www.humanrights.go.kr

수사기관의 개인정보 수집 관련 제도 개선 토론회

| 일시 | 2014년 12월 22일(월) 14:00~17:00

| 장소 | 국가인권위원회 배움터(8층)

국가인권위원회

PROGRAM

수사기관의 개인정보 수집 관련 제도 개선 토론회

- 주 제 : 수사기관의 개인정보 수집에 대한 문제점과 제도개선
- 일 시 : 2014.12.22.(월) 14:00~17:00
- 장 소 : 국가인권위원회 배움터(8층)

시간	순서	내용 및 발표자
14:00 ~ 14:10	개회 및 소개	[개회 및 참석자 소개] 좌장 : 이상영 (방송통신대학교 법학과 교수)
14:10 ~ 14:50	발표	[발제] – 통신비밀보호법의 압수수색과 감청 등에 대한 제도 개선 오길영 (신경대학교 경찰행정학과 교수) – 개인정보호보법 목적 외 이용·제공 제한 조항에 대한 제도 개선 심우민 (국회 입법조사처 입법조사관)
14:50 ~ 15:50	토론	[토론] – 권헌영 (광운대학교 과학기술법학과 교수) – 이항우 (충북대학교 사회학과 교수) – 강장묵 (고려대학교 정보창의연구소 교수) – 이창범 (녹색소비자연대 이사) – 최성진 (인터넷기업협회 사무국장) – 이병선 (다음카카오 대외협력파트 이사)
15:50 ~ 16:00	질의 응답 및 폐회	[질의 응답 및 폐회] 좌장 : 이상영 (방송통신대학교 법학과 교수)

CONTENTS

수사기관의 개인정보 수집 관련 제도 개선 토론회

발제 01

통신비밀보호법의 압수수색과 감청 등에 대한 제도 개선

오길영 (신경대학교 경찰행정학과 교수)

소위 '카카오 사태'의 함의와 대응방안의 모색

신경대학교 교수 오길영

1. 디지털 통신에 대한 아날로그 입법

○ 금번의 사태는 고도 디지털시대에 부합하지 않는 고전적 아날로그 입법이 가져오는 총체적인 문제점을 되돌아볼 수 있는 계기라 할 수 있다. 즉 디지털 통신의 본질과 특성에 부합하지 않는 아날로그 방식의 자의적 해석이 결국 전방위적인 사찰의 형태로 악용되고 있음을 보여주는 극명한 사태로서, 이는 이미 디지털 통신매체의 보급과 함께 진행되어온 공공연한 사회문제로서 비단 금번 '카카오 사태'에서 처음 드러난 것이 아니다.

○ 고전적 의미의 감청은 통신이 끝나면 '휘발'되어 그 통신의 내용이 세상어디에도 존재할 수 없는 경우를 상정한다. 과거 유선전화나 무전기 정도를 생각하면 이해가 쉬울 것이다. 즉 그 '실시간'을 놓치면 더 이상 '지득 또는 채록'할 수 없기 때문에 종래의 감청은 당연히 실시간으로 진행되어졌고, 따라서 굳이 '실시간'이라는 요건을 법문에다 명시할 필요도 없었다. 이것이 바로 통신비밀보호법이 상정하고 있는 '아날로그' 마인드이다. 그러나 요즘의 디지털 통신은 저절로 휘발되지 않는다. 디지털 통신에서의 휘발은 어디까지나 옵션일 뿐이다. '비휘발', 즉 '저장' 옵션이 선택되는 한 디지털 통신의 내용은 마치 결제를 위한 서류마냥 차곡차곡 쌓여 통신이 끝나면 한 권의 책처럼 추려져 수사기관에 전달된다. 그 결과 서버로 날아오는 통신데이터를 서버입구의 '앞'에서 수집하면 감청, 서버입구의 '뒤'에서 수집하면 압수·수색이 된다. 즉 메기를 보(洑)의 앞에서 잡느냐 뒤에서 잡느냐의 차이일 뿐, 전화를 엿듣느냐 범행도구를 찾느냐의 차이가 아니다. 다시 말해 디지털 통신에 있어서는 감청과 압수·수색의 본질은 같다. 둘 다 복사(copy)일 뿐이다.

○ 혹자는 감청과 압수·수색의 구분기준을 '시점'으로 판단하기도 한다. 즉 '송·수신의 완료여부'를 기준으로 해석할 것이 아니라, 감청은 영장의 발부시점으로부터 '장래의 통신'을 대상으로 하고 압수·수색은 '과거의 통신'을 대상으로 한다고 해석하는 것이다. 그러나 이러한 해석의 문제점은 '긴급감청'에서 발생한다. 긴급감청은 긴급한 사유가 있을 때에 일단 감청을 시행하고 사후영장을 발부받는 제도인데, 만약 며칠간 저장되는 '카카오톡' 대화내용에 대해 긴급감청을 시행하고 영장을 신청한다면 이는 감청영장이어야 하는가 아니면 '과거'이므로 압수·수색영장인 것인가? 논리적 모순을 피할 수 없다. 여기서의 '긴급'과 '사후'영장의 의미는 놓쳐버릴 수 있는 '실시간'을 보호하겠다는 의미이고, 그 말은 결국 '휘발성'을 상정하고 있다는 이야기이다.

○ '통신사실확인자료'의 경우에도 동일한 문제가 생긴다. 기본적으로 아날로그 통신의 개념을 상정하고 있는 이러한 용어가 확대·적용되면서 적지 않은 혼란이 발생하고 있다. 대표적인 '통신사실확인자료'로서 '통화시간'과 '실시간 기지국정보'를 비교해보라. 통신의 존재를 전제로 하고 있는 '통신사실확인자료'의 본연의 정의에 비추어 보면, '통화시간'의 경우에는 문제가 없으나 '실시간 기지국정보'는 사용자의 통신여부와 무관하게 진행되는 "기지국과 단말기사이의 기술적 교신"에 불과하다.[1] 즉 '기지국 정보'는 통신사실확인자료의 범주에 포함될 수 없음에도 불구하고, 동일한 허가서에 의해 집행되고 있는 것이 현실이다.

○ 이러한 입법상 무관심의 결과는 결국 천문학적인 인권침해의 결과로 귀착된다. 즉 최근 몇 년 간의 통계를 기준으로 계산하자면, 연간 대략 2000만개의 통신데이터의 제공이 실시된다.[2] 요컨대 우리입법은 각각의 디지털 정보가 가지는 특성을 제대로 고려하고 있지 않고 있으며, 이렇듯 단순한 주먹구구식 개념획정으로는 결코 디지털을 제대로 다스릴 수 없다는 것이다. 즉 끊임없이 변모해가는 디지털의 특성상 멀지 않은 미래에 그 입법의 기능을 상실하거나 또 다른 문제를 야기할 것이다. 이러한 이유로 디지털에 관한한, 디지털에 부합하는 새로운 접근방식이 필요하다는 것이다.

1) 오길영, "통신데이터 남용의 실태와 그 쟁점", 민주법학 제55호(민주주의법학연구회, 2014), 20-22쪽.
2) 오길영, 위의 글, 3-4쪽.

2. 디지털 정보에 대한 영장주의의 혼란

○ 감청과 압수·수색은 필연적으로 국민의 기본권을 제한한다. 따라서 이러한 강제수사의 방법을 동원하기 위해서는 반드시 법관이 발부한 영장에 의해야만 한다. 즉 법관은 수사기관이 청구한 내용을 살펴보고, 수사의 진행이라는 공익과 이로 인해 침해되는 기본권을 저울질하는 심사숙고의 시간을 보내야만 한다. 결국 영장주의는 인권의 마지막 보루인 것이다. 그러나 '디지털'에 관한한 우리네 보루가 그리 미덥지 못한 것이 사실이다. 왜냐하면 '디지털'의 특성을 제대로 감안하지 못한 맹목적인 '아날로그'형 영장주의의 실천이라는 현실이 작지 않은 모순을 불러오고 있기 때문이다. 입법미비와 법원의 부실한 통제가 어우러져, 소위 '전방위'적인 감청과 '싹쓸이'식 압수·수색을 방치하고 있다는 비난이 바로 그것이다.

○ 문제의 핵심은 디지털 통신의 경우 그 당사자와 내용이 과거 아날로그 때와는 차원이 다르다는 데에 있다. '1:1 통신'이라는 말을 상기해 보라. 유선전화의 시대에 이런 말이 어디 어울리기나 하겠는가? 우리는 현재 무한통신의 시대에 살고 있으며, 여기서의 당사자는 이미 헤아릴 수 없다. 이 말은 곧, '1인'에 대한 감청으로 침해되는 통신비밀의 당사자가 더 이상 '1+1'이 아니라는 것이다. 이제 감청영장의 발부를 고민하는 법관은 '1+∞'의 기본권침해를 고려해야 한다. 다시 말해 아날로그 감청영장은 가벼우나 디지털 감청영장은 헤아릴 수 없이 무거운 것이라는 것이다. 따라서 일반적으로 '감청 대상자와 그 상대방'이라는 형태로 표현되는 감청영장상의 문구에 대하여는 새로운 접근이 필요하다. 즉 이제는 그 침해의 최소화를 위한 법원의 의지가 구체적인 형태로 나타나야 한다는 것이다. 1인의 감청대상자 때문에 희생되는 수십 또는 수백 명의 권리를 생각해보라. 결국 '그 상대방'도 특정되어야 할 것이며, 특정이 불가능한 경우에는 '구분되는 형태로 익명화'(예를 들어, 대화자A, 대화자B … 등)되어 제공되는 것이 바람직할 것이다. 만약 익명화된 상대방 가운데 공범의 존재가능성이 있다면 이는 그(예를 들어, 대화자B)에 대한 별도의 영장으로 해결해야 할 문제인 것이다.

○ 소위 '패킷감청'이라 불리우는 '회선감청'에서도 마찬가지이다. 이는 음성통화를 제외한 모든 데이터통신에 대한 감청을 말하는데, 쉽게 생각하면 네트워크를 사용하는 모든 행위를 퍼담는 것이다. 무선공유기를 사용하는 사무실에서 근무하는 어떤 이가 패킷감청의 대상이 되면, 그 사무실의 모든 사람이 함께 털리는 것을 알고 계시는가? 공유기가 임의로 분배하는 'MAC table'을 수사기관이 알아낼 방도가 없기 때문에, 과장님도 부장님도 동시에 털릴 수밖에 없다. 그 내용 또한 가관이다. 만약 요즘 유행하는 '결합상품'을 신청한 집이라면, 서재에서 옷을 구입하는 엄마의 웹서핑부터 거실에서 IPTV로 보고 있는 아빠의 뉴스프로그램은 물론 핸드폰으로 찍은 셀카를 클라우드에 백업하는 동생의 사진까지, 몽창 털린다. 물론 감청영장이 허가하는 대상은 '혐의사실과 관련된 사항(probable cause)'일 뿐이므로 굳이 의미 없는 패킷들까지 열어보겠느냐 하는 생각을 할 수 있으나, 일단 맛을 봐야 '단지 쓴지' 구분이 가능한 것 아니겠는가? 점쟁이가 아닌 이상, 일단 털고 난 뒤에야 골라낼 수 있다.

○ 이러한 문제는 압수·수색에 있어서도 똑같다. 핸드폰이 이미 압수된 자에 대해 디지털 저장매체의 압수·수색을 허가한 어느 영장의 문구를 살펴보기로 하자. 영장은 그 대상에 관하여 "위의 장소·차량·신체에 소지·관리·보관·사용하고 있는 컴퓨터(PC), 카메라, 캠코더, 녹음기, 차량 네비게이션, 디지털 정보저장매체(USB, CD, HDD, MP3, PDA, 전자수첩, 디지털테이프, 프린트기, 기타 각종 메모리 등) 및 동기기·매체에 수록된 내용"이라고 명기하고 있다. 디지털 기기로 뭐가 더 있을 수 있을까? '모든 디지털기기의 종합'이라는 표현을 나열하는 방식으로 적어 놓은 것과 다름없다. 즉 무형의 정보인 디지털의 특성상 미리 '특정'하는 것이 불가능하다는 이유로 상상가능한 모든 기기를 쭉 나열해 놓은 것이다.

○ 결과적으로 이 영장은 '싹쓸이'를 허가하는 셈이다. 따라서 이를 두고 '강제수사의 비례성'이 충족된 영장이라 평가할 수 없음은 물론, 대상물을 '특정'해야 한다는 영장주의의 취지 또한 무색하여 '포괄영장(general warrant)'이라는 비난을 피하기도 힘들 것이다. 그러나 디지털은 방도가 없기 때문이라고들 하면서, 현실은 이렇게 진행되고 있다. 즉 디지털이라는 이유만으로 인권보장을 위한 헌법 원리는 오히려

고도의 침해수단으로 둔갑되고, 그러한 바탕위에서 한 개인의 내밀한 프라이버시가 영장의 정당성을 통해 철저하게 침탈되고 있는 것이 오늘날 우리의 현주소이다. 이는 곧 디지털에 관한한 헌법원리의 적용을 상당부분 포기하고 있다는 것을 의미하기도 한다. 따라서 법관이 해야 할 숙고의 초점은, 단지 적법·위법의 절차적 문제만이 아니라 오히려 '프라이버시에 대한 합리적인 기대권(reasonable expectation of privacy)에 관한 면밀한 심사이어야 한다.

3. 문제의 기원: 데이터(data)의 무체성(intangibleness)

○ 디지털 증거가 넘쳐나는 현실을 뒤로 하고, 우리는 아직 압수의 대상물을 유체물(tangible objects)로 한정하고 있다. 형사소송법 제106조 제1항과 제2항은 명시적으로 '물건'이라는 표현을 사용하고 있고 신설된 동조 신설된 제3항과 4항의 경우에도 차이가 없다. 즉 제3항은 그 전단에서 "압수의 목적물"이 "컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체"라는 표현을 사용하고 있다. 유체물인 정보저장매체 자체의 압수를 상정하고 있는 것이다. 그 문장의 후단에서는 "기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다"고 하여, 이를 전단과 합치면 결국 '유체물인 디지털저장매체를 압수할 경우에는 (매체 자체를 통째로 압수하는 것이 아니라) 제한된 부분만을 출력 또는 복제해 와야 한다'는 의미이다. 다시 말해 이 조항에서 입법자는 디지털 저장매체를 통째로 압수하는 것을 금지하고자 하였을 뿐이므로, 여전히 압수의 대상은 유체물을 상정하고 있다고 해야 할 것이다. 제4항은 앞의 제3항의 내용, 즉 일정한 범위의 데이터를 복제하는 것을 "정보를 제공받은 경우"라고 하여 압수라는 표현을 전혀 사용하고 있지 않다. 요컨대 입법자는 유체물만을 압수의 대상으로 파악하고 있다고 할 것이다.

○ 한 때 형사법학계에서 정보(Information)라는 무체물(Intangible objects)에 관한 접근방법론을 화두로 논의가 진행된 바 있다. 압수의 개념에 있어 '유체물'에 대한 '점유'의 획득을 전제로 하고 있는 대륙법계 체제에 있어서는, 압수대상으로서 전자정보를 수용할 때 그 법리의 구성이 그리 쉽지 않기 때문에 제법 긴 시간의 해석론이 진행된 바 있다. 그러나 긍정설[3]과 부정설[4] 그리고 절충설[5], 이 모두는

그 논의의 토대가 아날로그식 접근법에 머물러 있어 명쾌한 법리를 내세우지 못하였다. 결국 이는 입법의 미비이지 해석론으로 보완될 여지는 없어 보인다. 형사법 체계의 대원칙인 '유추해석 금지의 원칙'에 비추어 보아도 그러하고, 확장해석을 한다고 하여도 무체물의 성질에 부합하는 이론구성을 해내기는 현실적으로 곤란하다. 결국 법률의 개정을 통해서 입법적으로 해결해야 할 문제이라는 점에 대해서는 '수사실무계'에서도 공감하는 바이기도 하다.[6] 본격적인 디지털 증거의 시대인 지금의 모습을 생각해 볼 때 눈과 귀를 막고 '아날로그 마인드'로 버티는 것이 바람직하지도 않거니와, 현실적으로 무체물에 대한 명정은 압수에 대한 이론구성의 토대로 기능하기 때문에 실무에서의 고충을 덜어주기 위한 작업이기도 하다.

○ 그러나 여기서, 그 입법의 형태에 대해서는 다소 고민의 여지가 있다. 가장 많이 회자되는 방식으로, 기존의 형사소송법의 규정에다 단순히 '정보'(information)를 추가하는 방안을 생각해 볼 수 있다. 즉 현재 우리 형사소송법이 취하고 있는 "증거'물'이나 몰수할 것으로 사료되는 '물건'"에다 '정보'를 추가하는 것인데, 필자는 이러한 방식에 대해서는 부정적이다. 왜냐하면 현재 감청 및 압수·수색의 대상이 되고 있는 디지털 정보의 종류가 다양하고 실제 그 보호법익이 상이한 데에도 불구하고, 수사실무에서는 별다른 구분 없이 일괄적으로 압수 또는 획득되고 있기 때문이다. 이에 대한 좋은 사례로 미국의 경우를 들 수 있다. 미국은 연방형사소송절차규칙(Federal Criminal Rules of Procedure)상의 압수의 대상물로 '정보'(information)를 추가한 바 있다.[7] 그러나 이러한 개정을 통해 디지털 데이터에 대한 압수의 개념을 둘러싼 혼란을 완전히 잠재우지는 못하고 있는 것으로 판단된다. 미국에서의 압수의 개념은 개인이 '점유물의 이익(possessory interests

3) 박수희, "전자증거의 수집과 강제수사", 한국공안행정학회보 제29호(2007), 138-139쪽; 조국, "컴퓨터 전자기록에 대한 대물적 강제처분의 해석론적 쟁점", 형사정책 제22권 제1호(2010), 104-105쪽.

4) 탁희성, "전자증거의 압수·수색에 관한 일고찰", 형사정책연구 제15권 제1호(2004), 26-28쪽; 권양섭, "디지털 포렌식 법률체계 구축방안", 법학연구 제35집(한국법학회, 2009), 368-369쪽; 강동욱, "디지털 증거 수집에 관한 형사소송법 개정안에 대한 검토", 법학연구 제8권 제3호(경상대학교 법학연구소, 2010), 165-166쪽.

5) 전명길, "디지털증거의 수집과 증거능력", 법학연구 제41집(한국법학회, 2011), 324-326쪽.

6) 제294회 국회, 사법제도개혁특별위원회회의록 제7호, "디지털 증거 수집의 문제점과 개선방안에 관한 공청회"(국회사무처, 2010), 12쪽, 대검찰청 이완규 검사의 진술내용 참조.

7) Federal Criminal Rules of Procedure §41(a)(2)(A).

in that property)'에 대한 '유의미한 방해(meaningful interference)'라고 보고 있는데,[8] 여기까지는 점유의 이전을 압수의 본질적 요소로 보는 우리의 경우와 큰 맥락에서 유사하다고도 할 수 있다. 복사 이후에 원본 데이터가 원래의 자리에 그대로 남아 있으니 점유의 이전 등 이익의 손상이 전무하다는 본질적인 문제는, 미국에서도 동일한 골칫거리이다.[9] 판례 또한 오락가락하고 있다.[10]

○ 이에 대하여 미국 학계에서의 논의는 어떠한가? Kerr는 이에 대하여 점유에 초점을 맞추지 않고 오히려 '방해의 여부'를 주목하면서 난관을 극복해 가고 있다. 즉 잔존하는 점유의 이익에 손상이 없다고 하여도 데이터를 복사하는 당시 데이터 전송을 위한 케이블을 연결하는 등 장비를 설치하는 행위 자체가 이미 '유의미한 방해'이라는 것이다.[11] 즉 복사가 아니라, 복사를 위해 장비를 연결하고 조작하는 행위가 이미 개인이 누려야 할 점유이익을 '방해'한다는 것이다. 한편 Goldfoot의 입장에서는 이러한 논의는 무의미해진다. 하드디스크에 담긴 데이터는, 가상공간 밖에서는 존재하지 않는 것으로 종이로 인쇄되는 경우 이상의 의미는 없다고 본다.[12] 또한 복사장비의 설치를 위한 행위 자체가 '유의미한 방해'에 해당된다는 논리에 대하여는, 이러한 논리대로라면 점유자 스스로가 컴퓨터를 작동시키기 위해 접촉하는 행위조차 '유의미한 방해'일 것[13]이라면서 직접적인 반증으로 '무접촉 복사'(Touchless Copy)의 예를 들고 있다.[14] 요컨대 해당 규정을 신설한 미국의 경우에도 여전히 데이터의 압수 자체에 대한 해석을 두고 논박이 오가고 있는 상황이다.

---

8) "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property.": *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

9) 이러한 입장을 취하여 압수임을 부정한 사례로는 *Arizona v. Hicks*, 480 U.S. 321 (1987).

10) 핸드폰 압수라는 동일한 경우에 대하여, 핸드폰의 압수와는 별개로 그 안의 데이터에 접근하기 위해서는 별도의 영장이 필요하다는 판례(*State v. Smith*, 920 N.E. 2d 949, 955 (Ohio 2009))와 핸드폰 자체와 그 안의 데이터를 구별할 실익이 없으므로 별도의 영장 없이 불필요하다는 판례(*People v. Diaz*, 244 P.3d 501, 509(Cal., 2011))가 혼재되어 있는 상황이다.

11) Orin S. Kerr, "Searches and Seizures in a Digital World", *Harvard Law Review* 제119권(2005), 561쪽.

12) Josh Goldfoot, "The Physical Computer and the Fourth Amendment", *Berkeley Journal of Criminal Law* 제16권(2011), 154-155쪽.

13) Goldfoot, 앞의 글, 159쪽.

14) Goldfoot, 앞의 글, 160쪽.

4. 현실적인 문제: 압수·수색의 방법론

○ 대략 2010년을 전후하여 디지털 정보에 대한 구체적인 압수·수색의 방법론에 대하여 치열한 공방이 있었다. 먼저 수사실무계의 주장[15]을 간추리자면 크게 다음의 3가지로 정리해 볼 수 있다. ① 압수·수색의 목적달성을 위해 압수·수색의 요건을 강화해서는 안 된다는 것,[16] ② 파일의 이전, 사본 또는 복제 등을 명문화하여 비밀번호 등이 설정된 경우 그 소유자 등의 협력을 강제할 수 있어야 한다는 것,[17] ③ 보전명령제도나 필터링제도, 원격 압수·수색 등 수사의 효율성 도모를 위한 새로운 제도를 도입하자는 것[18] 등이 그것이다. 이에 대하여 법원측[19]은 전체적으로는 유보적인 입장이라고 할 수 있는데, 그러나 그 통제의 방식에 있어서만큼은 사후적 통제가 아니라 '사전소명' 등의 사전통제를 통해 대상물 '특정'의 필요성이 있다는 취지[20]를 피력하고 있다.

○ 한편 학계의 주장은 수사편의에 주목하는 학설[21]과 인권옹호에 주목하는 학설[22]이 대립하고 있다. 전자의 경우 수사실무계의 주장과 다름이 없고,[23] 후자의 경우 압수·수색영장 적부심제도의 도입을 주장한다.[24] 한 가지 흥미로운 사실은 양자 모두 '제3자에 의한 필터링 제도'를 주장하고 있다는 것이다. 그러나 전자의 경우 여기서의 제3자를 '중립성을 가지는 또 다른 수사기관'으로 해석하고,[25] 후자의 경우에는 '검찰도 피의자도 아닌 독립적인 제3자'로 해석한다[26]는 차이가 있다. 대표적인 대립을 살피자면 여기까지이다. 한편 "요증사실과의 유관한 정보와 무관한 정보가 혼재되어 있을 경우 '별도의 영장'을 발부받도록 하자"는 소위

15) 제294회 국회, 앞의 자료, 대검찰청 이완규 검사와 안성수 검사의 논지.
16) 제294회 국회, 앞의 자료, 11-14쪽.
17) 제294회 국회, 앞의 자료, 12-13쪽 및 19쪽.
18) 제294회 국회, 앞의 자료, 13쪽 및 18-19쪽.
19) 제294회 국회, 앞의 자료, 수원지방법원 백강진 판사의 논지.
20) 제294회 국회, 앞의 자료, 16쪽 및 25쪽.
21) 제294회 국회, 앞의 자료, 성균관대학교 법학전문대학원 노명선 교수의 논지.
22) 제294회 국회, 앞의 자료, 고려대학교 법학전문대학원 박경신 교수의 논지.
23) 제294회 국회, 앞의 자료, 5-8쪽.
24) 제294회 국회, 앞의 자료, 8-10쪽.
25) 국가인권위원회, 사이버 수사 및 디지털 증거수집 실태조사(2012), 193-194쪽.
26) 박경신, "E-메일 압수수색의 제문제와 관련법률개정안들에 대한 평가", 법학연구 제13집 제2호(인하대학교 법학연구소, 2010), 297쪽.

'Tamura-Carey식 방안'[27]과 "포괄적인 압수는 곤란하나 포괄적인 수색은 가능하다"는 '운용방식의 재해석 방안'[28] 등 영장제도 자체에 대한 논의도 주목할 만하다.

○ 한편 미국의 경우, 디지털 증거의 압수·수색과 관련하여 가장 주목을 받았던 것은 역시나 Kerr의 글[29]이 아닌가 생각한다. 2005년을 전후하여 쏟아져 나온 Kerr의 논문들은 디지털 증거가 가져오는 새로운 문제점들을 제기하고 그 논의의 필요성을 주지시키기에 충분했다. 그의 문제의식은 디지털 증거에 대한 압수·수색의 절차가 수정헌법 제4조의 영장주의의 원칙과 부합하지 않는다는 점에서 기인한다. 그는 디지털 증거의 압수·수색의 절차를 크게 '물리적 수색(physical search)→물리적 압수(physical seizure)→전자적 수색(electronic search)'[30]의 3단계로 구분하면서 그 논의를 시작한다.[31] 이러한 두 차례의 수색이 가져오는 가장 큰 문제점은 역시나 포괄영장(general warrant)의 문제이라고 분석한다. 즉 영장의 발부형태에 대하여, 흔히 우리나라의 영장에서 발견되는 '모든 종류의 디지털 기기'를 나열하는 방식인 '물리적인 접근'의 경우와 '대상이 되는 디지털 증거 그 자체'를 명정하는 방식으로 구분하면서,[32] 전자의 경우 그러한 광범위(overbroad)한 대상물의 설정은 결국 수정헌법상의 '상당한 이유(probable cause)'를 가질 수 없다고 판단한다.[33] 반면에 후자의 경우는 이러한 광범위성의 문제를 피할 수는 있으나, 실제 영장 집행의 방법에 대하여 정확한 해답을 마련해 주지 못한다는 것이 문제이라고 분석한다.[34] 이러한 문제에 대한 해결책으로 그는 연방형사소송절차규칙 제

27) 조국, "디지털증거에 대한 압수수색", 대법원 사법제도비교연구회 2010년 3월25일 발표문.
28) 오기두, 대법원 사법제도비교연구회 2010년 3월25일 토론문.
29) Orin S. Kerr, "Searches and Seizures in a Digital World", *Harvard Law Review* 제119권(2005); Orin S. Kerr, "Search Warrants in an Era of Digital Evidence", *Mississippi Law Journal* 제75권(2005); Orin S. Kerr, "Digital Evidence and the New Criminal Procedure", *Columbia Law Review* 제105권(2005); Orin S. Kerr, "Four Models of Fourth Amendment Protection", *Stanford Law Review* 제60권(2007) 등.
30) Orin S. Kerr, "Search Warrants in an Era of Digital Evidence", *Mississippi Law Journal* 제75권(2005), 91쪽.
31) 국내의 논의에서 흔히 등장하는 '전자적 압수'는 그 해석상 제외하고 있다. 왜냐하면 저장매체의 압수를 인정하는 것에는 문제가 없으나, 파일 그 자체의 복사행위 등을 압수로 인정하는 것이 일반적인 해석상 곤란하므로 문제가 있다는 것이다. 그가 이 부분을 위해 새로운 해석론을 주장하고 있음은 앞서 살핀 바와 같다: Orin S. Kerr, 앞의 글(각주 30), 102쪽 및 133쪽.
32) Orin S. Kerr, 앞의 글(각주 30), 101쪽.
33) Orin S. Kerr, 앞의 글(각주 30), 101-102쪽.
34) Orin S. Kerr, 앞의 글(각주 30), 102쪽.

41조의 개정을 주장한다. 즉 디지털 증거의 경우 필연적으로 발생하는 두 차례의 수색을 인정하고 '물리적 수색'단계에서의 대상과 '전자적 수색'단계에서의 대상, 이 '양자'를 적시하는 영장제도의 도입을 하자는 것이다.[35] 이러한 논의에 뒤이어 그는, 그 보호법익이 되는 프라이버시권으로 시야를 넓혀간다. 즉 영장집행의 실무적 행태가 '프라이버시에 대한 합리적인 기대권(reasonable expectation of privacy)'을 충족하는지에 대한 판단의 문제를 4가지의 모델[36]을 통해 수정헌법의 원리에 비추어 검토를 진행한다. 다시 말해 디지털 증거에 대한 압수·수색의 방법론의 문제가 영장자체의 적법성 문제를 넘어 프라이버시의 문제로 연결되게 된 것이다.

○ 이러한 시각은 미국 법조에 큰 파장을 불러 일으켰던 코진스키(Alex Kozinski) 판사[37]의 논리로 이어진다. 메이저리그 야구선수들의 스테로이드(steroid) 약물복용 혐의와 관련한 압수·수색의 집행과정에서, 야구선수는 물론 다른 종목 선수들의 검사결과가 혼재되어 있는 디렉토리(소위 Tracey Directory) 전체에 대한 광범위한 압수수색[38]을 두고 벌어진 유명한 사건(United States v. Comprehensive Drug Teating, Inc.)[39]에 대한 결과로 코진스키 판사가 제시한 가이드라인이 바로 그것이다. 이 사건에 대해 제9순회 지부 연방항소법원은 남발된 당해 영장(subpoenas)에 대해 '불합리한 보험증권(unreasonable insurance policy)'과 같다고 평가하면서, 영장의 집행이전에 수사기관은 관련성이 있는 정보와 수반되는 노력들에 대하여 담당판사에게 충분한 설명을 반드시 해야 한다고 판단하였다.[40] 나아가 전원일치 의견으로 ① 전자적 수색에 대하여 '업데이트'된 'Tamura'원칙을 적용하기로 하면서 ② 이러한 전자적 수색과 관련하여 법관은 '수사기관의 법집행상

35) Orin S. Kerr, 앞의 글(각주 30), 132쪽.

36) The Probabilistic Model, The Private Facts Model, The Positive Law Model, The Policy Model 등이 그것이다. 지면관계상 이에 관한 상세를 논할 수는 없으나 그 이론적 정치함이 뛰어나다고 평가하고 싶다. 구체적인 내용은 Orin S. Kerr, "Four Models of Fourth Amendment Protection", Stanford Law Review 제60권(2007), 507-524쪽.

37) 2010년 당시, 제9순회 지부 연방항소법원(A Ninth Circuit Court of Appeals) 판사임.

38) Kimberly Nakamaru, "Mining for Manny: Electronic Search and Seizure in the Aftermath of United States v. Comprehensive Drug Testing", *Loyola of Los Angeles Law Review* 제44권(2011), 776-777쪽.

39) 621 F.3d 1162 (9th Cir. 2010).

40) Kimberly Nakamaru, 앞의 글, 796-797쪽.

의 이익'과 '불합리한 압수와 수색으로부터 자유로워야 할 개인의 권리', 이 양자의 이익형량에 대하여 고도의 주의(Greater vigilance)가 필요함을 설시하였다. 그러나 구체적인 이익형량의 방법이나 'Tamura'원칙의 '업데이트'하기 위한 기술적인 방안에 대한 언급은 없었다.[41]

○ 이에 대하여 코진스키 판사는 이 문제를 해결할 수 있는 구체적인 방안으로 5가지의 가이드라인을 제시하였다. 즉 "① 치안판사(magistrate judges), 즉 영장담당판사는 디지털 증거의 경우 수사기관이 플레인뷰(plain view)원칙에 의존하려는 것을 포기해야함을 주장해야 한다. 대상정보가 혼재되어 있을 경우 그 ② 구분(segregation) 편집(redaction)작업은 반드시 특별한 자(specialized personnel)에 의해 진행되어야 하며, 만약 그 자가 수사기관측의 '컴퓨터 관련인(computer personnel)'일 경우에는 그 사람은 영장의 목표가 된 정보 이외의 어떠한 정보도 담당수사관에게 공개해서는 안된다는 영장내용에 수사기관이 동의해야 한다. ③ 영장의 내용은 당해 정보를 파괴(destruction)할 수 있는 현실적인 위험을 필히 밝히고 있어야 한다. ④ 수사기관의 수색방식(search protocol) '상당한 이유(probable cause)'에 부합하는 정보만을 색출(uncover)해내도록 고안되어야 하고, 그 정보는 담당요원(case agents)의 검증을 거친 것이어야 한다. ⑤ 수사기관은 관련성이 없는 정보에 대해서 폐기(destroy)하거나 환부(return)해야 하며 그 보관기간과 보관물목에 대한 치안판사의 허가내용을 보관해야 한다" 등[42]이 그것이다. 이러한 코진스키 판사의 가이드라인은 미국 법무성(the Department of Justice)과의 마찰을 빚으면서 추후 제9순회법원 스스로 철회하게 되나, 디지털 증거의 압수·수색의 실무에 있어서는 여전히 살아있는 일종의 원칙으로 기능하고 있는 것이 현실이다.[43]

41) Kimberly Nakamaru, 앞의 글, 797쪽.
42) Kimberly Nakamaru, 앞의 글, 797-798쪽.
43) Kimberly Nakamaru, 앞의 글, 799쪽.

5. 구체적인 문제: 압수·수색의 실천론

○ 국내의 논의는 주로 코진스키의 제2원칙에 대하여 주목하면서, 소위 '제3자 필터링 제도'라는 공통된 명칭하에 서로 다른 해석을 하고 있음은 앞서 살핀 바와 같다. 코진스키의 원안대로라면 수사편의에 주목하는 학설 쪽의 해석이 맞다.[44] 그러나 우리네 수사실무의 행태를 고려하자면, 코진스키의 제2원칙을 원안 그대로 도입한다는 것이 타당성을 가지기 힘들다. 남발되는 영장청구와 주먹구구식 집행이 현실인 우리나라의 환경에서, 수사기관내부에서 코진스키가 상정하는 중립성을 가진 특별한 요원이 존재할 수 있는가하는 점이다. 또한 인권옹호에 주목하는 학설의 입장도 마찬가지이다. 현재 우리나라의 포렌식 산업의 현실[45]에 대한 성의 있는 고려가 빠져있다는 것이 문제이다. 따라서 객관성을 가질 수 있는 제3자를 검찰 외부에서 찾아낸다는 것도 이론적으로는 동의할 수 있으나 거의 현실성이 없다는 것이 문제이다. 요컨대 코진스키의 제2원칙은 우리 현실에는 크게 부합하지 않는다. 다만 이를 통해 코진스키가 추구하고자 했던 함의, 즉 '수사기관 스스로 전자적 수색을 집행한다는 것은 타당하지 않다'라는 의미만 남는다.

○ 그렇다면 어찌하란 말인가? 이 부분에 대하여 우리 대법원은 이미 '보석' 같은 설시를 펼친 바 있다: 『 전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문

44) Stephen E. Henderson, "What Alex Kozinski and the investigation of Earl Bradley teaches about Searching and Seizing Computers and the Danger of inevitable Discovery", *Widener Law Review* 제19권(2013), 129-136쪽.

45) 간략히 언급하자면, 검찰의 증거에 반증할수 있는 용기 있는 포렌식 전문가를 찾는다는 것이 현재로서는 매우 힘든 일이다.

서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다. 한편 검사나 사법경찰관이 압수·수색영장을 집행할 때에는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), **혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때** 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 **피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지**, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다 』 (대법원 2011.5.26.자 2009모1190 결정, 굵은 글씨체와 밑줄 표시는 필자)

○ 즉 “피압수·수색의 당사자 또는 변호인이 참여”해야 한다는 것이다. 대법원의 논지의 흐름을 정리하자면, ① 혐의사실과 관련된(즉 probable cause) 부분만을 ② 출력 또는 복사하는 방식으로 집행되어야 하는 것이 원칙이고, ③ 현장 사정상 도저히 불가능한 경우에 한하여(보충성) ④ 예외적으로 저장매체 자체를 반출할 수 있는데 ⑤ 이러한 예외의 적용을 위해서는 당해 영장자체가 예외의 적용을 허용하고 있어야 하며, 저장매체가 수사기관에 옮겨져 수색을 할 경우 ⑥ 피압수·수색의 당사자 또는 변호인의 ‘계속적’인 참여권이 보장됨은 물론 ⑦ 피압수·수색의 당사자 또는 변호인의 참여가 배제된 상태에서는 저장매체에 대한 열람·복사 등의 압수·수색의 집행이 금지된다는 것이다.

○ 이 판결에 대해서 필자는, 미국에서의 논의가 무색해질 정도로 매우 출중한 판단이라고 평가하고 싶다. 특히 “혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때”라는 설시 부분에서 살필 수 있듯, 우리 대법원도 이미 프라이버시권에 대한 배려를 하고 있다는 점을 알 수 있다. 또한 학계에서 논해지고 있는 제2원칙의 실천방안 공방에 대하여, “피압수·수색의 당사자 또는 변호인이 참여”라는 명쾌한 해석을 내어 놓았다. 나아가 “문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙상 당연하다”라고 하여 코진스키의 제4원칙과 동일한 입장임을 확인함과 동시에 수사편의에 치우쳐 있는 수사실무계에 대하여 제대로 된 일침도 가하고 있다.

○ 그렇다면 압수·수색의 범위에 대한 제한, 즉 ‘혐의사실과 관련된 정보’만의 색출을 위한 실무적인 방안은 무엇인가 하는 문제가 남는다. 먼저 수색의 방식(Search Protocols)을 당사자가 확인하여 진행하는 방안, 즉 ‘특별한 접근(special approach)’을 생각해 볼 수 있다.[46] 이는 검색어의 특정이나 파일의 종류 또는 대상 폴더, 나아가 사용되는 포렌식 설비 등을 수색의 시점에서 수시기관과 피압수·수색의 당사자가 서로 확인하며 진행하는 것이다. 이러한 수색의 범위는 판사의 영장에 의하게 되는데, 당해 수색의 방식이 판사의 영장이 허가한 범위이내라는 점에 대한 입증은 수사기관이 부담하게 된다.[47] 이럴 경우 전자적 수색의 범위와 방법에 대한 판사의 면밀한 판단이 전제되어야 하고, 이러한 판단을 구하기 위해서 수사기관은 영장의 신청에 있어 구체적인 압수·수색의 전략과 그 타당성을 상세하게 기록해야 한다. 다시 말해 전자적 수색에 대한 법원의 심사절차가 필요하다는 것이고, 이는 필연적으로 수색의 이전에 진행되어야 하므로 사전적 통제로 기능하게 된다. 즉 영장 자체에서 그 대상과 범위는 물론 수색의 방법과 수단까지

46) 이를 ‘Carey-Winick Doctrine’이라고도 한다. 이에 관한 상세는 Lily R. Robinton, “Courting Chaos: Conflicting Guidance from Courts Highlights the Need for clearer Rules to Govern the Search and Seizure of Digital Evidence”, *Yale Journal of Law and Technology* 제12권(2010). 339-342쪽 참조.

47) Steven R. Morrison, “What's Old is New Again: Retaining Fourth Amendment Protections in Warranted Digital Searches”, NACDL's Fourth Amendment Advocacy Committee(2014), 18쪽.

를 한정한다는 것인데, 이에 대해서는 미국에서도 찬반논란이 있다.[48]

○ 미국의 경우에는 통상 영장청구단계에서 진행되는 선서진술서(affidavit)를 통해 법원과 수사기관의 사전협의가 있게 되는데, 그렇다면 이렇듯 압수·수색을 계획하는 단계에서 이 모든 것을 미리 예측하여 완결된 상태에서 영장이 청구되어야 한다는 문제가 생긴다. 결국 이러한 논리는 실무적인 한계를 동반할 수밖에 없다는 것이다. 이러한 문제점에 대하여 미국의 절충설은 나름의 방안을 논의한 바 있다. ① 원칙적으로 좁은 범위의 수색(narrow search)이 요청되나, 꼭 필요한 경우에는 파일 하나하나(file-by-file)를 수색할 수 있다. ② 영장상의 범위 이외의 증거이거나 모호한 경우에는 별도의 영장이 요청되나, 단 금제품(contraband)에 해당할 경우에는 플레인뷰의 원칙이 적용된다. ③ 내밀한 정보 또는 당사자 이외의 자에게 관련된 파일의 색출을 위한 제도의 운용 등[49]이 그것이다. 간추리자면 '원칙을 설정'하고 이에 '예외를 병행'하는 것이다. 결국 제2영장, 즉 별도의 추가영장을 예정하고 있다.

6. 새로운 보호법익의 등장: 프라이버시에 대한 합리적인 기대권 (reasonable expectation of privacy)

○ 코진스키의 가이드라인 내용은 참으로 많은 생각을 하게 한다. 무엇보다 제1원칙인 소위 '플레인뷰(plain view)의 적용금지'는 그야말로 감동적이다. 미국에서 플레인뷰의 원칙은 유체물의 압수·수색에 있어서 필수적인 사항으로 받아들여지고 있다.[50] 예를 들어 혐의자의 주택을 압수·수색하기 위해 영장을 발부받아 현장에 도착한 상황에서, 영장에 적시되지 않은 범행의 도구를 발견하였다고 할 경우 이를 두고 영장상의 대상물이 아니어서 압수의 대상에서 제외되고 유죄입증의 증거에 사용할 수 없다고 엄격히 해석한다면 당해 수사의 효율을 제고하기란 난망하기 때

48) Christina M. Schuck, "a Search for the caselaw to support the computer search "Guidance" in United States v. Comprehensive Drug Testing", Lewis & Clark Law Reviews 제16권(2012), 773-778쪽.
49) Lily R. Robinton, 앞의 글, 343-346쪽.
50) 우리나라에서는 플레인뷰의 원칙이 아직 적용되지 않고 있음은 주지의 사실이다.

문이다. 따라서 유체물의 경우 플레인뷰의 적용이 합당함은 오랜 미국법원의 판례에서 확인할 수 있듯이 충분히 동의가능한 원칙이라 할 것이다. 그러나 플레인뷰가 디지털 증거와 적용되는 순간, 이는 전혀 새로운 의미로 변모하게 된다. 하나의 디지털 저장매체 내부에 저장되어 있는 수많은 정보들은 각 주제별로 각각의 공간에 정연히 정리되어 있을 수 없다. 압수대상 정보는 다른 정보들과 혼재되어 있는 것이 일반적이고, 대상정보를 찾아내기 위해 무관한 정보들을 모두 들추어보게 된다면 그야말로 전방위적인 저인망식 수사가 될 것이다.[51] 특히 그 무관한 정보들 가운데에서 새로운 범죄의 혐의사실이 발견된다면 이는 참으로 난감한 문제가 아닐 수 없다. 유죄의 입증을 필수적인 수색과 그 과정에서 희생되는 개인의 프라이버시권에 대한 이익의 형량, 그 결과로 나온 것이 바로 '플레인뷰의 적용금지' 원칙인 것이다. 즉 수색의 대상은 당초 발부된 영장의 범위내로 제한되고, 설사 그 과정에서 새로운 증거가 발견된다고 하더라도 당해 증거는 증거능력이 배제되어야 한다는 것이다. 따라서 제한적 수색만이 허락된다는 것이 디지털 증거의 압수와 수색의 원칙이고, 수사기관은 영장의 발부단계에서 이러한 대상과 범위의 설정에 관하여 미리 고민하지 않으면 안 된다.

○ 이는 '디지털 증거에 관한한 영장의 포괄성은 어쩔 수 없다'고들 하는 우리 법조실무계에 대하여는 크나큰 귀감이 되는 것이라 할 수 있다. 우리의 경우 대다수의 논의는 포괄영장을 방지하기 위한 제도개선의 입장, 즉 형사소송절차 개선의 문제로 다루고 있는데 반하여, 미국의 많은 논의들이 주목하고 있는 법익은 제도의 실천이 아니라 프라이버시권 자체이다. 물론 그 논의의 시작점에서는 미국도 역시 혐의사실과의 관련성, 즉 '상당한 이유(probable cause)'의 실천을 위한 논의가 주류를 이루었다. 그러나 그 논의가 진행되면서 이러한 초점은 점차 피압수·수색의 당사자 또는 당사자가 아닌 자가 가지는 수정헌법에 의해 가지는 '프라이버시에 대한 합리적인 기대권(reasonable expectation of privacy)'으로 점차 변화되어 왔다. 다시 말해 디지털 정보에 있어서는 '영장집행의 적법·타당'에 대한 논의가 아니라 '프라이버시권에 대한 최소침해'가 그 핵심인 것이다. 따라서 더 이상 프라이버시권을 아무 때나 장난삼아 주장해보곤 했던 '빛 좋은 개살구'이어서는 곤란하

51) Lily R. Robinton, 앞의 글, 334-339쪽.

고, 가장 구체적이고도 직접적인 기본권으로서 기능해야 한다는 것이다. 이러한 관점의 변화, 다시 말해 디지털 분야에 있어서만은 가장 중요한 보호법익이 프라이버시권이라는 것을 우리 법조가 하루빨리 수용해야만 한다. '생생히 살아 숨 쉬는 프라이버시권', 이것이 바로 디지털 시대에 부응하는 새로운 패러다임이기 때문이다.

<참고문헌>

강동욱, “디지털증거 수집에 관한 형사소송법 개정안에 대한 검토”, 법학연구 제8권 제3호, 경상대학교 법학연구소, 2010.

권양섭, “디지털 포렌식 법률체계 구축방안”, 법학연구 제35집, 한국법학회, 2009.

박경신, “E-메일 압수수색의 제문제와 관련법률개정안들에 대한 평가”, 법학연구 제13집 제2호, 인하대학교 법학연구소, 2010.

박수희, “전자증거의 수집과 강제수사”, 한국공안행정학회보 제29호, 2007.

오기두, 대법원 사법제도비교연구회 2010년 3월25일 토론문.

오길영, “통신데이터 남용의 실태와 그 쟁점”, 민주법학 제55호, 민주주의법학연구회, 2014.

전명길, “디지털증거의 수집과 증거능력”, 법학연구 제41집, 한국법학회, 2011.

조국, “디지털증거에 대한 압수수색”, 대법원 사법제도비교연구회 2010년 3월25일 발표문.

_____, “컴퓨터 전자기록에 대한 대물적 강제처분의 해석론적 쟁점”, 형사정책 제22권 제1호, 2010.

탁희성, “전자증거의 압수·수색에 관한 일고찰”, 형사정책연구 제15권 제1호, 2004.

국가인권위원회, 사이버 수사 및 디지털 증거수집 실태조사, 2012.

제294회 국회, 사법제도개혁특별위원회회의록 제7호, “디지털 증거 수집의 문제점과 개선방안에 관한 공청회”, 국회사무처, 2010.

Christina M. Schuck, “a Search for the caselaw to support the computer search “Guidance” in United States v. Comprehensive Drug Testing”, Lewis & Clark Law Reviews 제16권, 2012.

Josh Goldfoot, “The Physical Computer and the Fourth Amendment”, Berkeley Journal of Criminal Law 제16권, 2011.

Kimberly Nakamaru, “Mining for Manny: Electronic Search and Seizure in the

Aftermath of United States v. Comprehensive Drug Testing", Loyola of Los Angeles Law Review 제44권, 2011.

Lily R. Robinton, "Courting Chaos: Conflicting Guidance from Courts Highlights the Need for clearer Rules to Govern the Search and Seizure of Digital Evidence", Yale Journal of Law and Technology 제12권, 2010.

Orin S. Kerr, "Searches and Seizures in a Digital World", Harvard Law Review 제119권, 2005.

_____, "Search Warrants in an Era of Digital Evidence", Mississippi Law Journal 제75권, 2005.

_____, "Digital Evidence and the New Criminal Procedure", Columbia Law Review 제105권, 2005.

_____, "Four Models of Fourth Amendment Protection", Stanford Law Review 제60권, 2007.

Stephen E. Henderson, "What Alex Kozinski and the investigation of Earl Bradley teaches about Searching and Seizing Computers and the Danger of inevitable Discovery", Widener Law Review 제19권, 2013.

Steven R. Morrison, "What's Old is New Again: Retaining Fourth Amendment Protections in Warranted Digital Searches", NACDL's Fourth Amendment Advocacy Committee, 2014.

발제 02

개인정보호보법 목적 외 이용·제공 제한 조항에 대한 제도 개선

심우민 (국회 입법조사처 입법조사관)

「개인정보 보호법」상 범죄 수사 등을 위한 개인정보의 목적 외 이용·제공 규정의 검토

국회입법조사처
NATIONAL ASSEMBLY RESEARCH SERVICE
국회입법조사처
입법조사관 심우민(법학박사)
legislation21@gmail.com
http://legislation.kr

Contents

01 범죄수사와 개인정보의 활용

01 범죄수사와 개인정보의 활용(1)

개인정보의 목적 외 활용규정(「개인정보 보호법」)

제18조(개인정보의 목적 외 이용 · 제공 제한) ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

..... (중간 생략) .....

7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우

..... (이하 생략) .....

01 범죄수사와 개인정보의 활용(2)

관련 규정의 해석

- 범죄 수사 목적 등을 위한 개인정보의 목적 외 이용 및 제공 규정은 「개인정보 보호법」상 대표적인 공공기관에 대한 특례(의무 완화) 규정임(행정안전부, 2011)
  - ✓ 범죄수사의 평의를 위해 공공기관이 보유하고 있는 개인정보에 대해서는 정보주체의 동의 없이 목적 외로 이용 또는 제공할 수 있게 하기 위함
  - ✓ 「개인정보 보호법」을 근거로 적용할 경우, 수사기밀 유출 등 수사활동에 장애가 발생하여 범죄예방 및 처단이 어려워짐을 우려
- 이 규정이 가지는 가장 큰 특징은 영장에 의하지 않고도 범죄수사에 필요하다고 한다면 수사기관 등은 공공기관에 관련 개인정보의 제공을 요청할 수 있음

02 관련 규정의 체계 분석

02 관련 규정의 체계 분석(1)

타법상 이용·제공 규정 1: 「정보통신망법」

제24조의2(개인정보의 제공 동의 등) ② 제1항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

타법상 이용·제공 규정 2: 「위치정보법」

제21조(개인위치정보 등의 이용 · 제공의 제한 등) 위치정보사업자등은 개인위치정보주체의 동의가 있거나 다음 각호의 1에 해당하는 경우를 제외하고는 개인위치정보 또는 위치정보 수집 · 이용 · 제공사실 확인자료를 제18조제1항 및 제19조제1항 · 제2항에 의하여 이용약관에 명시 또는 고지한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니된다.
1. 위치정보 및 위치기반서비스 등의 제공에 따른 요금정산을 위하여 위치정보 수집 · 이용 · 제공사실 확인자료가 필요한 경우
2. 통계작성, 학술연구 또는 시장조사를 위하여 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우

02 관련 규정의 체계 분석(2)

타법상 이용·제공 규정 3: 「신용정보법」

제32조(개인신용정보의 제공 · 활용에 대한 동의) ① 신용정보제공 · 이용자가 대출, 보증에 관한 정보 등 대통령령으로 정하는 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 개인으로부터 다음 각 호의 어느 하나에 해당하는 방식으로 미리 동의를 받아야 한다.

..... (중간 생략) .....

④ 신용정보회사등이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제3항까지를 적용하지 아니한다.
5. 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우
6. 범죄 때문에 피해자의 생명이나 신체에 심각한 위험 발생이 예상되는 등 긴급한 상황에서 제5호에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공하는 경우. 이 경우 개인신용정보를 제공받은 검사는 지체 없이 법관에게 영장을 청구하여야 하고, 사법경찰관은 검사에게 신청하여 검사의 청구로 영장을 청구하여야 하며, 개인신용정보를 제공받은 때부터 36시간 이내에 영장을 발부받지 못하면 지체 없이 제공받은 개인신용정보를 폐기하여야 한다.

..... (중간 생략) .....

9. 그 밖에 다른 법률에 따라 제공하는 경우

02 관련 규정의 체계 분석(3)

참고: EU 「개인정보보호규칙(안)」(GDPR)

제6조(처리의 적법성) 1. 개인정보 처리는 다음 중 하나 이상에 해당하는 경우에만 적법하다.

..... (중간 생략) .....

(f) 개인정보처리자가 추구하는 정당한 이익의 목적에 부합하는 경우(정보주체 특히 아동의 이익 또는 기본권리 및 자유가 개인정보처리자의 이익보다 우월한 경우는 제외). 그러나 공공기관이 업무를 수행하는 과정에서 처리하는 개인정보에 대해서는 이 항이 적용되지 아니한다.

..... (중간 생략) .....

4. 개인정보를 추가로 처리하는 목적이 개인정보가 수집된 목적과 일치하지 않는 경우 제1항의 (a)—(e)에서 언급된 근거 중 최소한 하나 이상에 해당되는 법률적 근거를 갖추고 있는 경우에만 개인정보를 처리할 수 있다. 특히 이는 계약 조건이 변경되는 경우 반드시 적용되어야 한다.

02 관련 규정의 체계 분석(4)

(구) 「공공기관의 개인정보 보호에 관한 법률」

제10조 (처리정보의 이용 및 제공의 제한) ① 보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니 된다.

② 보유기관의 장은 보유목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한하여야 한다.

③ 보유기관의 장은 제1항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다.

1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조에 따른 공공기관개인정보보호심의위원회의 심의를 거친 경우

..... (중간 생략) .....

6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우

..... (이하 생략) .....

02 관련 규정의 체계 분석(5)

관련 규정의 체계적 특수성

- 「개인정보 보호법」상 범죄 수사 목적 등을 위한 개인정보의 목적 외 이용 및 제공 규정은 다른 법률 및 입법례와는 달리 매우 광범위한 예외를 설정하고 있음
  - ✓ 이는 기본적으로 (구)「공공기관의 개인정보 보호에 관한 법률」의 취지와 내용을 그대로 옮겨온 것이라고 판단됨

동법상 제약규정: 「개인정보 보호법」

> **제18조(개인정보의 목적 외 이용 · 제공 제한)** ⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

03 판례의 검토

03 사례의 검토(1)

개인정보자기결정권

➢ 헌재 2005. 5. 26. 99헌마513, 2004헌마190(병합)

개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.

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.

03 사례의 검토(2)

개인정보자기결정권의 제한

➢ 헌재 2005. 5. 26. 99헌마513, 2004헌마190(병합)

개인정보자기결정권에 대한 제한은 헌법 제37조 제2항에서 규정하고 있는 국가의 안전보장, 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 명확히 규정한 경우에만 가능하며 그 경우 개인의 인격자체를 훼손시키는 것과 같이 본질적인 내용은 결코 침해할 수 없다. ..... (중간 생략) ..... 특히 고도정보화사회에서 정보를 통한 타인이나 사회세력, 국가권력에 의한 지배는 헌법상 허용되지 아니하며, 그것을 허용하는 경우에는 인간의 존엄과 가치와 개인 인격의 자유로운 발현은 도저히 확보될 수 없는 것이다.

그런데 이 사건에서 문제되고 있는 개인의 지문정보는 만인부동 · 종생불변의 특징을 지니고 있기 때문에 개인의 고유성 · 동일성을 나타내는 중요한 정보이다. ..... (중간 생략) ..... 고도정보화사회에서는 특히 다음과 같은 점에서 지문정보의 오 · 남용으로 인해 국민 개인의 기본적 인권이 침해될 가능성이 크다고 할 수 있다.

03 사례의 검토(3)

수사를 위한 개인정보 목적 외 활용 의 정당화(1)

➢ 헌재 2005. 5. 26. 99헌마513, 2004헌마190(병합)

같은 법(공공기관의개인정보보호에관한법률) 제5조 및 제10조 제2항 제6호는 그 규정취지가 기본권침해의 우려가 매우 큰 개인정보화일의 경우에도 그것이 소관업무를 수행하기 위하여 필요한 범위 안에서는 그 보유를 허용하고, 그것이 범죄수사를 위한 것이라면 다른 기관에 제공하는 것을 허용하고자 하는 것으로 볼 수 있으므로, 그보다 기본권침해의 우려가 덜하다고 할 수 있는 일반문서에 의한 개인정보의 경우에도 같은 범위와 목적 하에서 당연히 그 보유 및 제공을 허용하는 취지로 보아야 할 것이다.

따라서 같은 법 제10조 제2항 제6호는 컴퓨터에 의하여 이미 처리된 개인정보뿐만 아니라 컴퓨터에 의하여 처리되기 이전의 원 정보자료 자체도 경찰청장이 범죄수사목적을 위하여 다른 기관에서 제공받는 것을 허용하는 것으로 해석되어야 하고, ... (중간 생략) ..... 주민등록법시행규칙 제9조가 시장 · 군수 또는 구청장은 주민등록증발급신청서를 관할 경찰서의 파출소장에게 송부하여야 한다고 규정하고 있는 것도 같은 맥락으로 볼 수 있다.

그렇다면 경찰청장이 청구인 오○익 등의 지문정보를 보관하는 행위는 공공기관의개인정보보호에관한법률 제5조, 제10조 제2항 제6호에 근거한 것으로 볼 수 있다.

03 사례의 검토(3)

수사를 위한 개인정보 목적 외 활용 의 정당화(2)

➢ 헌재 2005. 5. 26. 99헌마513, 2004헌마190(병합)

범죄자 등 특정인의 지문정보만 보관해서는 17세 이상 모든 국민의 지문정보를 보관하는 경우와 같은 수준의 신원확인기능을 도저히 수행할 수 없는 점, ... (중간 생략) ..... 다른 여러 신원확인수단 중에서 정확성 · 간편성 · 효율성 등의 종합적인 측면에서 현재까지 지문정보와 비견할만한 것은 찾아보기 어려운 점 등을 고려해 볼 때, 이 사건 지문날인제도는 피해 최소성의 원칙에 어긋나지 않는다.

이 사건 지문날인제도로 인하여 정보주체가 현실적으로 입게 되는 불이익에 비하여 경찰청장이 보관 · 전산화하고 있는 지문정보를 범죄수사활동, 대형사건사고나 변사자가 발생한 경우의 신원확인, 타인의 인적사항 도용 방지 등 각종 신원확인의 목적을 위하여 이용함으로써 달성할 수 있게 되는 공익이 더 크다고 보아야 할 것이므로, 이 사건 지문날인제도는 법익의 균형성의 원칙에 위배되지 아니한다.

결국 이 사건 지문날인제도가 과잉금지의 원칙에 위배하여 청구인들의 개인정보자기결정권을 침해하였다고 볼 수 없다.

04 입법상 문제점

04 입법상 문제점(1)

고려해야 할 쟁점

➢ **법률유보 및 명확성 원칙**

✓ 가장 논리적인 결론은 모든 개인정보에 대하여 그 수집 및 처리 등에 관한 법률적 근거를 구체적이고 명확히 하도록 하는 것임(권헌영, 2007)

✓ 규범명확성 원칙은 해당 법규정으로부터 정보주체가 법적상황을 인식하고 이에 따라 자기의 행동을 준비할 수 있도록 하기 위한 법적 근거를 마련하라는 입법자에 대한 요구이며, 이에 따라 규범명확성원칙은 정보주체에게 국가정보처리의 투명성을 확실한 정도로 보장함(김일환, 2012)

➢ **목적구속의 원칙**

✓ 원래 목적과는 다른 목적의 개인정보 이용 및 처리는 매우 제한된 범위 내에서만 인정되는 또 다른 법률상 근거를 필요로 하는 새로운 기본권 제한임(권헌영, 2007 / 김일환, 2012)

04 입법상 문제점(2)

「주민등록법」

제1조(목적) 이 법은 시(특별시 · 광역시는 제외하고, 특별자치도는 포함한다. 이하 같다) · 군 또는 구(자치구를 말한다. 이하 같다)의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것을 목적으로 한다.

제24조(주민등록증의 발급 등) ②주민등록증에는 성명, 사진, 주민등록번호, 주소, 지문(指紋), 발행일, 주민등록기관을 수록한다. 다만, 혈액형에 대하여는 대통령령으로 정하는 바에 따라 주민의 신청이 있으면 추가로 수록할 수 있다.

「개인정보 보호법」

제25조(영상정보처리기기의 설치 · 운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치 · 운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집 · 분석 및 제공을 위하여 필요한 경우

04 입법상 문제점(3)

「형의 실효 등에 관한 법률」(1)

제5조(수사자료표) ① 사법경찰관은 피의자에 대한 수사자료표를 작성하여 경찰청에 송부하여야 한다. 다만, 다음 각 호의 자에 대하여는 그러하지 아니하다.
1. 즉결심판(卽決審判) 대상자
2. 사법경찰관이 수리(受理)한 고소 또는 고발 사건 중 불기소처분 사유에 해당하는 사건의 피의자

② 수사자료표를 작성할 사법경찰관의 범위는 대통령령으로 정한다.

제5조의2(수사자료표의 관리 등) ① 경찰청장은 수사자료표의 보존 · 관리를 위하여 책임자를 지정하여야 한다.
② 경찰청장은 수사자료표를 범죄경력자료와 수사경력자료로 구분하여 전산입력한 후 관리하여야 한다.
③ 범죄경력조회 또는 수사경력조회에 대하여 회보할 때에는 그 용도, 작성자 · 조회자의 성명 및 작성일시, 그 밖에 필요한 사항을 구체적으로 밝혀야 한다.

04 입법상 문제점(4)

「형의 실효 등에 관한 법률」(2)

제6조(범죄경력조회 · 수사경력조회 및 회보의 제한 등) ① 수사자료표에 의한 범죄경력조회 및 수사경력조회와 그에 대한 회보는 다음 각 호의 어느 하나에 해당하는 경우에 그 전부 또는 일부에 대하여 조회 목적에 필요한 최소한의 범위에서 할 수 있다.
1. 법죄 수사 또는 재판을 위하여 필요한 경우
2. 형의 집행 또는 사회봉사명령, 수강명령의 집행을 위하여 필요한 경우
3. 보호감호, 치료감호, 보호관찰 등 보호처분 또는 보안관찰업무의 수행을 위하여 필요한 경우
4. 수사자료표의 내용을 확인하기 위하여 본인이 신청하는 경우
5. 「국가정보원법」 제3조제2항에 따른 보안업무에 관한 대통령령에 근거하여 신원조사를 하는 경우
6. 외국인의 체류허가에 필요한 경우
7. 각군 사관생도의 입학 및 장교의 임용에 필요한 경우
8. 병역의무 부과와 관련하여 면역병 및 사회복무요원의 입영(入營)에 필요한 경우
9. 다른 법령에서 규정하고 있는 공무원 임용, 인가 · 허가, 서훈(敍勳), 대통령 표창, 국무총리 표창 등의 결격사유 또는 공무원연금 지급 제한 사유 등을 확인하기 위하여 필요한 경우
10. 그 밖에 다른 법률에서 범죄경력조회 및 수사경력조회와 그에 대한 회보를 하도록 규정되어 있는 경우

② 수사자료표를 관리하는 사람이나 직무상 수사자료표에 의한 범죄경력조회 또는 수사경력조회를 하는 사람은 그 수사자료표의 내용을 누설하여서는 아니 된다.
③ 누구든지 제1항에서 정하는 경우 외의 용도에 사용할 목적으로 범죄경력자료 또는 수사경력자료를 취득하여서는 아니 된다.
④ 제1항에 따라 범죄경력자료 또는 수사경력자료를 회보받거나 취득한 자는 법령에 규정된 용도 외에는 이를 사용하여서는 아니 된다.
⑤ 제1항 각 호에 따라 범죄경력조회 및 수사경력조회와 그에 대한 회보를 할 수 있는 구체적인 범위는 대통령령으로 정한다.

04 입법상 문제점(5)

「형의 실효 등에 관한 법률」(3)

제8조의2(수사경력자료의 정리) ① 다음 각 호의 어느 하나에 해당하는 경우에는 제2항 및 제3항 각 호의 구분에 따른 보존기간이 지나면 전산입력된 수사경력자료의 해당 사항을 삭제한다.
1. 검사의 혐의없음, 공소권없음, 죄가안됨 또는 기소유예의 불기소처분이 있는 경우
2. 법원의 무죄, 면소(免訴) 또는 공소기각의 판결이 확정된 경우
3. 법원의 공소기각 결정이 확정된 경우

② 제1항 각 호의 경우에 대한 수사경력자료의 보존기간은 다음 각 호의 구분에 따른다. 이 경우 그 기간은 해당 처분이 있거나 결정 또는 판결이 확정된 날부터 기산(起算)한다.
1. 법정형(法定刑)이 사형, 무기징역, 무기금고, 장기(長期) 10년 이상의 징역 · 금고에 해당하는 죄: 10년
2. 법정형이 장기 2년 이상의 징역 · 금고에 해당하는 죄: 5년
3. 법정형이 장기 2년 미만의 징역 · 금고, 자격상실, 자격정지, 벌금, 구류 또는 과료에 해당하는 죄: 즉시 삭제. 다만, 제1항제1호의 기소유예 처분이나 제1항제2호 · 제3호의 판결 또는 결정이 있는 경우는 5년간 보존한다.

04 입법상 문제점(6)

개인정보 보호법령 및 지침·고시 해설(행안부)

[범죄수사, 공소제기 및 유지를 위한 경우의 예외 및 한계 필요성](109면)

범죄수사 등을 위한 경우라 하더라도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우에는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 없음

- 입법적 차원의 규율 가능성 과 방식은?

들어주셔서 감사합니다

토론

- 권헌영 (광운대학교 과학기술법학과 교수)
- 이항우 (충북대학교 사회학과 교수)
- 강장묵 (고려대학교 정보창의연구소 교수)
- 이창범 (녹색소비자연대 이사)
- 최성진 (인터넷기업협회 사무국장)
- 이병선 (다음카카오 대외협력파트 이사)

수사기관의 개인정보 수집 관련 제도 개선 토론문

광운대학교 과학기술법학과 교수 권헌영

MEMO

MEMO

수사기관의 개인정보 수집 관련 제도 개선 토론문

충북대학교 사회학과 교수 이항우

MEMO

MEMO

수사기관의 개인정보 수집 관련 제도 개선 토론문

고려대학교 정보창의연구소 교수 강장묵

MEMO

MEMO

수사기관의 개인정보 수집 관련 제도 개선 토론문

녹색소비자연대 이사 이창범

MEMO

MEMO

수사기관의 개인정보 수집 관련 제도 개선 토론문

인터넷기업협회 사무국장 최성진

MEMO

MEMO

수사기관의 개인정보 수집 관련 제도 개선 토론문

다음카카오 대외협력파트 이사 이병선

MEMO

MEMO

수사기관의 개인정보 수집 관련 제도 개선 토론회

인 쇄 : 2014년 12월
발 행 : 2014년 12월

발행처 : 국가인권위원회
주 소 : (100-842) 서울특별시 중구 무교동길 41 금세기B/D
(을지로1가 16번지)
전 화 : 02) 2125-9759 FAX : 02) 2125-9733
Homepage : www.humanrights.go.kr

인쇄처 : 경성문화사 (02) 786-2999)

ISBN 978-89-6114-393-6-93360

수사기관의 개인정보 수집 관련 제도 개선 토론회

국가인권위원회

100-842 서울시 중구 무교로 6 (을지로 1가) 금세기빌딩
02-2125-9700

ISBN 978-89-6114-393-6-93360