

새정부 개인정보정책 방향과 정보인권을 위한 세미나

단국대학교 법과대학 교수 정 준현

1. 문제의 인식

○ 정보사회의 특징

- 비대면성, 익명성, 개방성, 효과의 실시간 파급성

○ 정보화기술

- IPV⁶와 RFID를 통한 모든 사람과 사물에 대한 고유번호 부여가능
- “공유된 개념의 정형화된 명세서”인 온톨로지(Ontology)와 웹 정보자원의 의미를 이해하고, 정보의 검색, 추출, 해석, 가공등 제반 처리를 사용자를 대신하여 지능형 에이전트(intelligent agent)가 수행하는 컴퓨터 중심의 기술인 시맨틱 웹(Semantic Web)
- CCTV 등 각종 기기와 GPS기능 등의 융합 및 융합기기와 기능의 인터넷을 통한 원격통제
- “Cloud Computing”에 의한 정보자원활용의 극대화 및 “Big data”기술에 의한 정형 또는 비정형 데이터 가치의 극대화 및 미래예측(범죄예방 프로그램; “Minority Report” 등) 및 생산과 소비의 최적화를 통한 지구자원의 한계 극복)

○ 문제점으로서 현실생활의 사이버의존성 내지 종속성의 심화

- “빅데이터 사회”, “소셜네트워킹 사회” 및 전자정부에 기반을 둔 “스마트워크사회” 등
- 개인생활의 라이프 로그(Life-log)화 : 일정한 범위의 개인정보 공유에 의한 자의적 로깅 정보와 기업이나 악의자에 의한 트래킹 정보
- 포털검색의 단서 찾기 점화기능(Priming effect) 및 빅데이터 기술 : 신상털기, 사회공학적 공격 단서제공
- 각종 맬웨어에 기반을 둔 전자적 공격 및 SNS를 이용한 사회공학적 공격(소셜엔지니어링) 등의 진화·발전·융합
- 사이버의 Black Out ⇒ 개인, 사회 및 국가적 대혼란 / 사이버공간의 실재성
- 예측하기 어려운 고도 위험사회 / 사생활이 없는 사회(Zero Privacy Society)

○ 국제사회의 흐름

※유럽사이버범죄센터(European Cybercrime Centre)

- 2013년 1월14일 공식출범
- 온라인사기와 같은 조직화된 범죄활동 / 온라인상 아동 성추행과 같은 심각한 피

해유발범죄 / EU의 주요인프라 및 정보시스템을 대상으로 하는 범죄 등 3대 범죄에 주력

* 사이버범죄조약(부다페스트조약)(4장 48개 조문)

- 유럽 31개국, 미국, 일본, 필리핀 등 34개국 비준

* 국제정보보안조약(안)(5장 23개 조문)

- 러시아, 중국 등 상하이협력기구 회원국(카자흐스탄, 키르기스스탄, 타지키스탄, 우즈베키스탄) ⇒ 아시아 역내 군사동맹의 가능성

※ 지구촌 유일의 냉전대립국가로서의 우리 환경과 사이버안전

- 2013년 올해 중 OECD 정보보호 고위급회담 및 10월의 사이버공간회의 예정 / 2014년의 ITU 전권회의 개최 예정

2. 검토되어야 할 사항.

○ 헌법상 국가의 책무

- 모든 국민은 인간으로서의 존엄과 가치(기본권) 및 행복추구권 보유 ⇒ 기본권 목록의 개방성(헌법 37조 1항)

- 국가의 보장책무(헌법 제10조의 과소보호금지원칙)와 질서유지책무(헌법 제37조 제2항의 과잉금지원칙) ⇒ 기본권에 대한 보장의 최대성과 침해의 최소성

○ 정보주체의 권리

- 혼자남아 있을 권리로서 사생활권 ⇒ 정보자기통제권 ⇒ “잊혀질 권리” 내지 “검색당하지 아니할 권리”의 구현가능성(특히, SNS와 관련)

- 정보자기결정권의 지배를 받는 개인정보의 범위

- 정보약자로 전락할 가능성의 상존(하나의 “ID”와 “Pass Word”에 의한 사이버생활의 불가능성과 망각가능성 및 외부자에 의한 침해가능성)

○ 고도정보사회의 위험과 위험책임의 부담자

- 이용자(피해자)의 권리요건 사실에 대한 입증책임 ⇒ 서비스제공자의 고의 또는 과실이 없음에 대한 입증책임(입증책임의 전환) / 보증인적 지위의 강화(착한 사마리안) ⇒ 원인행위와 결과에 있어서 인과관계가 없음에 대한 입증책임으로 진화·발전(?)

○ 데이터의 활용(지식산업사회)

- 개인식별정보의 유용성과 위험성 및 개인에 관한 비식별정보의 데이터베이스화를 통한 자원활용의 최적화 및 빅데이터 기술에 의한 개인지배가능성(예측서비스 등)

○ 정보화와 일자리창출

- 각 영역의 “정보화” 내지 “M2M”로 인한 사무 및 산업의 자동화로 인한 일자리 감소에 대한 엄격한 평가와 대안의 발굴(서비스업의 흥수)

- 개인정보자기통제권의 범위설정과 사회 및 국가안전을 위한 개인감시의 균형
 - 개인의 “정보자기통제권” 내지 “검색당하지 아니할 권리” vs 사회안전망으로서의 Web-cam(CCTV) / SNS 등의 순기능과 역기능
 - ※ 각종 사이버테러 또는 좀비프로그램 등 각종 악성프로그램 등에 의한 위협예방을 위한 모니터링 내지 패킷감청의 한계 vs 사후복구의 곤란성 / 개인적·사회적 및 국가적 보호법의 전체에 대한 침해의 실시간 또는 잠재된 과급가능성 ⇒ 정보주체의 사회적 수인한도의 범위? / 검색당하지 아니할 권리의 요건과 범위
 - ※인터넷 경제의 GDP성장 기여율은 최근 5년 평균 16%로 지구촌 6위(사이버안전의 국가경제의존도)
- 적대세력에 의한 사이버위협과 사이버전에 대한 법적 개념정립(평상시 및 전쟁시의 사이버위기 대응체제의 법제화)
- 국가사이버의 안전을 위해 개인의 정보자기통제권 또는 개인의 정보화기기에 대한 지배권을 제한할 수 있는 객관적인 도구개념의 법제화
- CCTV 등 사회안전망에 대한 국가 또는 자치단체에 의한 통제의 가능성과 통제범위(?)

3. 맺는 말

- 정보주체의 정보자기결정권과 정보사회의 사회적 수인의무의 범위
 - 개인정보의 국외이전에 대한 통제권과 “잊혀질 권리” 내지 “검색당하지 아니할 권리”의 인정여부 및 범위
 - 계층적 정보불평등(Digital Divide) 시정의 방안(정보화의 효율성과 공공안전성간의 비교교량 필요)
- 정보자기결정권의 제한에 대한 법률적 요건(예측가능성 확보방안)
 - 헌법 제37조제2항의 기본권제한의 목적으로서 국가안전보장, 질서유지 및 공공복리 등 중국목적개념의 중간목적개념화의 방안
 - 국가 통일적인 차원의 사이버보안계획체계 및 그에 따른 행위제한 법제의 부존재
- 위험사회에 있어서 정보주체의 보호
 - 정보침해로 개인의 재산 및 인격에 대하여 발생한 피해에 대한 위험부담책임의 입법정책방향
 - 동의없는 정보에 대한 제재규정의 삭제여부와 목적 외 사용에 대한 제재강화 필요성
- 기타(IT업체의 사회적 기업화와 일자리 창출 등)