문, 53면.



개인정보침해로 인한 정신적 손해배상액 산정 시 고려사항으로 총 11가지 항목에 대해 항목별 피해등급을 5단계로 구분하여 배상액 산정기준을 제시하는 방식이다.<sup>309)</sup>

첫째, 침해기간에 대해서는 개인정보 침해기간이 길수록 정신적 고통의 양 또한 늘어난다. 둘째, 침해빈도는 침해기간이 짧더라도 침해행위가 빈번하게 이루어졌다면 정보주체가 받는 정신적 고통은 침해기간이 길고 침해행위가 드물게 일어난 경우보다 정신적 고통이 크다. 셋째 침해정보의 민감성에 대해서는 대·중·소 3단계로 구분하였는데 사상, 신념, 과거의 병력 등 민감도가 높은 경우에는 가중치를 높게 부여하였다. 넷째, 침해정보의 노출범위에 대해서 피해자의 개인정보가 다수인에게 유포될수록 피해는 확대될 수밖에 없고, 유출된 개인정보의 도용에 의한 후속피해의 개연성도 커지게 된다. 다섯째 피해자의 과실이 많고 적음에 따라 경감기준을 마련하여 제시하였으며, 여섯째, 침해행위를 통해 얻은 이익의 정도에 따라 위자료 금액의 가중치 기준 금액을 제시하였다. 일곱째, 침해의 동기를 악의적 목적, 고의·중과실, 선의·경과실로 구분하여 위자료 금액의 차등기준을 제시하였다. 덧붙여 사회생활상의 불이익, 침해 후의 피해회복조치, 가해자의 사회적 책임, 후속손해의 발생 등을 위자료 금액 산정 시 고려해야 할 항목으로 제시하였다.<sup>310)</sup> 이에 따라 위 연구는 다음과 같이 피해배상등급을 제시하였다.

[표 14] 개인정보 침해에 대한 정신적 손해배상 산정기준<sup>311)</sup>

(단위 : 1점당 1만원)

산정 요소		계산기준(해당 피해배상등급에 따름)				
		5	4	3	2	1
침해 기간	장	+ 20	+ 15	+ 10	+ 8	+ 5

309) 이창범, 김분미, 전계 논문, 145면.

310) 차건상, 전계 논문, 2012, 58면.

311) 이창범, 김분미, 전계 논문, 145면 내지 146면.

		중	+ 15	+ 10	+ 8	+ 5	+ 3
		단	+ 10	+ 8	+ 5	+ 3	+ 1
침해 빈도		과다	+ 20	+ 15	+ 20	+ 8	+ 5
		다	+ 15	+ 10	+ 8	+ 5	+ 3
		소	+ 10	+ 8	+ 5	+ 3	+ 1
침해정보의 민감성		대	+ 50	+ 30	+ 20	+ 15	+ 10
		중	+ 25	+ 15	+ 10	+ 8	+ 5
		소	+ 20	+ 10	+ 5	+ 3	+ 2
침해정보가 노출된 범위	특정	일반 개인	+ 20	+ 10	+ 8	+ 5	+ 3
		업무관련자	+ 20	+ 10	+ 8	+ 5	+ 3
		개인정보판매상	+ 30	+ 20	+ 20	+ 15	+ 10
	불특정	언론매체	+ 50	+ 30	+ 30	+ 20	+ 10
		인터넷 등	+ 30	+ 15	+ 10	+ 10	+ 5
		인쇄물 기타	+ 20	+ 10	+ 10	+ 8	+ 5
피해자의 과 실		대	-50	-30	-20	15-	-10
		중	-30	-20	-10	-8	-8
		소	-10	-8	-5	-5	-5
침해를 통해 얻은 이익		대	+ 50	+ 20	+ 10	+ 10	+ 5
		소	+ 20	+ 10	+ 5	+ 5	+ 3
침해의 동기 및 목적		악질적 목적	+ 30	+ 20	+ 15	+ 10	+ 8
		고의·중과실	+ 15	+ 10	+ 8	+ 5	+ 3
		선의·경과실	-10	-8	-5	-3	-3
사회생활 상 의 불이익		대	+ 30	+ 20	+ 15	+ 10	+ 8
		중	+ 20	+ 15	+ 10	+ 8	+ 5
		소	+ 10	+ 8	+ 5	+ 3	+ 1
침해후의 피 해회복 조치		불량	+ 20	+ 10	+ 8	+ 5	+ 3
		양	-20	-10	-8	-5	-3
가해자의 사 회적 책임		중대	+ 20	+ 15	+ 10	+ 8	+ 5
		중	+ 10	+ 8	+ 5	+ 3	+ 1
후속손해의 발생		극대	+ 50	+ 30	+ 20	+ 15	+ 10
		대	+ 20	+ 15	+ 10	+ 8	+ 5
		소	+ 10	+ 8	+ 5	+ 3	+ 2

## 5. 기존 모델에 대한 검토

JNAS JO 모델의 경우 질병, 사상, 범죄경력 등의 민감 개인정보가 유출될 경우 개인의 정신적 피해에 대한 가중치가 반영되지 못하였으며 개인정보 노출범위 기간 등 피해 규모에 대한 항목이 고려되지 않았다는 문제점이 있고, CVM을 이용한 위자료 산정방식의 경

우 개인정보의 중요도에 따른 위자료 적용기준이 미흡하고, 유출기간 또는 범위에 다른 피해 규모 등이 고려되지 않았고, 기업의 감정 기준에 대해 정량적 기준이 없다는 난점이 있다.

## II. 통합적 손해배상액 산출모델의 제안

(객관요소와 주관요소를 순차적으로 고려하는 방식)

### 1. 서설

우리나라에서 개인정보유출 사고로 인한 손해배상액은 재산적 손해의 발생이 입증된 경우를 제외하면 5만원 내지 30만 원 정도의 수준에 머물러 왔다. 그런데 최근 정보통신망법의 개정으로 인하여 정보통신서비스 제공자들이 고의 또는 과실로 해당 법을 위반한 경우 또는 개인정보가 분실, 도난, 누출된 경우에 대해 300만원의 법정손해배상을 하도록 하는 조항이 신설되었다(정보통신망법 제32조의2).<sup>312)</sup>

이는 최근 반복된 개인정보유출사고를 예방하기 위한 입법자의 의지가 반영된 것으로 보이고, 이에 따라 향후 법원의 위자료 산출방식에도 현저한 변화가 있어야 할 것이다. 개인정보의 유출로 인한 위자료를 기존과 동일하게 5만원 내지 30만원으로 산출하는 것은 더 이상 현행법에 부합하지 않는 법해석이 될 것이다.

따라서 개인정보의 유출사고와 관련하여 개인정보의 종류 및 양, 개인정보 유출사고의 태양(유형), 유출사고와 관련한 피해자는 물론 가해자와 관련한 모든 참작요소들을 종합적으로 고려하여, 300만원의 범위에서 구체적 타당성이 있는 위자료를 산출할 필요성이 있다.

---

312) 개인정보보호법에도 동일한 내용의 개정안이 제출되어 있다.

이에 본 논문에서는 개인정보 자체 및 피해자, 가해자 측의 참작요소를 종합적으로 고려한 제2모델의 위자료 산정방식을 기본으로 한 통합적 산출모델을 제안한다. 통합적 산출모델에서는 우선 법관의 자의가 개입되기 어려운 객관적 요소인 개인정보 자체와 관련된 요소<sup>313)</sup> 및 유출사고의 태양과 관련된 요소를 종합하여 위자료 액수의 출발점을 제시하고, 이를 토대로 피해자와 가해자에 대한 참작 요소를 종합적으로 고려하여 최종 손해배상액을 산출하도록 하였다.<sup>314)</sup>

## 2. 구체적인 손해배상액 산출 과정

### 가. 1단계 - 재산적 손해와 정신적 손해의 구분 단계

재산적 손해가 발생하였는지 여부를 판단하여, 재산적 손해 중 통상 손해와 특별손해 중 예견가능성이 있는 손해를 판단하는 단계이다. 다만 이 단계에서 재산적 손해의 범위가 구체적으로 입증되지 않는 경우에는 법원이 변론 전체의 취지에 나타난 간접사실들을 종합하여 재산적 손해의 액수를 판단할 수 있고,<sup>315)</sup> 재산적 손해를 인정하지 않는 경우에는 위자료의 보완적 기능을 활용하여 위자료 액수를 증액하는 방식으로 손해배상액수를 판단할 수도 있다.<sup>316)</sup>

### 나. 2단계 - 유출정보에 대한 객관적 평가단계

---

313) 기존연구들에서는 피해자 측의 요소로 포함되어 있는 개인정보 관련 참작요소의 경우 피해자 측과 가해자 측 어느 한 쪽과만 연관되어 있는 것이 아니고, 손해배상판단과 관련하여서 개인정보 자체의 특성이 검토되어야 할 필요성이 있고, 이러한 특성은 법관의 자의가 배제될 수 있는 객관적인 요소에 해당한다. 따라서 본 논문에서는 개인정보 자체에 대하여는 이를 별도의 항목으로 분리하여 검토하였다.

314) 이러한 단계적 산정방식은 개인정보보호법상 과징금의 산정방식을 참조한 것이다.

315) 위 서울중앙지방법원 2011. 11. 11. 선고 2010가합118427 판결.

316) 위 대법원 1984. 11. 13. 선고 84다카722 판결. 다만 위자료의 보완적 기능을 활용하는 경우 위자료의 속성상 재산적 손해배상에 대한 어느 정도의 보완적 기능을 가지는 것은 불가피하지만 그 정도를 넘어 만연히 재산적 손해배상의 대체물로 활용되어서는 안 되고 한 점을 주지하여야 할 것이다.

유출된 개인정보의 자체와 관련하여 위자료에 영향을 미칠 수 있는 여러 가지 요소들을 고려하는 단계이다. 이 단계에서는 유출된 개인정보의 가치평가와 관련하여 제1모델 및 제2모델을 기초로 제4모델의 산정방식 및 개인정보보호법에 규정된 과징금<sup>317)</sup>의 산정원칙을 참작한다.

### (1) 유출 개인정보의 기초 가치산정

우선 제1모델에 따라 기본정보의 가치를 정보의 종류에 상관없이 특정가액으로(위 모델에서는 500엔)<sup>318)</sup>으로 부여하고, 여기에 해당 정보가 민감 정보인지 여부 및 고유식별정보인지에 대한 가중치를 적용하여 도출된 값을 유출 개인정보의 기초가치로 설정한다. 나아가 고유식별정보의 경우 개정 개인정보보호법 제24조의2에 반영된 입법자의 의도 및 주민등록번호 유출에 대한 국민은행 사건 판례<sup>319)</sup>의 취지에 따라 주민등록번호가 포함되어 있는 경우 가장 높은 단계의 가중치를 적용한다.

### (2) 개인정보 유출의 태양

그런데 제1모델은 침해기간, 침해빈도 등 침해행위의 태양을 고려하지 아니한 난점이 있으므로 이 부분에 대한 보완을 위하여, 제2모델 및 제4모델을 참작하여 침해기간에 따라 3단계(장, 중, 단)로, 침해

---

317) 과징금은 행정법상 의무의 이행을 강제로 담보하기 위한 목적으로 이용된다. 한편 불법 행위법은 사회 구성원들에게 바람직한 행위지침을 제시하고 그러한 행위로 나아갈 인센티브를 부여함으로써 불법행위를 예방하게 하는 목적도 추구한다. 따라서 이무이행을 강제하고 수범자의 불법행위를 예방한다는 점에서는 양자가 일맥상통하는 측면이 있다. 따라서 개인정보보호법 상 입법자의 개인정보보호에 대한 의지 기준이 반영된 과징금 산정 기준 또한 일정 정도 위자료 산정에 참작될 소지가 있는 것이다.

318) 한화로는 약 5,000원 내외의 금액으로 설정할 수 있을 것이다.

319) 서울고등법원 2007. 11. 27. 선고 2007나33059 판결.

빈도에 따라 3단계(과다, 다, 소)의 가중치를 적용한다. 또한 침해정보가 노출된 범위를 2개의 유형(특정, 불특정)으로 구분한 뒤 이를 2단계로 나누어 가중치를 적용한다.

### (3) 유출된 개인정보의 양

한편 얼마나 많은 개인정보가 유출되었는지도 손해배상의 참작요소로 고려되어야 할 것인데, 이에 대해서는 주민등록번호 유출로 인한 과징금 산정방식에 관한 개인정보보호법 시행령 별표1의2의 기준을 참조하여, 유출된 개인정보의 개수가 10만 건<sup>320)</sup>을 넘어서는 개인정보유출사고의 경우에 대한 높은 가중치를 적용한다.

위 각 사항을 정리하면 다음 표와 같다.

[표 15] 유출정보에 대한 객관적 평가

항 목	내 용	반영정도
기본정보의 가치	5,000원	
민감정보인지 여부	민감정보	++
	비민감정보	+
고유식별정보인지 여부	고유식별정보 (주민등록번호 포함)	+++
	고유식별정보 (주민등록번호 불포함)	++
	비식별정보	+
침해 기간	장기	+++

320) 개인정보보호법 시행령 별표1의2는 주민등록번호의 유출사고를 매우 중대한 위반행위, 중대한 위반행위, 일반 위반행위의 3가지로 분류하고, ① 고의 또는 중과실로 인하여 10만 건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손된 경우인 “매우 중대한 위반행위”에 대해서는 과징금의 기본 액을 3억 5천만 원으로 하고, ② 고의 또는 중과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우 및 경과실로 인하여 10만 건 이상의 주민등록번호가 분실 등이 된 경우인 “중대한 위반행위”에 대해서는 산정기준액을 2억 3천만원으로 하고 있으며, ③ 경과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우인 “일반 위반행위”에 대하여는 1억 원을 산정기준액으로 규정한다.

	중기		++
	단기		+
침해 빈도	과다		+++
	다		++
	소		+
유출된 정보의 확산 범위	특정	개인정보판매상	++
		일반 개인, 업무관련자	+
	불특정	언론매체	++
		인쇄물, 인터넷	+
유출된 정보의 양	10만건 이상		++
	10만건 미만		+

#### 다. 3단계 - 유출 사고에 대한 객관적 평가 단계

위와 같이 개인정보 자체와 관련된 객관적인 사항만을 반영하여 도출된 기초 위자료 금액은 모든 유형의 개인정보 유출사고에서 손해배상액 산출의 출발점이 될 것이다. 그런데 개인정보 유출사고는 위에서 본 것과 같이 5가지 유형<sup>321)</sup>으로 분류할 수 있을 것인데, 각 유형에서 개인정보처리자의 비난가능성 및 개인정보처리자가 책임을 부담하는 법적근거가 상이하므로 각 유형에 따라 손해배상에 대한 가중치를 달리 적용할 필요성이 있다. 특정 개인정보 유출사고가 어떠한 유형에 해당하는지 또한 비교적 분명하므로 법관의 자의가

321) 임종인, 이숙연, 전계 논문, 225면.

- |  |
|--|
| <p>제①유형: 개인정보처리자(그 피용자와 그로부터 개인정보 취급위탁을 받은 자(수탁자)를 포함한다)의 과실로 개인정보가 유출된 경우</p> <p>제②유형: 개인정보처리자의 과실과 제3자(해커 등)의 고의로 인한 불법행위가 경합하여 개인정보가 유출된 경우</p> <p>제③유형: 개인정보처리자의 피용자, 수탁자가 고의로 개인정보를 유출한 경우</p> <p>제④유형: 개인정보처리자가 동의를 받지 아니하고 개인정보를 제3자에게 제공하거나 이전한 경우</p> <p>제⑤유형: 개인정보처리자가 동의 없이 정보를 수집하거나, 동의 받은 목적과 달리 사용하거나, 이용자의 동의철회, 열람, 정정 등 요구를 받고도 이행하지 아니하는 경우</p> |
|--|

개입될 여지가 적다. 따라서 마지막 4단계에서 다양한 참작요소들을 종합적으로 판단하기 위한 전 단계로서 유출사고의 유형에 따른 가중치를 미리 적용하여 둘 필요성이 있다.

제①유형의 경우에는 순수한 과실책임이므로 개인정보처리자의 책임에 비난가능성이 비교적 낮아서 가장 낮은 가중치를 적용한다. 제②유형의 경우에는 개인정보보호법 및 정보통신망법이 규정한 관리조치의무를 위반하여 해커의 침입을 방지하지 못하였다는 점에서 비난가능성이 크지만 이 또한 성질상 과실책임의 일종에 불과하므로 보통의 가중치를 적용한다. 제③, ④, ⑤유형의 경우는 개인정보처리자 스스로 개인정보의 유출을 의도했다는 점에서 비난가능성이 매우 크므로 가장 높은 가중치의 적용이 필요하다.

위 각 사항을 정리하면 다음 표와 같다.

[표 16] 유출사고에 대한 객관적 평가

항 목	내 용	반영정도
3, 4, 5유형	개인정보처리자, 피용자, 수탁자의 고의	+++
2유형	개인정보처리자의 과실과 해커의 고의 경합	++
1유형	개인정보처리자, 피용자, 수탁자의 과실	+

#### 라. 4단계 - 피해자와 가해자에 대한 주관적 평가단계

위와 같이 유출된 개인정보 자체와 관련된 요소 및 유출사고 자체의 유형에 따른 가중치를 적용하여 객관적 손해배상액을 도출한 다음, 제2모델이 제안하는 방식인 피해자와 가해자의 주관적인 제반 참작요소를 반영하여 최종적인 손해배상액을 산출한다.

##### (1) 피해자 측 참작요소 반영



피해자 측 요소와 관련해서는 피해자에게 사회생활상 불이익 또는 후속 재산적손해가 발생한 경우(특히 재산상 손해의 발생이 인정되나 그 액수 산출이 불가능한 경우에 높은 가중치를 적용) 가중치를 적용한다. 다만 피해자의 과실이 있는 경우에는 위자료를 감액한다.

[표 17] 피해자 측 참작요소

항 목	내 용	반영정도
사회생활상 불이익	스팸문자, 스팸메일 등 사회생활상 불이익 발생	++
	사회생활상 불이익 미발생	+
후속손해	재산적 손해 발생 (but, 손해액 입증 곤란: 위자료의 보완적 기능)	+++
	재산적 손해 발생 (손해액 입증)	++
	재산적 손해 미발생	+
피해자의 과실	피해자의 무과실	0
	피해자의 과실	-

## (2) 가해자 측 참작요소 반영

가해자 측 요소와 관련해서는 개인정보의 수집 및 보관의 동기 및 목적이 무엇인지(영리를 목적으로 한 것인지 여부 및 필수정보의 수집에 해당하는지 여부), 침해의 동기<sup>322)</sup>가 무엇인지, 침해행위로 이익을 얻었는지, 가해자의 사회적 책임은 어떠한지, 가해자인 기업의 재산상태 및 손해배상으로 인한 재무적 영향의 정도는 어떠한지,<sup>323)</sup> 개인정보영향평가를 실시하였는지, 사후조치는 신속·적절하였는지, 피해자에 대한 피해회복조치가 실시되었는지 여부를 종합적으로 고려한다.

322) 개인정보 유출사고 중 3, 4, 5유형에 해당하여 개인정보처리자가 인식 및 의도 하에 개인정보를 유출시키는 경우에도 침해의 동기는 선의인 경우가 있을 수 있다.

323) 개인정보 유출사고 중 1, 2 유형에 해당하는 경우에만, 손해배상결과로 파산에 이를 결과가 명백한 경우에 한하여 참작이 가능하다는 점은 앞에서 전제한 바 있다.

[표 18] 가해자 측 참작요소

항 목	내 용	위자료
개인정보 수집동기	범죄관련 동기	+++
	영리적인 동기	++
	비영리적인 동기	+
정보수집 필요성	필요성이 없거나 낮은 경우	++
	필요성이 높은 경우	+
침해의 동기, 목적	일반적인 경우	0
	선의인 경우	-
침해로 인한 이익	이익이 있는 경우	++
	이익이 없는 경우	+
사회적 책임	공공기관, 정보통신서비스제공자 등	++
	일반적인 경우	+
가해자의 재산상태	배상으로 인하여 자력을 상실하는 경우 (과실로 인한 유출 유형에 한하여 참작 가능)	-
개인정보 영향평가	영향평가를 실시하지 않은 경우 및 영향평가를 실시하고 보완조치를 취하지 않은 경우	+
	영향평가를 실시하여 보완한 경우	-
사후조치	사후조치가 없었거나, 지연되거나, 부적절한 경우	++
	사후조치가 신속, 적절한 경우	-
피해회복	피해자에 대한 피해회복 노력이 없는 경우	+
	피해회복을 위한 적극적인 노력이 있었던 경우	-

### 3. 결어

위와 같이 4단계에 거친 통합된 산정모델을 통한 판단을 거칠 경우, 재산적 손해와 정신적 손해의 구별 및 상호 영향관계가 명확해지고, 개인정보의 종류 및 양, 개인정보 유출사고의 태양(유형), 피해자는 물론 가해자와 관련한 모든 참작요소들을 종합적으로 고려하여 구체적으로 타당성 있는 손해배상액의 산출이 가능해 질 것으로 기대한다.

## 제5장 결 론

개인정보 침해사고는 일단 발생하면 대량의 피해자가 발생하지만 피해의 입증은 물론 사업자의 고의 내지 과실을 입증하는 것도 쉽지 않다는 특성이 있다. 이에 개인정보보호법과 정보통신망법은 개인정보 침해사고에 대하여 입증책임을 전환하여 피해자인 이용자가 보다 용이하게 손해배상을 받을 수 있도록 하였다.

그러나 개인정보처리자의 과실 유무 판단 및 손해의 발생 여부와 그 범위에 대한 판단은 사안 중심적 성격이 강하여 거의 대부분 법관의 재량에 달려 있다고 해도 과언이 아니다. 이에 따라 개인정보 침해사고의 손해배상소송에서도 정보주체가 쉽게 납득할 수 없는 원고 청구 기각 판결이 나오거나, 침해와 손해가 충분히 인정되는 경우에도 손해배상액수가 매우 적은 수준에 머무르고 마는 등 개인정보 유출로 인한 피해자의 구제 여부 및 정도가 일관되지 않다.

이에 본 논문에서는 개인정보처리자인 기업 등이 기울여야 하는 주의의무의 정도에 대한 법령상 기준과 기타 세부 기준들을 정보자체, 개인정보처리자, 외부적 고려요소, 사후조치 등으로 분류하여 개인정보처리자의 과실 여부 판단에 대한 명확한 기준을 제시하고자 하였고, 위자료 판단의 요소들을 개인정보 자체, 피해자 및 가해자 측의 참작요소로 나누어 상세하게 검토하였다.

나아가 손해배상 액수 산출에 대해 4단계의 판단을 거친 통합적 산출모델을 제시하여 손해배상액 산정에 정형성을 도모하고자 하였다.

이에 따르면 객관적 요소인 개인정보 자체와 관련된 요소 및 유출 사고 태양과 관련된 요소를 종합하여 위자료 액수의 출발점을 산출하고, 이를 토대로 피해자와 가해자에 대한 참작 요소를 종합적으로 고려하여 최종 손해배상액을 산출한다.

이러한 정형화된 판단을 통한 민사적 구제가 충분히 이루어진다면 합리적인 사업자들은 개인정보의 침해로 인한 손해배상의 책임을 지는 것보다 그 유출이나 도용의 사전방지를 위한 노력을 기울이게 될 것이다.

다만 개인정보의 처리로 인하여 발생할 수 있는 경제적 가치나 정보주체 스스로에 대한 편익을 감안하였을 때, 위에서 제시한 요소들을 개인정보처리자의 책임을 가중하는 방향 일변도로만 해석·적용할 것이 아니고, 사안에 따라서는 기업의 책임을 감소시키는 방향으로 적용될 수 있어야 함을 밝혀둔다.

## 참 고 문 헌

### 【국내문헌】

#### [단행본]

- 이창범, 『개인정보 보호법』, 법문사, 2012.1.  
김주영, 손형섭, 『개인정보보호법의 이해』, 법문사, 2012.  
고학수, 『개인정보보호의 법과 정책』, 박영사, 2014.  
권영성, 『헌법학원론(개정판)』, 법문사, 2008.  
박준서, 주식 민법 {채권각칙(6)} 2000. 3. (제3판)  
박준서, 주식 민법 {채권각칙(7)} 2000. 3. (제3판)  
박준서, 주식 민법 {채권각칙(8)} 2000. 3. (제3판)  
이홍섭, 박진섭 공저, 『정보보호관리』, 생능출판사, 2003.  
U. Beck, 홍성태 옮김, 『위험사회』, 새물결, 1997.  
Cooter·Ulen, 한순구 역, 『법경제학 (5th ed.)』, 경문사, 2009.

#### [논문]

- 고학수, "개인정보보호의 법, 경제 및 이노베이션", 경제규제와 법(Journal of Law & Economic Regulation) 제5권 제2호 (통권 제10호) (Vol. 5. No. 2 (Serial No. 10), 2012. 11.  
이원우, "개인정보보호를 위한 공법적 규제와 손해배상책임, 개인정보누출을 중심으로", 사단법인 행정법이론실무학회 (행정법연구 제30호 2011. 8.)  
정상조, 권영준, "개인정보의 보호와 민사적 구제수단", 법제 58권 3호 통권 630호 (2009. 3.)

임종인, 이숙연, “개인정보관련분쟁의 사례분석과 대안의 모색”, 정보법학 제12권 제2호, 2008. 12. 219면.

한국정보화진흥원. 새로운 미래를 여는 빅데이터 시대, 2013.

서울대학교 기술과 법센터, 개인정보의 보호에 관한 입법론 (SNU CLT Working Paper 2006-3, 연구진: 정상조, 권건보, 박재우)

손형섭, “연예인의 프라이버시권 법리”, 법조 통권 제635호, 2009.

윤주희, “개인정보 침해현황과 이용자보호”, 법학논총(제33권 제1호), 2013. 4. 19.

정보통신 윤리위원회, “인터넷 개인정보 침해 대응방안 연구”, 2006.

김일환, 김민호, 지성우, “개인정보보호 법규 위반에 대한 징벌적 과징금의 성격 및 합리적 처분 기준 연구”, 방송통신위원회, 2011. 11.

구태인, “개인정보 보호법의 제문제”, 법학평론 제3권 (2012. 12.)

정상조, “광고기술의 발전과 개인정보의 보호”, 저스티스 통권 제106호

임종인, “개인정보 유출로 인한 기업의 책임”, 상장협연구 제59호 2009. 4.

윤중수, “개인정보보호법제개관”, 정보보호법학회 2008. 9. 27. 세미나 발표 논문

임건면, “개인정보의 의의와 귀속관계”, 『중앙법학』, 중앙법학회, 2005. 12.

최진혁, 박준석, “개인정보 유출 최소화를 위한 통합 접근통제 모델 연구”, 한국공안행정학회보 제38호(2010)

남길현, “국내외 개인정보보호법 동향과 기업의 대응전략,” 정보보호학회지 (2011. 12)

전은정, 김학범, 염홍열, “미국의 개인정보보호 법·제도 동향” 정보보호학회지, 제22 권 제1 호, 2012. 2.

차건상, “개인정보 유출에 따른 손해배상액 산정기준에 관한 연구”, 숭실대학교 박사학위논문, 2012.

권홍 외 3, “CVM을 이용한 국내 개인정보 침해사고의 위자료 산정”, 정보보호학회논문지 제22권 제2호, 2012. 4.

정태운, “민법 제760조”, 민법주해(XIX), 박영사

김재형, “2012년 분야별 중요판례분석 - 민법(하)”, 법률신문 2013. 2. 28.

- 고형석, "개인정보침해와 피해구제에 관한 연구", 법조 제60권 제10호, 2011.
- 박동진, "불법행위법상 주의의무의 기능", 고시계 45권 11호(2000.11)
- 이승길, "정보화 사회에서의 개인정보권의 침해와 그 구제", 중앙법학 제11집 제1호
- 정보통신정책연구원, "개인정보보호 제도 시행의 경제·사회적 파급효과 분석연구(2001. 12.)
- 한국정보보호진흥원, "개인정보의 경제적 가치 산정 연구의 필요성", 2001. 12.
- 김정택, "특성불안과 사회성과의 관계: Spielberger의 STAI를 중심으로", 고려대학교 석사학위논문, 1978.
- 진성철, 김인경, "인터넷 이용자의 개인정보 유출 가능성에 대한 심리적 불안에 관한 연구: 성별, 이용량, 이용 빈도를 중심으로", 중앙대학교, 2011. 10.
- 서중희, "비재산적 손해배상(위자료)과 '정신적 고통'과의 관계 - 법인의 무형손해를 중심으로", 2011. 5. 동아법학 제51호
- 이동진, "미국 불법행위법상 비재산적 손해의 배상과 그 한계", 민사법학 제66호(2014.3)
- 한국개인정보보호진흥원, 2003 개인정보분쟁조정사례집
- 한창희, 채승완, 유병준, 안대환, 박채희, "기업의 개인정보 유출로 인한 경제적 피해규모 산출방법", 한국전자거래학회지 제16권 제4호
- 김재광, "개인정보보호법에 관한 새로운 법적 문제", 강원법학 제36권 (2012.6)
- 권홍, "CVM을 이용한 개인정보 침해사건의 위자료 산정", 충북대학교 석사학위논문, 2011. 2.
- 김선석, "위자료의 산정과 그 기준에 관한 제문제." 재판자료 제21집(법원행정처), 1984.

## 【외국문헌】

[단행본]

Lawrence Lessig, Code (Basic Books, 1999)

[논문]

Vincent R. Johnson, “Cybersecurity, Identity Theft, and the Limits of Tort Liability”, 57 S.C.L.Rev. 255, 305 (2005).

Richard W. Wright, “Hand, Posner, and Myth of the ”Hand Formular“”, 4 Theoretical Inq. L. 145(2003).

JNSA, “2009年 情報セキュリティインシデントに関する 調査報告書”, JPO Japan Network Security Association, September 2010.



Abstract

Corporate Liability for  
Infringement of Personal  
Information  
– A Study on Compensation  
for Damages

Shin Jae Hyung

Intellectual Property Law

College of Law

The Graduate School

Seoul National University

The evolution of information-oriented society has resulted in increased utilization of services in social, economic, and cultural areas that require personal information. The collection and

utilization of personal information has beneficial effects in first, maximizing the values that could be derived from such information and second, reducing the costs that needs to be paid and risks that needs to be taken by an individual or the government. However, the downside of personal information utilization are that privacy rights or personal rights could be violated and that unauthorized acquisition and processing of personal information could be misused in various crimes.

If sufficient compensation for damage is followed after data spill in civil remedies, business operators would likely to put more effort on preventing the spillage of data before the damage of private information takes place. If the compensation is low the business operators would think less of protecting valuable personal information.

The compensation should not be calculate arbitrarily by the court without specific guidelines, so it is necessary to take into account all factors that could affect the determination of the alimony and moreover, a proper algorithm should be made in order to improve the predictability and verifiability of calculating alimony.

In this article, I have reviewed the concept and nature of personal information, what data spill is, how damage of personal information should be differentiated from violation of personal information, and made effort in setting the standard criteria in determining the degree of damage in personal information.

To assess the compensation for psychiatric harm, I have

reviewed the criteria used inside and outside Korea, and subdivided the factors depending on whether it is related to the personal information itself or related to the victim or the assailant. Based on these factors, I have proposed a four step integrative model in calculating the compensation. This integrative model is unique in that it quantifies the damages of personal information and considers various factors related to the assailant, whereas previous studies have only focused on the data spill itself or the victim.

In integrated calculation model, final damages are to be computed through the following process: i) decide property damage by classifying damages into property damage and mental damage; ii) compute basic damages by deciding objective factors, such as types of leaked personal information and nature of infringement of personal information; and iii) finalize damages by overall considering subjective factors, such as victims and assailants. It is expected that the type and predictability in deciding damages arising from leakage of personal information would be found through said step-by-step computation process.

**keywords : personal information protection, personal information infringement, personal information leakage, liability for damages, noneconomic damages, compensation.**

*Student Number : 2013-21304*