형사정책연구 Korean Criminological Review
제25권 제4호(통권 제100호, 2014 · 겨울)

개인정보 침해사고를 막지 못한 자의 형사책임*

전 현 욱**

국 | 문 | 요 | 약

정보보호조치의무 미이행 구성요건은 결과적 가중범과 유사한 구조를 가지는데, 구성요건을 체계적으로 해석해 보면 불법의 실질이 과실로 인한 정보유출 결과발생에 있는 것으로 볼 수 있으므로 결국 과실범의 성격을 갖는 것으로 보아야 한다. 그런데 ① 의무 미이행에 관한 사실상의 고의 및 ② 정보유출에 대한 주의의무 위반, 그리고 ③ 과실과 정보유출 결과의 인과관계를 입증해 내는 것은 현실적으로 매우 어려울 것으로 생각된다. 정보보호조치의무의 내용이 본질적으로 기술종속적인 것이어서 의무 미이행 구성요건의 구체적인 내용이 백지형법의 형식으로 되어있으며, 내용의 보충 후에도 그리 명확하지 않기 때문에 ① 인식의 객체(고의)가 불분명할 수밖에 없고, 행위자에게 어느 수준까지의 예견과 회피의무를 ② 주관적(과실)으로 기대할 수 있는지를 확인하기 곤란할 뿐만 아니라, ③ 객관적(인과관계)으로 기대해야 하는지도 분명하지 않기 때문이다.

그래서 주요 정보유출 사건은 거의 대부분 혐의 없음 또는 증거불충분 등을 이유로 불기소 처분으로 종결되었으며, 오히려 불기소 처분은 민사상 면책의 근거로 원용되기도 하는 등, 해당 규정은 사실상 애초의 입법의도와는 정반대로 작용하고 있다. 게다가 정보유출 사고 발생시 피해자가 동시에 피의자 될 우려가 높아 오히려 수사에 적극적으로 협조하지 않는 이유가 된다. 형법의 가능성과 한계를 고려하지 않고 진지한 형법이론적 성찰 없이 여론에 의해 무리하게 입법된 형법적 수단은 개인정보에 대한 보호를 강화하기 위해서 결코 실효적이라고 하기 어렵다. 사회는 이를 면책을 위한 최소한의 조건으로 받아들이며, 기업은 다만 처벌받지 않는 수준의 정보보호기술만 도입하려 하므로 정보보호의 수준은 법이 정한 의무기준에 머무르게 된다. 정보침해사고를 막지 못한 보안담당자에게 형사책임을 지우는 방식으로는 결코 정보보호 강화라는 정책적 목적을 달성할 수 없으며, 이러한 부작용이 확인되는 경우 형법은 행정법 또는 민사법적 제재수단에 자리를 양보해야 한다.

❖ 주제어 : 정보보호조치의무, 개인정보, 과실범, 백지형법, 책임

---

* 이 논문은 한국사이버안보법정책학회 7월 월례세미나에서 발표한 글을 보완하여 작성되었다.
** 한국형사정책연구원 부연구위원

Ⅰ. 들어가며

최근 경찰은 약 1200만명의 고객정보를 탈취하여 휴대전화 개통 및 판매 영업에 활용한 해킹사건에 대하여 이를 막지 못한 "KT"의 정보보안팀장과 담당 임원(상무)을 개인정보 보호조치의무 불이행 혐의로 수사하여 지난 5월 기소의견으로 검찰에 송치한 바 있다.[1] 개인정보 침해사고를 막지 못한 자에 대한 형사처벌은, 2008년 6월 13일 개정된 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제73조 제1호에 정보보호조치의무 미이행자에 대한 구성요건의 형태로 처음 도입되었다. 해당 규정은 2010년 개인정보의 암호화 등 기술적 보호조치를 이행하지 않은 인터넷 중고자동차 사이트와 네비게이션 업체의 보안담당 팀장과 대표 등에게 처음 실제로 적용되었으며[2], 이 사건의 피고인들은 약식기소된 후 형사절차를 거쳐 벌금형이 확정되었다고 한다. 이후 다수의 유사한 사례에서 고객의 정보를 해킹당한 업체들이 "피해자"가 아닌 "피의자"로 수사를 받게 되는 상황이 발생하였다.

"정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제73조 제1호는, 2008년 초 "옥션"의 대규모 개인정보 유출사건으로 인하여 개인정보 보호에 대한 국민적 관심이 매우 높아져있던 상황에서 보다 강력한 법적 보호조치를 원하는 여론에 힘입어, 당시 "과태료" 대상이었던 정보보호조치의무 미이행 등 "위법성이 큰 일부 행위를 형사처벌 대상으로 상향 조정"[3]하기 위하여 입법된 것으로, 동시에 같은 법 제64조의3 제1항 제6호에 과징금을 부과할 수 있도록 하는 근거규정도 함께 추가되었다. 이로 인하여, 법이 정하고 있는 정보보호조치의무를 이행하지 않은 자에게는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제76조 제1항 제3호에 의하여 3천만원 이하의 과태료 부과대상이 될 뿐만 아니라, 이로 인하여 개인정보가 "분실·도난·

1) 경향신문, 2014. 3. 7. "정보 관리 소홀 드러나면 KT 경영진도 형사처리 방침" 참조. 그러나 지난 11월 검찰은 개인정보유출 "고의"가 없었으며, 타 통신사의 개인정보보호조치 수준과 비교하여 KT의 조치 수준이 미흡했다고 보기 어렵다는 이유로 무혐의 처분하였다. 연합뉴스, 2014. 11. 9. "검찰 '홈피 해킹사건' KT 상무·보안팀장 무혐의" 참조.

2) 해당 사건에 대한 상세한 내용은 서울지방경찰청 보도자료, 2010. 3. 15. "개인정보 보호조치 의무불이행, 고객정보 유출업체 최초 입건" 참조.

3) "정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안(의안번호 8039)"의 제안이유 및 주요내용 참조.

누출·변조 또는 훼손"되었다면, 매출액의 100분의 1이하에 해당하는 과징금이 부과될 수 있으며, 동시에 2년 이하의 징역 또는 1천만원 이하의 벌금에 처해질 수도 있게 된 것이다. 또한 법인 역시 제75조(양벌규정)에 의하여 1천만원 이하의 벌금으로 처벌된다.

그러나 국회 과학기술정보통신위원회의 법률안 검토보고서[4]에서 적절하게 지적한 바와 같이, "개인정보 보호의 필요성이 높아졌다고 하더라도 제재수단을 상향조정하는 것은 다른 법률과의 형평성이나 과잉금지의 원칙 등을 고려하여 신중하게 결정"되어야 하며, "특히, 민감한 개인정보인 신용정보, 의료정보 등에 대한 의무위반행위에 대한 벌칙 및 과태료가 모두 개정안보다 낮다는 점에서 개정안과 같이 정보통신서비스 제공자등에 대하여만 과도하게 처벌하는 것은 형평성 차원에서 불합리"한 "과잉규제"인 것으로 보인다. 그럼에도 불구하고 해당 개정안은 2008년 5월 국회 본회의에서 재석 174인 만장일치로 가결되었으며 6월 공포되었다.

개인정보 침해사고를 막지 못한 자에 대한 형사처벌 구성요건은 2011년 "개인정보 보호법"이 제정되면서 제73조에 "안전조치의무" 미이행자에 대한 처벌규정으로 다시 한 번 도입되었다. "개인정보 보호법" 제73조는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"의 구성요건구조에 "물리적" 조치만을 추가하여 거의 그대로 입법되었으며, 이로 인하여 보안담당자는 2중의 처벌규정 아래에 놓이게 되었다. 하지만 "제재 강화에 따라 개인정보의 안전한 관리와 개인정보 침해 민원의 감소가 기대"[5]된다는 입법이유와는 반대로, 해당 구성요건이 신설된 이후에도 대규모 정보유출사고는 끊임없이 계속하여 발생하고 있으며, 정보보호조치의무 규정은 구성요건의 불명확성 등으로 인하여 오히려 대부분의 주요 정보유출 사건에서 정보통신서비스 제공자들에게 면책사유가 되고 있는 것이 현실이다.[6] 이는 해당 구성요건이 형법이론에 대한 이해와 검토 없이 만들어진 탓으로 사실상 적용 가능성이 매우 낮기 때문이다.

---

4) 과학기술정보통신위원회, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안 검토보고서, 2008. 5., 30쪽.

5) "정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안(의안번호 8039)" 참조.

6) 주요 사건들의 불기소 처분 이유는 다음과 같다. 2011. 7. SK커뮤니케이션즈, 혐의 없음; 2011. 11. 넥슨, 증거불충분, 2012. 7. KT, 혐의 없음. 2014. 11. KT, 혐의 없음.

이하에서는 "개인정보 침해사고를 막지 못한 자의 형사책임"을 규정하고 있는 국내법의 구성요건과 실제 적용상의 한계점을 분석하고, 이에 대한 형사정책적 검토를 통해 적절한 대안을 제시하고자 한다.

Ⅱ. 현행법상 형사책임 주체

현행법상 정보침해사고를 막지 못한 자의 형사책임에 관한 규정은 다음과 같다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조(개인정보의 보호조치) ① **정보통신서비스 제공자등**이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 **대통령령**으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자

제75조(양벌규정) 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지 또는 제74조제1항의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

개인정보 보호법

제29조(안전조치의무) **개인정보처리자**는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 **대통령령**으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
1. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 자

제74조(양벌규정) ② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

1. 정범 – 정보보호책임자

"정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제28조는 해당 구성요건의 적용 대상을 "정보통신서비스 제공자 등"으로 규정하고 있다. 같은 법 제2조 제1항 제3호는 "정보통신서비스 제공자"란「전기통신사업법」제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다"라고 정의하고 있다. "전기통신사업법"에 따르면 전기통신사업자란 "전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공"하는 자를 말한다.[7] 또한 "전기통신서비스 제공자 등"이란 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제25조 제1항에 의하여 "정보통신 서비스 제공자와 그로부터 제24조의2 제1항(개인정

7) **전기통신사업법 제2조(정의)** 이 법에서 사용하는 용어의 뜻은 다음과 같다. (생략) 6. "전기통신역무"란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다. (생략) 8. "전기통신사업자"란 이 법에 따른 허가를 받거나 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다. (이하 생략)

보 제공 동의)에 따라 이용자의 개인정보를 제공받은 자"를 의미한다. 그러므로 이 규정들을 종합적으로 해석해 보면 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"에 의하여 정보보호조치의무 미이행의 형사책임을 지게 될 자는 전기통신사업을 직접 운영하는 자이거나, 전기통신역무를 이용하여 정보를 제공(또는 매개)하는 자이거나, 그로부터 이용자의 개인정보를 제공받은 자로 한정된다.

또한 "개인정보 보호법" 제29조는 해당 구성요건의 적용 대상을 "개인정보처리자"로 규정하고 있다. 같은 법 제2조 제5호는 "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다"라고 정의하고 있다. 그러므로 통신서비스 제공 또는 개인정보 처리와는 무관하게 시스템의 보안에 관한 부분만을 분리하여 용역을 제공하는 보안업체의 경우 일반적으로 해당 규정들에 의하여 정보보호조치의무를 직접 부담하게 되는 자가 아니며, 따라서 정보보호조치의무 미이행으로 인하여 개인정보가 분실·도난·유출·변조 또는 훼손당한다 하여도 별도의 특별한 사정이 없는 한 해당 구성요건 위반의 정범이 되지 않는 것이 원칙이다.[8)]

예컨대, A기업의 정보보호 책임자가 B가 자사의 정보보호에 관한 부분을 X보안업체에게 외주용역을 주었으나 X보안업체의 기술력 부족 또는 부주의로 인하여 보안사고에 적절하게 대응하지 못하고 정보유출이 발생한 경우, 실제 정보보호에 실패한 행위자는 X보안업체의 보안업무 담당 직원임에도 불구하고 X보안업체 또는 그 업체의 보안업무 담당 직원은 처벌되지 않게 된다. 반면 B와 A기업의 경우 용역업체의 선정 및 관리감독의 소홀 등을 이유로 정보보호조치의무를 이행하지 않은 것으로 판단된다면 경우에 따라 형사책임을 질 수도 있게 된다. 만약 정보유출사고에 대하여 B와 A기업을 처벌하는 것이 정당하고 필요한 경우라면,[9)] 현행법상의 형사책임 주체에 관한 규정은 실제 행위 주체인 X보안업체 또는 그 업체의 보안업무 담당 직원을 처벌하지 못하는 흠결을 갖고 있다고 할 수 있을 것이다.

8) 이 글의 작성 과정에서 검찰과 경찰의 사이버범죄 수사실무 담당자로부터 같은 취지의 의견을 확인한 바 있다.

9) 정보보호조치의무 미이행을 처벌하는 구성요건의 정당성과 필요성에 관해서는 후술한다.

2. 보안업체의 공범 성립 가능성

물론 X보안업체의 보안업무 담당 직원이 A기업 또는 B와 의사연락 하에 정보보호조치의무를 이행하지 않은 경우라면 "형법" 제33조[10]에 의해 공범의 죄책을 질 가능성은 있다. 그러나 일반적이고 A기업이 "갑"이고 X보안업체가 "을"인 현실을 고려하면 "을"이 "갑"의 행위를 교사 또는 방조하는 경우를 생각하기는 어려울 것이다. 또한 X보안업체와 X보안업체의 담당 직원은 비신분자이므로 진정신분범의 간접정범도 성립할 수 없다.

만약 X보안업체측에 기능적 행위지배가 인정된다면 일단 공동정범이 성립할 수 있는 것으로 볼 여지가 있다. 앞에서 살펴본 바와 같이 현행법상 해당 구성요건은 정보보호조치의무를 가지는 자에게만 적용되므로 진정신분범(의무범)으로 보아야 하는데, 진정신분범에 가담한 비신분자의 공동정범 성립 가능성에 대하여는 이견이 있다.[11] 그러나 "형법" 제33조의 문언이 명시적으로 공동정범의 규정을 적용할 것을 선언하고 있으므로 이러한 문제는 입법적으로 해결된 것으로 볼 수 있을 것이다.[12] 하지만 이하에서 검토할 바와 같이 정보보호조치의무 미이행 처벌 구성요건은 행위자에게 "정보유출에 대한 고의"가 없어야만 성립할 수 있는 범죄이므로, 이를 과실범의 성격을 갖는 것으로 보면 공동의 의사와 기능적 행위지배를 생각할 수 없어, 법리적으로 공동정범의 성립은 생각하기 어렵다.[13] 게다가 X보안업체의 담당 직원에게 정보유출의 고의가 있는 경우라면, 실행행위를 스스로 수행한 X보안업체

---

10) **형법 제33조(공범과 신분)** 신분관계로 인하여 성립될 범죄에 가공한 행위는 신분관계가 없는 자에게도 전3조의 규정을 적용한다. 단, 신분관계로 인하여 형의 경중이 있는 경우에는 중한 형으로 벌하지 아니한다.

11) 이에 대하여 상세한 내용은 천진호, 공범과 신분 규정에 대한 입법론적 검토, 형사법연구 제22호, 한국형사법학회, 2004, 301쪽 이하 참조.

12) 같은 생각으로 배종대, 형법총론, 제11판, 홍문사, 2013, 150/6; 오영근, 형법총론, 제2판, 박영사, 2012, 36/19.

13) 과실범의 공동정범과 관련한 논의에 대하여 상세한 내용은 이정원, 과실범에서의 정범과 공범 - 과실범의 범죄구조를 중심으로 -. 형사법연구 제16호, 한국형사법학회, 2001, 116쪽 이하 참조. 다만 과실범의 공동정범을 인정하는 우리 판례의 태도에 따르면 X보안업체의 담당자에게 공동정범이 성립할 가능성이 있다. 이러한 판례의 태도에 대한 비판적 분석으로 이승호, 과실범의 공동정범에 관한 판례의 검토와 학설의 정립, 형사법연구 제23권 제2호, 한국형사법학회, 2011, 151쪽 이하, 특히 166쪽 이하 참조.

의 담당 직원을 직접정범으로 하여 고의의 정보유출행위에 바로 해당하는 다른 죄[14]가 성립하므로, 이 논문에서 논의하고자 하는 정보보호조치의무 미이행죄가 아니라 별개의 정보보호 관련 구성요건이 적용되어야 한다. 그러므로 X보안업체의 담당 직원은 논리적으로 이 죄의 공동정범이 될 수 없다.

Ⅲ. 구성요건에 대한 검토

1. 결과적 가중범과 유사한 구성요건 구조

가. 의무 미이행에 대한 인식과 의욕

우리 "형법"은 고의행위를 처벌하는 것을 원칙으로 하고 있으며[15], 과실행위는 법률에 특별한 규정이 있는 경우에만 예외적으로 처벌한다.[16] 과실범은 "개별구성요건에서 인정되는 예외적 현상"[17]이므로, 형법 제13조와 제14조를 종합적으로 해석해 보면 명시적으로 과실범을 처벌한다는 "특별한 규정"이 있지 않은 경우 모든 구성요건은 원칙적으로 고의행위에 대해서만 적용되는 것으로 보아야 한다.

그러므로 과태료 처분 대상 행위에서부터 출발한 정보보호조치의무 미이행 처벌 구성요건처럼 본래 "행정상의 단속을 주안으로 하는 법규라 하더라도 명문규정이 있거나 해석상 과실범도 벌할 뜻이 명확한 경우를 제외하고는 형법의 원칙에 따라 고의가 있어야 벌할 수 있으며,"[18] 따라서 해당 구성요건이 비록 과실범과 친한 진

14) 예컨대 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다", 제71조 제11호 "5년 이하의 징역 또는 5천만원 이하의 벌금"; 개인정보 보호법 제59조 제3호 "정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위", 제71조 제6호 "5년 이하의 징역 또는 5천만원 이하의 벌금" 등.

15) **형법 제13조(범의)** 죄의 성립요소인 사실을 인식하지 못한 행위는 벌하지 아니한다, 단, 법률에 특별한 규정이 있는 경우에는 예외로 한다.

16) **형법 제14조(과실)** 정상의 주의를 태만함으로 인하여 죄의 성립요소인 사실을 인식하지 못한 행위는 법률에 특별한 규정이 있는 경우에 한하여 처벌한다.

17) 배종대, 형법총론, 제11판, 홍문사, 2013, 53/1.

정부작위범 형식으로 규정되어있다 하여도, 행위자의 과실에 대한 명시적인 언급이 없으므로 원칙적으로는 고의범 구성요건으로 보고[19] 이를 해석의 출발점으로 삼는 것이 바람직할 것이다. 따라서 정보통신서비스 제공자 등이나 개인정보처리자인 행위주체는 "대통령령으로 정하여 요구하는 수준의 정보보호조치의무를 충분히 이행하지 않는다"는 사실에 대한 인식과 의욕이 있어야만 한다.

나. 개인정보 침해에 대한 과실

그런데 고의의 인식대상은 단지 행위와 관련된 객관적 구성요건요소에 그치지 않는다. 결과범의 경우 "행위객체에 대한 행위주체의 구성요건적 행위에 의하여 행위자가 발생시키려고 의도하는 결과"[20] 역시 고의의 인식대상에 포함되어야만 한다. 자신의 행위로 인해 발생하게 될 결과에 대한 인식 없이는 당연히 법익침해의 불법고의가 성립할 수 없는 것이다. 정보보호조치의무 미이행 처벌 구성요건은 개인정보의 "분실·도난·유출·변조 또는 훼손"이라는 결과발생을 객관적 구성요건 요소로 하고 있다.

하지만 만약 행위자가 미필적으로라도 개인정보의 침해라는 결과를 인식하고 의욕했다고 하면, 현행법상 해당 행위의 불법에 대한 형법적 평가는 단지 정보보호조치의무 미이행의 수준에 그쳐서는 안 되며 의도적인 정보침해행위라는 관점에서 판단되어야 한다. 그러므로 행위자에게 정보침해에 대한 고의가 있는 경우 정보통신서비스 제공자 등이나 개인정보처리자의 정보보호조치의무 미이행은 당연히 별개의 정보침해 구성요건의 정범 또는 최소한 방조범에 해당하게 된다.[21] 만약 정보보호조치의무 미이행 구성요건을 무리하게 고의범으로 해석하려 하면, 필연적으로 사

18) 대판 2010. 2. 11. 2009도9807.

19) 해당 구성요건을 고의범으로 해석해야 한다는 견해로 김진환, 개인정보 보호조치 위반 사건 수사의 문제점과 대책, 고려대학교 정보보호대학원 석사학위논문, 2013, 18쪽.

20) 이정원, 구성요건적 고의의 인식대상에 관한 소고, 형사법연구 제13호, 한국형사법학회, 2000, 96쪽.

21) 예컨대 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조의2 제1항 "이용자의 개인정보를 취급하고 있거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다.", 제71조 제5호 "5년 이하의 징역 또는 5천만원 이하의 벌금"; 개인정보 보호법 제59조 제2호 "업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위", 제71조 제5호 "5년 이하의 징역 또는 5천만원 이하의 벌금" 등.

실상 대부분의 정보보호조치의무자들의 구성요건 해당성이 배제될 수밖에 없다.[22] 결국 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"과 "개인정보 보호법"상의 처벌구성요건을 체계적으로 해석하면, 정보보호조치의무 미이행 처벌 구성요건은 당연히 침해의 결과에 대한 인식과 의욕이 없었던 경우에만 적용될 수 있는 구조로 입법되어 있음을 알 수 있다.[23]

즉, 해당 구성요건은 기본범죄(정보보호조치의무 미이행 행위)에 대한 인식과 의욕은 있으나 중한 결과(정보유출 결과)에 대한 인식과 의욕이 없는 경우에만 적용될 수 있어, 마치 결과적 가중범과 유사한 형식을 갖게 되는 것이다. 그런데 이때 정보보호조치의무 미이행 구성요건에 해당한다고 판단하기 위해서는 당연하게도 결과적 가중범과 마찬가지로 중한 결과에 대한 예견가능성이 필요한 것으로 보아야 한다. 우리 형법은 결코 무과실 책임을 인정하지 않기 때문이다. 행위자에게 주의의무 위반의 과실이 있고 이로 인하여 정보유출의 결과가 발생한 경우에만 이에 대한 과실책임을 인정할 수 있다.

그런데, 일반적인 결과적 가중범과는 달리 정보보호조치의무 미이행 구성요건의 경우에는 "기본범죄"가 없다. 정보유출의 결과가 발생하지 않은 단순한 의무 미이행은 현행법상 범죄가 아니며 단지 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제76조 제1항 제3호와 "개인정보 보호법" 제75조 제2항 제6호에 의하여 3천만원 이하의 과태료 처분이 가능한 행위에 불과하기 때문이다. 즉 정보보호조치의무 미이행 구성요건에 있어서 기본이 되는 행위는 고의범을 구성하지 않으므로, 결과적으로는 오로지 과실로 인하여 정보유출의 결과가 발생한 경우에만 처벌되는 구조를 갖게 되는 것이다. 과태료 대상인 기본행위는 업무상 과실범죄의 "업무"처럼 단순히 과실의 전제가 되는 행위에 불과하며, (진정)신분범의 표지에 수반하는 것일 뿐이다. 따라서 해당 구성요건의 범죄불법의 실질은 고의에 의한 기본행위에서는 찾을 수 없으며, 과실로 인한 결과에 해당하는 부분에만 있다고 할 수 있다.

22) 그래서 실제 상당수의 피의자들에게 "고의"가 없다는 이유로 무혐의 처분이 내려졌다.

23) 그러나 현실적으로 주관적 구성요건 요소에 대한 입증 곤란 등을 이유로 결과에 대한 확정적 고의가 확인되는 경우만 별개의 정보유출 구성요건의 적용 대상이 될 것으로 생각된다. 입증이 현실적으로 불가능한 미필적 고의 단계에서 검찰은 고의의 입증이 필요 없는 정보보호조치의무 미이행 구성요건을 선택하게 될 가능성이 높다.

그러므로 정보보호조치의무 미이행 구성요건은 명시적으로 과실범을 처벌한다는 특별한 규정을 두고 있지 않음에도 불구하고 구성요건의 체계적 해석상 과실범의 성격을 갖는 것으로 보아야 한다.

다. 과실의 주관적 귀속

정리하자면, 앞의 예에서 A기업의 정보보호책임자 B에게 정보보호조치의무 미이행 구성요건이 성립하기 위해서는, ① 대통령령으로 정하고 있는 수준의 보호조치를 충분히 이행하지 않는다는 점에 대한 인식과 의욕, 즉 과태료 처분 대상인 기본행위에 대한 사실상의 고의가 있었다는 점이 입증되어야 하며, ② 해당 의무의 불이행으로 인하여 정보유출의 결과가 발생할 수 있다는 점에 대한 예견가능성 및 회피가능성이 있었어야 할 뿐만 아니라, ③ 동시에 주의의무 위반과 정보유출의 결과 사이의 인과관계 역시 명백하게 확인되어야 한다. 즉, 정보보호조치의무의 세부적인 내용은 과태료 처분 대상인 기본행위에 있어서는 고의의 인식대상이며, 동시에 정보유출이라는 결과의 발생원인인 주의의무위반의 내용이 된다.

그런데 해당 구성요건의 경우에는 행위주체가 정보보호업무 담당자로 국한되는 진정신분범의 형태를 갖는다는 점에서 업무자인 행위자에게 일반인보다 높은 수준의 인식 또는 예견가능성, 또는 "고도의 주의능력"[24]이 인정된다는 반론이 제기될 수 있을 것이다. 이러한 입장에 따르면 법이 대통령령 등에 유보하여 정하고 있는 정보보호조치의무를 실제로 이행하지 않았다는 사실관계만으로도 대부분의 경우 정보보호책임자에게 정보보호조치의무 위반의 고의가 간주될 수 있으며, 더 나아가 침해의 결과발생에 대한 주의의무 위반이 있는 것으로 추정될 수도 있을 것으로 생각된다.

하지만 상술한 바와 같이 결과적 가중범이 결과에 대한 무과실 책임을 의미하는 것은 결코 아니므로, 실제로 "결과의 발생을 예견"[25]할 수 있었던 경우에만 성립할 수 있다. 이때 예견가능성은 행위자의 "주관적 예견가능성"을 의미하며[26] 객관적으

24) 배종대, 형법각론, 제7판, 홍문사, 2010, 22/1.

25) 형법 제15조 제2항 "결과로 인하여 형이 중할 죄에 있어서 그 결과의 발생을 예견할 수 없었을 때에는 중한 죄로 벌하지 아니한다."

로 예견할 것을 기대할 수 있었던 경우라 하더라도 구체적인 사건에서 개별적인 행위자에게 이를 예견하고 회피할 능력이 없었던 경우라면 중한 결과에 대한 책임을 행위자에게 주관적으로 귀속시켜서는 안 된다는 것이 전통적인 형법의 책임원칙이다. 따라서 실제 정보보호업무 담당자의 보안관련 기술과 개인적 능력이 충분하지 못하여 객관적으로 요구되는 수준의 주의의무를 준수할 가능성이 없었다면 행위자는, 설령 객관적인 관점에서 구성요건 해당성을 인정할 수 있다 하더라도[27], 최소한 형사책임에 있어서는 원칙적으로 면책되어야 한다. 행위자에게 과실책임이 있는지 여부를 판단하기 위해서는 정보보호조치의무의 주관적 이행 가능성을 고려해야 하는 것이다. 물론 형사소송법의 일반원칙에 따라 행위자에게 이러한 능력이 있었음에 대한 입증책임은 당연히 검사에게 있는 것으로 보아야 한다. 결국 정보보호조치의무는 과태료 처분 대상인 기본행위에 있어서는 이행되지 않았음이 객관적으로 확인되기만 하면 충분하지만, 정보유출의 과실책임과 관련해서는 주의의무의 구체적인 내용이 되기 때문에 행위자의 실제 능력을 고려하여 주관적으로 판단되어야 한다.

물론 이때 주관적으로 능력이 부족하여 기대가능성이 없는 행위자를 정보보호 업무 담당자로 임명한 상급의 의사결정권자에게 감독상의 과실책임을 인정할 가능성도 생각해 볼 수 있다. 그러나 이러한 견해는 결과적으로 타인의 행위에 대한 형사책임이 된다는 점에서 이미 주관적 예견가능성 및 회피가능성의 범위를 벗어나고 있으며, 과실책임의 범위를 사실상 무과실의 영역으로 확대하는 것이다. 당연하게도 무과실 형사책임은 법치국가원칙에 어긋나며[28], 형사책임에서 주의의무 위반은 원칙적으로 행위자의 주관적 예측가능성과 회피가능성을 기준으로 확정되어야 한다.

행위자가 스스로 자신의 능력범위를 넘는 일을 하겠다고 나선 경우라면 인수과실의 책임을 부담해야 하는 것으로 볼 수 있는 여지도 있다.[29] 의료과실을 인정함에 있어 의료인에게 객관적인 수준의 의료능력을 요구하는 것처럼[30] 보안업무와 관련

26) 배종대, 형법총론, 제11판, 홍문사, 2013, 159/5.

27) 과실범의 주관적 측면과 객관적 측면의 구별에 대해서는 이용식, 과실범에 있어서 주의의무의 객관적 척도와 개인적 척도, 서울대학교 법학 제39권 3호, 1998, 29쪽 이하, 특히 61-62쪽 참조.

28) 배종대, 형법총론, 제11판, 홍문사, 2013, 159/45~47.

29) 기존의 주관적 과실론에 대한 비판적 시각에서 허용되지 않는 위험을 초래한 자에게 "인수과실" 등의 과실책임을 인정하는 견해로 한정환, 정상의 주의태만·주의의무위반과 과실, 형사법연구 제20호, 한국형사법학회, 2003, 155쪽 이하 참조.

하여서도 스스로 관련 업무를 맡은 경우라면 해당 영역에서 일반적으로 요구되는 기술적 능력을 주의의무의 기준으로 요구할 수 있지도 모른다.[31] 그러나 의료기술에 비하여 정보보호기술의 발전 속도는 훨씬 빠를 뿐만 아니라, 사람의 생명에 직접 연결되는 의료영역에 비하여 경제적 이해관계가 더 많은 영향을 줄 수 있는 정보보호 관련 업계에서 일반적·객관적·규범적으로 요구되는 기술적 조치의 수준은 객관적으로 그리 명확하지 않다. 그러므로 인수과실 개념의 형법이론적 정당성은 별론으로 하더라도 실제 사례에서 이를 인정하기도 쉽지 않을 것으로 보인다. 항목을 바꿔 살펴볼 백지형법 형태의 구성요건 구조로부터 그 이유를 보다 상세하게 확인할 수 있다.

2. 백지형법과 죄형법정주의 원칙

가. 법률주의 원칙 위반

"정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제28조 제1항은 물론 "개인정보 보호법" 제29조 역시 정보보호조치의무의 내용을 다만 매우 추상적으로 언급하고 있을 뿐이며, 그 구체적인 실질은 "대통령령"에 의하여 정하도록 하고 있다. 물론 백지형법은 입법기술적으로 불가피하며, 현실적으로 사전에 미리 구성요건의 모든 내용을 의회가 만든 법률로 명확하게 기술해 두는 것은 불가능하다.[32] 특히 기술발전에 의하여 구성요건의 능동적 대응이 필요한 정보보호의 영역에서는 더욱 그러할 것이다.

그러나 헌법재판소가 정당하게 설시한 바와 같이 백지형법은 "긴급한 필요가 있거나 미리 법률로써 자세히 정할 수 없는 부득이한 사정이 있는 경우에 한정되어야 하고 이 경우에도 법률에서 범죄의 구성요건은 처벌대상인 행위가 어떠한 것일 것이라고 이를 예측할 수 있을 정도로 구체적으로 정하고 형벌의 종류 및 그 상한과

30) 대판 2010. 10. 28. 2008도8606.

31) 형사책임의 객관화 경향과 이에 대한 법이론적 비판에 관해서는 이상돈, 법학입문, 법문사, 2009, 74쪽 이하 참조.

32) 배종대, 형법총론, 제11판, 홍문사, 2013, 12/6.

폭을 명백히 규정하여야"[33] 죄형법정주의의 법률주의 원칙에 반하지 않을 것이다. 물론 현실적으로 정보보호조치의무의 구체적인 내용은 당시의 보안기술수준에 종속될 수밖에 없으며, 보안기술은 매우 다양한 분야에서 빠른 속도로 발전하고 있다는 점에 비추어 보면, 해당 구성요건을 모두 미리 법률로 자세히 정하여 둘 수 없는 부득이한 사정이 있는 경우에 해당한다는 점에는 이론의 여지가 없을 것이다. 또한 해당 구성요건이 형벌의 종류 및 상한과 폭을 명백히 규정하고 있다는 점도 그러하다.

하지만 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제28조 제1항[34]과 "개인정보 보호법" 제29조를 통해 알 수 있는 처벌대상 행위의 외연은 다만 개인정보가 "분실·도난·유출·변조 또는 훼손"되지 않도록 하기 위해 필요한 조치라는 점뿐이며, 보충규범을 통해 비어있는 내용이 보충되지 않는 한 구체적으로 행위자에게 요구되는 의무의 내용이 무엇인지 즉, 행위자가 어떠한 행위를 하지 않으면 처벌되는 것인지를 알 방법이 전혀 없다. 심지어 해당 조치를 하지 않아 개인정보에 대한 침해가 발생한 경우 바로 행위자를 처벌하는 것으로 정하고 있어 일단 정보침해가 발생하였다는 사실만으로도 결과적으로는 보안조치의 기술적 수준이 충분하지 않았다는 사실이 반증되므로, 문리해석상 현재의 기술수준에서 정보침해를 막기 위해 가능한 모든 조치를 요구하는 것으로 해석될 가능성도 있다.

물론 정보보호담당자는 언제나 가능한 범위 내에서 최신의 보안기술을 익히고 활용해야 할 것이지만, 모든 정보보호담당자가 항상 최첨단의 보안기술에 대한 높은 이해 수준을 유지하고 있을 것을 기대한다는 것은 현실적으로 불가능하며, 또한 형법은 결코 국민에게 불가능한 의무를 형벌로 강요해서는 안 된다. 설령 주관적으로 기대할 수 없는 수준의 주의의무를 법률로 정한다 해도, 책임원칙을 위반하지 않고

33) 헌재 1991. 7. 8. 91헌가4 같은 견해로 대판 2000. 10. 27. 2000도1007 "긴급한 필요가 있거나 미리 법률로써 자세히 정할 수 없는 부득이한 사정이 있는 경우에 한하여 수권법률(위임법률)이 구성요건의 점에서는 처벌대상인 행위가 어떠한 것인지 이를 예측할 수 있을 정도로 구체적으로 정하고, 형벌의 점에서는 형벌의 종류 및 그 상한과 폭을 명확히 규정하는 것을 전제로 위임입법이 허용된다."

34) "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제28조 제1항은 6개호에 걸쳐 행위자의 의무를 추가로 기술하고 있다. 그러나 제1호 내지 제5호의 내용은 여전히 추상적이며, 심지어 같은 항 제6호는 "그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치"라고 하여 사실상 그 내용의 범위를 무한히 확대한다.

서는 발생한 침해결과에 대한 과실책임을 행위자에게 귀속시킬 수 없다. 만약 그렇다면 이는 결국 무과실의 결과책임이 된다. 그렇기 때문에 해당 구성요건이 형법이론적으로 정당한 것이 되기 위해서는, 정보보호조치의무의 내용이 법령에 의하여 가능한 한 구체적으로, 그리고 평균적인 정보보호담당자에게 예측 가능할 뿐만 아니라 통상의 업무수행과정을 통해 합리적인 노력과 비용으로 습득하여 적용할 것을 기대할 수 있는 수준과 범위 내에서 명확하게 정해져야만 한다.

나. 오히려 명확성을 저해하는 보충규범

그런데 대통령령 등을 통해 구성요건의 내용을 보충한다고 해도, 정보보호조치의무의 구체적인 내용은 그리 명확해지지 않는다는 점에서 더 큰 문제를 확인할 수 있다. "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제28조 제1항의 구성요건은 같은 법 시행령 제15조에 의해 보충된다. 이 조항은 같은 법 제28조 제1항 제1호 내지 제5호의 내용에 상응하여 총 5개항에 걸쳐서 구성요건을 보충하여 내용을 보다 명확히 하려한다. 그러나 법 제28조 제1항 제2호를 구체화하는 령 제15조 제2항은 제5호에서 "그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치"를 모두 포함하는 것으로 규정하고 있으며, 또한 법 제28조 제1항 제4호를 구체화하는 령 제15조 제4항은 제4호에서 "그 밖에 암호화 기술을 이용한 보안조치"라고 하여 그 내용의 외연을 무한히 확대함으로써 결국 구성요건을 전혀 한정적으로 구체화하지 못하고 있다. 더 나아가 령 제15조 제6항은 보다 구체적인 기준을 방송통신위원회 고시에 다시 한 번 유보하여 대통령령을 통한 구성요건의 보충을 사실상 포기하고 있는 것으로 보인다.

"개인정보 보호법" 제29조의 경우도 사정은 결코 다르지 않다. 이 조항 역시 같은 법 시행령 제30조에 의하여 구성요건의 내용이 보충된다. 그러나 령 제30조 제1항은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제28조 제1항 제1호 내지 제5호의 내용을 거의 그대로 옮겨놓은 구조를 가지고 있으며 다만 제6호에서 "물리적 조치"를 추가하고 있을 뿐이다. 또한 령 제30조 제3항은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령" 제15조 제6항과 마찬가지로 보다 구체적인 기준을 안전행정부장관 고시에 다시 한 번 유보하고 있다.

물론 명확성을 확보하는데 도움이 되기만 한다면 백지형법을 "고시"를 통해 보충하는 것 그 자체가 문제가 되지는 않는다. 백지형법의 보충규범은 "원칙적으로 헌법 제75조, 제95조에서 예정하고 있는 대통령령, 총리령 또는 부령 등의 법규명령의 형식"[35]을 벗어나지 않는 한, 다른 법률, 대통령령, 규칙, 고시 등의 형태로 구체적인 상황과 필요에 따라 이용될 수 있기 때문이다. 그러나 "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령" 제15조 제6항에 근거한 방송통신위원회 고시인 "개인정보의 기술적·관리적 보호조치 기준"은 상당한 분량임에도, 행위자에게 정보보호조치의무의 내용을 구체적이고 완결적으로 명확하게 제시하였다고는 할 수 없는 정도에 그치는 것으로 보인다. 그렇기 때문에 이 고시는, 68쪽에 이르는 이른바 "해설서"에 의하여 다시 한 번 설명되고 있으며, 결과적으로는 이 "해설서"가 실질적인 보충규범의 역할을 하고 있는 셈이다.

"개인정보 보호법 시행령" 제30조 제3항에 근거한 안전행정부 고시인 "개인정보의 안전성 확보조치 기준" 또한 10개조로 구성되어 있으며, 내용을 보다 분명하게 밝히기 위하여 역시 48쪽에 이르는 분량의 "해설서"에 의하여 설명되고 있다. 이에 더하여 안전행정부는 무려 453쪽에 이르는 "개인정보 보호법령 및 지침·고시 해설"을 발간한 바 있다. 그러나 백지형법의 구성요건 보충이 시행령과 고시를 거쳐 고시에 대한 "해설서"의 단계에 이르고 있다는 점만으로도, "법률에서 범죄의 구성요건은 처벌대상인 행위가 어떠한 것일 것이라고 이를 예측할 수 있을 정도로 구체적으로" 정하라는 헌법재판소의 합헌적 백지형법에 대한 조건을 충족한다고 단언하기 어렵다는 지적에는 넉넉히 동의할 수 있을 것이다.

이처럼 정보보호조치의무 미이행 구성요건에 대하여 법률 및 시행령은 물론 고시와 고시에 대한 해설서 등을 통해서 내용을 명확히 하려 하지만, 이미 그 분량이 지나치게 많아져 오히려 명확성을 저해하는 것이 되어버렸다. 그래서 구성요건 해당성을 확정하기 위해서는 법률부터 고시의 해설서에 이르는 모든 규범의 내용을 숙지하고 이행해야만 한다. 즉, 정보보호담당자가 법이 정하고 있는 정보보호조치의무를 완수하여 형사처벌을 면하기 위해서는 위에서 열거한 법률, 시행령, 고시의 내용을 모두 알아야 할 뿐만 아니라, 각각의 내용이 하나라도 개정될 때마다 이를 모

35) 헌재 2010. 7. 29. 2008헌바106 참조.

두 확인하여 철저히 준수해야 하는 것이다. 더욱이 법집행기관은 정보침해사고가 발생한 경우 매번 피해 업체의 의무준수여부를 확인하기 위하여 고시 등의 개정 시기를 확인하고, 침해 사고 발생 당시의 법령 등의 기준에 의해 인정되는 정보보호조치의무의 내용을 빠짐없이 준수하였는지에 관하여 수사해야만 한다.

다. 정보보안기술과 명확성의 근본적인 한계

이처럼 복잡다단한 단계를 통해 구성요건의 내용을 보충해야 하는 반면, 세부적인 내용을 보충할수록 오히려 불명확해지는 이러한 현상은 바로 기술과 법률의 채워지지 않는 간극으로 인한 것이라고 할 수 있다.[36] 과학은 지속적으로 발전하고 있으며 매 순간 새로운 기술적 수단이 등장한다. 그런데 법규범은 아무리 최신의 기술을 반영하여 입법한다 하더라도, 시간적으로 입법되는 순간의 기술수준에 머물러 있을 수밖에 없으며, 따라서 과학기술영역처럼 지속적으로 변화하는 영역을 규율하는 구성요건의 경우 그 내용을 상세하게 정할수록 더 잦은 개정이 필요하게 된다. 그렇기 때문에 어느 정도는 미래를 향해 열려있는 개념을 사용해야 하며, 이러한 이유로 인하여 특히 과학기술영역에서 백지형법은 입법기술상 불가피한 것이라고 할 수 있다.

그런데 오늘날 정보보안기술은 눈부신 속도로 발전하고 있으며 지금 이 순간에도 새로운 해킹기법과 이를 막기 위한 기술적 조치들이 연구되고 있다. 그런데 정보보안기술의 발전의 속도가 너무 빠르고 그 범위가 너무 넓기 때문에 이 영역을 규율하는 법률은 보다 더 포괄적이 되고, 더욱 더 상세한 보충규범을 필요로 하게 되었다. 하지만 이미 정보유출을 막기 위한 관련 기술의 범위는 그 내용에 대한 규범적 설명을 위해서 수십 쪽 분량의 해설서를 필요로 하게 되었고, 그나마도 미래를 향해 더욱 더 열린 추상적인 개념으로 가득 차게 된 것이다.[37]

게다가 수시로 새로운 기술이 등장하는 상황에서 행위자에게 항상 기술적으로 가

---

36) 정보통신 기술발전과 이를 규율하는 형사법적 개념의 모호성에 대한 분석으로는 전현욱, 개인정보보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 37쪽 이하 참조.

37) 이 "해설서" 또한 구성요건 해당행위를 완결적으로 구체화하고 있지 못하며, 많은 경우 요구되는 의무를 충족하기 위한 행위방법을 예시적으로 열거하거나 기술 발달에 따라 변화할 수 있는 것으로 설명하는데 그치고 있다.

능한 범위 내에서 적극적으로 최선의 보안조치를 확인하여 이행하도록 요구하는 것은 거의 언제나 지나치게 과도한 비용부담을 강요하는 것이 된다. 따라서 법규범은 보안을 위한 수범자에게 무제한의 비용 지출을 강요할 수 없으며, 결국 해설서는 정책적 판단을 통해 현실적으로 가능한 범위에서 의무의 한계를 선언하는 역할을 맡아야 한다. 그렇기 때문에 법규범이 선언한 의무를 모두 준수한다고 해도 형법을 통해 보호하고자 하는 법익, 즉 "정보"는 결코 완전하게 보호될 수 없다는 근본적인 한계를 영원히 해소할 수 없게 된다.

게다가 정책적 판단이라는 것은 결국 누군가의 자의에 의하여 결정된 것일 수밖에 없기 때문에, 법령을 통해 정해진 정보보호조치의무의 구체적인 내용은 정보보안기술의 전문가에게조차 명확하지 않게 된다. 이러한 상황 속에서 만들어진 형사처벌규정의 전제조건인 정보보호조치의무 기준의 예측가능성은 낮을 수밖에 없으며, 핵심형법의 구성요건 요소와는 달리 전문지식에 의한 반론과 이의제기가 가능한 종류의 것이 되어버린다. 그렇기 때문에 법령이 고시와 해설서를 통해 구체화하고자 하는 구성요건에는 여전히 해석과 다툼의 여지가 너무나도 크게 남아있으며, 결과적으로는 행위자에게 규범이 적극적으로 내면화되어 적극적 일반예방을 달성할 가능성은 더 낮아진다. 이러한 상황에서 정책적 결단을 통해 만들어진 구성요건의 내용은 필연적으로 죄형법정주의 원칙을 통과하기에는 너무나도 불명확한 것이 될 수밖에 없으며, 따라서 형사법적 강제를 통한 정보보호는 실패 수밖에 없다.

실제 법령이 요구하는 정보보호조치의무 중 "관리적 보호조치"의 경우 시행령과 고시 및 해설서에서 단계적으로 그 내용을 구체화하고 있음에도 불구하고, "기술적 보호조치"에 비하여 상대적으로 그 명확성이 훨씬 떨어지기 때문에, 실무에서는 행위자가 그 내용을 자의적으로 해석하여 운영하는 사례가 많다고 한다.[38] 그 자의적 해석이 정보보호에 적합하지 않는 경우 사실상 정보가 유출될 위험성은 높아짐에도 불구하고, 실제 유출된 경우에도 법리상 처벌이 불가능하게 되는 문제가 발생한다. 또한 상대적으로 다소 명확한 것으로 보이는 "기술적 보호조치"의 경우에도 보안장비의 "설치" 보다 "운영"과 관련한 내용의 명확성이 훨씬 떨어지게 된다. 그래서

38) 김진환, 개인정보 보호조치 위반 사건 수사의 문제점과 대책, 고려대학교 정보보호대학원 석사학위논문, 2013, 18쪽.

대부분의 경우 법적 기준에 맞는 보안장비 및 소프트웨어가 설치되어 있으나, 실무상 제대로 운영되지 않은 경우가 많을 뿐만 아니라, 이 경우 형사사법기관간에도 의무 이행 여부에 대한 판단이 달라질 우려가 있다고 한다.[39]

게다가 이러한 이유로 인식의 대상이 명확하지 않은 의무 미이행의 고의와, 주의의무의 내용이 명확하지 않은 정보유출에 대한 과실을 확인하고 입증하는 것 역시 매우 어렵게 된다.

3. 인과관계의 입증한계

정보보호조치의무 미이행 처벌 구성요건은 결과범으로 거동범이 아니며, 단지 법령이 정하고 있는 의무를 이행하지 않았다는 것만으로는 부족하고, 과실로 인하여 정보유출의 결과가 발생한 경우에만 성립한다는 것은 이미 앞에서 살펴본 바 있다. 따라서 객관적으로 보호조치의무를 이행하지 않았으며, 법이 요구하는 보호조치의무를 다하지 않았다는 점에 대한 인식과 의욕이 있어야 할 뿐만 아니라, 정보유출의 결과에 대해서는 미필적으로라도 고의가 없어야 하고, 더 나아가 주관적으로 정보유출에 대한 예견가능성과 회피가능성이 있었음에도 주의의무 위반으로 인하여 정보유출의 결과가 발생해야만 정보보호조치의무 미이행 처벌 구성요건의 해당성이 인정된다.

이때 과실과 정보유출 사이에 조건관계조차 성립하지 않는 경우는 인과관계가 당연히 부인될 수밖에 없다. 개인정보가 유출되었으나 법령이 정하고 있는 보호조치의무를 모두 이행했다 하더라도 이를 막을 수 없었던 경우에는 결과는 행위에 객관적으로도 귀속되지 않는다. 예컨대 "접속기록의 위조·변조 방지를 위한 조치"[40]의무를 이행하지는 않았으나, 해킹의 수법을 분석한 결과 이를 이행했다 하더라도 정보유출을 막을 수 없었음이 밝혀진 경우라면 결과에 대한 인과관계가 인정될 수 없

39) 경찰이 기소의견으로 송치한 사건에 관하여 검찰이 구성요건해당성을 인정하지 않고 불기소처분한 경우가 적지 않다고 한다. 이에 관해서는 김진환, 개인정보 보호조치 위반 사건 수사의 문제점과 대책, 고려대학교 정보보호대학원 석사학위논문, 2013, 17쪽 참조. 상술한 KT 사건도 바로 이러한 경우에 해당한다.

40) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조 제1항 제3호.

고 과실의 미수가 되어 당연히 의무 미이행의 기본행위에 대한 과태료 처분 대상이 될 뿐이다. 그러므로 해당 구성요건이 적용되기 위해서는 마침 정보관리담당자가 이행하지 않은 정보보호조치의무로 인해 발생한 보안상의 취약점을 해커가 직접 이용하여 정보유출사고를 발생시킨 경우로 제한된다. 그런데 보안조치의무사항이 해설서 수십쪽에 달하며 그나마도 명백하지 않은 상황에서 정보보호담당자가 미이행한 조치와 해커가 이용한 기술적 수단이 마침 부합하여 인과관계가 확인된다는 사실을 수사기관이 입증하는 것은 결코 쉬운 일이 아닐 것으로 생각된다.[41)]

게다가 형법상 인과관계가 인정되기 위해서는 단순히 선행행위가 결과발생에 대하여 자연과학적 조건관계에 있다는 점만으로는 충분하지 않다. 인과관계를 인정하기 발생한 결과가 "행위자의 작품" 평가될 수 있는지[42)], 또는 그 결과를 행위에 객관적으로 귀속시킬 수 있는지에 관한 규범적 검토가 전제되어야만 비로소 확인된다. 그런데 기술종속성으로 인하여 명확성에 근본적인 한계를 가질 수밖에 없는 구성요건은 이러한 판단도 매우 어렵게 만든다. 인과관계는 객관적 관점에서 보아 행위자가 행위 당시에 행위로부터 결과발생에 이르는 인과의 진행을 예견하고 이를 이용한 것으로 평가할 수 있었는지 여부를 확인하는 것(객관적 상당인과관계설[43)])으로 이루어지며, 이성적 판단을 통해 결과의 발생을 예견할 수 없었던 것으로 확인되면, 그 결과는 규범적으로 행위자의 작품으로 평가될 수 없다. 이때 예견가능성은 전적으로 기술적 이해의 정도에 의존할 수밖에 없다. 그러나 정보침해를 예방하기 위해

41) 제3자의 독립행위가 개입하여 결과를 발생시키는 경우는 바로 전통적인 형법이론에서 인과관계를 단절시키는 대표적인 사례로 설명된다. 강학상 비유형인과관계나 단절인과관계가 바로 여기에 해당한다. 그런데 정보보호조치의무 미이행 구성요건에서 정보유출의 결과는 제3의 인물인 해커의 독립된 행위에 의한 결과이다. 따라서 단순하게 생각하면 정보보호조치의무 미이행 행위가 정보유출을 직접적으로 야기한 것이라고 할 수 없다. 하지만 해당 구성요건에서 인과관계가 요구되는 "결과"는 정보유출 그 자체가 아니라 정보유출을 막지 못한 것이며, 정보보호조치는 해커의 해킹처럼 정보를 유출시키기 위한 행위가 아니라 정보의 유출을 막기 위한 행위이다. 다시 말해서, 이미 행위 당시부터 해커의 공격은, 언제 어떠한 방법이 될지는 정확하게 알 수 없지만, 당연히 "예측가능한 것"이며, 따라서 막아야 하는 것으로 이미 전제되어 있기 때문에, 행위로부터 결과발생에 이르는 인과의 진행에 대한 예견가능성에 전혀 개입하지 않는다. 따라서 정보보호조치의무 미이행의 과실로부터 출발한 인과진행은 해커의 해킹행위에 의해 추월되거나 단절되지 않는다. 그러나 현실적으로 이를 합리적 의심의 여지를 남기지 않을 정도로 "입증"해 내는 것은 전혀 다른 문제이다.

42) 이상돈, 법학입문, 법문사, 2009, 67쪽 이하 참조.

43) 배종대, 형법총론, 제11판, 홍문사, 2013, 51/26.

필요한 관리적, 기술적, 물리적 조치의 내용을 명확하게 확정할 수 없으면, 주의의무 위반 여부를 확인하는 것도 쉽지 않을 뿐만 아니라, 이를 미이행할 경우 어떠한 침해가 발생할 것인지를 예측하는 것도 근본적인 어려움에 봉착할 수밖에 없으며, 따라서 이성적 고려를 통하여 인과진행을 예견할 수 있었음을 입증하여 인과관계를 확인하는 것은 사실상 거의 불가능한 일이 된다.

반면 정책적 결단을 통해 규범적으로 설정된 법령이 정한 보호조치의무의 기준은 언제나 더 우월한 기술에 의한 정보유출 가능성을 전제로 하므로 추상적 관점에서 정보유출의 예견가능성은 언제나 인정될 수밖에 없다. 기술의 우월성은 통시적인 관점에서 항상 상대적인 것이기 때문에 망을 완전히 분리해두지 않는 한 방어기술보다 우월한 공격기술은 언제나 존재할 가능성이 있으며, 따라서 정보유출의 위험은 결코 완전히 예방될 수 없다. 그러므로 정보사회에서 정보유출은 과실책임의 주관적 귀속을 제한하는 일종의 "허용된 위험"에 해당하는 것이어서, 따라서 정보보호담당자에게 정보유출이 추상적인 수준에서 항상 예측 가능한 것이라는 점을 들어 언제나 인과관계를 쉽게 인정하는 것은 결코 타당하지 않다.

Ⅳ. 결론 - 불가능한 임무를 부여받은 형법

지금까지 논의한 바를 요약하면 다음과 같다. 정보보호조치의무 미이행 구성요건은 결과적 가중범과 유사한 구조를 가지는데, 구성요건을 체계적으로 해석해 보면 불법의 실질이 과실로 인한 정보유출 결과발생에 있는 것으로 볼 수 있으므로 결국 과실범의 성격을 갖는 것으로 보아야 한다. 그런데 실무상 해당 구성요건을 적용하기 위해 ① 의무 미이행에 관한 사실상의 고의 및 ② 정보유출에 대한 주의의무 위반, 그리고 ③ 과실과 정보유출 결과의 인과관계를 "합리적 의심"을 배제할 수 있을 정도까지 입증해 내는 것은 현실적으로 매우 어려울 것으로 생각된다. 왜냐하면, 정보보호조치의무의 내용이 본질적으로 기술종속적인 것이어서 의무 미이행 구성요건의 구체적인 내용이 역시 이른바 백지형법의 형식으로 되어있으며, 게다가 내용의 보충 후에도 그리 명확하지 않기 때문에 ① 인식의 객체(고의)가 불분명할 수밖

에 없고, 행위자에게 어느 수준까지의 예견과 회피의무를 ② 주관적(과실)으로 기대할 수 있는지를 확인하기 곤란할 뿐만 아니라, ③ 객관적(인과관계)으로 기대해야 하는지도 분명하지 않기 때문이다.

그래서 주요 정보유출 사건은 거의 대부분 혐의 없음 또는 증거불충분 등을 이유로 불기소 처분으로 종결되었으며, 오히려 불기소 처분은 민사상 면책의 근거로 원용되기도 하는 등, 해당 규정은 사실상 애초의 입법의도와는 정반대로 작용하고 있다. 그럼에도 불구하고 형사처벌 가능성은 여전히 남아 있으므로, 정보보호담당은 언제나 전과자가 될 위험을 무릅써야 하기 때문에[44], 유능한 보안담당자가 외주 보안업체로 이직하는 경우가 많다고 한다.[45] 상기한 바와 같이 외주 보안업체는 해당 구성요건의 정범이 되지 않기 때문이다. 게다가 정보유출 사고 발생시 피해자가 동시에 피의자 될 우려가 높아 오히려 수사에 적극적으로 협조하지 않는 이유가 되기도 하며, "갑"인 정보보호담당자가 보안사고의 원인을 "을"인 외주 보안업체의 탓으로 돌리는 경향을 초래하기도 한다.[46]

물론 개인정보보호 그 자체는 당연히 정당하고 필요한 일이라는 점에는 다툼의 여지가 없을 것이다. 국가는 법과 제도를 이용하여 개인정보에 대한 실효적 보호를 국민에게 제공해야 할 의무를 갖는다. 그러나 일단 이 글의 논의 대상인 정보보호조치의무를 미이행 처벌 구성요건에 국한해서 논한다면, 형법의 가능성과 한계를 고려하지 않고 진지한 형법이론적 성찰 없이 여론에 의해 무리하게 입법된 형법적 수단은 개인정보에 대한 보호를 강화하기 위해서 결코 실효적 수단으로 활용되고 있다고 보기 어려울 뿐만 아니라, 오히려 더 큰 부작용을 만들어내고 있는 것으로 보인다. 정책적 목표를 달성하기 위해 불가능한 임무를 부여받은 형법은 필연적으로 제대로 집행될 수 없으며, 다만 강제로 부여된 목적과는 달리 형법 고유의 논리에 의해 처벌대상을 찾을 뿐이다. 반면 사회는 이를 면책을 위한 최소한의 조건으로 받아들이며, 따라서 기업은 다만 처벌받지 않는 수준의 정보보호기술만 도입하고 그 이상은 불필요한 비용으로 생각하게 된다. 결국 오히려 정보보호의 수준은 법이

44) 한국일보, 2010. 3. 24. "고객정보 못지킨 죄, 보안담당 혼자 저라?" 참조.
45) 보안뉴스, 2012. 10. 10. "해킹 당하면 무조건 보안담당자 책임? 형사처벌 조항은"
46) 데일리시큐, 2013. 4. 2. "보안업체에 사고책임 전가하는 농협…면피할 생각만!"

정한 의무기준을 넘지 못하게 되므로 기술적 발전 가능성을 저해하고 전반적인 보안 수준을 낮춰 오히려 정보유출사고가 더 심각해지는 원인이 되기도 한다.[47] 정보침해사고를 막지 못한 보안담당자에게 형사책임을 지우는 방식으로는 결코 정보보호 강화라는 정책적 목적을 달성할 수 없으며, 이러한 부작용이 확인되는 경우 형법은 행정법 또는 민사법적 제재수단에 자리를 양보해야 한다.

47) 이를 "조종의 트릴레마"라고 한다. 상세한 내용은 토이브너, 이상돈 역, 법제화 이론, 한국법제연구원, 2004, 35쪽 참조.

참고문헌

1. 단행본

과학기술정보통신위원회, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안 검토보고서, 2008.

배종대, 형법총론, 제11판, 홍문사, 2013.

오영근, 형법총론, 제2판, 박영사, 2012.

이상돈, 법학입문, 법문사, 2009.

토이브너, 이상돈 역, 법제화 이론, 한국법제연구원, 2004.

2. 논문

김진환, 개인정보 보호조치 위반 사건 수사의 문제점과 대책, 고려대학교 정보보호대학원 석사학위논문, 2013.

이승호, 과실범의 공동정범에 관한 판례의 검토와 학설의 정립, 형사법연구 제23권 제2호, 한국형사법학회, 2011.

이용식, 과실범에 있어서 주의의무의 객관적 척도와 개인적 척도, 서울대학교 법학 제39권 3호, 서울대학교, 1998.

이정원, 과실범에서의 정범과 공범 – 과실범의 범죄구조를 중심으로 –, 형사법연구 제16호, 한국형사법학회, 2001.

이정원, 구성요건적 고의의 인식대상에 관한 소고, 형사법연구 제13호, 한국형사법학회, 2000.

전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010.

천진호, 공범과 신분 규정에 대한 입법론적 검토, 형사법연구 제22호, 한국형사법학회, 2004.

한정환, 정상의 주의태만·주의의무위반과 과실, 형사법연구 제20호, 한국형사법학회, 2003.

3. 언론보도

경향신문, 2014년 3월 7일자, “정보 관리 소홀 드러나면 KT 경영진도 형사처리 방침”
데일리시큐, 2013년 4월 2일자, “보안업체에 사고책임 전가하는 농협…면피할 생각만!”
보안뉴스, 2012년 10월 10일자, “해킹 당하면 무조건 보안담당자 책임? 형사처벌 조항은”
서울지방경찰청 보도자료, 2010년 3월 15일자, “개인정보 보호조치 의무 불이행, 고객정보 유출업체 최초 입건”
연합뉴스, 2014년 11월 9일자, “검찰 ‘홈피 해킹사건’ KT 상무·보안팀장 무혐의”
한국일보, 2010년 3월 24일자, “고객정보 못지킨 죄, 보안담당 혼자 저라?”

Criminal Responsibility of Security Manager for Personal Information Leakage

Chun, Hyun-Wook

In many cases, incident of leakage of personal information occurs because of negligence of duty of protection the information by the security manager. In legal terms, neglecting duty of protection of personal information comes under an act of criminal negligence. In practice, to apply legal elements of neglecting duty of protection of personal information to cases following should be proved; the security manager's intention of neglecting his/her duty of protecting information; negligence breach of duty on preventing information leakage; and possibility of excluding "reasonable suspicion" from the causal relationship between negligence and leakage of information. Specifically, duty of protecting personal information is closely related to technologies and legal elements of negligence of duty is covered by so-called "Blanketstrafgesetz (blank criminal law)." For these reasons, it is difficult to prove intention behind leakage of information, and to define the scope of responsibility of the security manager when it comes to preventing any possible leakage.

Because of the practical issues, most of information leakage cases were closed with non-prosecution disposition or being cleared of suspicion on grounds of insufficient evidence. Furthermore, non-prosecution disposition is sometimes used as a ground for exempting civil liabilities while criminal responsibility on him/her still remain for the case of personal information leakage. When an information leakage incident occurs, the security manager becomes a victim and at the same time the suspect which makes he/she not actively cooperate to investigation into the incident. In some cases, the security manager pins all blames of information leakage incident on the subcontract company.

It is true that a nation has the duty to protect personal information of people with laws and regulations, though, any legal measures, which have formulated not reviewing sanctions and dispositions under the criminal law but accommodating the public opinion, may cause bigger problems in the future. What should be considered is that any law or regulation shall not fulfill its original purpose if it is enacted for the purpose of achieving policy objectives, but be only used as a legal ground to punish offenses. Under this circumstances, companies in charge of protecting personal information of customers may show the tendency of using technologies which are only acceptable under the law to be exempted from unnecessary legal reasonabilities. Simply put, if companies do their duties of protecting personal information only within the scope of law rather than take any proactive measures so that they do not take any legal responsibility it would result in impeding advancement in new technologies required to protect further personal information, may degrade their level of protection, and cause information leakage incident on the rise.

Policy goals of preventing information leakage incident should not be met by imposing criminal responsibility of information leakage incident on the security manager. To appropriately deal with information leakage cases under the criminal law, limits of the law providing criminal responsibilities for security managers in charge first.

❖ Keyword: duty of protection the information, personal information, criminal negligence, Blanketstrafgesetz(blank criminal law), criminal responsibility

투고일 : 11월 28일 / 심사(수정)일 : 12월 17일 / 게재확정일 : 12월 17일