정보보호를 위한 정보공유 법정책* **

- 현황과 개선방안 -

양 천 수***

I. 서 론

현대 지능정보사회에서는 사물인터넷 등을 통해 초연결사회가 구현되면서 세상의 모든 것이 연결되고, 이로 인해 과거에는 상상할 수 없을 정도로 엄청난 양의 정보가 생성 및 축적되는 빅데이터 사회가 실현되고 있다.[1] 이러한 지능정보사회에서는 한편으로는 사이버 보안이 침해될 가능성이 그 만큼 높아지고 있다. 초연결사회가 구현되면서 스마트폰과 같은 개인 소유 사물인터넷을 해킹하는 것만으로도 전체 인터넷 연결망의 보안을 손쉽게 침해할 수 있게 된 것이다. 그러나 다른 한편으로는 엄청난 빅데이터로 축적되는 정보를 분석함으로써 과거에는 존재하지 않았던 새로운 시각이나 통찰, 사회적 공리를 획득할 수 있게 되었다.[2] 바로 이 때문에 정보를 빅데이터로 축적하는 것이 그 무엇보다 중요해지고, 또한 이렇게 축적된 빅데이터를 다양한 방식으로 공유하는 것 역시 그 만큼 중요해지고 있다. 빅데이터로서 축적된 정보를 다양한 주체가 공유함으로써 새로운 시각이나 통찰 그리고 사회적 공리를 창출

* 투고일자 : 2018. 5. 31. 심사일자 : 2018. 6. 15. 게재확정일자 : 2018. 6. 17.

** 이 글은 필자가 참여한 연구보고서 『안전한 지능정보사회 구축을 위한 정보보호관련 법제도 개선방안 연구』(과학기술정보통신부, 2018)에서 필자가 집필한 부분을 일부 바탕으로 하여 이를 대폭 수정 및 보완한 것입니다.

*** 영남대학교 법학전문대학원 교수・법학박사

1) 현대 초연결사회 및 빅데이터에 관해서는 양천수, 『빅데이터와 인권: 빅데이터와 인권의 실제적 조화를 위한 법정책적 방안』(영남대학교출판부, 2016); 양천수, 『제4차 산업혁명과 법』(박영사, 2017) 등 참고.

2) 이를 보여주는 연구로는 빅토르 마이어 쇤베르거・케네스 쿠키어, 이지연 (옮김), 『빅데이터가 만드는 세상』(21세기북스, 2013) 참고.

할 수 있는 가능성도 그 만큼 제고될 수 있기 때문이다. 이는 정보보호에 대해서도 그대로 적용할 수 있다. 정보보호와 관련된 정보를 빅데이터로 축적하고 이를 정보보호와 관련된 주체나 거버넌스가 공유할 수 있도록 함으로써 정보보호에 필요한 새로운 시각이나 통찰 혹은 방법을 획득할 수 있는 것이다. 이러한 맥락에서 정보공유는 지능정보사회에 대응하는 정보보호 관련 제도 및 방법을 구현하는 데 중요한 방법이 될 수 있다. 달리 말해, 현대 초연결사회에서는 정보공유가 정보보호를 실현할 수 있는 중요한 방법이 되고 있는 것이다. 이러한 맥락에서 이 글에서는 현행 정보보호 관련 법체계가 마련하고 있는 정보공유제도의 현황과 문제점을 검토하면서, 이를 어떻게 개선하는 것이 바람직한지 살펴보고자 한다.

II. 정보공유 일반론

본격적인 논의를 하기 전에 정보 및 정보공유가 현대사회에서 어떤 의미를 갖는지 살펴보도록 한다.

1. 현대사회에서 정보의 의의

(1) 인식의 원천으로서 정보

'정보'(information)는 인식의 원천이 된다. 왜냐하면 정보는 의미의 기본단위이기 때문이다. 정보가 존재해야만 비로소 우리는 그 무엇인가를 의미 있는 것으로 인식할 수 있다. 현대 체계이론(Systemtheorie)의 관점에서 보면, 정보는 '구별'에 기반을 둔다.[3] 우리가 특정한 기준에 따라 인식대상을 구별함으로써 비로소 정보가 형성된다는 것이다. 달리 말해, 정보는 구별이라는 틀을 필요로 한다. 사실 이러한 관념은 이미 '개념'이라는 말에서 확인할 수 있다. 특정한 개념을 만들어가는 과정 자체가 이러한 개념에 속하는 것과 속하지 않는 것을 구별하는 과정이기 때문이다. 예를 들어, 우리가 '법'이라는 개념을 설정하면, 이러한 법 개념을 통해 법인 것과 법이 아닌 것을 구별할 수 있게

3) 체계이론에 관해서는 우선 N. Luhmann, *Soziale Systeme* (Frankfurt/M., 1984) 참고.

된다.

한편 이러한 정보와 구별해야 할 개념이 있다. '데이터'(data)가 그것이다. 흔히 정보와 데이터는 혼용되는 경우가 많다. 양자가 거의 같은 의미를 갖기 때문이다. 다만 양자의 관계를 엄밀하게 살펴볼 때, 가령 무엇이 더욱 근원적인 것인가를 논의할 때 견해가 대립한다.[4] 이에 관해서는 정보를 더욱 근원적인 것으로 파악하는 견해도 있지만, 일반적으로는 데이터를 가장 근원적인 개념으로 파악한다. 데이터가 정보를 구성한다는 것이다. 이에 따르면, 빅데이터를 구축한 후 '데이터 마이닝'(data mining)을 통해 이를 분석하면 과거에는 알지 못했던 유의미한 정보가 도출된다.[5] 이를테면 독감에 관한 검색어를 빅데이터로 구축한 후 이를 수학적 알고리즘에 바탕을 둔 데이터 마이닝을 통해 분석하면, 언제 어디서 독감이 유행할 지를 예측할 수 있는 정보를 획득할 수 있는 것이다.[6] 이때 데이터 마이닝이란 빅데이터에 대한 구별방법이라고 할 수 있으므로, 이는 다음과 같이 재해석할 수 있다. 빅데이터를 어떤 데이터 마이닝을 통해 구별하는가에 따라 각기 다양한 정보가 도출될 수 있다는 것이다.

(2) 소통의 기본단위로서 정보

정보는 현대 초연결사회에서 중요한 소통의 기본단위이자 기초가 된다. 이는 체계이론이 분명하게 보여준다. 체계이론에 따르면, 소통(Kommunikation)은 '정보'(Information), '통지'(Mitteilung), '이해'(Verstehen)로 구성된다.[7] 정보가 통지를 통해 상대방에게 전달되고, 이렇게 전달된 정보가 상대방에 의해 이해됨으로써 소통이 이루어진다는 것이다. 여기서 알 수 있듯이, 정보는 소통의 출발점이자 기초가 된다. 체계이론에 따르면, 이러한 소통이 이루어져야 비로소 현대사회를 구성하는 '사회적 체계'(soziale Systeme)가 형성 및 작동할 수 있다. 사회적 체계는 소통으로 구성되기 때문이다. 이렇게 보면, 현대사

---

4) 양자의 관계에 관해서는 윤지영・이천현・최민영・윤재왕・전지연, 『법과학을 적용한 형사사법의 선진화 방안(IV)』(한국형사정책연구원, 2014), 54쪽; Marion Albers, *Informationelle Selbstbestimmung* (Baden-Baden, 2005), 87쪽 아래 등 참고

5) '데이터 마이닝'에 관해서는 정용찬, 『빅데이터』(커뮤니케이션북스, 2013), 42쪽 아래 참고.

6) 빅토르 마이어 쇤베르거・케네스 쿠키어, 앞의 책, 10쪽 참고.

7) 게오르그 크네어・아민 낫세이, 정성훈 (옮김), 『니클라스 루만으로의 초대』(갈무리, 2008), 114쪽 참고.

회에서 정보는 사회적 체계가 형성되고 작동하는 데 대한 출발점이 된다.

(3) 권력의 원천으로서 정보

예전부터 정보는 권력의 원천으로 기여하였다. 더 많은 정보를 갖는 자가 더 많은 권력을 누리는 경우가 많았다. 그 때문에 정보기관은 오랜 동안 핵심 권력기관으로 작동하였다. 이는 현재 우리나라에서 국가정보원이 갖는 위상이 잘 보여준다. 이처럼 정보는 권력의 원천이 되었기에 정보를 공유하는 것보다 정보를 독점하고자 하는 경향이 더 강하였다. 정보를 공유하는 것은 곧 권력을 공유 또는 약화시키는 것이라고 여겼기 때문이다. 그러나 정보를 독점함으로써 권력을 강화하고자 하는 것은 오늘날의 초연결사회와는 맞지 않는다. 모든 것이 연결되는 현대 초연결사회에서는 정보를 독점하겠다는 것 자체가 불가능한 발상이기 때문이다.

(4) 현대사회에서 정보가 갖는 의미

이렇게 인식과 권력의 원천이자 소통의 출발점이 되는 정보의 의미는 현대사회에서 더욱 강화되고 있다. '빅데이터 사회'나 '지능정보사회'라는 개념이 시사하는 것처럼, 현대사회에서 정보는 그 무엇보다 중요한 자원이자 성장동력이 되고 있다. 빅데이터를 다양한 구별방식으로 분석함으로써 이전에는 생각하기 힘들었던 다양한 통찰과 사회적 공리를 획득하고 있기 때문이다. 또한 주식시장과 같은 각종 금융시장이나 부동산시장 등이 잘 보여주는 것처럼, 정보는 유용한 경제적 자원이 되고 있다. 정보가 새로운 부의 창출로 이어지고 있는 것이다. 이뿐만 아니라, 정보는 현대 안전사회를 구현하는 데 중요한 기초가 된다.[8] 각종 재난이나 범죄에 대한 빅데이터를 구축함으로써 재난이나 범죄를 사전에 효과적으로 예측 및 예방할 수 있는 것이다. 이러한 이유에서 정보기관뿐만 아니라 경찰이나 검찰도 더 많은 정보를 획득하기 위해 노력하고 있는 것이다.

---

8) 안전사회에 관해서는 양천수, "현대 안전사회와 법적 통제: 형사법을 예로 하여", 『안암법학』 제49호(2016. 1), 81-127쪽 참고.

2. 현대사회에서 정보공유의 의의

(1) 현대사회에서 정보공유의 의의

이처럼 현대사회에서 정보의 의미가 그 무엇보다 중요해지면서 정보를 공유하고자 하는 경향이 점점 더 강해지고 있다. 이른바 '정보민주주의'에 의해 정보독점이 비판되고, 정보를 공개하고 공유하려는 경향 및 요청이 늘어나고 있는 것이다. 법체계 역시 이를 법적으로 뒷받침한다. 이를테면 「정보공개법」이나 「전자정부법」 등이 공공정보에 대한 공개와 공유를 법적으로 근거 짓는다. 정보를 공개하고 공유하는 것이 현대 민주주의 원리에 부합할 뿐만 아니라, 이렇게 하는 것이 사회적 공리를 증진시키는 데 더 적합하기 때문이다. '정보독점에서 정보공유로', 이것이 바로 현대사회를 대변하는 표어인 셈이다.

(2) 빅데이터 형성 및 이용으로서 정보공유

사물인터넷 등을 통해 모든 것이 연결되는 현대 초연결사회에서 정보공유는 더욱 특별한 의미를 갖는다. 현대 초연결사회에서 정보공유는 바로 빅데이터를 형성하고 이를 이용한다는 의미를 담고 있기 때문이다. 인터넷을 통해 모든 것이 연결되는 초연결사회가 구현되면서 사회의 거의 모든 영역에서 엄청난 데이터가 축적되고 있다. 정보공유를 통해 이러한 데이터를 공유하게 되면 자연스럽게 엄청난 양의 빅데이터가 형성될 수 있다. 그리고 데이터 마이닝을 통해 이러한 빅데이터를 분석하면 이전에는 알지 못했던 새로운 정보를 획득할 수 있다. 이 점에서 볼 때 정보공유야말로 현대사회에서 아주 중요한 자원인 빅데이터를 형성하는 데 중요한 방법이 된다.

3. 정보의 유형

정보공유를 인정한다고 해서 모든 정보를 공유할 수 있는 것은 아니다. 이를테면 개인정보는 정보주체의 명시적인 사전동의를 받지 않으면 공유대상이 될 수 없다. 따라서 과연 어떤 정보를 공유대상으로 삼을 수 있을지를 파악하

려면, 정보를 유형화할 필요가 있다. 정보는 다음과 같이 유형화할 수 있다.

(1) 개인정보와 일반정보

먼저 정보는 개인정보와 일반정보로 유형화할 수 있다. 개인정보는 개인적 정보주체와 관련을 맺는 정보를 말한다. 개인정보보호법 제2조 제1호에 따르면, 개인정보란 "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)"를 말한다. 이러한 개인정보에 대해서는 개인정보보호법이 적용되기에, 원칙적으로 정보공유의 대상이 될 수 없다. 이에 대해 일반정보는 이러한 개인정보에 속하지 않는 정보를 말한다. 일반정보, 즉 비개인정보는 개인정보보호법이 적용되지 않으므로 이는 원칙적으로 정보공유의 대상이 된다.

(2) 공공정보와 민간정보

일반정보는 다시 공공정보와 민간정보로 유형화할 수 있다. 「공공기관의 정보공개에 관한 법률」 제2조 제1호에 따르면, 공공정보란 "공공기관이 직무상 작성 또는 취득하여 관리하고 있는 문서(전자문서를 포함한다. 이하 같다)·도면·사진·필름·테이프·슬라이드 및 그 밖에 이에 준하는 매체 등에 기록된 사항"을 말한다. 이때 공공기관이란 「공공기관의 정보공개에 관한 법률」 제2조 제3호에 따르면, 국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제2조에 따른 공공기관, 그 밖에 대통령령으로 정하는 기관을 말한다. 이러한 공공정보 중에서 행정기관이 생성하는 정보를 '행정정보'라고 부른다. 이를테면 「전자정부법」 제2조 제6호에 따르면, 행정정보란 "행정기관등이 직무상 작성하거나 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호, 문자, 음성, 음향, 영상 등으로 표현된 것"을 말한다. 이때 행정기관이란 "국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속기관, 지방자치단체"를 말한다(전자정부법 제2조 제2호). 이러한 공공정보는 「공공기관의 정보공개에 관한 법률」 제3조에 따라 원칙적으로 공개되어야

하고, 「전자정부법」 제4장은 행정정보를 적극적으로 공동이용할 것을 규정한다. 이와 달리 민간정보, 예를 들어 개인기업, 정보통신서비스 제공자 등이 보유하는 정보는 법률에 의해 그 공개나 공유가 강제되지는 않는다.

3. 정보공유의 유형

한편 정보공유는 다음과 같이 유형화할 수 있다.

(1) 공공기관 간 정보공유

첫째는 공공기관 사이에서 이루어지는 정보공유이다. 전자정부법에 의해 이러한 정보공유는 원칙적으로 허용되고 또한 적극 장려된다. 이는 상호적으로 이루어진다.

(2) 공공기관과 민간의 정보공유

둘째는 공공기관과 민간의 정보공유이다. 이는 비상호적으로 이루어진다. 그 이유를 다음과 같이 말할 수 있다. 민간은 「공공기관의 정보공개에 관한 법률」에 따라 공공기관에 정보공개를 청구할 수 있고, 예외사유에 해당하지 않는 한 공공기관은 이에 응해야 한다. 반대로 공공기관이 민간에 정보공개를 요구한다고 해도, 법률에 특별한 사유가 없는 한, 민간이 이에 반드시 응해야 하는 것은 아니다. 양자 사이에서 정보공유가 이루어지려면 원칙적으로 공공기관과 민간이 정보공유에 관해 서로 합의해야 한다.

(3) 민간 간 정보공유

셋째는 민간 사이에서 이루어지는 정보공유이다. 여기에는 '상호성원칙'이 적용된다. 따라서 민간은 자유롭게 정보공유에 합의할 때 비로소 정보공유를 할 수 있다. 이는 법이 강제할 수 없다.

III. 정보공유제도의 현황

1. 법적 근거

현행 법체계는 정보공유를 어떻게 규율하고 있는가? 현재 우리 법체계는 독자적인 법률로써 정보공유를 규율하고 있지는 않다. 각기 다양한 법률에서 단편적으로 이를 규율하고 있을 뿐이다. 이를 아래에서 살펴보도록 한다.

(1) 「공공기관의 정보공개에 관한 법률」

정보공유가 이루어지려면, 먼저 정보가 독점되지 않고 다른 기관이나 주체에게 공개될 수 있어야 한다. 정보가 공개되어야만 비로소 공유될 수 있기 때문이다. 이 점에서 「공공기관의 정보공개에 관한 법률」은 의미가 있다. 왜냐하면 「공공기관의 정보공개에 관한 법률」은 제3조에서 "정보공개의 원칙"이라는 표제 아래 "공공기관이 보유·관리하는 정보는 국민의 알권리 보장 등을 위하여 이 법에서 정하는 바에 따라 적극적으로 공개하여야 한다."고 규정함으로써 공공기관은 같은 법 제9조가 규정하는 비공개정보에 속하지 않는 한 원칙적으로 정보를 공개해야 한다고 선언한다.

(2) 전자정부법

한편 이렇게 공개되는 정보는 다른 기관 등에 의해 공유될 수 있어야 한다. 이러한 정보의 공유 및 이용은 전자정부법이 규율한다. 전자정부법 제4장은 "행정정보의 공동이용"이라는 표제 아래 행정정보를 적극적으로 공유하고 이용할 것을 규율한다. 예를 들어, 전자정부법 제36조는 "행정정보의 효율적 관리 및 이용"이라는 표제 아래 제1항에서 "행정기관등의 장은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관등과 공동으로 이용하여야 하며, 다른 행정기관등으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 같은 내용의 정보를 따로 수집하여서는 아니 된다."고 규정한다. 여기서 알 수 있듯이, 전자정부법 제36조 제1항은 행정기관 간의 정보공유를 규정한

다. 나아가 제2항은 “행정정보를 수집·보유하고 있는 행정기관등의 장은 다른 행정기관등과 「은행법」 제8조 제1항에 따라 은행업의 인가를 받은 은행 및 대통령령으로 정하는 법인·단체 또는 기관으로 하여금 행정정보보유기관의 행정정보를 공동으로 이용하게 할 수 있다.”고 정한다. 제2항에 따르면, 행정정보는 행정기관 사이에서만 공유될 수 있는 것이 아니라, 행정기관과 은행과 같은 비행정기관 사이에서도 공유될 수 있다.

다만 여기서 주의해야 할 점은, 전자정부법이 공유하도록 하는 정보는 행정정보라는 것이다. 행정정보는 행정기관이 생산한 정보로서 공공기관이 생산한 공공정보보다는 그 외연이 좁다. 그 점에서 전자정부법은 정보공유에 관한 기본법으로서 작동하기에는 아직 미흡하다고 말할 수 있다.

(3) 정보통신기반 보호법

미국의 정보공유법이 시사하는 것처럼,[9] 정보공유가 완전하게 이루어지려면 행정기관 간뿐만 아니라 행정기관과 여타 공공기관, 더 나아가 행정기관과 민간 사이에서도 정보공유가 원활하게 이루어질 수 있어야 한다. 이를 가능하게 하려면, 이에 대한 법적 근거 및 이러한 정보공유를 총괄하는 거버넌스가 마련되어야 한다. 하지만 우리 법체계는 아직 이에 관한 충분한 법적 근거를 마련하고 있지 않다. 다만 정보통신기반 보호법은 미흡하지만 정보공유·분석센터에 관한 규정을 두고 있다. 가령 정보통신기반 보호법 제16조는 “정보공유·분석센터”라는 표제 아래 제1항에서 다음과 같이 규정한다.

> ① 금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 각호의 업무를 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다.
> 1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
> 2. 침해사고가 발생하는 경우 실시간 경보·분석체계 운영

나아가 같은 법 제16조 제4항에서는 “정부는 제1항 각호의 업무를 수행하

9) 이에 관해서는 양천수 외, 『안전한 지능정보사회 구축을 위한 정보보호관련 법제도 개선방안 연구』(과학기술정보통신부, 2018) 참고.

는 정보공유·분석센터의 구축을 장려하고 그에 대한 재정적·기술적 지원을 할 수 있다."고 정한다.

이러한 규정들은 다음과 같은 시사점을 제공한다. 첫째, 정보공유·분석센터는 금융, 통신과 같은 정보통신기반시설을 보호하는 것을 목표로 한다는 것이다. 둘째, 정보공유·분석센터는 해당 정보통신기반시설의 취약점, 이에 대한 침해요인 및 그 대응방안에 관한 정보를 제공하고, 해당 정보통신기반시설에 대한 침해사고가 발생하는 경우 이에 대한 실시간 경보 및 분석체계를 운영하는 업무를 수행한다는 것이다. 셋째, 정보공유·분석센터를 운용하는 주체는 해당 정보통신기반시설을 운영 및 관리하는 주체가 된다는 점이다. 따라서 공공기관뿐만 아니라 민간기관 역시 정보공유·분석센터를 운용할 수 있다. 넷째, 정부는 정보공유·분석센터를 구축 및 운용하는 자에게 재정적·기술적 지원을 할 수 있다는 것이다.

그렇지만 여기에는 다음과 같은 문제가 있다. 첫째, 정보공유·분석센터에 관한 규정은 단 한 개 조문만으로 이루어져 있어 너무 빈약하다는 점이다. 둘째, 각 정보통신기반시설을 중심으로 하여 구축 및 운용되는 정보공유·분석센터를 총괄할 수 있는 거버넌스가 명확하지 않다는 점이다. 셋째, 각 정보공유·분석센터 사이에서 정보공유가 이루어질 수 있는지, 만약 이루어질 수 있다면 이는 어떻게 가능할 수 있는지 등에 관해 명확한 법적 근거가 없다는 점이다.

(4) 국가사이버안보법안

지난 2017년 1월 3일 정부가 제안한 「국가사이버안보법안」은 정보공유에 관해 상당히 의미 있는 규정을 두고 있다. 물론 이 법안은 여러 비판을 받았고, 아직 법률로 제정되지 못하고 있다. 그렇지만 이 법안이 제시하는 규정들은 그 비판여부에 상관없이 살펴볼 만한 가치가 있다. 특히 정보공유에 관해 비교적 상세한 규정을 마련함으로써 정보공유제도가 어떤 방향으로 나아가야 할지에 대해 비판적인 시사점을 제공한다.

우선 국가사이버안보법안은 "국가안보를 위협하는 사이버공격을 예방하고, 사이버위기에 신속하고 적극적으로 대처함으로써 국가의 안전 보장 및 국민의 이익 보호에 이바지함을 목적으로 한다."(제1조) 여기서 알 수 있듯이, 국

가사이버안보법안이 직접적인 예방대상으로 삼는 것은 “국가안보를 위협하는 사이버공격”이다. 이 점에서 국가사이버안보법안이 모든 정보보안 침해행위를 대상으로 하는 것은 아니다. 다만 실제적으로는 “국가안보를 위협하는 사이버공격”의 범위를 어떻게 설정해야 할지 문제가 될 수 있다.

한편 정보공유에 관해 국가사이버안보법안은 제12조에서 “사이버위협정보의 공유”라는 표제 아래 모두 여섯 항으로 구성된 비교적 상세한 규정을 두고 있다.

> ① 다음 각 호의 정보를 공유하기 위하여 국가정보원장 소속으로 사이버위협정보 공유센터를 둔다.
> 1. 사이버공격 방법에 관한 정보
> 2. 악성프로그램 및 이와 관련된 정보
> 3. 정보통신망, 정보통신기기 및 소프트웨어의 보안상 취약점에 관한 정보
> 4. 그 밖에 사이버공격의 예방을 위한 정보
> ② 책임기관의 장은 소관 사이버공간의 제1항에 따른 정보(이하 “위협정보”라 한다)가 다른 책임기관의 사이버안보를 위하여 필요하다고 인정하는 경우 대통령령으로 정하는 바에 따라 소관 사이버공간의 위협정보를 제1항에 따른 사이버위협정보 공유센터(이하 “공유센터”라 한다)의 장에게 제공할 수 있다. 이 경우 공유센터의 장은 사이버안보를 위하여 위협정보의 공유가 필요하다고 판단되는 책임기관의 장에게 위협정보를 제공하여야 한다.
> ③ 누구든지 제2항에 따라 공유된 위협정보를 사용할 때에는 사이버안보 목적에 필요한 최소한의 범위에서 사용·관리하여야 한다.
> ④ 공유센터의 장은 위협정보를 공유하는 경우 국민의 권리가 침해되지 아니하도록 기술적·관리적 또는 물리적 보호조치를 마련하여야 한다.
> ⑤ 공유센터의 장은 제4항에 따른 기술적·관리적 또는 물리적 보호조치에 관한 사항을 심의하기 위하여 책임기관 및 민간 전문가 등이 참여하는 사이버위협정보 공유협의회를 구성·운영하여야 한다.
> ⑥ 제1항부터 제5항까지의 규정에 따른 공유센터의 설치·운영, 공유센터의 장에게 제공하는 위협정보의 범위 등에 필요한 사항은 대통령령으로 정한다.

이 규정에서 크게 세 가지 의미 있는 사항을 발견할 수 있다. 첫째, 독자적인 사이버위협정보 공유센터를 설치한다는 것이다. 둘째, 이러한 사이버위협정보 공유센터를 국가정보원장 소속으로 설치한다는 것이다. 셋째, 사이버위협정보 공유센터와 책임기관 사이에 상호적인 정보공유를 인정한다는 것이다. 이렇게 볼 때, 국가사이버안보법안이 마련하고 있는 정보공유 규정은 꽤 진일보한 것이라고 평가할 수 있다. 다만 이 법안이 아직 법률로 제정되지 못하고 있다는 점, 사이버위협정보 공유센터는 '국가안보를 위협하는 사이버공격'에 관한 정보를 대상으로 한다는 점에서 정보공유에 관한 원칙적인 규정이 될 수 없다.

IV. 정보공유제도 개선방안

1. 문제점

이처럼 현행 법체계가 마련하고 있는 정보공유제도를 살펴보면, 여러 측면에서 문제점이 보인다. 이는 크게 세 가지로 말할 수 있다. 먼저 정보공유에 관한 법적 근거가 너무 빈약하다는 것이다. 앞에서 검토한 것처럼, 현행 법체계는 정보공유를 법적으로 뒷받침하는 법적 근거를 충분하게 확보하지 못하고 있다. 이는 독자적인 정보공유법을 제정 및 시행하고 있는 미국과 비교할 때 큰 차이가 있는 부분이다. 다음으로 정보공유를 총괄할 수 있는 거버넌스가 아직 없다는 것이다. 마지막으로 어떤 원칙에 의해 그리고 어떤 방법으로 정보공유를 실행할 것인지가 명확하지 않다는 것이다. 현대 지능정보사회에 맞게 정보공유를 실현하려면 이러한 문제점을 해소할 필요가 있다.

2. 기본원칙

정보공유를 법제화하는 경우에는 다음과 같은 원칙을 준수해야 한다.

(1) 상호성 원칙

첫째, 정보공유는 상호성 원칙에 따라 이루어져야 한다. 말하자면 정보는 상호적으로 공유되어야 한다. 어느 한 쪽이 다른 한 쪽으로부터 정보를 받으면서도 반대로 정보를 제공하지 않는 것은 상호성 원칙에 반하는 것으로서 바람직하지 않다. 특별한 사유가 없는 한 정보는 상호적으로 공유되어야 한다.

(2) 자발성 원칙

둘째, 정보공유는 자발성 원칙에 따라 이루어져야 한다. 이는 특히 공공기관과 민간 사이에서 정보공유가 이루어질 때 적용된다. 공공기관 사이에서는, 무엇보다 행정기관 사이에서는 전자정부법에 따라 정보공유가 이루어지기 때문에 별도의 합의가 필요 없는 경우가 많다. 그렇지만 공공기관과 민간 사이의 정보공유를 강제하는 법적 근거는 아직 없기에 두 주체 사이에서 정보공유가 이루어지려면 원칙적으로 자발적인 합의가 있어야 한다. 그렇게 해야만 비로소 상호적인 정보공유도 실현될 수 있다.

(3) 개인정보보호 원칙

셋째, 정보공유는 개인정보를 보호하면서 이루어져야 한다. 이를 위해 다음 세 가지 방법을 사용해야 한다. 우선 개인정보가 아닌 비개인정보, 즉 일반정보가 공유대상이 되어야 한다. 다음으로 개인정보를 공유하고자 하는 경우에는 개인정보보호법에 따라 정보주체의 명시적인 사전동의를 받아야 한다. 마지막으로 정보주체의 사전동의를 받기 어려운 경우에는 익명화조치를 통해 개인정보를 비개인정보로 바꾸어 공유해야 한다.

(4) 목적구속성 원칙

넷째, 정보공유는 본래 설정된 목적에 적합하게 이루어져야 한다. 이 경우에는 지능정보사회에서 정보보호를 효과적으로 실현하기 위해 정보공유를 하는 것이므로, 정보보호가 아닌 다른 목적으로 정보를 공유하는 것은 허용될

수 없다.

(5) 비례성 원칙

다섯째, 정보공유는 비례성 원칙을 준수해야 한다. 이는 무엇보다도 개인정보를 공유할 때 적용된다. 개인정보를 공유할 때 비례성 원칙, 즉 적합성 원칙, 필요성 원칙, 상당성 원칙을 준수해야 한다.

3. 개선방안

지능정보사회에 대응하는 정보공유를 실현할 수 있도록 정보공유제도를 다음과 같이 개선해야 한다.[10]

(1) 독자적인 법적 근거 마련

가장 먼저 정보공유에 대한 충분한 법적 근거를 마련해야 한다. 제일 이상적인 방법은 미국처럼 독자적인 정보공유법을 제정 및 시행하는 것이다. 그게 어렵다면, 일단 정보통신기반 보호법을 개정하여 정보공유에 관한 독자적인 장을 만들 필요가 있다. 현재는 한 개 조문으로 정보공유·분석센터를 규율하는데, 이는 지능정보사회에 대응하는 정보공유제도를 실현하는 데 부족하다. 앞으로 정보통신기반 보호법을 개정하여 정보공유에 관한 부분을 대폭 확충할 필요가 있다.

(2) 독자적인 거버넌스 구축

다음으로 각 영역별로 존재하는 정보공유 및 분석센터를 총괄하는 독자적인 거버넌스를 구축할 필요가 있다. 이는 크게 두 가지 방안으로 실현할 수 있다. 첫째는 독일의 경우처럼 정보보호 업무를 총괄하는 독자적인 정보보호

---

10) 정보공유제도 개선 일반에 관해서는 윤광석, “행정정보공동이용제도의 개선방안에 관한 연구”, 『정보화정책』 제19권 제4호(2012. 겨울); 강성용·이성기·박형식, “효율적 범죄 수사 지원을 위한 금융정보분석원 개선 방안 연구”, 『경찰학연구』 제12권 제2호(2012. 6); 표경수, “재난안전정보 수집·공유를 위한 법제도 개선 방안』 제678호(2017. 9) 등 참고.

청을 신설하여 이러한 정보보호청이 각 정보공유·분석센터를 총괄하도록 하는 것이다. 둘째는 과학기술정보통신부장관 소속으로 정보보호를 위한 정보공유·분석센터를 설치하여 이를 통해 각 정보공유·분석센터를 총괄하도록 하는 것이다.

(3) 공공기관과 민간의 정보공유 강화

이어서 공공기관과 민간의 정보공유를 강화할 필요가 있다. 이는 정보공유 관련 법령에 명시하는 것이 바람직하다. 특히 정보보호에 효과적인 관련 제품을 생산할 수 있도록 공공기관이 정보보호 관련 정보를 적극적으로 민간에 제공하고, 반대로 민간이 정보보호에 관해 획득한 노하우를 공공기관에 제공할 수 있도록 유도해야 한다. 물론 이 경우에 상호성 원칙과 자발성 원칙이 적용되어야 한다.

(4) 정보공유 프로그램 개발

나아가 적시에 정보공유를 실행할 수 있도록 미국처럼 정보공유 전문프로그램을 개발하여 운용할 필요가 있다. 전통적인 방식으로 정보를 주고받는 경우에는 제때에 필요한 정보를 획득하지 못할 수 있다. 따라서 실시간으로 정보를 공유할 수 있도록 전문프로그램을 개발 및 가동해야 한다. 이러한 프로그램에 접속하는 것만으로도 정보공유가 이루어질 수 있도록 해야 한다.

(5) 정보공유 남용에 대한 제재

마지막으로 정보공유가 남용되는 것을 방지할 수 있도록 이에 대한 제재방안을 강구해야 한다. 역사와 현실이 보여주는 것처럼, 정보는 언제나 남용될 수 있다. 무엇보다도 현대사회에서 생성되는 빅데이터는 데이터 마이닝을 통해 다방면에 걸쳐 사용될 수 있기에 다양한 정보를 공유하는 기관이나 주체는 본래 목적에서 벗어난 남용의 유혹에 빠질 수 있다. 이는 특히 개인정보를 공유하는 경우에 문제가 된다. 따라서 정보공유가 남용되지 않도록 이에 관한 제재방안을 마련해야 한다.