

● 제322회 국회(임시회) ●
제2차 미래창조과학방송통신위원회

개인정보보호 및 피해 확산 방지를 위한 입법청문회 자료집

◆ 일 시 : 2014년 2월 13일(목) 10:00

◆ 장 소 : 국회 미래창조과학방송통신위원회 회의실(본청 627호실)



국회 미래창조과학방송통신위원회



개인정보보호 및 피해 확산 방지를
 위한 입법청문회 참고인(발제자)
 명단

소속 및 직위	성명	비고
중앙대학교 법학전문대학원 교수	김성천	새누리당 추천
법무법인 지향 변호사	이은우	민주당 추천
고려대학교 정보보호대학원 원장	임종인	새누리당 추천
진보네트워크센터 정책활동가	장여경	민주당 추천
한국인터넷진흥원 인터넷침해대응본부 본부장	정경호	새누리당 추천
파수닷컴(주) 대표이사	조규곤	민주당 추천

목 차

01_ 의견진술

김 성 천 중앙대학교 법학전문대학원 교수 1

02_ 의견진술

이 은 우 법무법인 지향 변호사 15

03_ 의견진술

임 종 인 고려대학교 정보보호대학원 원장 37

04_ 의견진술

장 여 경 진보네트워크센터 정책활동가 49

05_ 의견진술

정 경 호 한국인터넷진흥원 본부장 61

06_ 의견진술

조 규 곤 파수닷컴(주) 대표이사 81

01

의견진술

김성천 중앙대학교 법학전문대학원 교수

의견진술

김성천 중앙대학교 법학전문대학원 교수

개인정보보호 및 피해 확산 방지를 위한 입법청문회 발제

- 피해유형 중 스팸 관련사항을 중심으로 -

1. 들어가며

□ 개인정보의 유출로 인한 피해의 유형은 대체로 다음과 같을 것임

- 스팸 메일·문자·전화
- 보이스 피싱
- 스미싱
- 휴대폰 소액결제 부정과금

□ 이 가운데 스팸 관련 사항을 중심으로 서술함

2. 국내 유통 스팸 현황

□ 국내 유통 전체 스팸 총량은 관계기관의 규제정책 시행의 결과로 다소 감소하고 있으나 악성 스팸은 전송경로를 다양화하면서 활발하게 유포되고 있음

□ 국내 유통 스팸은 이를 통하여 이용자의 시간 낭비와 시스템에 대한 과부하 등을 통하여 연간 약 2조원 이상의 경제적 손실을 입고 있는 것을 파악됨

- 시간당 임금을 1만원으로 계산하였을 때 스팸 1백만통을 기준으로 제목을 확인하는 10초의 시간, 스팸 중 1%의 내용을 확인하는 1분의 시간, 스팸 중 0.01%에 대하여 반응을 보이는 5분의 시간, 스팸을 기반으로 하는 사기의 피해 등을 합산하면 3천 68만원
 - 스팸 필터링 시스템에 의해 걸러지지 않고 도착하는 개인별 메일의 수를 하루 20건으로 잡을 경우 위 계산방식에 따르면 연간 2조 2,703억 2천만원의 경제적 손실
- 스팸으로 인한 피해는 개인정보의 유출로 인한 경우와 그렇지 않은 경우가 있지만, 일반적으로는 개인정보의 유출로 인한 것이라고 볼 수 있음
 - 전달매체별로 나누어 보면 전자우편의 경우에는 전부 개인의 메일 주소가 유포된 것 때문에 발생하는 피해이고, 유·무선 전화의 경우 일부 무작위로 전화를 하는 경우도 있지만 대부분 개인정보가 유출된 경우임
 - 전자우편에 이어 다량의 스팸 송신 경로인 휴대폰 문자를 이용한 스팸의 경우 도박(약 30%)과 대출(약 25%) 등의 불법정보가 최고 순위를 기록하고 있고, 수신된 정보에 대한 이용자의 확인율이 높기 때문에 범죄피해로 이어지는 경우가 많아 문제임
 - 스팸은 불필요한 시간 낭비를 유발하여 경제적 손실을 야기하고, 이를 통해 정작 필요한 정보의 확인이 어렵게 만들며, 과도한 트래픽을 야기하여 정보통신망의 원활한 작동을 방해하고, 사기·도박 등 범죄피해를 야기하는 등 많은 폐해를 가지고 있음

3. 현행 스팸규제 법제의 현황과 문제점

(1) 규제 법제 현황

- 우리나라의 현행 스팸규제 법제는 매체에 따라 Opt-out 방식과 Opt-in 방식 두 가지를 혼용하고 있음

	Opt-out 방식	Opt-in 방식
관련 규정	정보통신망법 제50조 제1항	정보통신망법 제50조 제2항
해당 매체	<ul style="list-style-type: none"> ① 전자우편 ② 그 밖에 대통령령으로 정하는 매체 : ‘정보통신망을 통하여 수신자의 연락처로 부호·문자·화상 또는 영상을 전자문서 등 전자적 형태로 전송하는 매체’ (정보통신망법 시행령 제61조 제1항) 	<ul style="list-style-type: none"> ① 전화 ② 팩스 <p>[예외]</p> <ul style="list-style-type: none"> ① 재화 등의 거래관계를 통하여 수신자로부터 직접 연락처를 수집한 자가 그가 취급하는 재화 등에 대한 영리목적의 광고성 정보를 전송하는 경우 (제50조 제2항 단서 제1호) ② 「전자상거래 등에서의 소비자보호에 관한 법률」 제13조 제1항에 따른 광고 및 「방문판매 등에 관한 법률」 제6조 제3항에 따른 전화권유의 경우 (제50조 제2항 단서 제2호)
금지 내용	이용자가 명시적인 수신거부의사를 표명하였음에도 영리목적의 광고성 정보를 송신하는 행위	<p>수신자의 동의를 받지 않은 채 수신자의 전화나 팩스에 영리목적의 광고성 정보를 송신하는 행위</p> <p>동의 여부와 관계없이 오후 9시부터 그 다음 날 오전 8시까지 영리목적의 광고성 정보를 송신하는 행위</p>
제재 내용	3천만원 이하 과태료 (정보통신망법 제76조 제1항 제7호)	3천만원 이하 과태료 (정보통신망법 제76조 제1항 제7호)

(2) 문제점

1) 정보통신기기의 발전현실과 괴리된 이원적 규제방식

- 종래 인터넷을 통한 정보의 송신과 수신은 컴퓨터를 사용하였고, 전화기는 음성대화를 중심으로 사용하면서 문자 메시지 전송서비스를 부가적으로 사용하는 정도에 그쳤었음
- 이에 따라 필요할 때만 이용하는 컴퓨터에 전송되는 광고성 정보와 착신음이 울리거나 문자 도달 알림이 있게 되면 거의 즉시 반응을 할 수밖에 없는 전화기에 전송되는 정보의 경우를 차별적으로 취급하는 법제가 마련되었던 것임
- 그러나 인터넷을 이용한 메신저가 휴대전화기에서도 사용이 가능하게 되었으며, 인터넷 메신저를 통해 음성통화가 가능하기 까지의 상황이 되면서, 컴퓨터와 전화기의 구별이 점차 의미를 잃어가고 있음
- 따라서 매체에 따라 Opt-in 및 Opt-out 방식으로 이원화하여 스팸을 규제하는 법제는 이제 지양되어야 할 단계에 도달한 것 아닌가 생각됨

※ 참고: 유럽연합과 일본의 경우 Opt-in 방식의 일원적 규제법을 가지고 있음

2) 방문판매자 또는 전화권유판매자에 대한 예외 인정

- 정보통신망법 제50조 제2항은 전화 및 팩스를 통한 정보 송신의 경우에는 Opt-in 방식의 규제를 한다고 하면서도, 방문판매법 제6조 제3항에 따라 방문판매자 또는 전화권유판매자가 재화 등을 판매하고자 소비자에게 미리 판매의 권유를 위한 것임과 성명이나 명칭, 판매하는 재화 등의 종류와 내용을 밝히는 경우에는 사전 동의 없이 정보의 송신이 가능하도록 예외를 인정하고 있음

- 이 예외규정으로 인하여 전화 및 팩스를 이용한 광고에 대한 규제가 사실상 무력화 되어 있는 상황임
- 이는 사업자의 편의를 생각한 예외규정이기는 하지만 이로 인한 사생활 침해가 심각한 실정임

3) 개인정보 수집·처리·제3자 제공 부동의시 계약거부에 대한 규제 미흡

- 개인정보처리자는 정보주체가 개인정보의 수집·처리·제3자 제공 등에 동의하지 않는다는 것을 이유로 계약의 체결을 거부할 수 없다고 하는 규정이 있기는 함 (정보통신망법 제22조 제4항)
- 그러나 이 조항은 선언적 규정에 불과하며 정보주체가 동의하지 않는다는 것을 이유로 계약의 체결을 거부하더라도 아무런 제재도 부과되지 않고 있음
- 이용자는 개인정보처리자가 요구하는 대로 정보제공에 동의하든가 아니면 계약을 포기해야 하는 현실임
- 그 계약이 해도 되고 안 해도 되는 것일 경우에는 모르겠으나 예를 들어 자동차보험과 같은 경우에는 자동차를 운전하는 한 보험 없이 차량운행을 한다는 것은 생각하기 힘들에도 불구하고, 사업자가 원하는 대로 개인정보의 수집·처리·제3자 제공에 동의하지 않으면 보험계약이 사실상 불가능한 현실임

4) 수신거부의사 표명을 쉽게 해주는 방식에 대한 통제 미흡

- Opt-out 방식 규제가 가지고 있는 또 한 가지 현실적인 문제점은 명시적인 수신거부의사를 표명하기가 너무 어렵다는 점
- 이와 관련하여 정보통신망법은 제50조 제4항 제4호를 통해서 영리목적의 광고성 정보를 전자우편이나 그 밖에 대통령령으로 정

하는 매체를 이용하여 전송하는 자는 ‘수신거부의 의사표시를 쉽게 할 수 있는 조치 및 방법에 관한 사항’을 대통령령으로 정하는 바에 따라 광고성 정보에 구체적으로 밝혀야 한다고 규정하고 있기는 함

- 관련규정인 정보통신망법 시행령 제61조 제2항에 따른 [별표 6]을 보면 전자우편의 경우 본문란에 다음과 같은 내용이 있음

매체구분	명시사항 및 명시방법
전자우편	1. 제목란에 관한 사항 2. 본문란에 관한 사항 다. 수신자가 수신거부의 의사를 쉽게 표시할 수 있게 하기 위한 안내문을 명시하고 수신거부여부를 간편하게 선택하는 방식의 기술적 조치를 하여야 한다. 이 경우 그 안내문과 기술적 조치는 한글 및 영문으로 명시하여야 한다. 라. 수신자가 수신거부를 하는 때에 전송에 이용된 수신자의 연락처 외의 개인정보를 전송자에게 제공하도록 요구하는 내용을 명시하여 수신거부를 어렵게 하여서는 아니 된다.

- 그런데 실제로 원하지 않는 영리목적의 광고성 전자우편을 수신하였을 경우, 이에 대한 수신을 거부하는 일은 해당 메일을 삭제하는 일보다 훨씬 복잡하고 시간도 많이 소요될 뿐 아니라 불가능하도록 되어 있는 경우도 많아 매우 번거로운 일임

- 자신이 가입했던 인터넷 사이트에서 보내는 전체메일을 더 이상 수신하고 싶지 않아 수신거부를 하고자 할 경우, 대부분 단순히 ‘수신거부’ 태그를 누름으로써 수신거부 의사표시가 완료되는 것이 아니라, 태그를 누르면 해당 사이트에 로그인 하도록 유도가 되고, 로그인을 한 이후에 다시 수신거부 메뉴를 찾아 가서 이를 클릭하고 저장하도록 프로그래밍 되어 있음

- 여기서 아이디와 패스워드는 새로운 개인정보가 아니기 때문에 이를 요구해도 위법은 아니지만, 자신이 해당 사이트에 가입할 당시의 아이디와 비밀번호를 기억하지 못하는 경우에는 수신거부가 아예 불가능한 일이 되어 버리며, 많은 경우 프로그램 오류로 수신거부가 불가능하게 되어 있음
- 전화의 경우 영리목적의 광고성 전화를 걸면서 ‘재화 등을 판매하고자 소비자에게 미리 판매의 권유를 위한 것임과 성명이나 명칭, 판매하는 재화 등의 종류와 내용’을 밝히기만 하면 그러한 전화가 허용되고, 그에 대한 수신거부는 이용자가 따로 전화를 거는 등의 조치를 통해서 이루어지도록 규정되어 있음

매체구분	명시사항 및 명시방법
전화	1. …… 2. 수신자의 거부 또는 수신동의의 철회용 자동응답전화번호 등의 전화번호 또는 전화에 갈음하여 쉽게 수신자의 거부 또는 수신동의의 철회를 할 수 있는 방식을 정보가 끝나는 부분에 명시하고, 그 전화번호나 방식을 이용하여 수신자의 거부 또는 수신동의의 철회를 하는 때에 수신자가 비용을 부담하지 아니함을 함께 명시하여야 한다. 3. 수신자가 수신자의 거부 또는 수신동의의 철회를 하는 때에 전송에 이용된 수신자의 연락처 외의 개인정보를 전송자에게 제공하도록 요구하는 내용을 명시하여 수신자의 거부 또는 수신동의의 철회를 어렵게 하여서는 아니 된다.

- 가장 합리적이고 간편한 방식은 원하지 않는 영리목적의 광고성 전화를 받았을 바로 그 당시에 텔레마케터에게 수신거부의 의사 표시를 하는 것일 텐데 이에 대한 규정은 없음
- 광고전화의 내용을 끝까지 듣고 수신거부용 전화번호를 메모한 다음 그 번호로 전화를 해서 수신거부를 하는 것은 너무 번거로운 일이라고 생각됨

5) 과태료 부과 규정의 실효성 한계

- 정보통신망법 제76조 제1항 제7호에 따라 금지된 스팸을 발송하는 행위에 대해서는 과태료가 부과되도록 하고 있는데 실제로 부과된 과태료에 대한 징수금액 현황을 보면 다음과 같음

<표> 스팸에 대한 연간 과태료 부과 및 납부 현황

구 분	부과액	법원이관	순징수대상액	납부액	미납액	납부율
2005년	3,488,800	2,616,600	872,200	49,900	822,300	5.7%
2006년	15,846,740	4,460,420	11,386,320	149,440	11,236,880	1.3%
2007년	18,284,273	6,118,734	12,165,539	118,870	12,046,669	1.0%
2008년	4,416,222	1,090,533	3,325,689	30,424	3,295,265	0.9%
2009년	41,332,145	5,160,358	36,171,787	794,366	35,377,421	2.2%
2010년	30,106,408	6,394,881	23,711,527	665,317	23,046,210	2.8%
합 계	113,474,588	25,841,526	87,633,062	1,808,317	85,824,745	2.1%

- 스팸 방지를 위해서 많은 공적 예산이 투입되고 과태료 절차를 위해서도 비용이 소요됨에 비하여 평균 2.1%의 징수율은 지나치게 적다고 할 수 있음
- 이와 같은 현상은 스팸 발송자들이 명의대여 전화기(일명 ‘대포폰’)을 활용하고 있어서 스팸 메시지를 발송한 휴대폰의 소유자를 찾아내더라도 대부분 무자력자인 관계로 과태료를 부과하는 것이 사실상 불가능함으로써 있게 되는 일임
- 따라서 대포폰을 규제하기 위한 통신이용자 실명제 등의 도입이 시급한 현실임

4. 스팸규제 법제 개선방안

(1) Opt-in 방식으로의 규제 원칙 통일

- 본래 영세사업자를 위하여 전자우편 등은 Opt-out 방식의 통제를 가하도록 규정이 만들어진 것이나, 현재 상황은 전자우편을 통한 스팸도 감내하기 어려운 수준에 도달하였음
- 따라서 전자우편을 포함하여 스팸의 유형과 관계없이 모두 Opt-in 방식에 의한 규제를 원칙으로 하는 것이 타당할 것으로 생각됨
- 영세사업자를 위한 배려가 꼭 필요하다면, 예외적으로 일정 규모 이하의 사업자에 대해서만 Opt-out 방식의 규제를 계속하는 것으로 함이 타당할 것으로 판단됨

(2) 방문판매자 또는 전화권유판매자에 대한 예외 지양

- 오는 전화는 일단 받게 된다는 측면에서 전화광고를 Opt-out 방식으로 규제하기는 곤란하다는 원칙이 당연히 타당함
- 문제는 정보통신망법 제50조 제2항 단서가 ‘방문판매법 제6조 제3항에 따라 방문판매자 또는 전화권유판매자가 재화 등을 판매하고자 소비자에게 미리 판매의 권유를 위한 것임과 성명이나 명칭, 판매하는 재화 등의 종류와 내용을 밝히는 경우에는 사전 동의 없이 정보의 송신이 가능하도록 예외를 인정’하고 있는 것임
- 전화광고를 Opt-out 방식으로 규제한다고 하면서 이와 같은 예외를 허용한다는 것은 전화광고의 일반적인 유형에 대해서 예외를 허용하는 것으로서 결국 Opt-out 방식으로 규제하지 않겠다는 것이나 마찬가지로

- 따라서 정보통신망법 제50조 제2항 단서의 예외는 폐지하여야 마땅하나 일자리 등의 측면에서 전격적인 삭제가 곤란하다면,
- ‘재화나 용역을 판매하고자 미리 소비자에게 판매의 권유를 위한 것임과 성명이나 명칭, 판매하는 재화 등의 종류와 내용을 문자전송을 통해서 밝히고’ 문자를 확인할 정도의 일정시간 이후에 문자를 전송한 바로 그 번호로 전화를 걸어 소비자가 수신하는 경우에는 정보의 전송이 가능하도록 하는 정도의 조치는 필요하다고 생각됨

(3) 개인정보처리 허용요건의 합리화

- 개인정보처리자는 정보주체가 개인정보의 수집·처리·제3자 제공 등에 동의하지 않는다는 것을 이유로 계약의 체결을 거부할 수 없다고 하는 정보통신망법 제22조 제4항의 규정은 이를 강제할 장치가 없기 때문에 실효성을 담보할 수 없음
- 따라서 이용자의 입장에서는 재화나 용역의 제공을 받고자 하는 경우 사업자가 요구하는 범위의 개인정보의 수집·처리·제3자 제공 등에 동의하지 않을 수가 없음. 동의가 강제되고 있는 상황임
- 그렇다고 소비자가 개인정보의 제공을 전면적으로 거부함에도 무조건 계약을 체결하도록 강제하기도 곤란하다면, 소비자나 사업자의 입장에서 벗어나 제3자의 객관적인 시각에서, 개인정보의 수집·처리·제3자 제공 범위를 합리적으로 확정하여 그 범위 내에서 개인정보가 수집되고 처리되도록 할 필요가 있음
- 이와 같은 개인정보처리의 허용범위는 계약의 유형과 내용에 따라 달리 정해져야 할 것인바, 사업자가 각 계약 유형별로 수집·처리하고자 하는 개인정보의 범위를 설정하여 이에 대한 승인을 정부에 신청하고, 주무부처에서 이를 심사한 후 필요한 범위를 다

시 설정하여 승인하도록 하는 방법이 합리적일 것이라고 생각됨
(현재 프랑스가 이와 같은 규제방식을 취하고 있음)

- 나아가 이와 같은 개인정보처리 허용범위에 대한 승인 내역은 공개되어 여론의 감시를 받아야 할 것이며, 국회에 정기적으로 보고되어야 할 것임

(4) 수신거부의사 표시의 곤란성 해소

1) 전자우편의 경우

- 정보통신망법 시행령은 “수신자가 수신거부의 의사를 쉽게 표시할 수 있게 하기 위한 안내문을 명시하고 수신거부여부를 간편하게 선택하는 방식의 기술적 조치를 하여야 한다.”(제61조 제2항에 따른 [별표 6])고 있는데, 수신거부여부를 간편하게 선택한다는 것이 한번의 클릭으로 거부의사의 표시가 완료되는 것을 의미한다는 점은 명시하지 않고 있음
- 이로 인하여 수신거부 태그를 클릭한 이후에도 해당 전자우편을 발송한 웹사이트로 다시 접속하게 되고 로그인을 하여야 하는 등의 번거로운(간편하지 않은) 절차를 거쳐야 하는 현실이 해소되지 않고 있음
- 따라서 ‘수신거부여부를 간편하게 선택하는 방식의 기술적 조치’가 무엇을 의미하는가에 대한 보다 명확한 규정의 제정이 필요함

2) 전화의 경우

- 영리목적의 광고성 전화를 받았을 바로 그 당시에 텔레마케터에게 수신거부의 의사표시를 할 수 있도록 관련규정을 개정하여야 하겠음

- 지금과 같이 광고전화의 내용을 끝까지 듣고 수신거부용 전화번호를 메모한 다음 그 번호로 전화를 해서 수신거부의 의사표시를 하는 것은 너무 번거로운 일이라고 생각됨

(5) 통신이용자 실명제의 실시

- '명의대여 휴대폰이 각종 탈법·불법행위에 이용되고 있는 바, 이를 규제하는 방안으로는
 - ① 명의 대여 자체를 규제하는 방안
 - ② 명의대여자를 규제하는 방안
 - ③ 실질 사용자를 규제하는 방안 등이 있음
- 효율적인 규제를 위해서는 명의대여 자체를 금지하는 규정을 마련하고 이를 위반한 경우에는 실질적 사용자는 물론이고 명의대여자도 형사처벌을 하는 방식(실명등기법과 동일한 방식)을 도입할 필요가 있고, 이는 전기통신계약과 관련된 사항이므로 전기통신사업법에 도입하는 것이 바람직함
- 탈법·불법행위에 이용되는 휴대폰의 명의를 대여하는 사람들은 무자력자이어서 과태료를 부과해도 이를 징수할 수가 없는 관계로 벌칙규정이 규제의 실효성을 담보하지 못하고 있으나, 제재의 내용을 형벌(벌금)로 전환하게 되면 환형유치가 가능하기 때문에 규제의 실효성을 확보할 수 있음

02

의견진술

이 은 우 법무법인 지향 변호사

의견진술

이은우 법무법인 지향 변호사

1. 카드사 고객정보 유출 사태로 본 우리나라 개인정보의 취약성

가. 카드사 고객정보 유출 사고의 원인

(1) 막을 수 있는 사고였는가, 필연적인 사고인가?

- 인재¹⁾라고 보는 것은 절반의 이해.
- 개인정보 유출사고의 대부분은 내부 유출 사고임.

(2) 문제는 무분별한 개인정보 수집, 활용(금융지주회사, 제휴사, 신용정보 조회, 신용정보 조사, 신용정보집중기관, 마케팅 활용), 약한 내부 통제에 있음.

나. 우리의 특수한 상황이 고려되어야 한다

(1) 높은 본인식별과 낮은 익명성

- 실명서비스 위주
 - ▶ 인터넷 실명제의 여파
 - ▶ 위헌 결정(2012) 이후에도 변하지 않는 정책
 - ▶ 익명서비스 권리 확립되어 있지 못함
- 주민등록번호

1) “금번 고객정보 유출사건은 기본적인 보안절차만 준수하였더라도 충분히 막을 수 있었던 전형적인 인재(人災) 사고였으며, 이번 사건은 KCB 직원이 3개 카드사의 위·변조 방지시스템 용역 과정에서 카드사 고객정보를 대량 갈취한 사건이고, 외부인의 USB사용 차단, 고객정보 암호화 등 안전성 준수사항이 있었음에도, 카드사가 이를 제대로 이행하지 않은 것이 원인”

(2) 본인식별 가능, 재식별 가능

- 핵심 식별자 역할을 하는 실명 식별된 식별자가 많음 - 주민등록번호, 휴대전화번호, 이메일, 트위터, 카카오톡
- 대부분 실명가입 강제하고, IP, 휴대폰 고유식별번호, MAC Address 등 식별가능한 정보 수집 보편화
- 익명화 조치에도 불구하고 재식별 가능. (익명화 조치를 했을 때 개인정보가 아닌 것으로 취급하기 어려움).

(3) 정보의 집중도 높음

- 높은 신용카드 보급률(세계 1위)과 광범위한 제휴서비스
- 대기업(대규모 기업집단 경제 집중 심화 및 기업집단 내외 제휴 활성화)
- 높은 IT 보급률(초고속 인터넷 보급으로 인터넷 이용 활성화, 높은 스마트폰 보급률로 방대한 데이터 집적 가능, IPTV 655만, 종합유선방송 517만, 위성방송 379만, 총 1,551만), 통신 가입비율(이동통신2013년 6월말 가입자수 5,410만명, 스마트폰 가입자 수 2013년 6월말 가입자수 3,556만명, LTE 가입자 2,200만명), 포털 독점 심화
- 금융지주회사들

다. 우리나라의 개인정보의 흐름도



라. 더 늦기 전에

- 제2, 3의 사고 발생의 가능성은 언제나 존재
- 사고의 유형
 - ▶ 규모 : 대규모 유출형, 소규모 유출형, 소수 표적형
 - ▶ 유출되는 정보 : 신분정보, 경제정보, 민감정보(위치정보, 의료정보, 구매내역 정보 등)

2. 근본적인 문제 해결이 필요

가. 개인(신용)정보의 수집, 생성, 유통과정의 점검

- 개인(신용)정보의 수집은 최소수집, 목적명확, 개인정보 주체의 통제권 보장에 부합하는가?
- 개인(신용)정보의 공유는 적절한가?
- 개인(신용)정보의 오남용의 가능성은 차단되고 있는가?
- 개인(신용)정보 오남용의 가능성을 효과적으로 감독할 수 있는가?

나. 이미 유출된 개인(신용)정보의 위험을 없애거나 줄여야 함

- 명의도용 방지를 위한 대응방안의 마련
- 피싱, 스미싱 등의 방지를 위한 대응방안의 마련
- 무분별한 마케팅 활용을 방지하기 위한 대응방안의 마련

다. 재발방지를 위한 근본적 제도 개선

- 주민등록번호 제도의 개선
- 본인 인증 제도(성인인증, 연령인증 등)

- 신용정보 유통과 관련한 제도의 개선
- 전 사회적인 개인정보 유통 점검과 제도 개선
- 개인정보 보호 법제 보완
- 감독, 권리구제 기구 점검

3. 개인정보의 수집, 활용, 유통과 관련한 정보통신 분야의 가장 큰 위협 - 거대정보집적자 - 빅데이터와 프로파일링

가. 거대정보 집적자의 개인정보 포식 문제

(1) 금번 카드사의 고객정보 유출도 거대정보 집적자로부터의 유출

- 신용카드사들과 금융지주회사들의 개인신용정보 집적

금융지주 계열사 간 공유된 주요 고객정보(2011~2012년)

단위: 천

금융지주사명	제공사	이용사	종도	공유 고객정보 내용	제공 건수			
우리 우리은행·광주은행·경남은행·우리투자증권·우리이비바생명보험·우리자산운용·우리피아넷실·우리금융저축은행	우리은행	우리이비바생명	마케팅	주민등록번호, 이름, 직장명, 부서명, 전자우편 등 16개 항목	194만9천			
	광주은행	우리은행	대출 업무	주민등록번호, 이름, 중도금 대출잔액, 지역 주소, 휴대전화번호	200			
신한 신한은행·신한카드·신한금융투자·신한생명·신한IFP파리비자산운용·신한캐피탈·제주은행·신한저축은행	신한은행	신한카드	마케팅	실명번호(주민등록번호 등), ATM 이용 일자, 이용기간, 이용 금액 등	38만4995			
				실명번호, 최근 3개월 유동성 평단, 최근 3개월 내 청구 거래 여부	1만54			
	신한카드	신한은행	고객분석	실명번호, 직장 주소, 직장 1차 회단 지명명 등	36만2816			
				실명번호, 이름, 회사명, 상품 구분 등	2088만6790			
	신한은행	마케팅	마케팅	실명번호, 스마트폰 종류, 결제계좌 신한 여부	19만1601			
				실명번호, 최근 12개월 롯데화점 이용 금액	52만1099			
	신한생명	신한카드	마케팅	실명번호, 최근 6개월 접속 건수, 최근 6개월 접속 수 등	107만6848			
				실명번호, 최근 3년간 자동차 정검·수리업체 이용 여부 등	5만			
신한생명	신한카드	마케팅	실명번호, 이름, 결혼 여부, 결혼기념일, 직장명, 부서명 등	5천				
			실명번호, 이름, 계약일자, 월납보험료, 납입 방법, 상품 종류, 직장명, 휴대전화번호 등	22만450				
한국투자 한국투자증권·한국투자저축은행·한국투자신협은행·한국투자별류자산운용	한국투자증권	한국투자별류 자산운용	마케팅	이름, 주민등록번호, 주소, 연락처 등 4개 항목	6천			
				하나은행	하나생명	보험상품 텔레마케팅	기준연월일, 주민등록번호, 이름, 전화번호(지역·직장·휴대전화), 주소(지역·직장), 직장명, 직위, 카드번호, 카드 유효기간, 결혼 여부, 자녀 수, 전자우편, 신규 카드 발급 여부	17만5천
							하나SK카드	결제 계좌 변경 텔레마케팅
				하나은행	하나캐피탈	대출상품 텔레마케팅	기준연월일, 이름, 주민등록번호, 전화번호(지역·직장·휴대전화), 주소(지역·직장), 직장명, 직위, 스마트폰 평점	2만
							하나생명	하나캐피탈
KB KB국민은행·KB국민카드·KB투자증권·KB생명보험·KB자산운용·KB부동산신협·KB인베스트먼트·KB신용정보·KB저축은행	KB국민은행	KB생명보험	보험상품 텔레마케팅	이름, 주민등록번호, 연락처, 카드번호, 유효기간 등	1305만			
				KB국민카드	마케팅 SMS 발송	주민등록번호, 스마트폰 번호, 스마트폰 OS 정보	410만2천	
한국스탠다드치타드 한국SC은행·한국SC저축은행·한국SC캐피탈·한국SC증권·한국SC핀드서비스	SC은행	SC저축은행	SC은행에서 도림문(신용여신) 거절된 고객을 저축은행으로 흡수하기 위한 설문조사	이름, 연락처, 드림폰 필수일, 신청일 번호, 예상 대출 한도, 예상 금리	300			
				한국의씨 한국씨티은행·한국씨티그룹캐피탈·씨티금융 판매서비스·씨티크레딧서비스신용정보	씨티은행	마케팅 (중복구매 고객 파악)	주민등록번호, 주소, 전화번호, 직종, 연소득, 대출계좌번호, 대출 신규 금액, 금리, 대출 실행일, 대출 만기일 등 17개 항목	20만7천
BS 부산은행·BS투자증권·BS신용정보·BS캐피탈·BS정보시스템·BS저축은행	BS저축은행	신용대출 마케팅	이름, 주민등록번호, 휴대전화번호 등 20개 항목				6만	
			메리츠 메리츠화재해상보험·메리츠증권증권·메리츠자산운용·리츠파트너스·메리츠캐피탈	메리츠화재	복합정보 수내역 지점 홍보	이름, 주소, 연락처, CMA 보유 금액 등 7개 항목	1990	
메리츠화재	메리츠캐피탈	신용 대출 상품 판매				이름, 연락처, 전자우편, 주소, 휴대전화번호, 직업, 경력 등 9개 항목	4만2천	
			메리츠증권	메리츠증권	복합정보 수내역 지점 홍보	이름, 주소, 연락처, 소유 차종, 월납입보험료 등 6개 항목	409	
DGB 대구은행·카드넷·대구신용정보·DGB캐피탈	대구은행	카드넷				학생증 카드 출결시스템 구축	학생증 관련 정보-NBS(교과부 관리) 번호, 이름, 교통카드번호	3천
			DGB캐피탈	마케팅 활용 (계정 안내장)	업세명, 사업지번호, 주소, 전화번호, 여신잔액, 신용등급 등 9개 항목		2700	
NH농협 NH농협은행·NH농협생명보험·NH농협손해보험·NH농협증권·NH-CA자신운용·NH농협캐피탈·NH농협신용	농협은행	농협생명			보험 텔레마케팅	이름, 생일, 연령, 휴대전화번호, 지역 전화번호, 직장 전화번호, 전자우편, 카드 가입일자, 최근 카드 사용일자 등 23개 항목	264만	

*고객정보 이용 가능 계열사들(2012년 기준)
 자료: 민주당 김기석 의원실, 17개 금융지주사 금융위협회 제출 자료 요약

[출처 : 한겨레 21(2014. 2. 17. 박현정 기자)]

(2) 거대정보 집적자의 특징

- 대규모 : 사용자 규모 1천만명 이상, 5천만명 이상, 점유율 50% 이상
- 네트워크 효과 : 규모가 점점 커지고, 점유율이 상승
- 플랫폼 : 활동의 기반
- 정보집적의 가속화 : 다양화, 심화

- Big Data 기반의 플랫폼 구축
 - 국내 스마트폰 보급대수가 3,000만대를 넘어서는 등 다양한 Mobile Device의 확산
 - 강력한 플랫폼을 가진 사업자가 ICT 시장의 주인공으로 부상
 - 다양한 Data의 양적, 질적 팽창으로 인해 Big Data 기반의 플랫폼 구축을 통한 차별적 경쟁력 강화의 중요성이 부각됨
- 플랫폼
 - 다양한 고객그룹들 간의 거래를 촉진하여 새로운 가치를 창출하는 중개 수단(Intermediary)
 - 가입자와 이용자를 끊임없이 모여들게 하고 일정한 lock-in효과를 갖도록 하는 Ecosystem 형성이 중요
 - 플랫폼은 기술적인 운영표준(iOS, Android OS), 가입자 기반 서비스 체계(Facebook, Twitter), 시장(Amazon, T store) 등 다양한 형태로 존재하며, 최근 '개방성'을 바탕으로 Global 확장이 가속화되면서 그 형태와 규모가 진화/확대되고 있음
- 플랫폼의 높은 성장 잠재력, 구글의 사례
 - 플랫폼 사업은 다양한 인접서비스와의 연계성 및 Global시장으로의 확장 측면에서 아주 높은 성장 잠재력을 가지고 있음.
 - Google의 사례
 - 수백만의 3rd Party를 광고 플랫폼인 애드센스로 끌어당김으로써 롱테일 광고라는 새로운 Ecosystem을 조성하였고, 모바일 시장에서도 안드로이드 OS를 기반으로 플랫폼 경쟁력을 확보하면서 높은 성장세를 보임.
 - 소비생활 전 영역에 걸쳐 구매행동 및 인식 패턴 정보를 분석할 수 있는 DB를 보유하고, 이를 활용하여 차별화된 서비스를 제공할 수 있는 Big Data 기반의 플랫폼 구축이 미래 핵심 경쟁 요소로 부각.

(3) 거대정보 집적자의 사례

- 통신사 : SKT, KT, LGU+
- 포털 : 네이버, 다음, 구글
- 소셜네트워크 서비스 : 카카오톡, 라인, 페이스북
- 금융사(신용카드사, 은행, 보험, 증권 등), 제휴 서비스(OK 캐쉬백 등)

나. 거대정보 집적자의 개인정보 포식의 문제점

(1) 개인정보주체의 동의나 인식 없는 개인정보 융합

- 플랫폼 기반의 개인정보의 집적
- 집적된 개인별 정보 (통신사, 금융사, 포털)

(2) 집적된 개인정보 유출 위험

- 정보 활용 = 접근 가능성 = 유출 가능성
(정보가 활용된다는 것은 접근 가능하다는 것이고, 이는 유출 가능하다는 것을 의미함)

(3) 소비자 주권 침해

- 원하지 않는 마케팅의 희생양

(4) 개인정보 집적으로 형성하는 독점과 산업생태계 침해

- 플랫폼 사업자로의 정보 독점
- 우월한 정보를 바탕으로 한 독점 강화

다. 해결방안

(1) 최소수집의 원칙

- 서비스에 필요한 최소한의 정보만 수집
(예 - 네비게이션 정보는 사용 후 위치정보 삭제)

(2) 선택권의 실질적 보장

- 개인정보 통제권 보장

(3) 소비자 보호

- 적극적 소비자 보호 조치

라. 국제적 흐름

(1) ICCDP(International Conference of Data Protection and Privacy Commissioners) 우루과이 선언(2012, 국제 개인정보 보호 감독기구 회의, 2012년 우루과이 회의에서 채택)

① 배경

- 다양한 원천으로부터 수집한 정보를 바탕으로 프로파일링을 할 경우, 정보의 정확성, 최초 수집시의 목적과의 불일치 등으로 위험이 큼.
- 이와 관련한 개인정보 보호 원칙이 중요하며, 목적 제한의 원칙이 매우 중요함.

② 투명성과 신뢰 - 최대한 고지

- 고지할 내용 - 수집되는 방법, 프로파일의 사용 목적 등을 정보주체에게 알려야 함
- 더 잘 고지할수록 개인은 그의 데이터에 대해 더 잘 통제할 수 있다.

③ 운용의 단계에서의 3단계 검토

- 먼저, 프로파일링을 이용할 필요가 있는지 여부에 대한 판단이 이루어져야 한다.
- 둘째, 어떤 가정과 어떤 데이터가 프로파일링의 기초를 형성할지를 결정해야 한다.
- 셋째, 실제로 프로파일이 어떤 방식으로 적용될지를 결정해야 한다.
- 각 단계별로 분리해서 판단하고, 별도 감독이 이루어지는 것이 바람직하다.

(2) 바르샤바 선언(2013)

① 명확하게 확정

- 프로파일링을 시작하기 전에 미리 특정한 프로파일링 운용의 필요성과 실제 용도를 명확하게 확정하고, 적절한 보호조치가 마련되어야 한다.

② 제한. 최신성과 정확성

- Privacy by design의 원칙에 부합하도록 가정과 데이터의 양을 의도한 적절한 목적에 필요한 범위의 수준으로 제한. 데이터는 가능하다면 의도된 목적에 충분하도록 최신성과 정확성을 보장해야 한다.

③ 지속적 확인

- 결과를 향상시키고 오류를 줄이기 위해서 프로파일과 알고리즘이 지속적으로 확인되어야 한다.

④ 고지와 통제

- 가능한 한 최대한의 범위에서 프로파일의 결합 방법, 프로파일이 사용되는 목적을 포함하여 프로파일링 운영에 대해 사회에 알려야 한다. 그리고 개인들이 가능하고, 적절한 최대한의 범위에서 개인정보에 대한 통제권을 유지할 수 있도록 보장하여야 한다.

⑤ 접근, 개입

- 개인에게 중대한 법적 영향을 미치거나, 개인의 이익이나 지위에 영향을 주는 결정에 대해서는 그 개인에게 그의 접근권, 수정권과 인간의 개입권이 보장되어야 한다.

⑥ 감독

(3) 유럽연합 개인정보감독기구의 Working Party 29(EU WP 29) 프로파일링에 대한 의견서

① 프로파일링에 대한 분명한 정의 규정과 규율이 필요하다

- 프로파일링의 정의
- “프로파일링”은 개인의 특성이나 개인의 어떤 측면, 특히 개인의 건강, 경제적 상태, 업무 처리, 개인의 취향, 관심, 행위의 신뢰성,

위치나 이동에 대한 분석이나 예측을 위한 개인정보의 자동화된 처리를 의미한다.

② 빅데이터 처리의 두 가지 경우를 구분

- 추세나 정보의 상호관계를 밝히기 위한 경우
 - 비밀유지, 데이터의 안전성, 기능적 분리를 보장하기 위해 필요한 기술적, 조직적 수단을 갖추어야 한다.
- 개인의 취향, 행동, 태도를 분석하거나 예측하기 위한 경우
- 거의 언제나 자유롭고, 특정되고, 충분히 인지되고, 모호하지 않은 사전 동의가 있어야 한다. 특히 직접 광고(Direct marketing), 행태 광고, 데이터 판매, 위치 기반 광고, 추적 기반 디지털 시장 조사(digital market research)의 경우
- 그렇지 않은 경우에는 추가적 사용은 호환가능한 것으로 볼 수 없다.

③ 프로파일링에 대한 규율 - 더 투명하게

- 정보주체에게 상세한 정보를 제공해야 한다
 - 정보주체의 정보가 프로파일링의 목적으로 사용되고, 프로파일을 생성하게 될 것이라는 점을 인식해야 함,
 - 어떤 목적으로 프로파일링이 이루어지는지 알아야 함,
 - 자동화 절차의 내재된 판단기준을 이해해야 함.

④ 정보주체의 강화된 통제권

- 명시적 동의
- 추가적으로
 - 프로파일의 접근권(Right to access the profile)
 - 수정, 삭제권,(Right to modify or to delete the profile)
 - 프로파일로 인한 조치나 결정을 거부할 권리(Right to refuse any measure or decision based on the profile),
 - 이의를 할 권리(사람에 의한 개입 포함)

- ⑤ 정보처리자의 책임성과 신뢰성이 더 필요
 - 사전 영향 평가 필요
 - 정보처리자에 의한 안전조치가 필요
- ⑥ 이익의 균형
 - 추가적으로 이익 균형이 필요함. 반드시 사안별로 영향이 평가되어야 함. 그에 따라 적절한 조치가 취해져야 함.
- ⑦ 위험의 평가
 - 위험을 평가하기 위해서 호환 가능성, 안전조치의 평가가 필수적
- ⑧ 공개
 - 결정의 기준, 프로파일을 생성하게 한 데이터의 원천을 공개. 개인의 수정과 업데이트를 가능하도록 해야 함.
- ⑨ 개인정보주체의 권리 강화
 - 개인정보 주체의 권리 강화, 소비자와 정보처리자의 균형이 중요 (개인정보 주체의 간편하고, 사용자 친화적 직접 접근권, 이익의 공유, 선택권 보장 등)

(4) 우리나라 개인정보보호법의 현황

- ① 개인정보 자동처리에 대한 규율이 없음
 - 개인정보의 자동화된 처리와 관련한 정보주체의 권한이 충분히 보장되지 못함
 - 자동처리에 대한 거부권이 보장되지 않음
 - 자동처리에 대한 제한이 없음
- ② 프로파일링에 대한 정보주체의 권리가 미약함
 - 프로파일링과 관련한 개인정보 주체의 통제권 미약.
 - 정확한 고지가 되어 있지 못함.

(5) 현행 개인정보보호법에 대한 두 가지 입장

- ① 옵트 아웃화론 - 개인정보 정의 규정 완화론(방송통신위원회
- 빅데이터 가이드라인)

- 개인정보의 개념을 대폭 축소하고 대신 고지의무와 처리 거부권 신설하여 옵트 아웃화하자는 견해(2012, 최경진, 정준현, 지성우, 구태언)
- 현재 "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)로 정의.
- 괄호 부분을 삭제하자는 견해
- 단독으로 식별가능한 정보가 아닌 다른 정보와 결합하여 식별가능한 정보는 개인정보에서 제외해야 한다.
- 대신 프로파일링 처리 거부권 및 고지의무 신설. 이 경우 사실상 옵트 아웃화 됨.

② 개인정보 주체 권리보장 강화론

- 개인정보 주체의 프로파일링에 대한 거부권 규정이 없음
 - 개인정보 주체의 프로파일링에 대한 거부권 보장 필요
 - 자동화된 의사결정으로 인한 차별, 부당한 대우 가능성 높아짐.
- 개인정보 주체의 프로파일링에 대한 권한 미약
 - 개인정보 주체의 프로파일링 과정 전반에 대한 권한 보장 필요
 - 프로파일링에 대한 상세한 내용의 고지 의무 명확하게 할 필요
 - 개인정보 주체의 동의 및 선택권 보장
 - 데이터에 대한 이의권, 삭제, 정정, 처리 중단 요청권의 실효적 보장
- 개인정보 주체의 권리구제와 감독기능 강화
 - 개인정보 주체의 신속한 권리구제를 받을 권리 보장 및 감독기구의 권한 강화 필요

마. 구체적 사례

(1) SKT의 이동전화서비스 개인정보의 수집, 이용

• 수집하는 개인정보의 항목

- 식별정보 : 성명(법인명), 주민(법인등록번호), 여권번호, 외국인등록번호, 전화번호
- 연락처정보 : 주소, 전화번호, e-mail 주소
- 계좌정보 : 계좌(카드)번호, 예금주명 등
- 생성정보 : 발·수신번호(통화상대방번호 포함), 통화시각, 사용도수, 서비스이용기록, 접속로그, 쿠키, 접속 IP 정보, 결제기록, 이용정지기록, 멤버십 정보(멤버십 가입고객에 한함), 기타 요금 과금에 필요한 데이터 및 이를 조합하여 생성되는 정보(요약개인정보, 데이터마이닝 분석 및 고객세분화 정보, 선호도, 라이프스타일, 사회적 관계 추정 정보), Application 사용관련정보(사용 App.정보, 사용량 등) : 발·수신번호, 통화시각, 사용도수, 위치정보(기지국위치, GPS정보), 서비스 이용기록, 접속로그, 쿠키, 접속IP정보, 결제기록, 이용정지 기록 등 : 서비스 이용의 요금정산 및 위치기반 서비스, 개인맞춤 서비스 제공
- 기타 서비스 제공 관련 필요 정보 : 2.에 따른 개인위치정보, 단말기 정보(모델, IMEI번호, USIM번호, 단말기 S/W버전 정보 등), 직업, 국가유공자 증명·복지할인 증명 등 각종 증명, 부가서비스·번호이동·할부매매계약 내역, 이동전화 서비스 가입 및 해지일·이동전화 가입 기간 등
※ 위 정보는 가입 당시 정보뿐만 아니라 정보 수정으로 변경된 정보를 포함합니다.

• 개인정보의 보유·이용기간

- 서비스 계약 해지 시까지(단, 여러 서비스에 가입한 경우 일부 서비스에 대하여만 해지하는 경우는 제외)

(2) 네이버의 웹서비스와 수집하는 정보

NAVER 전체보기

카테고리순 가나다순 쉽게 찾고 싶으실 때는 C키+또는 오른쪽 상단 이용하세요 예) 사전 검색

검색/백과 네이버캐스트 지식백과 인물관련 전문정보(학술) 뉴스라이브리리 검색등록 네이버SE 사이트 네이버트렌드	어학사전 > 영어/영영사전 일본어/번역 한자사전 중국어사전 국어사전 글로발화화 베트남어사전 프랑스어사전 안나어사전 몽골어사전 독일어사전 스페인어사전 러시아어사전 터키어사전	커뮤니티 지식인 블로그 카페 미투데이 오픈캐스트	뉴스/스포츠 스포츠 프로야구 뉴스 오늘의 신문 뉴스스탠드	금융/생활 부동산 증권/금융 가계부 --- 날씨 지도 교통 --- 자동저장 라이프키친 건강 라이프윌스폰 라이프머거진 라이프윌버스	문화/오락 게임 웹툰/만화 뮤직 영화 책 포토갤러리 TV캐스트 웹소설 N스토어/내서재
내서비스 메일 N드라이브 캘린더 메모 주소록 북마크 포토앨범 네이버me 쪽지 --- 마일리지 캐쉬	쇼핑 지식쇼핑 킷키투데이 체크아웃 샵N	주니어 > 동요세상 유아세상 보로로 놀이교실 TV만화 게임랜드	실치형 돌바 플리너 백신 캡처 포토뷰어 미디어플레이어 나눔글꼴 소프트웨어(자료실)	기능/도구 QR코드 단축URL 오픈스 문자메세지	모바일 > 네이버앱 핸드 지도 N드라이브 캘린더 뮤직 카메라 주소록 도돌잡
개발자센터 > 네이버맵 오픈소스 오픈API 오픈프로젝트	나눔센터 해피빈 파프너센터	네이버이야기 다이어리 스토리 인사이드 NAVER스토어	고객센터 아이디찾기 비밀번호찾기 회원정보변경 회원탈퇴 신고합니다. E-mail문의 요금관련문의 전화상담ARS안내 운영시간 (평일) 09:00 - 18:00	네이버비즈니스 키워드광고 지역정보샵 네이버쇼핑입찰 크로스미디어 디스플레이광고	

- 개인, 커뮤니티

- √ 블로그/ 카페/ 지식인/ 미투데이/ 오픈캐스트
- √ 개인, 단체의 관계, 활동 내용

- 내서비스

- √ 메일/ 캘린더/ 메모/ 주소록/ 북마크/ 쪽지/ N드라이브/ 마일리지/ 캐쉬
- √ 개인의 성향, 사회적 관계, 활동 내역

- 시사
 - √ 뉴스 댓글
 - √ 개인의 성향(정치, 경제, 사회, 문화), 사상, 의견
- 검색
 - √ 뉴스검색, 사이트 검색, 인물검색
 - √ 개인의 성향, 활동 내역
- 쇼핑
 - √ 지식쇼핑/ 체크아웃 / N샵(오픈마켓)
 - √ 개인의 소비성향, 기호, 소비활동
- 금융/ 경제
 - √ 부동산/ 증권, 금융/ 가계부
 - √ 개인의 경제활동
- 문화/ 오락
 - √ 게임, 만화, 음악, 영화, 책, 사진, TV, 서재
- 생활
 - √ 날씨/ 지도/ 교통
 - √ 개인의 이동정보
- 어린이
 - √ 동요/ 만화/ 놀이/ 게임
 - √ 어린이의 성향, 해당 가정의 자녀에 대한 정보

(3) 네이버의 개인정보 취급방침

- 수집하는 개인정보의 항목 및 수집방법
 - 서비스 이용과정이나 사업처리 과정에서 아래와 같은 정보들이 자동으로 생성되어 수집될 수 있습니다.

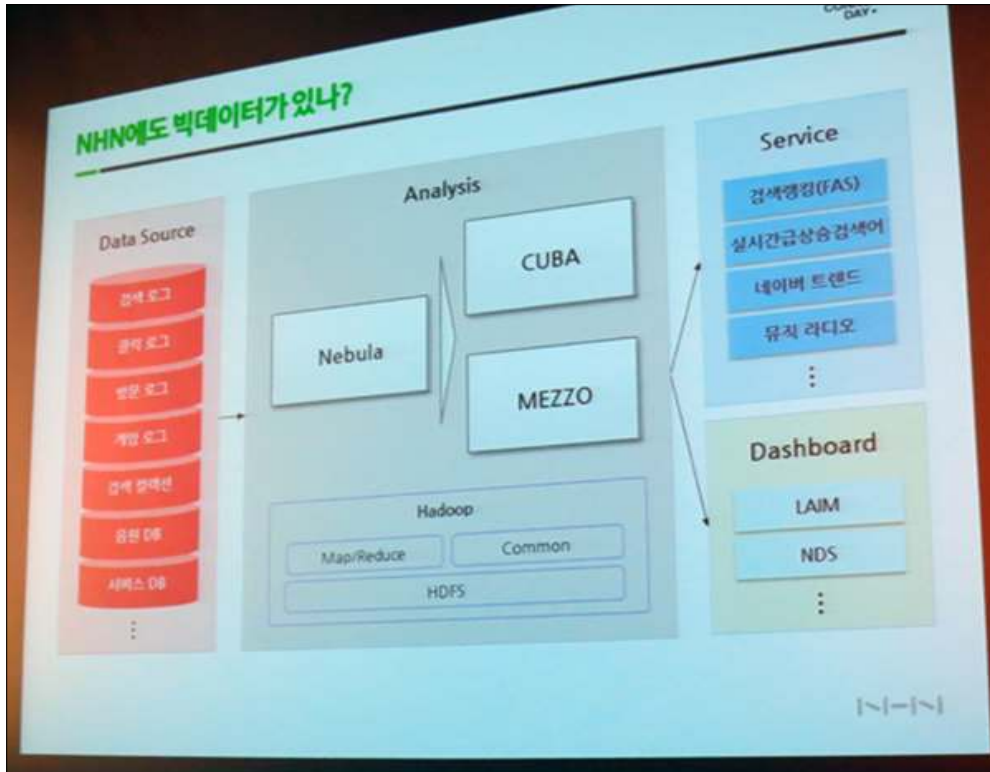
- IP Address, 쿠키, 방문 일시, 서비스 이용 기록, 접속로그, 불량 이용 기록, 결제기록
- 콘텐츠 제공, 특정 맞춤 서비스 제공
- 신규 서비스 개발 및 마케팅·광고에의 활용
 - 신규 서비스 개발 및 맞춤 서비스 제공, 통계학적 특성에 따른 서비스 제공 및 광고 게재, 서비스의 유효성 확인, 이벤트 정보 및 참여기회 제공, 광고성 정보 제공, 접속빈도 파악, 회원의 서비스이용에 대한 통계
- 회사의 쿠키 사용 목적
 - 이용자들이 방문한 네이버의 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부, 뉴스편집, 이용자 규모 등을 파악하여 이용자에게 광고를 포함한 최적화된 맞춤형 정보를 제공하기 위해 사용합니다.
 - 회사는 개인화되고 맞춤화된 서비스를 제공하기 위해서 이용자의 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다.

(4) NHN의 로그 데이터 저장(2012. 12. NHN 커넥트 데이)

- NHN은 2006년부터 모든 로그 데이터를 저장. 로그 데이터 중 필요한 정보만 빼내 저장하는 대신 이미지를 스캔하듯, 전체 로그를 스캔해 저장.
- 시작은 검색 로그, 클릭 로그, 방문 로그, 게임 로그, 검색 컬렉션, 음원 DB, 서비스 DB로 확장.
- 1일 발생하는 로그 데이터는 3TB

(5) 네이버 IDC 센터 '각'

- 10년간 네이버 서비스로 만들어진 데이터는 약 180페타바이트(PB)
- N드라이브에 하루 올라오는 데이터 400테라바이트(TB)



[NHN 미디어 데이 발표 프레젠테이션]



[NHN 데이터 센터 각]

(6) 네이버 개인정보의 프로파일링의 문제점

- 정보들의 결합시 개인에 대한 정보의 범위가 무한대로 확장됨
 - 각 분야의 정보는 결합을 전제로 하지 않은 것이었음.
 - 각 분야의 정보가 식별자를 매개로 결합될 경우 매우 민감하고 치명적인 정보가 됨.
- 부정확한 정보. 오해와 편견 야기할 정보 포함.
 - 결합, 평가의 대상으로 될 것을 전제하는 정보가 아닌 것이 많음.
 - 프로파일링의 대상이 되는 정보, 프로파일링의 결과, 목적을 모르는 경우 더 큰 문제.
- 익명성을 기대한 정보가 개인이 식별됨
 - 익명정보가 개인식별이 될 매개가 많음(휴대전화, IP, 이메일 주소 등)

(7) 네이버 개인정보 프로파일링과 관련한 개인정보 취급방침의 문제점

- 수집하는 정보의 범위 포괄적
 - 서비스 이용 내역(IP Address, 쿠키, 방문 일시, 서비스 이용 기록, 접속로그, 불량 이용 기록, 결제기록)을 수집한다고만 규정함
 - 구체적으로 어떤 정보를 어떻게 수집하는지 불명확함
- 정보수집의 목적과 활용범위 포괄적
 - “특정 맞춤형 서비스 제공, 신규 서비스 개발 및 마케팅·광고에의 활용”
 - “신규 서비스 개발 및 맞춤형 서비스 제공, 통계학적 특성에 따른 서비스 제공 및 광고 게재, 서비스의 유효성 확인, 이벤트 정보 및 참여기회 제공, 광고성 정보 제공, 접속빈도 파악, 회원의 서비스이용에 대한 통계”
 - “이용자들이 방문한 네이버의 각 서비스와 웹 사이트들에

대한 방문 및 이용형태, 인기 검색어, 보안접속 여부, 뉴스편집, 이용자 규모 등을 파악하여 이용자에게 광고를 포함한 최적화된 맞춤형 정보를 제공하기 위해 사용”

- “회사는 개인화되고 맞춤화된 서비스를 제공하기 위해서 이용자의 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용”
- 맞춤 서비스, 최적화된 맞춤형 정보, 광고의 의미가 지나치게 포괄적
- 익명성 보장도 안됨.
- 구체적인 프로파일링의 내용, 방식 등을 고지하지 않음.
 - 현재는 거의 모든 정보를 수집하여 맞춤형 서비스, 맞춤형 광고를 제공하기 위해 사용할 수 있는 것으로 규정함.
 - 어떤 정보를 어떻게 분석, 결합하여 어떻게 사용하는지를 밝히지 않음.

바. SKT와 NHN의 빅데이터 협력

- 2012. 11. 19. NHN-SKT, 미래 사업 발굴 위한 제휴 협약 체결
- 빅 데이터 사업 육성 협력
 - 양사는 공동 프로젝트 그룹을 구성, 빅데이터 전문 인력과 기술을 상호 교류함으로써 각 산업분야에서 단편적으로 활용되던 데이터 분석/활용 경험과 기술을 융합하고, 기존 인프라 시스템을 강화하여 빅데이터 비즈니스 성공사례를 만들어 갈 계획이다
- 양사 서비스 결합을 통한 신규 서비스 개발 협력
 - SK텔레콤의 스마트 네트워크 인프라와 NHN의 다년간 서비스 운영 노하우 결합을 통한 신규 서비스 개발 및 글로벌 진출 기회도 공동으로 모색한다.

- 양사가 보유한 데이터에 새로운 접근방법을 적용, 경영 혁신 방안을 도출함으로써 고객 니즈에 기반한 새로운 서비스 제공을 위해 협력하고, 맞춤형 서비스와 마케팅을 통한 효율성 증대도 이끌어낼 계획이다
- 소상공인 창업 지원 등 협력
 - 다양한 사회 공헌 방안을 강구, 개인 및 기업고객, 공공분야 등 사회 전반으로 양사 제휴 협력의 효용을 확대해 나갈 예정이다.
 - 가령 SK텔레콤의 상권분석 서비스와 네이버 지역정보 서비스를 결합, 소상공인의 창업 활동을 지원하는 방안 등이 검토될 예정이다

03

의견진술

임종인 고려대학교 정보보호대학원 원장

의견진술

임종인 고려대학교 정보보호대학원 원장

개인정보 유출 2차 피해 방지방안

□ 개요

- 개인정보 유출 2차 피해 방지를 위해서는 대포통장과 대포폰 근절을 통한 2차 범죄의 조건의 형성을 막고, 많은 2차 범죄(보이스피싱, 스미싱, 스캠, 소액결제)의 통로가 되고 있는 전화번호의 변작행위를 탐지하고 중단시킬 수 있어야 함
- 또한 기업들은 2차 피해를 막기 위해 유출 시 개인정보를 신속하고 편리하게 변경할 수 있도록 온·오프라인에서의 정보변경조치들을 갖출 것이 요구되며, 변경이 불가능한 주민등록번호체계 또한 변경 가능한 난수로 구성되는 번호체계으로 근본적으로 바꾸는 방안을 고려할 필요가 있음
- 침해사고 발생을 적시에 발견하여 2차 피해 최소화를 위해 신속하고 적절히 대응할 수 있도록 보장하기 위해 기업에 침해사고 발생을 모니터링하고 관련 증거를 확보할 수 있도록 하는 포렌식 준비도 제도를 도입하는 방안이 모색되어야 함
- 마지막으로 1차 범죄와 2차 범죄의 주요 발생지인 중국과의 협력을 실제적으로 이끌어내어 2차 범죄를 최소화하기 위한 지속적인 노력이 병행되어야 함

- 2차 범죄 피해를 막기 위한 근본적인 방안은 당연히 1차 범죄가 발생하지 않도록 하는 것임. 우선 법적 규제 강화와 동시에 단순한 규제준수가 아니라 타 기업과의 정보보호 수준경쟁을 통해 모든 기업의 보안이 상승을 유도할 수 있는 보안등급 공시제도 도입이 고려되어야 함
- 주민등록번호와 같은 민감 데이터의 경우 별도 시스템에 암호화 저장하고 필요할 때만 가장 안전한 조건에서 접근할 수 있도록 하고, 위탁업체 직원을 수탁업체 직원으로 의제함으로써 위탁업체 관리 책임을 강화하도록 하는 등 기업의 기술적·관리적 보호조치를 강화해야 함
- 유출 기업에 개인정보보호 강화를 위한 경각심을 부여하고 피해자들에 대한 실질적인 구제를 위해 법정 손해보상 제도를 도입하거나 고의나 중과실의 경우 징벌적 손해배상 제도를 도입하는 방안을 검토할 필요가 있음. 또한 일정 수준 이상의 개인정보를 보유한 기업의 경우 개인정보유출 손해보험 의무화를 통해 보안을 강화하는 동시에 피해 회원들의 실질적인 구제를 보장하는 방안을 고려해야 함

□ 2차 피해 방지 방안

1. 2차 범죄 조건 형성 방지 : 대포통장, 대포폰 금지

- 2차 범죄 피해를 막기 위해서는 2차 범죄가 용이하게 이루어질 수 있는 조건 형성 자체를 막아야 함. 이를 위해 근본적으로 대포통장과 대포폰을 금지해야 함
- 대포폰을 근절하기 위해서는 우선 전화 개통 시 본인여부를 확인하도록 하고, 휴대전화를 타인에게 넘겨줄 시 넘겨받을 실제 사용자를 신고하고,

이 때 실제 사용자에게 대한 본인여부 확인을 의무적으로 하게끔 할 필요가 있음. 또한 대포폰 알선, 중개, 권유 광고행위를 금지해야 함. 이미 이우현 의원안(2012.12.17.), 강기정 의원안(2012.8.8.)에도 대포폰 금지를 위한 본인확인 요건을 포함하고 있음

2. 2차 범죄 행위 검출 및 중단 : 전화번호 변작 금지

- 대부분의 2차 범죄들(보이스 피싱, 스미싱, 스팸, 휴대폰 소액결제)이 변작된 전화번호를 통해 이루어지므로, VoIP나 인터넷 문자발송을 통해 변작된 전화번호를 이용한 서비스를 검출하고 전송을 중단시키거나 원래의 전화번호를 표시함으로써 국민들의 피해를 막아야 함
- 이미 김희정 의원안(2012.9.5.), 정부안(2012.9.24.), 조해진 의원안(2012.9.10.)을 포함한 많은 법안에서 기간통신사업자의 의무로 변작 전화번호를 검출하고 차단하거나 원래 번호를 송출할 수 있는 기술적·관리적 조치를 의무화하고 있으며, 수사기관이나 당국 요청 시 범죄목적의 발신번호를 차단할 것을 의무화하고 있음. 또한 정부안(2012.9.24.)에서는 실제 국외번호로 왔을 경우 국외번호임을 수신자가 알 수 있도록 표시할 것을 요구하고 있음
- 이상일 의원안(2013.11.1.)은 스미싱 방지를 위해 인터넷 문자 발송 서비스 업체를 신고제가 아닌 등록제로 하고, 등록의 요건으로 발신번호 변작 방지를 위한 기술적 조치를 두고 있으며, 이연주 의원안(2012.6.15.)도 발신번호 변작 방지를 위한 기술적 조치를 의무화하고 있음

3. 유출 개인정보 무력화 : 개인정보 변경 지원

- 2차 범죄로 인한 피해를 최소화하기 위한 또하나의 방안은 유출된 개인정보의 가치를 하락시키거나 무력화시킴으로써 범죄에 사용되지 않도록 하는 것임
- 아이디나 패스워드, 계좌번호, 비밀번호, 카드번호 등 변경 가능한 데이터들은 신속히 변경하거나 해지함으로써 2차 범죄를 막아야 함
- 기업들은 유출발생 시 신속하게 사고사실과 피해사실을 고지하는 한편, 이러한 변경이 신속하고 편리하게 이루어질 수 있도록 역량과 관련 인터페이스를 사전에 갖추고 있도록 요구될 필요가 있음
- 카드 재발급과 같이 오프라인에서의 변경과 재발급이 요구되는 경우를 대비하여 유출피해자들이 유출피해로 인해 불편함과 고통을 느끼지 않도록 신속하고 추가적인 비용 발생 없이 편리한 재발급 업무가 이루어질 수 있는 역량과 절차를 갖출 것(재발급 카드 생산 및 처리 능력 확충 등)을 의무화할 필요가 있음

4. 주민등록번호 체계 개선 : 재발급 가능 난수형 주민번호

- 유출된 개인정보 중 재발급과 변경이 가능한 경우 2차적인 피해를 막기가 용이하지만, 주민등록번호처럼 변경이 불가능한 번호의 경우 2차 피해를 근본적으로 막기 어려운 상황임
- 따라서 주민등록번호의 사회적 활용도와 중요성을 감안하여 주민등록번호 체계를 개인정보 유출 피해자 요청 시 변경이 가능한 재발급 가능한 난수형 주민번호 체계로 근본적으로 전환할 필요가 있음

- 인구 증가량과 재발급 등을 고려하여 주민번호는 13자리의 난수로 발급되고, 재발급 요청 시에는 다른 번호와 충돌하지 않는 새로운 13자리 난수 번호를 부여받게 됨
- 무제한 재발급이 아닌 제한적 재발급으로, 재발급 제한 요건 등은 명확히 할 필요가 있음 (유출 피해 증명, 평생 재발급 건수 제한, 1년 재발급 건수 제한 등)
- 번호만으로 나이 성별 출신지역 등을 식별할 수 있는 기존 주민번호와는 달리 매번 임의의 난수를 주민번호로 부여하면 추가적인 개인정보 노출도 막을 수 있음
- 이러한 새로운 주민번호 제도의 도입과 관계없이 주민번호 수집 및 이용 최소화 원칙은 더 강력히 적용되어야 함

5. 포렌식 준비도 제도(Forensic Readiness) 도입

- 최재천 의원안(2013.8.21.)은 개인정보유출사고 발생 시 24시간 이내에 신고하도록 요구하고 있지만, 대부분 사고 발생 이후 상당 기간이 지난 후에야 사고 사실을 인지하게 되는 경우가 많아 법안의 현실성이 의심됨
- 많은 경우 사고 발생 시점이 한참 지난 이후 사고 발생 사실을 인지하게 되므로 유출 사고 이후 관련 증거가 훼손되거나 2차적 피해에 적시에 대응하지 못할 가능성이 높아짐. 즉, 2차적 피해는 사고발생 시점과 사고발견 시점 사이의 간격이 클수록 발생 가능성이 높으므로, 이 간격을 줄이기 위한 정책이 수립되어야 함
- 사이버 침해사고에서 확보된 증거가 많을수록 원인과 피해상황에 대해 정확하게 파악할 수 있어 적절한 2차적 피해 대응이 가능해지기 때문에 관련 증거를 훼손시키지 않고 적시에 더 많이 확보하는 것이 중요함

- 사고 발견이 아닌 사고 발생 이후 24시간 이내에 신고가 되기 위해서는 기업 내에 포렌식 관련 정책과 절차, 장비들이 갖춰져 있고, 일상적인 모니터링과 증거수집이 이루어져야 가능하므로, 24시간 고지제도 이전에 각 기업에 포렌식 준비도 마련을 요구하는 것이 더 현실적으로 보임
- 포렌식 준비도(Forensic Readiness) 제도란 상시적으로 사이버 사고 발생 여부를 탐지하고, 발생 시 증거를 수집하고 분석할 수 있는 정책을 수립하고 절차와 체계를 갖출 것을 의무화하는 제도를 말함
- 기업들에게 정보보호침해사고에 대한 증거들을 수집, 보존하게 하고, 정기적인 분석을 의무화하도록 하고, 포렌식 준비도를 갖추지 못했거나 사고를 적시에 발견하지 못했을 경우 책임을 지도록 할 필요가 있음
- 정통방법의 기술적, 관리적 보호조치의 요건 중의 하나로 포함시킬 필요가 있음

6. 중국과의 사이버분야 외교적 · 사법적 협력 강화

- 금융정보를 포함한 대한민국 전 국민의 개인정보를 이미 중국 해커들이 다 갖고 있다고 알려져 있고, 피싱 등 범죄적 목적으로 활용되어 실제 2차적 피해로 이어지고 있는 상황에서 국내 대응조치 강화만으로는 충분하지 못함
- 일단 중국으로 개인정보가 넘어간 경우 현재는 중국 측의 비협조로 2차, 3차 유출 경로를 찾기도 어렵고 2차 피해를 막기도 쉽지 않은 상황임
- 중국 내 대한민국 국민 개인정보 유통에 대한 금지 조치와 대한민국을 상대로 한 중국발 해킹과 2차 사이버범죄 발생 시 수사협조 및 사법공조와 관련된 중국과의 구체적인 협력 방안을 마련하기 위한 외교적 노력이

수반되어야 하며, 법률을 통해 특정 부처나 기관에 지속적인 노력을 보장하기 위해 명확한 임무를 부여할 필요가 있음

- 추가적으로, 휴대전화, 컴퓨터 중고품을 중국 등 해외 유통하는 사업자들에게 시스템 내의 데이터를 완전히 초기화할 것을 의무화하는 방안을 검토할 필요가 있음

□ 근본적 해결책 : 1차 피해 방지 방안

1. 보안등급 공시제 도입 : 보안 규제 패러다임 전환

- 기업 보안 강화는 법적 규제 강화를 통해 기본적인 베이스라인 보안 수준을 보장하는 동시에 보안등급 공시제를 통해 금융사간 정보보호 경쟁 시장을 형성함으로써 기업들이 자발적으로 더 높은 수준의 창조적인 보안 노력을 기울일 수 있도록 하는 방향으로 패러다임을 전환해야 함
- 보안등급 공시제는 기업의 보안수준을 투명하게 공시해 소비자들과 투자자들의 기업 선택 시 필요한 객관적인 기준을 제공해 선의의 보안경쟁을 이끌어낼 수 있을 제도임
- 예를 들어 A+부터 D까지 10단계의 등급을 만들어서 기업별로 등급을 매기고 해당 기업이 채택하고 있는 주요 보안 조치들에 대해 국민들에게 공시하고, 각 기업들 간에 A+를 받기 위한 정보보호 경쟁이 이루어지도록 해야 함

2. 법적 규제 강화와 보안감사 강화

- 기업들에 필수적인 보안 통제(데이터 암호화 등 기술적 보호조치, 아웃소싱 업체 관리 등 관리적 보호조치)들에 대한 법적 요구조건과 유출 사건 발생 시 기업과 CEO의 법적 책임을 강화함으로써 기업의 베이스라인 보안수준을 보장하는 한편, 정보보호 경쟁 조건을 형성해야 함
- 보안등급 공시제 도입 시, 부정공시행위에 대한 엄격한 법적 책임을 부여함으로써 제도의 효과성을 보장해야 함. 또한 일정 등급 이하의 기업에게는 페널티를 줌으로써 일정 등급 이상으로 유지될 수 있도록 해야 함
- 당국은 법률과 지침에 따른 각 업체의 준수여부와 함께 등급부여 과정과 공시된 내용에 대한 부정공시 여부에 대한 감사를 수행해야 함

3. 민감 데이터의 별도 시스템 암호화 저장 및 보안강화 의무화

- 보관된 개인정보 중 주민등록번호 등 특히 민감한 데이터의 경우 다른 데이터들과 별도의 시스템에 암호화하여 저장하고, Key 값으로 사용하지 않고 필요시에만(주민등록번호의 경우 본인확인 시) 다른 데이터들과 결합하여 사용할 수 있도록 해야 함
- 민감 정보가 저장된 시스템에 대해서는 특정한 자리에서 CCTV촬영 및 입회자 참여하에서만 접근하도록 내부통제를 하는 등 높은 수준의 보안이 제공되어야 함

4. 위탁업체 관리 강화 의무화

- 위탁업체에 대한 관리소홀과 내부통제 부재로 인해 위탁업체 직원에 의해 개인정보 대량 유출이 발생하는 경우가 많이 발생하고 있는 상황임

로, 위탁업체에게 위탁업체 관리를 강화하도록 의무화하는 한편, 관리 실패로 인한 엄격한 책임을 물어야 함

- 이를 위해 위탁업체 직원에 의한 개인정보 유출 시 위탁업체 직원을 수탁 업체 직원으로 의제, 직원 관리 책임 소홀에 따른 책임과 동등한 수준으로 책임을 부여하는 방안을 고려할 필요가 있음

5. 유출기업 책임 요건 및 처벌 강화

- 개인정보 유출사고가 발생해도 아무도 책임지지 않아 유출피해자들만 고통에 방치되는 상황이 빈번해지면서 실질적인 피해자 구제를 위한 법정 손해배상 제도 도입을 고려해볼 필요가 있음. 이미 권은희 의원안(2014.2.3.), 최민희 의원안(2012.8.22.)에서도 제안된 바 있음
- 특히 기업의 고의 혹은 중대과실에 의해 개인정보가 유출된 경우 징벌적 손해배상을 하도록 하는 징벌적 손해배상제도를 도입하는 방안 또한 고려되어야 함. 권은희 의원안(2014.2.3.)에서는 과징금에 대해서만 중대과실의 경우 과징금의 1/2 범위에서 가산이 가능하다고 하고 있음. 피해자들의 구제를 강화하고 기업들에게 억지력을 높이기 위해서는 과징금만이 아닌 손해배상에서 징벌적인 배상이 가능하도록 하는 방안을 고려해야 함
- 정통방법에 존재하는 기업의 면책규정이 법정에서 기업을 방어하기 위한 주요 수단으로 사용되고 있고, 기업간의 보안 경쟁과 혁신이 이루어질 수 있는 환경을 형성하기 어려운 상황임. 따라서 기업의 면책규정을 삭제하거나 엄격한 조건을 통해 과도한 해석을 하지 못하도록 제한할 필요가 있음. 이미 최민희 의원안(2012.8.22.)에서도 제안된 바 있음

6. 개인정보유출손해보험 의무화

- 일정 규모 이상의 개인정보를 보유하고 있는 기업에게 개인정보유출사고 시 손해보험 가입을 의무화하는 방안을 고려해야 함. 개인정보유출사고 발생 시 사회적인 비용을 최소화하고 실질적인 피해자 구제가 보장될 수 있도록 해야 함
- 보유하고 있는 개인정보의 양과 개인정보보호 수준과 관행에 따라 보험금이 결정될 수 있으므로, 기업들은 보험금을 낮추기 위해 개인정보 수집을 자제하고, 보안 강화를 위한 노력이 강화될 것으로 기대되며, 보안등급 공시제와 함께 기업의 보안강화 노력의 활성화를 가져올 수 있을 것임

□ 결 론

- 위의 2차 피해 방지 및 최소화 방안들과 함께 1차 피해 자체를 근본적으로 방지하고 최소화할 수 있는 방안들이 균형 있게 강화되어야 중장기적으로 실질적인 2차 피해 방지 효과가 달성될 수 있을 것임. 현재 나와있는 법안들은 2차 피해 방지를 위한 단기적인 조치들에 집중해 있음
- 기존의 대한민국 개인정보보호 패러다임이 비효과적이었다는 사실이 이미 다양한 결과들과 국민들의 비판을 통해 드러나고 있는 상황이므로, 보안등급공시제나 가변적 주민등록번호, 징벌적 손해배상제도, 포렌식준비도제도와 같은 새로운 패러다임으로의 전환을 고려해볼 조건이 충분히 형성되었다고 판단됨

04

의견진술

장 여 경 진보네트워크센터 정책활동가

의견진술

장 여 경 진보네트워크센터 정책활동가

최근 카드사태와 관련한 미방위 소관 법률 개정안 검토와 2차 피해 방지 대책에 대한 입장 - 개인정보 보호에서 정보인권으로 -

1. 입법안 평가

(1) 전기통신사업법 개정안 (9건), 이동통신기기 부정이용 방지법안(1건)

□ 그 구체적인 내용은 다음과 같음

- 보이스피싱 예방 등을 위한 발신번호 변작 방지 의무화
- 스피밍, 스팸 방지를 위한 인터넷발송 문자서비스 규제 강화
- 대출사기 등 불법행위에 사용된 전화번호 이용 정지
- 명의도용 등의 부정이용 방지를 위한 본인확인 및 시스템 구축

□ 기술적 조치 의무화로 전기통신사업자에 특정한 기술적 기준을 법률로 강제하는 제도는 신중히 도입할 필요가 있음. 해당 제도가 기술 발달 속도를 충분히 따라잡는 실효성을 갖출 수 있을지 의문스럽고, 법정 기술적 조치에 대한 최소 준수가 전기통신사업자의 면책 사유로 인정된다면 추후 개인정보 유출에 대한 이용자 손해배상이 어려워질 수도 있음. 특히 정보통신망 기간사업자가 불법정보 내용탐지 등을 이유로 DPI(Deep Packet Inspection) 등

의 기술적 조치를 도입한다면 이용자 통신의 비밀에 중대한 위협을 초래할 수도 있음

- 전화번호 변작을 일반적으로 금지할 경우 글로벌한 VoIP 서비스 시대에 이용자 권리를 침해할 우려도 있음. 현재는 “인터넷은 전 세계를 망라하는 거대한 컴퓨터 통신망의 집합체로서 개방성이 그 주요한 특징으로 하므로 외국의 보편적 규제와 동떨어진 우리 법상의 규제는 손쉽게 회피될 수 있고, 그 결과 우리 법상의 규제가 의도하는 공익의 달성은 단지 허울 좋은 명분에 그치게 될 수 있음”을 경고한 바 있음(2012. 8. 23. 2010헌마47·252(병합)).
- 한편 방송통신위원회가 다른 법률에 따라 권한이 있는 행정기관의 요청이 있거나 범죄행위에 이용되고 있다는 수사기관의 요청이 있는 경우 특정 전화번호 회선이나 해당 이용자에 대한 전기통신 역무 제공의 중지를 명할 수 있도록 하는 경우는 이용자의 이용권 자체를 박탈한다는 점에서 헌법상 기본권인 표현의 자유, 통신의 자유 침해로 이어질 수 있음. 현재는 해당표현물의 삭제 외에 이용자의 통신망 이용권 자체를 정지 또는 금지시킬 수 있도록 한 (구)불온통신의 단속 조항에 대하여 과잉금지원칙에 위반된다고 설시한 바 있음(2002. 6. 27. 99헌마480 전원재판부).
- 무엇보다 부정이용 방지를 명목으로 본인확인 시스템을 확대하는 것은 실효성을 담보할 수 없는 반면 정보인권 침해를 야기할 가능성이 매우 높음. 우선 휴대전화 개통시 본인을 확인하도록 강제하면 일부 사기 수법에 대해서 제한하는 효과가 있을지 모르지만, 휴대전화를 매개로 한 대부업, 결제대행, 채권추심업무가 중단되지 않는 한 수없이 많은 변종의 사기 수법(급전이 필요한 노숙인이나 채무자 본인이 개통토록 하는 등)이 등장할 수 밖에 없음. 휴대전화를 이용한 사기수법 중에는 이용자의 개인정보를 이용하는 경우도 많아, 이용자 보호를 위하여서는 오히려 휴대전화 개통

시 본인정보를 연동하는 관행을 재고해야 할 필요성이 증가하고 있음.

- 또한 주민번호를 이용한 본인확인 시스템 확대는 특정 본인확인 업체(현재 신용정보업체 3개, 공인인증발급기관 5개, 이동통신 3사)에 주민번호와 성명 등 본인확인 정보를 국가정책적으로 집중시키고 영리적 이용을 예외적으로 허용함으로써 대규모 개인정보 오남용과 유출 위험을 조장할 위험이 매우 큼. 이동통신사업자 역시 내외부자를 통한 개인정보 유출 사고에서 자유롭지 않았으며 (2012년 KT와 SK텔레콤의 협력업체 직원이 19만건의 휴대전화 가입자 정보를 홍신소 등에 유출 / KT에서 870만명의 고객정보 유출) 이번 카드사 정보유출의 범인이 본인확인기관인 코리아크레딧뷰로 직원으로 밝혀지는 등 본인확인기관 또한 개인정보 집중과 그로 인한 유출에서 자유롭지 못한 상황이라는 점을 엄중 경고하고자 함

현재 주로 쓰이고 있는 본인확인방법은 본인확인서비스를 제공하는 제3자인 신용정보회사를 통하여 이용자의 이름, 주민등록번호, 휴대폰, 신용카드 등의 정보를 이용하여 게시판 이용자가 본인인지 여부를 확인하는 것이다 (...) 본인확인제에 의하더라도 가해자가 주민등록번호와 명의를 도용하는 경우에는 가해자를 특정하기 어려움은 마찬가지이고, 위와 같은 가해자의 은폐시도에 따른 특정의 어려움은 통상의 불법행위에서도 발생하는 문제로서 일반적인 수사기법에 의하여 극복될 수 있다 (...) 나아가 현재 주로 이용되고 있는 신용정보회사에 의한 게시판 이용자의 이름, 주민등록번호 일치 여부를 확인하는 방법에 의한 본인확인, 주민등록번호를 부여받을 수 없는 외국인이나 주민등록번호가 없는 재외국민에 대하여 게시판에의 정보 게시를 봉쇄함으로써 그들의 표현의 자유를 사실상 박탈하는 결과에 이르고 있다. (2012. 8. 23. 2010헌마47·252(병합))

- 민간 영업을 위하여 행정정보 공동이용과 같은 국가정보 시스템을 이용한 본인확인을 의무화하는 것은 해당 개인정보의 목적 외 이용일 뿐 아니라 기본권을 과잉제한한다는 점에서 위헌적임
- 무엇보다 우리 개인정보보호법과 헌법에서는 익명 표현의 자유를 보장하고 있다는 사실을 상기할 필요가 있음. 휴대전화 명의 설정 역시 이용자의 사적 선택권의 문제임.

개인정보 보호법 제3조(개인정보 보호 원칙)

- ⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리 될 수 있도록 하여야 한다.

헌법 제21조 제1항에서 보장하고 있는 표현의 자유는 사상 또는 의견의 자유로운 표명(발표의 자유)과 그것을 전파할 자유(전달의 자유)를 의미하는 것으로서, 그러한 의사의 ‘자유로운’ 표명과 전파의 자유에는 자신의 신원을 누구에게도 밝히지 아니한 채 익명 또는 가명으로 자신의 사상이나 견해를 표명하고 전파할 익명표현의 자유도 포함된다 (...) 그런 측면에서 볼 때, 이 사건 본인확인제는 게시판 이용자가 게시판에 정보를 게시함에 있어 본인 확인을 위하여 자신의 정보를 게시판 운영자에게 밝히지 않을 수 없도록 함으로써 표현의 자유 중 게시판 이용자가 자신의 신원을 누구에게도 밝히지 아니한 채 익명으로 자신의 사상이나 견해를 표명하고 전파할 익명표현의 자유를 제한한다. (2012. 8. 23. 2010헌마47·252(병합))

(2) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정안(15건)

- 그 구체적인 내용은 다음과 같음
 - 통신과금서비스(휴대폰 소액결제) 이용자 권리보호
 - 개인정보 유출 방지 및 대응 의무 강화
 - 불법스팸 전송 규제 강화

- 통신과금 서비스와 정보통신서비스 이용에 있어 소비자의 동의권, 통지권 행사를 보완하고 개인정보 과기 등 개인정보 자기결정권을 보호하려는 조치들에는 일정한 의미가 있음.
- 그러나 기술적 조치 의무화에 대한 우려는 앞서 밝힌 바 대로임
- 개인정보 유출에 대한 손해배상의 경우 판례를 통해 그 대상과 정도가 정착해 가고 있으나, 사업자가 해당 이용자에 대한 유출 사실 통지 의무를 해태하거나 입증자료를 제공하지 않아 피해자가 피해사실 인지나 입증에 어려움을 겪는 경우가 있음. 이에 대한 제도 보완이 필요함.
- 현행법률이 이미 전화·모사전송기기에 영리목적의 광고성 정보를 전송하려는 자로 하여금 수신자의 사전 동의를 받도록 하였음에도 스팸 광고가 범람하는 이유는, 이미 휴대전화번호를 비롯한 방대한 양의 개인정보가 유출되어 불법적으로 사용되는 상황에서 기인한 측면이 큼. 그중 일부는 이용자로부터 ‘마케팅’ 목적으로 포괄동의를 받거나 사실상 강요하는 형식으로 동의를 득하여 합법적 외양을 갖추고 자사 혹은 위탁업체가 광고문자 전송을 하는 형태임. 이에 대해 정보주체가 실효성 있는 동의권 행사를 할 수 있도록 보장하는 조치가 필요함

2. 총평

(1) 정보인권 인식의 문제

- 아직도 개인정보 보호 문제가 ‘유출’에 국한되어 이해되는 경향이 많고, 심지어 ‘보안’ 기술의 적용과 동급으로 취급되고 있기도 한 것으로 보임. 그러나 개인정보 보호는 우선 우리 헌법재판소에서 실시한 개인정보 자기결정권의 보장 차원에서 이해될 필요가 있음

개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 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 (...) 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고 (...) 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치라고 할 수 있다. (2005. 5. 26. 99헌마513, 2004헌마190(병합))

- 결국 개인정보 보호란, 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 보장하는 차원에서 이해될 필요가 있음. 개인정보에 대한 정보주체의 결정권을 제약하는 정책은 원칙적으로 정보인권 침해로 볼 수 있음
- 개인정보 유출을 방지하기 위한 대책이 익명권 등 정보인권을 침해한다면 아이러니라 아니할 수 없음. 향후 대책에 있어 개인정보 보호 원칙과 정보인권을 반드시 고려해야 함

(2) 개인정보 보호 체계의 문제

□ 최근 카드사 대규모 개인정보 유출 사고에 비추어 입법안 전반적으로 그와 같은 사태를 예방할 수 있는 대책으로서 한계가 있음. 유사한 대책이 반복되어 왔음에도 어찌서 피해가 끊이지 않는지 근본적인 성찰이 필요할 때임. 중요한 검토 주제 중 하나로 감독 부처의 적절성을 들 수 있음

□ 박근혜 정부 출범 직후인 2013년 2 ~ 3월, 정보통신기술(ICT) 분야에서 개인정보 보호 주무부처와 관련한 갈등이 있었던 예를 상기할 필요가 있음. 새 정부의 정부조직 개편 원안(2013. 1. 22. 대통령직 인수위원회 발표)에서 ICT 진흥을 맡은 미래창조과학부가 개인정보 보호업무를 담당하도록 한 데서 본격적으로 불거진 이 논란은 결국 최종안에서 해당 기능이 방송통신위원회에 남게 되면서 마무리됨

관련하여 업계는 업무 효율성이 떨어지고 보안산업을 진흥해야 한다는 이유에서 뿐 아니라 빅데이터와 클라우드 등 개인정보를 활용해야 하는 미래 성장 산업의 장애물을 제거(전자신문 2013. 2. 27)하는 차원에서 개인정보 보호 업무의 미래부 이관을 지지하였음. 이에 반해 시민사회는 “한국소비자원의 통계에서도 볼 수 있듯이, 진흥과 규제를 함께하고 있는 금융과 통신 분야의 소비자피해가 가장 많이 발생하고 있다는 사실을 직시해야” 한다며 개인정보 보호 업무의 미래부 이관을 반대하였음. 국가인권위도 “개인정보보호감독기구의 독립성 및 기능을 강화해야한다는 의견”을 밝힘

이번에 1억 건이라는 사상 최대의 개인정보 유출사고를 금융권에서 미연에 방지하지 못한 원인 중 하나로 당국의 감독 부실이 지적되고 있다는 사실(SBS 2014. 1. 29)은 ICT 분야에 있어 개인정

보 보호 체계의 올바른 수립이 어떠한지 여부에 있어 큰 시사점을 던져 줌.

- 비록 미래부로 이관되지는 않았으나 개인정보 보호 업무를 방송통신위원회에서 수행하는 것에 대해서 원칙적인 검토가 필요할 때임. 인권시민단체들은 오랫동안 방통위와 행정안전부 등에 분산되어 있는 개인정보보호 업무를 개인정보보호위원회에 이관하고, 개인정보보호위원회의 역할과 권한을 강화하는 것이 개인정보보호를 위한 최선의 방안임을 주장해 왔음

원칙적으로 업종별 규제기관은 소관 행정부처와 관련 업계의 이해관계나 압력으로부터 자유롭지 못할 뿐 아니라, 방송통신위원회 역시 개인정보 보호를 업종의 이해관계 속에서 사고하는 한계를 노정해 옴. ‘빅데이터 산업 활성화’ 차원에서 현행 법률상 위임 범위를 넘어 이용자 동의권을 제한하는 내용의 빅데이터 가이드라인을 발표(2013. 12)한 것이 대표적임

유엔은 1990년 이미 “모든 국가들은 열거된 [개인정보보호] 원칙들의 준수를 감시할 독립된 기관을 설치해야만 하고 이러한 원칙들을 위반한 경우에 대비하는 처벌규정 및 개인보호규정들도 만들어야 한다”는 입장을 채택한 바 있음(개인정보 전산화 가이드라인). 따라서 정보통신망에서의 집행 기능 일부를 방통위가 담당하더라도 전문적이고 독립적인 국가 개인정보 보호 컨트롤타워로서 개인정보보호위원회를 강화할 필요가 있음

특히 2011년 개인정보보호법이 제정 시행된 후로는 규율 내용에 있어 정보통신망법과 중복되거나 모순되는 경우가 발생해 왔으며, 정보통신망법에 새로운 규정이 계속 추가되면서 혼란이 가중되고 있음. 이에 정보의 특수성을 고려한 항목에 대하여는 특별법적 논의를 검토하는 것이 합당하다 할지라도 그 외에는 일반법으로서

개인정보 보호법의 보충적 적용을 하는 방향으로 제도를 정비해 가는 것이 바람직하다는 의견을 청취할 필요가 있음.

- 정부 각 부처가 이기주의를 벗고 범정부적으로 국민의 개인정보를 보호하고자 최선을 다할 때 이미 전세계 인터넷에 유출되어 있는 개인정보로 유발될 수 있는 국민의 피해를 최소화할 수 있을 것임

(3) 주민번호의 원칙적 민간사용 금지

- 주민등록번호의 수집 및 이용은 원칙적으로 주민등록에 관한 사무에 국한해야 함. 그러나 정보통신망법은 주민등록번호의 사용 제한(제23조의2) 규정을 두어 왔음에도 “법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우”(제1항 제2호) 외에 “본인확인기관으로 지정받은 경우”(제1항 제1호)와 “방송통신위원회가 고시하는 경우”(제1항 제3호) 그 예외를 포괄적으로 인정해 왔음
- 인터넷 본인확인제에 대한 위헌 결정에도 불구하고 방송통신위원회가 본인확인기관이라는 기형적 산업을 육성하는 데 대한 국민적 불신과 외면이 계속되어 왔음. 이미 전세계 인터넷에 유포된 주민번호를 기초로 한 아이핀은 주민번호의 대안이 될 수 없음. 만능식별번호 체제를 유지하는 한, 전국민 주민번호 대규모 유출 사고와 유사한, 전국민 휴대전화번호, 전국민 아이핀 유출 사태를 피할 길이 없음. 우리사회에 필요한 대책은 주민번호와 같은 만능식별번호 체제를 벗어나 다른 나라처럼 원칙적으로 익명권을 존중하고 꼭 필요한 경우 목적별 번호를 도입하는 것으로 충분함.

05

의견진술

정 경 호 한국인터넷진흥원 본부장

의견진술

정 경 호 한국인터넷진흥원 본부장

개인정보 유출 피해 예방을 위한 입법 방향

□ 개 요

- 최근 대규모 개인정보 유출 사고로 국민 불안감이 증폭되고 스미싱, 스팸 등 2차 피해 발생이 우려
 - ※ 카드정보 유출 이후 사회적 관심사를 악용한 금융사 관련 스미싱이 일시적으로 증가(1월8일~2월4일 KISA는 금융사 사칭 스미싱 문자를 3,248건 탐지하여 대응)
- 이에, 국민을 대상으로 발생하는 사이버 금융사기 피해를 최소화하고, 개인정보 유출 사고를 예방하기 위해 제도적 보완 필요

□ 입법 추진 방향

- 현재 시행중인 스미싱, 보이스피싱 등 사이버 금융사기 대책은 주요 통신사 중심으로 시행하고 있어 근본적 피해 예방에 한계
 - 대책의 실효성을 높이고 중소 규모 통신사의 대책 이행을 담보하기 위해 통신사의 피해방지 조치를 법적으로 의무화

- 개인정보 유출 기업에 대한 처벌을 강화하여 기업 스스로 개인정보 보안을 강화도록 유도하고,
 - 피해를 입은 국민이 손해배상을 쉽게 받을 수 있도록 관련 제도 도입

- 근절되지 않는 불법 스팸 전송 규제를 강화할 수 있도록 악성스팸 전송자에 대한 형량 및 벌금을 높이고 심야시간대의 스팸 발송 제한

1. 보이스피싱 예방 등을 위한 발신번호 변작 방지 의무화

1. 문제점

- 발신번호를 조작해 수사기관이나 금융사를 사칭하는 보이스피싱 등에 의한 피해가 지속적으로 발생
 - 번호변작이 가능하기 때문에, 사칭을 막기 위한 대응방안 마련이 필요하나 법률 근거 부족

2. 제도상 미비점

- 현행 「전기통신사업법」은 영리나 위해를 목적으로 전화번호를 변작하거나 거짓으로 표시하는 것을 금지하고 있지만,
 - 변경 방지를 위해 필요한 조치의 주체가 명시되어 있지 않음
 - 변작하거나 거짓으로 표시한 발신인을 찾기 위해 필요한 정보를 요청할 수 있는 권한이 없음
- 범죄에 악용되는 것을 알면서도 발신번호 변작 서비스를 제공하는 사업자에 대한 억제력이 충분하지 못함

3. 개선방안

- 전기통신사업자의 기술적·관리적 조치 의무화
 - 전기통신사업자에게 거짓으로 표시된 전화번호의 차단 등 이용자의 피해 예방을 위한 조치 의무를 부과

- 미래부(인터넷진흥원에 위탁)에 자료제출 요구 등 권한 부여
 - 효율적인 법 집행을 위해 전기통신사업자를 대상으로 조치 의무 수행 여부 등을 검사하고 관련 자료 제출을 요구할 수 있는 권한을 전문기관(KISA)에 위탁하고 필요한 사항은 고시로 제정

- 보이스피싱 및 변작 서비스에 대한 처벌 규정 강화
 - 현행 '5천만원 이하 벌금'을 '3년 이하 징역 또는 1억 5천만원 이하 벌금'으로 상향 조정하여 억제력 강화

○ 법집행 실효성을 위하여 미래부(KISA)의 자료 제출 요구에 응하지 않는 전기통신사업자를 제재(벌금, 과태료 등)할 수 있는 수단마련 필요

2. 스미싱 방지를 위한 인터넷발송 문자서비스 규제 강화

1. 문제점

- 대부분의 스미싱 문자는 인터넷발송 문자 서비스를 통해 대량 발송
 - 자본금 1억 이하인 부가통신사업자는 신고가 면제되고, 미신고시 제재조항이 없어 인터넷발송 문자 서비스 현황 파악 곤란
 - 발송되는 문자의 원래 발신자를 명확히 구별할 수 있는 시스템 구축 필요(현재 10개 문자중계사업자만 구축)

2. 제도상 미비점

- 인터넷발송 문자서비스는 신고만으로 가능한 부가통신역무로,
 - 정부의 관리·감독이 어려워 이용자 피해 방지 미흡

3. 개선방안

- 미래부에 등록을 해야 하는 “특수한 유형의 부가통신역무”에 인터넷발송 문자서비스를 포함
- 인터넷발송 문자서비스를 제공하기 위해서 필요한 발신번호 변작방지를 위한 기술적 조치 계획 등 일정한 등록요건을 만족할 것을 요구
 - 사업자 계도 및 관리를 통해 안전한 환경 마련

○ 효율적인 법 집행을 위해 등록요건(기술적 조치 계획 및 필요 시스템 구비 등)을 심사할 수 있는 전문기관(KISA)에 위탁하고 필요한 사항은 고시로 제정 필요

3. 대출사기 등 불법행위에 사용된 전화번호 이용정지

1. 문제점

- 제도권 금융회사의 서민금융 위축으로 신용도가 떨어지는 취약계층의 자금조달은 미등록 대부업체와 같은 불법 사금융에 의존 증가
- 보이스피싱과 무분별한 스팸문자로 인하여 국민들의 피해가 발생

2. 제도상 미비점

- 선량한 서민들의 불법 사금융 이용을 원천적으로 차단하여 피해 발생을 사전에 예방할 수 있도록 제도적 장치의 마련이 필요
- 보이스피싱과 스팸문자의 발송에 이용되고 있는 전화회선을 차단할 수 있는 근거가 불명

3. 개선방안

- 대출사기 등에 이용되는 불법 대부광고에 기재된 전화번호를 차단할 수 있도록 전기통신사업법 개정
- 전화번호 이용의 차단은 해당 번호의 불법성을 판단할 수 있는 행정기관이 방송통신위원회에 요청하는 경우에만 조치
 - ※ 수사기관은 범죄행위에 제공되고 있는 전화회선의 차단을 서면으로 방송통신위원회에 요청

- 보이스피싱, 스팸 문자 등으로 인한 국민피해를 고려할 때, 이용중지(차단) 필요하나, **차단이전에 이용자에게 사전고지 필요**
- 미래부에서는 '13년 8월 "휴대전화 부정사용 피해방지 종합대책"을 마련하여 추진하고 있기 때문에
 - **차단 명령기관은 통신 서비스 부정사용 방지 등에 대한 정책 일관성을 고려하여 방통위보다는 미래부로 하는 것이 바람직**

4. 명의도용 등의 부정이용 방지를 위한 본인확인 및 시스템 구축

이동통신기기 부정이용방지에 관한 법률안

1. 문제점

- 이동통신기기가 생활필수품이 되었지만 이를 활용한 범죄행위 급증
- 불법으로 개통된 타인명의 휴대폰을 활용한 사기, 불법 스팸 등의 범죄행위가 급속히 증가하여 사회문제화
- 자금 제공 또는 유통의 조건으로 타인명의의 휴대전화를 이용하여 불법행위(스팸발송 등)를 하거나, 자금 회수에 이용하는 문제가 빈번하게 발생

2. 제도상 미비점

- 명의도용 되거나, 양수된 휴대전화를 이용하여 자금을 유통하는 행위에 대해서 금지할 수 있는 법제도 부재
- 타인명의의 이동통신기기를 이용하는 범죄행위가 급증하고 있음에도 이를 단속할 적절한 법적 근거 불명확

3. 개선방안

- 휴대전화를 양수하는 조건으로 자금을 유통하는 행위 또는 이를 권유·알선하는 행위 등을 금지
- 이동통신사업자가 휴대전화 개설 시 본인 사용 여부 등을 판단하여 휴대전화 개설 제한

- 휴대전화 가입 시, **본인확인을 실시간으로 할 수 있는 시스템 필요**
- 사망자, 유령법인 명의의 부정사용을 막을 수 있도록 **관련 국가, 공공기관 협력 필요**
- '이동통신기기 부정이용방지'에 관해서는 **별도 입법보다 전기통신사업법 내에 관련 조항을 포함하는 것이 일관성 유지 및 법집행 효율성을 제고할 수 있음**
- 본인확인에 사용된 개인정보는 보존(3년간) 없이 **즉각 파기를 원칙으로 하는 것이 필요**

5. 통신과금서비스(휴대폰 소액결제) 이용자 권리보호

1. 문제점

- 최근 휴대폰 소액결제를 이용한 사기가 많이 발생하고 있으며 특히 자신의 휴대폰 소액결제 한도액을 모르는 소비자들의 피해가 큼
- 피싱, 스미싱 등과 같은 신종 사기수법으로 휴대전화 소액결제를 유도하는 범죄가 증가

2. 제도상 미비점

- 휴대폰 소액결제로 이득을 취하는 통신과금서비스제공자의 이용자 권리보호 의무 미흡

3. 개선방안

- 통신과금서비스 계약 시 이의신청 및 권리구제 절차 명시, 약관 및 결제금액 변경 시 이용자에게 통지의무 부과
- 통신과금서비스를 통한 결제 사기 등 통신과금서비스이용자의 피해를 예방하기 위하여 정보보호 최고책임자 지정 및 기술적 조치 의무 부과

- 통신과금서비스 대가가 발생할 때마다 이용자 통지를 의무화하기 보다 사업자가 고객 서비스 형태로 제공하도록 유도 검토 필요
※ 신용카드 등 타 결제 수단과 비교하여 과도한 규제가 되지 않도록 규제 수위 검토 필요

- 정보통신망법 제45조의3에 의하여 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있기 때문에
 - 통신과금서비스제공자를 대상으로 별도의 정보보호 최고책임자를 지정할 수 있도록 하는 것은 중복 문제 발생

6. 개인정보 유출 방지 및 대응의무 강화

1. 문제점

- (손해배상) 개인정보 침해사고의 경우 권리침해는 명확하나, 그 손해액의 입증이나 산정이 어렵고 실손해가 소송비용보다 적어서 권리자 구제에 한계
- (처벌) 현행법은 개인정보 유출기업에 대해 과징금을 부과할 수 있도록 규정하고 있으나 부과요건이 까다롭고 과징금액이 소액
 - ※ 보호조치 위반과 개인정보 유출과의 인과관계를 입증하면 1억 원 이하의 과징금 부과 가능
- (파기) 개인정보 파기가 제대로 이루어 지지 않아 중고 IT기기의 디스크를 복구·재생할 경우 개인정보 유출의 위험이 있음
- (누출 통지·신고) 개인정보 유출시 정보통신서비스 제공자들은 이 용자에게 통지하고 방통위에 신고하여야 하나, 이를 하지 않거나 지체하고 있음

2. 제도상 미비점

- 법원은 개인정보 유출시 손해배상을 인정하지 않는 경우도 있으며 인정하는 경우에도 법원마다 배상액이 일정치 않음(10만원~100만원)
- 현행법은 개인정보의 수집·이용 목적이 달성됐거나 보유기간이 경과된 경우 개인정보를 파기하도록 단순 규정

- 현행법은 개인정보 누출 통지·신고를 ‘지체없이’ 하도록 규정하고 있으나 ‘지체없이’가 구체적으로 어느 정도의 기간인지 모호

3. 개선방안

- (피해구제 및 처벌) 이용자가 손해배상을 쉽게 받을 수 있도록 ‘법정손해배상제도’를 도입하고 개인정보 유출기업에 대한 과징금 상향 등 처벌 강화

※ 법정손해배상제도: 손해의 입증없이 법에서 정하는 일정금액을 청구할 수 있도록 하는 제도

- 개인정보 침해분쟁을 원활하게 해결하기 위해 분쟁해결기준 마련

- (파기) 개인정보 파기시 복구·재생할 수 없도록 필요한 조치를 하도록 법률에 명시적으로 규정하고 위반시 형사처벌을 하여 개인정보 유출 방지

- (누출 통지·신고) 개인정보 누출 통지·신고 기한을 ‘24시간 이내’로 명확하게 규정

- (손해배상) 법정손해배상제도의 도입은 권리자에 대한 피해구제의 실효성 강화뿐만 아니라 침해행위에 대한 사전적 예방 효과가 있을 것으로 기대
 - 다만, 법정손해배상액이 너무 과다할 경우 단 한번의 사고로 기업이 파산할 우려가 있으므로 이에 대한 신중한 검토가 필요
 - 개인정보 분쟁해결에 대해서는 온·오프라인 구분없이 개인정보 보호법에 따른 개인정보 분쟁조정위원회가 소관하고 있으므로 분쟁해결기준 또한 개인정보 보호법에 규정함이 타당
- (처벌) 개인정보가 유출된 경우 사업자에 대한 처벌 강화의 필요성은 공감하며 현행 제재수준이 미흡하므로 과징금 상향 필요

- 다만, 해킹 기술의 발달로 사업자가 개인정보 보호조치를 충실히 한 경우에도 개인정보 유출 가능성이 있으며, 이런 경우에도 과징금을 부과하는 것은 과실책임주의에 반할 소지가 있음
- (파기) 개인정보 파기시 복구·재생할 수 없도록 필요한 조치를 해야 함을 보다 명확히 규정하는 것은 필요하나, 위반시 처벌규정은 개인정보보호법 등 유사법률과 형평성 유지 필요
 - ※ 인쇄물은 파쇄, 하드디스크는 여러번 지우기 또는 덮어쓰기 방식으로 복구·재생할 수 없도록 조치
 - ※ 개인정보보호법은 개인정보를 파기하지 아니한 경우 3천만원 이하의 과태료를 부과하고 있음
- (누출 통지·신고) 개인정보 누출 통지·신고에 24시간 이내 요건을 부과하는 것은 타당
 - 온라인의 빠른 정보의 전파성을 고려할 때, 2차 피해 예방 및 이용자 알 권리를 보장하기 위해 원칙적으로 '신속한' 개인정보 누출 통지·신고는 바람직

7. 불법스팸 전송 규제 강화

1. 문제점

- 불법 대출, 도박, 불법 의약품 등 악성 불법 광고성 정보전송에 대한 형량이 재산상의 이익에 비해 지나치게 낮아 범죄억제 효과 미흡
- 전화나 팩스에 광고 전송 시 예외사항이 광범위하여 법 적용이 어려우며, 심야시간에 제한적인 광고전송이 가능하여 이용자의 불편과 짜증을 유발
- 정보통신서비스제공자는 스팸문자의 피해가 지속적으로 발생함에 따라, 이들 수단이 되는 서비스 제공 당사자로서 적극적인 대처 필요

2. 제도상 미비점

- 악성스팸 전송자에 대한 형량이 비교적 낮아 범죄 억제 효과가 미약
 - 도박, 불법대출, 불법의약품 등 정보통신망법 및 다른 법령에서 금지하는 재화 및 서비스에 대한 광고를 전송하는 경우에는 1년 이하의 징역 또는 1천만원 이하의 벌금으로 규정
- 전화·팩스 등의 광고성 정보 전송 시 사전 수신동의를 받아야 하나 예외 사항이 지나치게 넓고 불명확한 문제가 있으며, 별도 동의를 획득하면 심야 시간에 광고전송 가능
- 정보통신서비스제공자에 부여된 스팸방지 의무사항이 없어 사업자의 적극적인 대응이 어려움

- 정보통신서비스제공자는 자율규제 차원에서 스팸방지 조치를 취하고 있음

3. 개선방안

- 정보통신망법 제50조의8을 위반하여 광고성 정보를 전송한 자에 대한 형량을 3년 이하의 징역 또는 3천만원 이하의 벌금으로 상향
 - 불법광고가 사회에 미치는 악영향이 크다는 점에서 보다 강력한 규제를 위해 형량 상향 필요
- 전화나 팩스에 영리목적의 광고성 정보 전송 시 수신자의 사전 동의를 받거나 수신자가 요청하는 경우에만 전송이 가능하도록 함
 - 전화 및 팩스에 대한 예외사항을 삭제하여 거래관계에 따른 사전 동의 예외규정의 범위가 지나치게 넓은 현행 규정의 문제점 개선
- 심야시간에 수신자의 전화·모사전송기기에 대한 영리목적의 광고성 정보를 전송하는 행위를 금지하거나 제한
 - 심야시간대의 광고전송은 대다수 이용자의 불편을 초래하므로 광고 전송에 대한 제한이 필요함
 - ※ (현행) 정보통신망법상 야간시간(오후 9시~익일 오전 8시)에 전화, 팩스 등으로 광고성 정보를 전송하고자 하는 경우에는 수신동의 이외에 별도 동의를 받도록 하고 있음(본 개정안에서의 심야시간은 오전 0시~5시를 의미)
- 정보통신서비스제공자에게 스팸문자 발송 차단(전화번호 변작 차단 포함) 의무 부여

- 서면 또는 온라인 상에서 이용자의 동의를 받기 어려운 오프라인 사업자 (꽃배달, 대리운전 등)를 고려하여 **사전 수신동의를 받지 않아도 되는 예외 필요**
 - 다만, 일정기간 추가 거래가 없는 경우에는 광고를 전송할 수 없도록 하는 등의 보완 필요
- 정보통신서비스제공자에게 스팸 방지 의무가 부여되는 경우, 모든 광고성 정보의 전송에 대한 책임이 정보통신서비스제공자에게 전가될 수 있으며 서비스 제공에 과도한 부담이 될 수 있어 적절하지 않음
 - **스팸 방지 의무의 내용을 구체화**(정보통신망법을 위반하여 전송되는 광고성 정보의 차단 등) 하는 것이 바람직
- 송신인의 **전화번호 변작 행위를 차단**하기 위해서는 정보통신망법보다 전기통신사업자의 의무 등을 규정하고 있는 **전기통신사업법 개정을 검토하는 것이 타당**

06

의견진술

조규곤 파수닷컴(주) 대표이사

의견진술

조규곤 파수닷컴(주) 대표이사

개인정보유출 2차 피해방지 대책

최근의 대량 개인정보유출 사고로 인한 2차 피해는 크게 두 가지로 나누어 볼 수 있음.

- 물리적 공간에서의 피해
- 사이버 공간에서의 피해

개인정보, 예를 들어 주소, 전화번호 등이 유출되어 물리적 공간에서의 다른 범죄에 활용될 가능성은 충분히 있으나 본 발제에서는 논외로 하겠음.

사이버 공간에서의 향후 발생할 수 있는 피해로는 크게 두 가지로 나누어 볼 수 있음.

- 도용된 정보를 이용한 사이버 계정을 생성, 사이버 상에서 불법적 활동
- 사이버 상의 결제 수단을 통한 불법적인 금전 탈취

첫 번째의 경우, 크고 작은 여러 유형의 피해가 우려되고 있으나, KISA가 시행하고 있는 「주민번호 클린센터」 활동이 효과적이므로 더욱 확대할 필요 있음.

※ 각 개인들에게 본인의 주민번호가 이용되고 있는 인터넷 서비스를 알려주고 관리할 수 있도록 도와주는 서비스. 최근 이용자가 폭증하여 서버 증설을 하고 있음.

본 발제에서는 두 번째 사이버 결제 수단을 통한 금전 탈취를 방지하기 위한 장단기적인 대책에 대하여 주로 논하겠습니다.

현재 국내에서 쓰이고 있는 사이버 결제 수단은 다음과 같이 세 가지로 나누어 볼 수 있음.

- 신용카드를 통한 결제
- 금융계좌를 통한 이체/결제
- 통신사 계정을 통한 결제

이 모든 경우 이번 개인정보 유출에 의하여 여러 경로를 통하여 도용될 수 있는 잠재 위험에 놓여 있음.

단기 대책으로는

1. 모든 결제가 발생할 때에는 사용자에게 문자메세지나 이메일로 그 내용을 의무적으로 통지하여야 함. 발생하는 비용은 결제 서비스 사업자가 부담하는 것이 바람직함.
2. 사용자가 본인이 사용한 것이 아니라고 부인할 때 결제 서비스 사업자가 선 조치(환불) 후 분쟁 해결하여야 함. 책임 소재 규명을 위한 노력은 서비스 사업자가 주도적으로 하여함.
3. 단기적으로 사용자에게 영향을 줄 수 있는 기술적인 조치는 더욱 혼란을 가중시킬 수 있음.

중장기 대책으로는

1. 고객 정보를 다루는 사업자의 개인정보보호 역량 강화
 - 1.1. 내부자의 부주의, 고의에 의한 정보 유출을 방지하기 위한 내부 통제 프로세스, 이를 뒷받침하기 위한 솔루션의 도입을 서둘러야 함.

그 동안 보안 투자를 주로 사이버 테러와 같은 외부의 악의적인 공격으로부터 방어하는 것에 치중하였으나 그 것만으로 충분하지 않음.

- 1.2. 법률이나 감독기관의 보안가이드라인을 따르기에 현실은 어렵지만 더욱 직시해야 하는 것은 그 규정을 다 만족하여도 정보유출 사고는 생길 수 있다는 사실이며, 그 위험성을 줄이기 위한 투자를 획기적으로 늘려야 함.
- 1.3. 이를 독려하기 위하여 상장회사의 정보보호 투자 공시제 등을 검토하여 볼 필요 있음.

2. 개인정보보호 강화를 위한 입법 및 규정의 정비

- 2.1. 현재의 많은 입법 내용이나 감독기관의 관련 규정들이 매우 구체적인 기술적 조치를 포함하고 있음.
- 2.2. 그러나 이런 규정들은 항상 최소한의 의무 조항을 담을 수밖에 없는데도 불구하고 사업자들로 하여금 이 규정만 만족하면 보안 사고가 일어나지 않을 것처럼 생각하게 하고 있음. 또한 사고가 일어나더라도 사업자 책임이 없거나 책임이 줄어든다고 생각하게 하고 있음.
- 2.3. 현실적으로 지금처럼 빠르게 변화하는 기술 환경에서 어떤 기술적인 보안 조치도 오래 동안 유효하기는 쉽지 않음.
- 2.4. 이런 일률적인 보안 대책은 이것을 악용하려고 하는 범법자들에게는, 한 곳을 뚫으면 여러 곳을 뚫을 수 있어 오히려 취약점이 될 여지가 많음.
- 2.5. 따라서 법률에서는 새로운 사이버 상의 결제 수단을 다양하게 허용하되 만약 문제가 되었을 때 책임 소재를 분명히 하는 것이 법률 및 규정의 적절한 수준임.

- 2.6. 분쟁 발생 시 그 책임 소재를 법정에서 규명해야하는 것은 결제 서비스 사업자여야 함.
- 2.7. 책임 소재를 둘러싼 분쟁을 최소화하기 위한 기술적인 조치는 각 사업자들이 강구하는 것이 바람직하고 감독기관에서는 그 기술적인 조치의 허점들을 찾고 지적하는 수준에서 역할을 하는 것이 바람직해보임. 현재의 법률/규정을 좀 더 기술적으로 강화하려고 하는 시도는 바람직하지 않음.
- 2.8. 이로 인하여 사이버 결제 수단의 도입이 늦어 질 수도 있으나, 오히려 다양한 기술을 결합한 방안들이 도출 될 것이며 앞으로 더 건전한 사이버 공간을 만들 수 있는 기틀이 될 것임.
- 2.9. 오히려 이런 포괄적인 법률이나 규정이 관련 보안 산업의 경쟁력을 제고 하는 데에도 기여할 것임.