경제·인문사회연구회 협동연구 총서 19-66-01
연구총서 19-CB-03

KiC
KOREAN INSTITUTE OF CRIMINOLOGY

제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(II)
: 사물인터넷(IoT)과 블록체인

The Criminal Justice Response and Development Strategy in the age of the Fourth Industrial Revolution (II)
: The Internet of Things(IoT) and Blockchain

윤지영, 전현욱, 김진묵, 류부곤, 이병욱, 이원상

한국형사정책연구원

경제·인문사회연구회 협동연구 총서

“제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(Ⅱ): 사물인터넷(IoT)과 블록체인”

1. 협동연구 총서 시리즈

협동연구 총서 일련번호	연구보고서명	연구기관
19-66-01	제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(Ⅱ): 사물인터넷(IoT)과 블록체인	한국형사정책연구원 경찰대학 ㈜크라스랩

2. 참여연구진

연구기관		연구책임자	참여연구진
주관 연구 기관	한국형사정책연구원	윤지영 연구위원 (총괄책임자)	전현욱 연구위원 김진묵 부이사관(파견) 김민규 조사연구원
협력 연구 기관	경찰대학	류부곤 경찰대학 교수	이원상 조선대학교 교수
	㈜크라스랩	이병욱 대표이사	

발간사

컴퓨터와 인터넷, 휴대전화 등이 처음 등장했을 때에는 높은 가격이나 특정 영역에서의 업무 연계성 등으로 인하여 소수의 사람들만이 그 편의를 향유할 수 있었습니다. 그러나 이들이 구현될 수 있는 원리와 기반이 조성되는 데에 걸렸던 시간을 고려한다면, 집채 만했던 컴퓨터나 벽돌 만했던 휴대전화가 소형화되고, 그 가격이 떨어지는 데에는 그리 오랜 시간이 걸리지 않았습니다. 게다가 이러한 기능들은 모두 스마트폰 한 대에 집적되었고, 사람들은 손쉽게 해당 기술이 주는 혜택을 누리고 있습니다. 이에 오늘날 모바일 기기를 일상적으로 사용하고 있는 인류를 두고 '호모 모빌리쿠스(Homo Mobilicus)'라고 칭하기도 하지만, 정작 기술이 등장했던 초창기에 이러한 변화를 예상했던 사람은 많지 않았을 것입니다.

4차 산업혁명은 이미 별개로 존재하고 있는 오프라인과 온라인의 융합을 통해서 인간의 생활양식을 최적화시킬 것으로 기대되고 있습니다. 이른바 '스마트 트랜스폼(Smart Transform)'을 통해서 범죄예방이나 수사를 비롯한 형사사법 시스템 전반의 최적화도 도모될 것으로 예상되나, 그 과정에서 범죄의 발생 양상이 변화되고 처벌의 공백이 발생할 수도 있습니다. 이에 한국형사정책연구원은 첨단과학 기술의 발전을 기반으로 도래할 미래사회의 메가트렌드를 파악하고, 우리가 직면할 새로운 사회문제에 선제적·능동적으로 대응하고자 「제4차 산업혁명 시대의 형사사법적 대응 및 발전방안」이라는 이름의 3개년 과제를 개발하였습니다.

올해 진행된 2차년도(2019년) 연구에서는 연결망의 확대 및 암호화라는 양 측면에서 제4차 산업혁명의 기반이 되는 네트워크 혁신을 이끌고 있는 사물인터넷(IoT)과 블록체인 기술에 대해 다루었습니다. 해당 기술들에 대한 이해를 바탕으로 현실과 괴리되지 않은 논의를 전개하고자 이 분야 전문가와 함께 연구를 진행하였는바, 외부공동연구자로 참여해주신 이병욱 대표님께 감사드립니다. 또한 형사법적 쟁점들을 도출하고 향후 개선 방안을 모색하는데 기여해주신 외부공동연구자 류부곤, 이원상 교수님께도 고마운 마음을 전합니다. 무엇보다 자료 조사를 비롯하여 전체 연구과정

이 원만하게 진행될 수 있도록 노고를 아끼지 않으신 김민규 조사연구원과 임이랑 인턴연구원께 진심 어린 감사 인사를 전합니다.

2019년 12월

연구진을 대표하여

연구위원 윤 지 영

목 차

국문요약 ····· 1

제1장 윤지영

서 론 ····· 9

제1절 연구의 목적 ····· 11
1. 문제의 제기 ····· 11
2. 연구의 필요성 ····· 12
제2절 연구의 범위와 방법 ····· 14
1. 연구의 범위 ····· 14
2. 연구의 방법 ····· 15

제2장 윤지영

정보통신 기술의 발전과 형사법의 변화 ····· 17

제1절 컴퓨터 보급 및 인터넷 상용화에 따른 형사법적 대응 연혁 ····· 19
1. 컴퓨터 보급과 형사법적 대응 ····· 19
2. 인터넷 상용화와 형사법적 대응 ····· 38
제2절 정보통신 기술의 고도화에 따른 형사법적 과제 ····· 63
1. 모바일 디바이스의 발전과 형사법적 과제 ····· 63
2. 프라이버시 보호 기술의 발전과 형사법적 과제 ····· 77

제3장 윤지영·이병욱

사물인터넷(IoT) ····· 87

제1절 사물인터넷(IoT)의 기술적 이해와 특징(이병욱) ····· 89
1. 사물인터넷의 기술적 이해 ····· 89
2. 사물인터넷의 특징 ····· 97

제2절 사물인터넷으로 인한 범죄 발생 양상의 변화 가능성(윤지영) ·· 104
1. 사물인터넷과 범죄예방 ····· 104
2. 사물인터넷 관련 범죄 현황 및 변화 가능성 ····· 118

제3절 사물인터넷 관련 법제 정비 현황 및 그 한계(윤지영) ····· 127
1. 법제 정비 현황 ····· 127
2. 현행 법제도의 한계 ····· 150

제4장 전현욱·김진묵·류부곤·이병욱

블록체인 ····· 153

제1절 블록체인의 기술적 이해와 특징(이병욱) ····· 155
1. 블록체인의 등장 ····· 155
2. 블록체인의 정의 ····· 157
3. 블록체인의 속성과 논란 ····· 162
4. 블록체인과 암호화폐 ····· 170
5. 요약 ····· 185

제2절 블록체인 기술로 인한 범죄 발생 양상의 변화 가능성
(전현욱·김진묵) ····· 186
1. 블록체인 기술의 활용에 관한 형사정책적 이해 ····· 187
2. 암호화폐 관련 범죄의 고도화 및 신종범죄 ····· 201

제3절 블록체인 및 암호화폐 관련 법적 현황 및 그 한계(류부곤) ····· 231
1. 법률 적용과 법규 정비에 관한 현황 ····· 231
2. 현행법과 법정책적 동향에 대한 평가와 한계 ····· 252

제5장 윤지영·류부곤·이원상

네트워크 혁신 시대의 형사법적 대응 방안 ····· 255

제1절 형사법적 대응 방안(윤지영·류부곤) ····· 257

1. 형사실체법적 대응 방안 ····· 257
2. 형사절차법적 대응 방안 ····· 273

제2절 형사정책적 대응 방안(윤지영·이원상) ····· 297

1. 사이버보안 강화 방안(이원상) ····· 297
2. 형사정책적 활용 및 기타 고려 사항(윤지영·이원상) ····· 351

제6장 윤지영

결 론 ····· 363

참고문헌 ····· 369

Abstract ····· 387

표 차례

[표 2-1] 1986년 5월 12일 시행된 전산망보급확장과이용촉진에관한법률의 벌칙 ····· 32
[표 2-2] 1991년 12월 14일 개정된 전산망보급확장과이용촉진에관한법률의 벌칙 ····· 33
[표 2-3] 1995년 12월 6일 개정된 전산망보급확장과이용촉진에관한법률의 벌칙 ····· 34
[표 2-4] 1995년 형법 개정을 통한 컴퓨터 관련 범죄 대응 ····· 36
[표 2-5] 현행 정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 벌칙 규정 ····· 52
[표 2-6] 통신수단별 통신제한조치 현황 ····· 68
[표 3-1] 사물인터넷 응용분야 ····· 98
[표 3-2] 최근 5년 간 전체 사이버범죄 발생 및 검거 현황 ····· 119
[표 3-3] 최근 5년 간 정보통신망 침해범죄 현황 ····· 120
[표 3-4] 위치정보법 제15조 제1항 신구조문 대비표 ····· 146
[표 3-5] 정보통신망법 제32조의5, 제63조 신구조문 대비표 ····· 147
[표 3-6] 개인정보 보호법 제20조, 제25조 신구조문 대비표 ····· 149
[표 4-1] 2019년도 12대 공공선도 시범사업 선정 과제 ····· 190
[표 4-2] 암호화폐 범죄 분류체계 ····· 208
[표 4-3] 최근 3년간 거래소 해킹 사례 ····· 211
[표 4-4] 최근 4년간 크립토재킹 탐지현황 ····· 216
[표 5-1] 형법 제319조의2 신설안 ····· 260
[표 5-2] 형법 제164조 개정안(1안) ····· 262
[표 5-3] 형법 제164조 개정안(2안) ····· 262
[표 5-4] 형법 제164조 개정안(3안) ····· 263

그림 차례

[그림 2-1] 앨런 튜링 ····· 21
[그림 2-2] 콜로서스 ····· 21
[그림 2-3] 초기 아타나소프 베리 컴퓨터와 완성형의 아타나소프 베리 컴퓨터 ····· 23
[그림 2-4] 에니악 ····· 23
[그림 2-5] 요한 폰 노이만 ····· 24
[그림 2-6] 에드삭 ····· 24
[그림 2-7] 유니박 ····· 26
[그림 2-8] IBM 650 ····· 26
[그림 2-9] 애플 II ····· 28
[그림 2-10] IBM 퍼스널 컴퓨터 ····· 28
[그림 2-11] 아르파넷 개요 및 아르파넷 접속 신호 처리 장치(IPM) ····· 41
[그림 2-12] 아르파넷 ····· 41
[그림 2-13] 팀 버너스 리 ····· 44
[그림 2-14] 마크 앤드리슨 ····· 44
[그림 2-15] 스타트렉 속 통신장치 ····· 64
[그림 2-16] 모토로라 다이나택 8000X ····· 64
[그림 2-17] IBM 사이먼 ····· 67
[그림 2-18] 2007년 애플 아이폰 ····· 67
[그림 2-19] 스마트폰 지문인식 ····· 79
[그림 2-20] 스마트폰 얼굴인식 ····· 79
[그림 2-21] 스마트폰 홍채인식 ····· 80
[그림 2-22] 토르 브라우저 ····· 82
[그림 2-23] 토르 작동 방식 ····· 82
[그림 3-1] IoT가 도입한 새로운 차원 ····· 92
[그림 3-2] 스마트 트랜스폼 기술과 4단계 융합프로세스 ····· 105
[그림 3-3] 서울시 안심부스 ····· 110
[그림 3-4] 서울시 안심이 긴급신고 처리 흐름도 ····· 111
[그림 3-5] 안심이 피해자 관제화면 ····· 112

[그림 3-6] 안심이 앱 ····· 112
[그림 3-7] 샷 스포터 시스템 ····· 114
[그림 3-8] 구글 글래스 ····· 116
[그림 3-9] 항공기, 차량 HUD 이미지 ····· 116
[그림 3-10] 두바이 경찰의 스마트안경 ····· 118
[그림 3-11] 중국 경찰의 스마트안경 ····· 118
[그림 3-12] 연도별 IoT 취약점 추이(2013-2016년) ····· 121
[그림 3-13] 취약점 분류별 신고 추이(2013-2016년) ····· 121
[그림 3-14] 여수 버스정류장 음란영상 재생 장면 ····· 125
[그림 3-15] 필리핀 도심 한복판 음란영상 재생 장면 ····· 125
[그림 3-16] 뉴질랜드 상점 광고판 음란영상 재생 및 조치 이후 모습 ····· 126
[그림 4-1] 블록체인과 외부환경의 관계 ····· 174
[그림 4-2] 중개소를 통한 비트코인 거래 ····· 178
[그림 4-3] 최근 5년간 "블록체인" 키워드에 대한 관심도 변화 ····· 189
[그림 4-4] Coinhive의 자바스크립트 코드 ····· 214
[그림 4-5] 크립토재킹을 위한 악성코드 감염 후 CPU 사용률 증가 ····· 214
[그림 4-6] 2017년 검거된 크립토재킹 사건 ····· 215
[그림 4-7] 워너크라이 감염 화면 ····· 218
[그림 4-8] 랜섬웨어 유포 이메일 ····· 219
[그림 4-9] 공조수사 결과 발표 후 W2V 사이트 화면 ····· 221
[그림 5-1] CISA 조직도 ····· 311
[그림 5-2] 일본 사이버보안 정책 대응체계 ····· 337

국문요약

제4차 산업혁명은 현실과 가상을 융합하여 인간의 생활양식을 최적화시킬 것인데, 현실을 데이터화하는 '디지털 트랜스폼(Digital Transform)'과 데이터를 현실화하는 '아날로그 트랜스폼(Analog Transform)'이 합쳐진, 이른바 '스마트 트랜스폼(Smart Transform)'을 통해 구현될 것으로 전망된다. 스마트 트랜스폼은 ① 데이터화, ② 정보화, ③ 지능화, ④ 스마트화라는 4단계 선순환 구조를 가진다.

범죄예방 분야의 디지털 트랜스폼 제1단계는 데이터화로서, 112 및 119 신고는 물론이고 CCTV나 드론 등 다양한 사물인터넷 디바이스를 통해서 정보가 수집된다. 제2단계 정보화 과정에서는 성범죄자 신상정보와 같은 범죄이력은 물론이고 세금 체납 정보나 금융거래 정보 등이 모여서 빅데이터가 된다. 제3단계 지능화는 인공지능을 이용해서 수집된 정보가 분석되는 과정으로서, 과거 발생했던 범행 장소나 시간, 수법 등이 통합·분석된 후 향후 범죄 발생 가능성이 높은 지역이나 시간을 도출할 수 있다. 이러한 분석 결과를 토대로 제4단계 스마트화가 진행되는데, 범죄 발생 가능성이 높은 지역이나 시간대에 경찰력을 집중 배치하는 등 범죄예방 전략을 최적화시킴으로써 경찰 업무의 효율성을 높이고, 시민들이 범죄로부터 안전하다고 느끼는 체감치안지수를 향상시킬 수 있는 것이다. 또한 이 과정을 통해 형성된 빅데이터는 범죄가 발생했을 때 수사의 효율성을 제고시키기 위한 목적으로 지능화되어서 최적의 수사가 가능하도록 한다. 범죄예방 및 수사의 디지털 트랜스폼은 이미 시작되었는데, 미국의 범죄예측 프로그램인 'PredPol(Predictive Policing)'이나 'DAS(Domain Awareness System)'의 활용이 대표적이다.

범죄예방 및 수사의 디지털 트랜스폼 과정에서 사물인터넷(IoT)은 네트워크로 연결된 디바이스를 통해서 각종 데이터를 수집할 뿐만 아니라 정보를 공유하거나 활용할 수 있다. 종래의 CCTV나 차량번호판 판독기의 기능이 그 설치 목적에 부합하는 정보를 수집하는 것에 그쳤다면, 사물인터넷 기술의 발전에 힘입어 이들은 네트워크에 연결된 개별 디바이스로서 정보를 공유하거나 활용할 수 있게 되었다. 또한 디바이스

를 통해 수집된 정보의 이용 목적이나 범위도 확장될 수 있다. 일례로 기존의 방범용 CCTV는 현재 교통이나 재난 및 환경 등 여러 분야의 도시 상황을 통합해서 관리하는 데 활용되고 있는바, 국토교통부가 추진하고 있는 '스마트시티 통합 플랫폼 보급 사업'은 이러한 연계 서비스를 통해 스마트시티 구현을 위한 인프라를 구축하고자 한다.

한편 블록체인 기술은 정부와 기업을 중심으로 여전히 유망한 차세대 성장 동력 중 하나로 인식되고 있으나, 그 기술의 활용 정도는 여전히 '공공선도 시범사업'의 형식으로 그 가능성을 검토하고 있는 단계에 머물러 있다. 즉 우리나라는 물론이고 전 세계적인 차원에서도 블록체인 기술의 활용이 본격적인 궤도에 올랐다고 평가하기에는 아직 이른 것으로 보인다. 기술적 관점에서 블록체인 기술은 암호화폐와 필수적으로 연결되는 것은 아니지만, 현재까지 블록체인 기술의 발전은 암호화폐가 주도하였고, 암호화폐 이외의 영역에서 블록체인 기술이 거의 활용되지 못하고 있는 것이 현실이다. 그로 인해 블록체인과 관련된 법정책적 연구들 역시도 대부분 암호화폐와 관련된 논점들을 다루고 있다.

사물인터넷과 블록체인 기술은 연결망의 확대와 암호화라는 측면에서 제4차 산업혁명의 기반이 되는 네트워크 혁신을 이끌고 있는바, 이에 형사법적 대응 방안을 모색할 필요가 있다. 우선 사물인터넷과 관련해서는 기술의 발달에 따른 형법 규정을 정비할 것이 요청된다. 현행법상 정보통신망 침해를 통해 실제로 피해를 보는 주거자의 프라이버시는 법익으로서 제대로 보호되고 있지 않다. 종래에는 문을 닫고 집 안으로 들어가면 그 안의 사생활은 자연스럽게 보호되었으나, 오늘날 기술의 발전은 타인의 사생활 영역에 침입할 수 있는 방법을 다변화시켰다. 이에 개인의 사생활을 보호할 수 있는 입법정책의 강구가 요청되는 것이다. 물론 현행법은 정보통신망 자체에 대한 침입을 처벌하고 있으므로 굳이 사생활 자체를 직접적 보호법익으로 하는 형사정책이 필요한지에 대해서는 반론이 제기될 수 있다. 그러나 정보통신망의 침해에 대한 규제는 정보통신망 자체의 안정성을 확보하기 위한 행정형법적인 성격이 강하고, 실제로 사생활의 침해를 당하는 피해자를 직접적인 보호의 대상으로 하는 것이 아니어서 개인이 가지는 사생활의 비밀과 자유를 보호하는 형사입법으로는 부족하다. 이에 형법상 보호법익으로서 '기술적 수단으로부터 사생활의 보호'가 직접적으로 고려되어야 한다.

한편, 현행 방화죄 규정에서 '불을 놓아'라는 행위는 '목적물을 소훼시키는 일체의 행위'라고 해석되고 있다. 그런데 과연 사물인터넷을 조작해서 과열로 인해 화재를 일으킨 경우도 현행법상 방화죄로 처벌될 수 있는지가 문제된다. 이에 포섭되는 것으로 해석할 경우 자칫 죄형법정주의의 '명확성 원칙'에 반할 우려가 제기되고 있는 것이다. 컴퓨터가 상용화되면서 발생한 새로운 사안들에 대하여 기존 조문이 적용될 수 없어서 처벌의 공백이 발생했던 경험을 떠올린다면 사물인터넷을 이용한 방화죄도 목적론적 해석으로 처벌이 가능한 것으로 쉽게 결론짓고 넘어갈 일은 아니다. 이러한 문제의식 하에 현행 방화죄의 구성요건 중 '불을 놓아'라는 부분을 '직접 또는 도구나 통신 등을 이용해 불을 놓아'로 개정해야 한다는 의견이 제시된 바 있다. 다만 이 경우 도구나 통신 등을 이용하는 것으로 수단이 특정되면서 방화의 다양한 행위태양이 포섭되지 못할 우려가 제기된다. 이에 '불을 놓아'를 '불을 내어'라는 말로 바꾸는 방안도 모색 가능하다. 나아가 사물인터넷을 이용한 방화는 범죄자가 화재 현장에서 떨어진 곳에서 자신의 안전을 확보한 상태로 범할 수 있고, 인터넷이라는 확장적 수단을 이용하여 대규모 피해를 야기할 수 있다는 점에서 별도의 구성요건으로 신설하는 방안도 고려될 수 있을 것이다.

다음으로 암호화폐의 범죄적 이용에 대한 형법적 의미가 규명되어야 한다. 법원은 비트코인 등 암호화폐의 화폐성을 부정하고 있다. 또한 암호화폐는 디지털 정보의 형태로 존재하기 때문에 민법상 물건이나 형법상 재물에 해당할 수는 없지만 재산적 가치를 가지고 있고, 실제로 거래의 대상이 되고 있으므로 민·형법상으로 재산적 권리 혹은 재산적 이익이나 가치로서는 평가될 수 있는 가능성이 있다. 암호화폐는 민법상 채권의 목적물이 될 수 있고 현실적으로 거래소에서 시세에 따른 환금성을 가질 수 있으므로 형법상으로도 일정한 재산적 가치를 가지는 재산적 이익으로 평가할 수 있다. 따라서 암호화폐는 형법상 '이득죄'의 객체가 될 수 있다.

한편 암호화폐 자체에 대한 전자적 방식의 탈취행위는 컴퓨터등을 이용한 권한 없는 자금의 이체 등과 같은 구조로 보아 절도죄가 아닌 형법상 컴퓨터등 사용사기죄로 의율할 수 있을 것으로 보인다. 그러나 암호화폐 거래나 거래소에 대한 시세조종행위 등을 현행 형법의 범죄구성요건으로 포섭하기에는 난점이 있다. 다만 암호화폐 거래나 거래소의 특성상 비교적 소수의 담합만으로도 거래시장에 큰 혼란을 야기할

수 있으므로 시세조종행위나 미공개정보이용행위에 해당하는 시장교란행위 등에 대한 금지 및 처벌규정이 마련될 필요가 있다. 아울러 담합행위를 통한 시세조종행위의 과정에서 다수 타인의 계정 등을 이용하는 행위는 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해서도 규제와 처벌의 대상이 될 수 있으나 이러한 행위의 위법성을 보다 명확히 하기 위해서는 암호화폐 발행과 거래에 대한 근거법령에 관련 규정을 추가할 필요가 있다.

2018년 5월 대법원은 범죄의 대가로 비트코인을 취득한 범죄자들에 대해 그 비트코인을 몰수할 수 있다는 취지의 판결을 내렸다. 암호화폐의 형태와 종류 등이 매우 다양하고 변형된 형태가 계속 개발되고 있는 시점에서 비트코인이 몰수의 대상이 될 수 있다고 판단한 대법원의 판결이 암호화폐의 발행과 거래에 대한 법적인 차원에서의 전면적 수용으로 이어진다고 보기는 어렵다. 그러나 법적인 판단의 영역에서 암호화폐의 실체와 이에 대한 재산적 가치를 인정했다는 점은 어떤 식으로든 암호화폐의 발행과 거래에 대한 법적 규율이 필요하다는 신호로서의 의미는 충분히 부여될 수 있다. 나아가 형사절차법적인 측면에서도 현재 아무런 규정이 없는 암호화폐의 몰수에 관한 실무적 절차나 방법, 그리고 몰수된 암호화폐를 처분하기 위한 절차규정 등에 대한 입법적 과제를 연구자들과 입법자들에게 부과하고 있는 것이다.

이에 암호화폐 몰수와 처분에 관한 절차를 제안하면 다음과 같다. 일반적인 물건에 대한 몰수의 절차와 방법은 형사소송법상의 압수에 준한다. 즉 이미 압수영장이나 임의제출에 의해 압수되어 수사기관이 보관 중인 물건은 법원의 몰수결정에 의해 그 성격이 몰수물로 전환되는 것이고, 만약 아직 압수되어 있지 않다면 법원의 몰수결정에 의해 대상물을 압수하는 방법으로 몰수가 이루어진다. 그러므로 암호화폐에 대한 몰수 절차는 곧 암호화폐에 대한 압수 절차 및 방법에 대한 논의이다. 우선 계정생성과 이체의 방식으로 암호화폐를 압수하려면 법원 혹은 수사기관 명의의 계정을 만들고, 이에 대한 관리 절차가 마련되어야 한다. 법원이나 수사기관의 계정과 지갑(Wallet)은 해킹이나 거래소의 파산 등으로 인한 손실 등을 방지하기에 적절한 방식으로 마련되어야 하며, 이체의 과정에서 발생하는 수수료 등에 대한 처리 규정과 이체의 과정을 공식적으로 기록하고 문서화하여 일정기간 유지하는 절차에 관한 규정이 마련되어야 한다. 다음으로 법원이나 수사기관이 암호화폐의 계정을 만들고 이에 관한

절차를 마련하더라도 피의자나 피고인이 임의제출을 하지 않는 경우에는 이를 강제처분의 방식으로 압수할 방법이 마땅치 않다는 문제가 있다. 따라서 이 경우에는 압수수색영장의 대물적 효력에 의한 간접적인 방법을 사용하는 수밖에 없다. 압수수색영장의 효력범위에 피의자나 피고인의 개인기록(PC, 휴대전화, 메모 등)을 포함하도록 하여 거기서 얻어진 정보들을 이용하여 법원이나 수사기관이 암호화폐의 거래에 필요한 정보를 찾아내는 방법을 사용해야 할 것이다.

압수의 방식으로 몰수한 암호화폐의 처분에 대해서도 현재는 명확한 절차규정이 존재하지 않는다. 암호화폐를 '유가물'로 볼 경우, 압수되어 수사기관 등의 계정에 보관된 암호화폐는 '공매절차'를 통해 법정통화로 환가한 후 이를 국고에 납입하는 방식으로 처분해야 한다. 반면 몰수된 암호화폐를 '유가증권'으로 간주한다면 그 자체를 국고납입처분 해야 한다. 이 밖에 현재 암호화폐의 발행과 거래를 인정하지 않는 법정책을 적극적으로 반영하여 몰수한 암호화폐를 폐기의 대상으로 보아 폐기처분하기로 결정하는 방식도 생각해 볼 수 있으나, 이 경우 한 번 생성된 블록체인은 수정과 폐기가 불가능하다는 고유의 특성을 이용하는 암호화폐의 본질적 특성상 기술적으로 폐기가 가능한 것인지 의문이다. 요컨대 암호화폐에 대한 몰수를 법적으로 인정하고 실제로 몰수처분이 이루어진 이상 현실적으로는 유가물로 간주하여 공매한 후 국고에 귀속시킬 수 있도록 하는 것이 타당하고, 이에 대한 제도적 정비가 이루어져야 한다.

네트워크 혁신 시대에 사이버와 인터넷 환경에 상응하는 형사절차법의 개선이 이루어져야 한다. 범죄의 주된 실행무대가 다크넷 등의 인터넷 사이버 공간이고, 범죄실행의 단서나 증거도 모두 네트워크에 연결된 사이버 공간이나 전자통신기기에서 찾을 수 있는 상황이므로 이에 대한 수사활동도 네트워크와 사이버 공간을 직접 대상으로 하여 이루어질 수 있어야 한다. 이에 온라인 수색 혹은 네트워크 수사기법(NIT)이 도입될 필요가 있다. 또한 사이버 영역의 접근에 있어서 일정한 자격요건과 그에 대한 검증을 요구하는 일반적인 다크넷에 대한 수사활동을 위해서는 그러한 자격요건에 대한 가장이 필수적으로 요구된다. 만약 그것이 단순히 수사관이라는 신분을 공개하지 않는 부작위에 그치지 않고, 적극적으로 일정한 신분을 가공하여 증명해야 하는 작위를 요구하는 것이라면 일반적으로 허용되는 임의수사가 아닌 일종의 함정수사나 위법한 비밀수사로 평가될 수 있으므로 그에 대한 법적 근거가 요구되는바, 형사소송

법상 비밀수사관제도를 도입할 필요가 있다. 나아가 현행 형사소송법이 종이 형태의 물리적 영장제도를 전제하고 있고, 그 발부와 제시에 대한 규정이 엄격히 해석되고 있다는 점도 문제로 지적되고 있다. 적법하고 정확한 영장의 집행이라는 절차적 정당성을 훼손하지 않는 보완조치와 함께 전자적 방식으로도 영장의 발부와 제시가 이루어질 수 있도록 하는 형사소송법의 정비가 요청된다.

형사정책적 측면에서는 우선 사이버보안 기준이 재정립되어야 한다. 또한 사물인터넷이나 블록체인의 형사정책적인 활용 방안을 모색하는 것도 요청된다. 사물인터넷의 경우 이미 도입된 폴리스캠 등의 사용이 활성화될 수 있도록 이들 디바이스를 네트워크상에 연결시키고 자동으로 데이터가 전송될 수 있는 시스템이 구현될 필요가 있고, 시스템 운영 등을 규율하는 근거 법률이 정비되어야 한다. 나아가 사물인터넷에 대해서는 정보보호영향평가가 이루어질 것이 요구되며, 수사 및 재판의 효율성과 전문성을 제고시키기 위한 교육 프로그램을 정비하고 전담재판부를 도입하는 방안을 고려해 볼 수 있다. 한편 현재 비트코인 등 암호화폐와 관련해서는 형사법적으로 다양한 의문이 제기되고 있는데, 특히 수사 및 재판 등 형사절차상 이를 어떻게 처리할 지가 문제된다. 이에 법적 근거를 마련할 필요가 있으나, 암호화폐의 법적 성격을 규명하고 그 특징을 반영하여 입법화에 이르기까지는 어느 정도의 시간이 소요될 것이다. 그러나 암호화폐와 관련된 범죄가 늘고 있는 상황에서 법률의 불비로 인해 초래될 혼란을 막아야 할 것인바, 수사 실무 담당자들이 참조할 수 있는 가이드라인이 신속하게 제공되어야 한다.

최근 구글이 양자컴퓨터 개발에 성공했다는 언론보도가 나오면서 암호 자체가 무력화될 수 있다는 우려로 인하여 비트코인 등 암호화폐의 가격이 폭락하였다. 물론 이에 대해서는 회의적인 입장을 취하는 전문가도 있지만, 향후 양자컴퓨터가 구현되면 현재 우리가 논하고 있는 사물의 연결성이나 암호화의 수준은 컴퓨터 개발 초창기에 집채 만했던 '에니악'을 떠올리는 것처럼 평가될 지도 모른다. 1939년 세계 최초의 전자식 컴퓨터가 공개된 지 80여년 만에, 1969년 최초의 인터넷망인 '아르파넷'이 구축되고, 1973년 미국 모토로라의 마틴 쿠퍼 박사팀에 의해 셀룰러 시스템을 활용한 휴대전화가 개발된 지 50여년 만에, 그리고 2007년 애플의 '아이폰'이 등장한 지 불과 10여년 만에 세상이 바뀌었다. 더불어 그러한 기술적 진보는 범죄의 발생 양상을

변화시키면서 형사사법적 대응을 요청하고 있다. 사물인터넷과 블록체인은 이제 더 이상 미래의 기술이 아니다. 빛의 속도로 빨라질 것만 같은 기술의 발전으로 인해 어느 순간 또 다른 첨단기술들이 그 자리를 대체할지 모를 일이지만, 두 기술을 중심에 두고 논의를 전개한 이 보고서가 보다 신속하게 형사사법 분야의 제도를 개선하고 국가형사정책을 수립하는 데에 조금이라도 기여하기를 기대해 본다.

서 론

윤 지 영

제1장

서 론

제1절 | 연구의 목적

1. 문제의 제기

2019년 10월 25일 대통령직속 '4차산업혁명위원회'는 과학기술의 유례없이 빠른 발전 속에 사회 전반의 변혁에 대응하고자 '4차산업혁명 대정부 권고안'을 발표하였다. "1820년 세계 GDP의 3분의 1 가량을 차지했던 중국이 지난 200여 년 동안 진행된 산업화와 현대화의 역사 속에서 무려 3차례나 산업혁명의 기회를 놓치면서 1950년 세계 GDP의 20분의 1에도 미치지 못하는 낙오국이 되었다"는 후안강(胡鞍鋼) 칭화(淸華)대 국정연구원장의 발언을 적시하는 것으로 시작되는 대정부 권고안에는 다시 도래한 산업혁명의 시대에 결코 뒤처지지 않겠다는 정부의 의지가 담겨 있다.[1)]

2016년 세계경제포럼(World Economic Forum, WEF)의 연례회의 주제로 '제4차 산업혁명의 이해(Mastering the Fourth Industrial Revolution)'가 다루어지면서 세계

1) 이미 미국은 오바마 행정부 시절인 2016년 5월에 백악관 국가과학기술협의회(National Science and Technology Council) 기술위원회(Committee on Technology) 산하에 '기계학습 및 인공지능 소위원회(Subcommittee on Machine Learning and Artificial Intelligence)'를 설치했다. 또한 그 활동을 바탕으로 2016년 10월에 백악관 국가과학기술협의회(NSTC)는 '인공지능의 미래를 위한 준비(Preparing for the Future of Artificial Intelligence)'와 '국가 인공지능 연구 개발 전략 계획(The National Artificial Intelligence Research and Development Strategic Plan)'이라는 2권의 보고서를 발간했고, 같은 해 12월에는 '인공지능, 자동화, 그리고 경제(Artificial Intelligence, Automation, and the Economy)'라는 보고서를 발간하면서 인공지능 기술의 연구개발 및 정책 방향을 제시했다. The White House President Barack Obama Blog, https://obamawhitehouse.archives.gov/blog/2016/12/20/artificial-intelligence-automation-and-economy (2019년 10월 23일 최종접속).

적 이목이 집중되었고, 2016년 3월에는 구글의 인공지능 '알파고(AlphaGo)'와 이세돌 9단의 바둑 대국이 서울에서 개최되면서 인공지능에 대한 사회적 관심이 폭발적으로 증대되었다. 인간과 대화하는 기계의 구현은 요원할 것이라고 생각했던 사람들 앞에 선보여진 인공지능 기술의 발전 현황은 마치 4차 산업혁명의 서막을 울리는 팡파르와도 같았다. 그러나 여전히 4차 산업혁명이라는 개념이나 실체에 의문을 제기하는 사람들이 있고, 첨단기술이나 산업 혁신에 불편함을 느끼는 사람도 적지 않다. 이에 카풀 플랫폼 구축 등으로 모빌리티의 혁신을 모색하고자 했던 시도는 택시업계의 반대에 부딪혀 좌절될 위기에 처했고, 지능화 사회의 석유에 비유되는 데이터의 경우 그 활용보다는 보호에 무게 중심이 치우쳐 있다.

반면 중국은 어떠한가. 지난 200년 동안 후진국으로 전락했던 상황을 단숨에 만회라도 하듯이 세계 2위의 경제대국이 되었다. 더욱이 중국은 첨단기술 산업의 패권을 두고 미국과 경쟁하고 있는 거의 유일한 국가이며, 심지어 미국을 제치고 세계 1위의 유니콘 기업[2] 강국으로 부상하기도 했다.[3] 이는 권위주의 국가에서 시민들의 개인정보나 프라이버시의 가치를 경시하면서 이룩한 결과이기 때문에 긍정적으로 평가할 수만은 없다. 그럼에도 불구하고 4차 산업혁명을 주도할 기술 수준이나 혁신 역량의 측면에서 이미 중국보다 뒤처진 우리에게 이러한 사실은 커다란 자극제가 되고 있다.

2. 연구의 필요성

4차 산업혁명은 '현실과 가상이 융합하여 인간의 생활양식을 최적화시키는 것'으로 정의될 수 있는데, 이는 '데이터화, 정보화, 지능화, 스마트화'라는 4단계의 선순환 구조를 가지고 있다.[4] '더불어 잘사는 경제'라는 현 정부의 국정목표를 실현하기 위해 '과학기술 발전이 선도하는 4차 산업혁명'이 주요 전략과제로 선정되어 있는데, 이는

---

2) '유니콘(unicorn)' 기업이란 기업의 가치가 10억 달러, 즉 한화로 1조 원 이상인 비상장 스타트업 기업을 일컫는다. 스타트업 기업이 상장되기도 전에 1조 원 이상의 가치가 된다는 것은 마치 상상 속에 존재하는 동물인 유니콘과도 같다는 의미로 사용되고 있다. 미국의 우버나 에어비앤비, 중국의 샤오미, 디디추싱, 한국의 쿠팡이나 야놀자 등이 이에 해당한다.

3) "胡润研究院发布《2019胡润全球独角兽榜》", 胡润百富 2019.10.21., http://www.hurun.net/CN/Article/Details?num=E7190250C866 (2019년 10월 23일 최종접속).

4) 윤지영/임정호/이민화/김성돈, 제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(Ⅰ): 자율주행자동차와 드론, 한국형사정책연구원, 2018, 36면.

인공지능, 사물인터넷, 5G 등 제4차 산업혁명의 기반이 되는 초지능·초연결 기술의 확산을 장려하고 핵심기술을 개발하며 신산업을 육성함으로써 일자리와 성장 동력을 확보하고자 한다. 이러한 첨단과학 기술의 발전은 제조업 등 생산 방식에만 영향을 미치는 것이 아니라 범죄의 발생 양상이나 형사사법 시스템 전반에 상당한 영향을 미칠 것이다. 이미 컴퓨터 기술의 발전과 PC의 보급은 컴퓨터를 이용한 신종범죄가 출현하도록 했고, 그에 대응하기 위해 형법 개정이 단행되기도 했다. 인터넷의 상용화도 사이버 공간을 무대로 다양한 범죄가 등장하도록 했으며, 형사사법적인 대응이 지금까지 이어지고 있다.

그리고 다시 한 번 우리는 정보통신 기술의 혁신 시대를 맞이하고 있다. 사람이 아닌 사물도 인터넷으로 연결되어 정보를 수집·전달·공유하고, 네트워크 및 정보처리 과정에 암호화라는 기술이 접목되기 시작한 것이다. 2017년 5월 전 세계를 강타한 랜섬웨어 '워너크라이(WannaCry)'는 철도, 의료, 통신 등 중요 시설을 집중적으로 공격하였는데 해커들은 암호 해독의 대가로 가상화폐인 비트코인을 요구하였다.[5] 제4차 산업혁명 시대에는 사물인터넷의 보안 취약성과 비트코인의 익명성을 겨냥한 사이버 공격이 심화될 것이라는 우려가 고조되고 있는바, 「제4차 산업혁명 시대의 형사사법적 대응 및 발전 방안」 2년차 과제에서는 사물인터넷과 블록체인의 등장으로 인해 대두되는 형사법적 쟁점과 그 대응책을 모색하고자 한다.

---

5) 2017년 5월 12일 영국과 스페인 등에서 발생해 전 세계 150여개국에 최소 30만대 이상의 컴퓨터 시스템에 피해를 입힌 랜섬웨어인 WannaCryptor 즉, 워너크라이(WannaCry)로 인해 해커에게 최소 7만 달러 이상의 가상화폐가 지급되었는데, 랜섬웨어는 '시스템 및 데이터를 해커가 암호화하여 소유주의 접근을 막는 해킹'이므로 파일을 원상복구하기 위해서는 해커가 요구하는 대가를 치러야 했기 때문이다. 한국인터넷진흥원, 워너크라이 분석 스페셜리포트, 2017.10., 4-5면, https://www.krcert.or.kr/filedownload.do?attach_file_seq=1718&attach_file_id=EpF1718.pdf (2019년 10월 23일 최종접속); "워너크라이 사태 불러 온 다크넷과 비트코인", 중앙선데이 2017년 5월 28일자, https://news.joins.com/article/21613805 (2019년 10월 23일 최종접속).

제2절 | 연구의 범위와 방법

1. 연구의 범위

한국형사정책연구원은 첨단과학 기술의 발전을 기반으로 도래할 미래사회의 메가 트렌드를 파악하고, 우리나라가 직면할 새로운 사회문제에 선제적·능동적으로 대응하기 위해서 「제4차 산업혁명 시대의 형사사법적 대응 및 발전방안」이라는 이름의 3개년 과제를 개발하였다. 4차 산업혁명은 이미 별개로 존재하고 있는 오프라인과 온라인을 융합하는 것이고, 종래의 산업혁명들과 달리 특정한 기술로 인한 변화에 그치지 않는다. 제4차 산업혁명은 현실을 데이터화하는 디지털 트랜스폼(Digital Transform)과 데이터를 현실화하는 아날로그 트랜스폼(Analog Transform)이 합쳐진, 이른바 스마트 트랜스폼(Smart Transform)을 통해 구현될 것으로 전망된다.[6] 이러한 과정을 거쳐 범죄예방이나 수사를 비롯한 형사사법 시스템 전반의 최적화도 도모될 수 있다.

한편 제4차 산업혁명을 올바르게 이해하기 위해서는 기술 중심적인 기존의 시각을 뛰어넘어서 인간의 욕망과 기술의 순환이라는 관점에서 바라볼 필요가 있다.[7] 그러나 인터넷이 상용화되었을 초창기에 기술과 법률 사이의 간극으로 인하여 혼란의 시기를 겪었던 경험들을 떠올린다면, 개별 첨단기술의 등장으로 인해 변화되는 범죄의 양상이나 형사사법적인 대응 방안에 초점을 맞출 필요가 있다. 이에 3개년도 과제로 기획된 본 연구는 제4차 산업혁명을 견인할 주요 기술로 거론되고 있는 인공지능을 필두로 하여 그 기술이 상용화된 형태인 자율주행자동차와 드론, 사물인터넷과 블록체인, 그리고 가상현실(VR)이나 증강현실(AR) 및 3D 프린팅 기술이 범죄와 형사사법에 미칠 영향에 대하여 전망하고, 구체적인 대응 방안을 모색하고자 한다.

이미 종료된 1차년도(2018년) 연구에서는 4차 산업혁명이 형사사법 분야에 미칠 영향을 조망하였고, 인공지능 기술이 상용화된 대표적인 형태인 자율주행자동차와

---

6) 윤지영/임정호/이민화/김성돈, 앞의 보고서, 29-30면.
7) KCERN(창조경제연구회), 4차 산업혁명 국가 로드맵 작성을 위한 정책연구, 「창조경제 연구회 제46차 공개포럼」 보고서, 창조경제연구회, 2018, 178면.

드론에 대한 형사실체법적·절차법적인 쟁점을 고찰한 뒤 법령 제·개정 방안을 제언하였다. 올해 진행된 2차년도(2019년) 연구에서는 사물인터넷(IoT)과 블록체인에 대한 기술적인 이해를 바탕으로 하여 동 기술들이 범죄와 형사사법에 미칠 영향을 조망하고 합리적인 대응 방안을 논하고자 하였다. 그리고 내년에 진행될 3차년도(2020년) 연구에서는 '가상의 공간에서 현실감 있게 정보를 가시화'하는 가상현실(VR)과 증강현실(AR) 및 '현실의 공간에서 일정한 정보를 3차원 물건으로 구현'하는 3D 프린팅에 관한 기술적인 특징을 파악한 후, 동 기술들이 범죄와 형사사법에 미칠 영향을 논의하며, 그 대응 방안을 모색하고자 한다.

2019년 협동연구사업인 「제4차 산업혁명 시대의 형사사법적 대응 및 발전 방안(Ⅱ)」에서는 사물인터넷(IoT)과 블록체인을 다루고 있는바, 해당 연구는 총 6개의 장으로 구성되어 있다. 서론과 결론을 제외한 각 장에서는 「정보통신 기술의 발전과 형사법의 변화」, 「사물인터넷(IoT)」, 「블록체인」, 「네트워크 혁신 시대의 형사법적 대응 방안」에 대해 다루고 있다.

제1장 서론에 이어지는 제2장에서는 정보통신 기술의 발전과 형사법의 변화에 대해 서술하고 있다. 본 장에서는 컴퓨터 보급 및 인터넷 상용화에 따른 형사법적 대응 연혁에 대해 다루었다. 컴퓨터와 인터넷의 등장으로 인해 시작된 범죄의 변화와 형사법적 대응 추이를 살펴보았는데, 이러한 과정은 네트워크 고도화 및 다변화 시대에 형사법적 대응 과제를 도출하는 데 크게 참고되었다. 제3장과 제4장에서는 각각 사물인터넷(IoT)과 블록체인에 대한 기술적 이해와 특징에 대해 고찰하였고, 이를 토대로 해당 기술로 인해 발생할 범죄 양상의 변화 가능성을 논하였다. 또한 개별 기술의 상용화와 관련된 법규 정비 현황 및 그 한계에 대해서도 서술하였다. 그리고 제5장에서는 네트워크 혁신 시대의 형사법적 대응 방안을 모색하였는바, 형사실체법적·절차법적인 측면과 형사정책적인 측면을 나누어 서술하였다.

2. 연구의 방법

본 연구는 연결망의 확대와 암호화라는 측면에서 제4차 산업혁명의 기반이 되는 네트워크 혁신을 이끌고 있는 사물인터넷과 블록체인 기술에 대한 법적·제도적 쟁점

을 다룬 국내외 보고서와 단행본 및 논문 등을 중심으로 문헌연구를 수행하였다. 또한 정보통신 기술의 발전에 따른 형사법적 대응 연혁을 개괄하였으며, 미국, 독일, 일본 등 주요 국가들이 사물인터넷 및 블록체인 기술과 관련된 범죄에 어떻게 대응하고 있는지 비교법적으로 고찰하였다. 한편 해당 기술 분야 전문가와의 면담 및 유관 세미나 참석을 통해서 기술의 발전 현황과 그 활용 가능성에 대해 파악하였고, 법률 전문가와의 자문회의를 통해서 관련 법규 정비 동향을 검토하였다. 나아가 사물인터넷과 블록체인의 기술적 이해를 바탕으로 현실과 괴리되지 않은 논의를 전개하고자 이 분야 전문가와 공동연구를 진행하였고, 기술의 상용화 과정에서 문제되는 형사법적 쟁점을 도출하기 위해서 국내외 유관기관에 방문해서 전문가 간담회 및 세미나를 개최하였다. 특히 최근 들어 블록체인 기술이 적용된 암호화폐와 관련된 법적 문제가 대두되는 상황을 고려하여, 형사법 학계 및 실무계 종사자들을 대상으로 해당 기술에 대한 이해도를 제고시킬 수 있는 강연 프로그램을 기획·제공한 후 현행법의 적용 가능성과 그 한계에 대해 논의하는 장도 마련하였다.

정보통신 기술의 발전과 형사법의 변화

윤 지 영

제2장

정보통신 기술의 발전과 형사법의 변화

제1절 | 컴퓨터 보급 및 인터넷 상용화에 따른 형사법적 대응 연혁

1. 컴퓨터 보급과 형사법적 대응

가. 컴퓨터의 등장과 대중화

1) 컴퓨터의 등장

컴퓨터(computer)란 용어는 '계산하다'라는 의미를 가진 라틴어 'computare'에서 유래하였다.[8] 주판과 같이 계산에 이용되는 도구나 사람을 칭하던 컴퓨터는 오늘날 전자회로를 이용해서 수학적 계산은 물론이고 다양한 종류의 데이터를 처리하는 기기를 일컫고 있다. 1904년 영국의 전기공학자 존 플레밍(John Ambrose Fleming)은 진공 상태에서 전자의 흐름을 조절해서 신호를 변경하거나 증폭시킬 수 있는 진공관을 발명하였다.[9] 영국의 수학자이자 과학자였던 앨런 튜링(Alan Mathison Turing)은 1936년에 "결정문제에 대한 적용과 관련된 연산 가능한 수에 관하여(On Computable Numbers, with an Application to the Entscheidungsproblem)"[10]라는 논문을 발표하

8) Edith Law/Luis von Ahn, Human Computation(Synthesis Lectures on Artificial Intelligence and Machine Learning), Morgan & Claypool Publishers, 2011, p.1; "The Vocabularist: What's the root of the word computer?", BBC News 2016.2.2., https://www.bbc.com/news/blogs-magazine-monitor-35428300 (2019년 10월 23일 최종접속); 송성수, 발명과 혁신으로 읽는 하루 10분 세계사: 종이에서 로봇까지, 생각의힘, 2018, 131면.

9) H. F. Dylla/Steven T. Corneliussen, "John Ambrose Fleming and the Beginning of Electronics", Journal of Vacuum Science & Technology, Volume 23, Issue 4, A Vacuum Surfaces and Films, 2005, p.1244.

10) Alan M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem",

면서 입력과 연산, 출력 및 기억을 연속적으로 할 수 있는 가상의 '튜링 기계(Turing Machine)'라는 개념을 제시하였다.[11] 요컨대 진공관의 개발과 튜링 기계라는 개념 정립으로 인하여 근대적 컴퓨터의 핵심 부품과 기본적인 작동 원리가 마련된 것이다. 이후 튜링은 진공관을 이용해서 '콜로서스(Colossus)'라는 이름의 암호해독용 기계를 고안하였고, 1943년 12월에 제작된 콜로서스는 세계 최초로 실용화된 연산컴퓨터라는 평가를 받고 있다.[12][13]

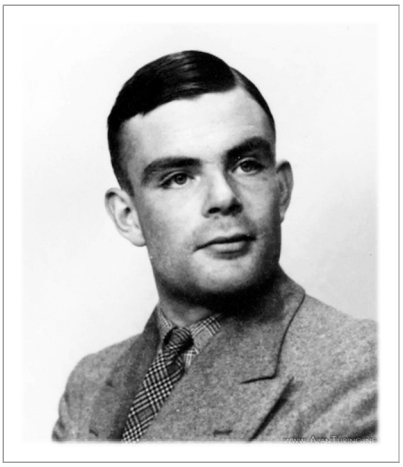
Proceedings of the London Mathematical Society, Volume s2-42, 1937, pp.230-265, https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/plms/s2-42.1.230 (2019년 10월 23일 최종접속).

11) Alan M. Turing, Ibid., pp.231-263, https://londmathsoc.onlinelibrary.wiley.com/doi/epdf/10.1112/plms/s2-42.1.230 (2019년 10월 23일 최종접속); B. Jack Copeland, Turing: Pioneer of the Information Age, Oxford University Press, 2012, pp.14-22.

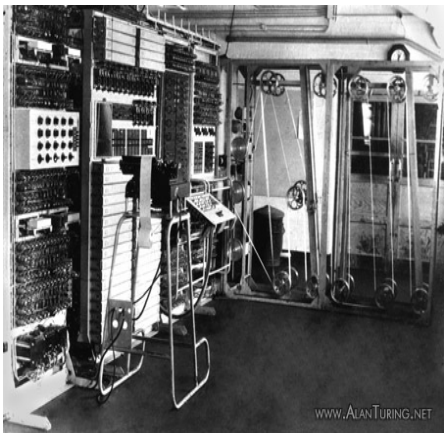
12) B. Jack Copeland, "Colossus: Its Origins and Originators", IEEE Annals of the History of Computing, Volume 26, Issue 4, IEEE, 2004, pp.40-43; Jonathan Peter Bowen, "Alan Turing: The Founder of Computer Science", A History of Computing in Three Parts, 2013 Gresham College/British Society of the History of Mathematics conference, 2013.10.31., https://www.gresham.ac.uk/lectures-and-events/alan-turing-the-founder-of-computer-science (2019년 10월 23일 최종접속).

13) 제2차 세계대전 당시 독일군은 '에니그마(Enigma)'라는 장치를 이용해서 암호를 만들었고, 영국은 이를 해독할 수 있는 방법을 찾고자 1939년에 '울트라 프로젝트(Ultra Project)'를 출범시켰다. 앨런 튜링이 포함된 이 프로젝트 팀은 암호에서 드러나는 통계적 규칙을 찾아서 암호의 유형을 확인하고자 진공관을 이용하여 콜로서스라는 컴퓨터를 만들었다. 콜로서스를 이용해서 독일군의 교신 내용을 확인할 수 있었던 연합군은 1944년 노르망디 상륙작전을 성공시켜서 제2차 세계대전의 결정적인 승기를 잡았다. 종전 후 영국은 군사기밀이라는 이유로 콜로서스 컴퓨터를 폐기하였고, 그 존재는 울트라 프로젝트에 참여했던 윈터보텀(Frederick William Winterbotham) 대위가 1974년에 「울트라 시크릿(The Ultra Secret: The Inside Story of Operation Ultra, Bletchley Park and Enigma)」이라는 책을 출간하면서 세상에 알려졌다. Harold C. Deutsch, "The Historical Impact of Revealing The Ultra Secret", Parameters: The U.S. Army War College Quarterly, Volume 7, Number 3, U.S. Army War College Publications, 1977, pp.16-32, https://ssi.armywarcollege.edu/pubs/Parameters/articles/1977/deutch%202.pdf (2019년 10월 23일 최종접속).

[그림 2-1] 앨런 튜링[14]



[그림 2-2] 콜로서스[15]



이보다 앞서 미국 아이오와 주립 대학의 존 아타나소프(John Vincent Atanasoff) 교수와 그의 조수인 클리포드 베리(Clifford Berry)는 '아타나소프 베리 컴퓨터(Atanasoff-Berry Computer)'를 개발하여 1939년 10월에 첫 시제품을 선보였다.[16] 그 약자인 'ABC'로 더 많이 알려져 있는 이 컴퓨터는 세계 최초의 전자식 컴퓨터로 인정받고 있으나[17] 실험적인 성격이 강하여 실용성과는 거리가 있었다는 평가가 내려진다. 한때 세계 최초의 전자 컴퓨터로 널리 알려졌던 것은 1946년 2월에 미국 펜실베니아 대학의 존 에커트(John Presper Eckert)와 그의 지도교수인 존 모클리(John William Mauchly)가 공개했던 '에니악(Electronic Numerical Integrator and

14) 이미지 출처: Alanturing.net 웹페이지, http://www.alanturing.net/turing_archive/graphics/photos%20of%20Turing/pages/alan8_psd.htm (2019년 10월 23일 최종접속).

15) 이미지 출처: B. Jack Copeland, Colossus, the first large-scale electronic computer, colossus-computer.com, http://www.colossus-computer.com/colossus1.html#sdfigurenote26anc (2019년 10월 23일 최종접속).

16) Kiril Lubenov Boyanov, "John Vincent Atanasoff: the inventor of the first electronic digital computing", CompSysTech '03 Proceedings of the 4th international conference on Computer systems and technologies: e-Learning, 2003.6.19-20, p.3; Marjie T. Britz, Computer Forensics and Cyber Crime, Pearson Education, 2013, p.27.

17) 1937년 미국의 벨 연구소(Bell laboratories)에 근무 중이던 수학자 조지 스티비츠(George Stibitz)는 이진법을 이용하는 최초의 전자식 계산기를 개발했다. M. M. Irvine, "Early Digital Computers at Bell Telephone Laboratories", IEEE Annals of the History of Computing, Volume 23, Issue 3, IEEE, 2001, p.22; IEEE Computer Society, George R. Stibitz, IEEE, https://www.computer.org/profiles/george-stibitz/ (2019년 10월 23일 최종접속).

Computer, ENIAC)'이었다.[18] 스위치와 계전기 대신에 진공관을 사용함으로써 당시에 존재했던 컴퓨터[19]에 비해 1,000배 이상 빠른 연산속도를 자랑했던 에니악은 당대 최고의 전문가들이 기계식 계산기를 이용해서 20시간 동안 풀어야 할 연산문제를 단 30초 만에 해결하였다.[20] 1만 7천 개 이상의 진공관을 사용하여 무게가 30여 톤에 달해서 괴물 컴퓨터라고 불렸던 에니악은 포탄이나 미사일 등의 탄도 계산[21]이나 수소폭탄 개발 등에 이용되었다. 영국의 콜로서스가 암호해독이라는 용도로 국한되었던 것에 반해 에니악은 범용 전자식 컴퓨터로서 그 의의가 있다.

---

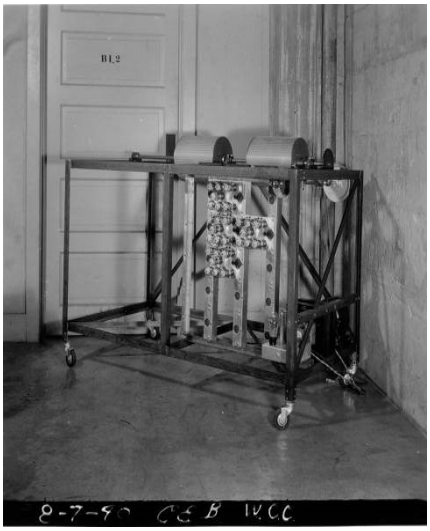
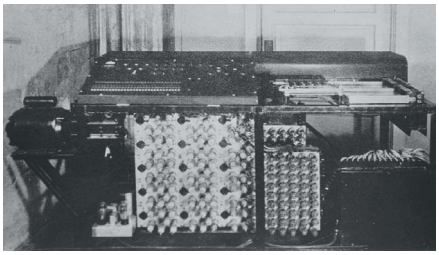
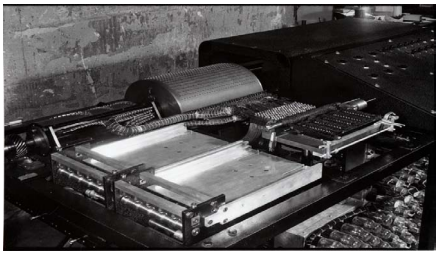
18) 1973년 법정 공방(Honeywell, Inc. v. Sperry Rand Corp., et al., 180 U.S.P.Q. 673, 1973 WL 903 (D.Minn.)) 끝에 에니악이 아닌 ABC가 세계 최초의 컴퓨터로 인정받게 된다. Bernard A. Galler, Software and Intellectual Property Protection: Copyright and Patent Issues for Computer and Legal Professionals, Quorum Books, 1995, pp.34-35; Joel A. Snow, "ENIAC or ABC?", Physics Today, Volume 54, Issue 6, American Institute of Physics, 2001, p.81, https://physicstoday.scitation.org/doi/full/10.1063/1.1387611 (2019년 10월 23일 최종접속).

19) 1944년 미국 하버드 대학의 하워드 에이킨(Howard Hathaway Aiken) 교수는 IBM의 지원을 받아서 자동으로 계산이 되는 전기 기계식 컴퓨터인 마크 원(Mark-Ⅰ)을 개발했다. 마크원은 계전기와 스위치, 전동기 등으로 구현되었으며 자동순차적 제어방식을 통해 수학이나 과학 분야의 문제 해결에 공헌하였으나 기계적인 제약으로 인해서 연산처리 속도는 늦었다고 한다. I. Bernard Cohen, Howard Aiken: Portrait of a Computer Pioneer(History of Computing), MIT Press, 2000, pp.141-145.

20) Tim Bergin, "Keynote Address: A Short History of Computing or How Did We Get to Aberdeen?", Thomas J. Bergin(ed.), 50 Years of Army Computing From ENIAC to MSRC, the Army Research Laboratory and the U.S. Army Ordnance Center & School, 2000, pp.12-13, http://thecorememory.com/EniacToMSRC.pdf (2019년 10월 23일 최종접속); "Announcing The Birth Of An 'Amazing Machine' And That 'Nothing Will Ever Stop' IBM", Forbes 2017.2.12., https://www.forbes.com/sites/gilpress/2017/02/12/announcing-the-birth-of-an-amazing-machine-and-that-nothing-will-ever-stop-ibm/#6a4cc0077307 (2019년 10월 23일 최종접속); Thomas Haigh/Mark Priestley/Crispin Rope, ENIAC in Action: Making and Remaking the Modern Computer, MIT Press, 2016, pp.1-3, pp.27-34.

21) 탄도 계산 과정은 대기나 온도, 풍속 등을 고려하여 약 200단계의 계산 과정을 거쳐야 했는바, 당시로서는 발사된 포탄이 목표점에 도달하기 전에 정확하게 계산 결과를 예측하는 것이 쉽지 않았다. "[이재구코너]괴물 컴퓨터 에니악(ENIAC) 등장", ZDNet 2010년 2월 11일자, http://www.zdnet.co.kr/view/?no=20100211094717 (2019년 10월 23일 최종접속); Martin H. Weik, The ENIAC Story, 1961, https://ftp.arl.army.mil/~mike/comphist/eniac-story.html (2019년 10월 23일 최종접속).

[그림 2-3] 초기 아타나소프 베리 컴퓨터[22]와 완성형의 아타나소프 베리 컴퓨터[23]

[그림 2-4] 에니악[24]



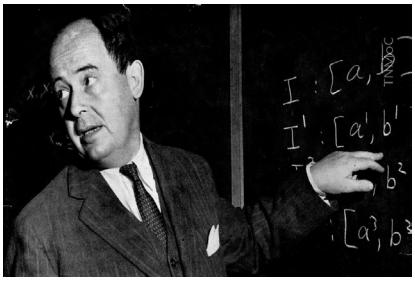

22) 이미지 출처: John V. Atanasoff, "Computing Machines for the Solution of Large Systems of Linear Algebraic equations", Iowa State University, 1982, p.29b, Fig.11, http://cdm16001.contentdm.oclc.org/cdm/fullbrowser/collection/p15031coll18/id/140/rv/compoundobject/cpd/143 (2019년 10월 23일 최종접속).

23) 이미지 출처: JVA Initiative Committee and Iowa State University 웹페이지, http://jva.cs.iastate.edu/operation.php (2019년 10월 23일 최종접속).

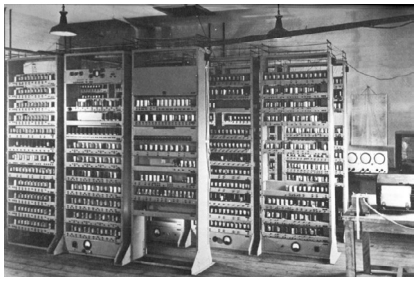
24) 이미지 출처: (좌) U. S. Army Photo, http://ftp.arl.army.mil/ftp/historic-computers/gif/eniac2.gif (2019년 10월 23일 최종접속). (우) Martin Campbell-Kelly, "Origin of computing", Scientific American, Volume 301, Number 3, Springer Nature, 2009.9., p.67, http://www.cs.virginia.edu/~robins/The_Origins_of_Computing.pdf (2019년 10월 23일 최종접속).

에니악을 비롯한 당시의 컴퓨터는 연산속도가 향상되었으나 새로운 작업을 할 때마다 회로와 기억장치를 교체해야 하는 불편함이 있었다. 이에 헝가리 출신의 미국 수학자인 요한 루드비히 폰 노이만(Johann Ludwig von Neumann)은 프로그램 내장 방식의 컴퓨터를 고안하였다. 그는 1945년에 "에드박에 관한 보고서(First Draft of a Report on the EDVAC)"를 발표하면서 컴퓨터 내부 기억장치에 소프트웨어 방식의 프로그램을 내장한 후 그 소프트웨어만을 바꾸어서 다양한 작업에 대응할 수 있다는 개념을 제시하였고,[25] 이는 오늘날 대부분의 컴퓨터에 적용되는 중요한 원리 중 하나가 되었다. 1949년 프로그램 내장 방식이 구현된 최초의 컴퓨터 '에드삭(Electronic Delay Storage Automatic Calculator, EDSAC)'이 등장했고, 1951년에는 에드삭을 개량한 '에드박(Electronic Discrete Variable Automatic Computer, EDVAC)'도 개발되었다.[26]

[그림 2-5] 요한 폰 노이만[27]



[그림 2-6] 에드삭[28]



25) John Ludwig von Neumann, "First draft of a report on the EDVAC", IEEE Annals of the History of Computing, Volume 15, Issue 4, IEEE, 1993, pp.28-75, https://ieeexplore.ieee.org/document/238389 (2019년 10월 23일 최종접속); Michael D. Godfrey/D. F. Hendry, "The Computer as von Neumann Planned It", IEEE Annals of the History of Computing, Volume 15, Issue 1, IEEE, 1993, pp.11-21, https://ieeexplore.ieee.org/document/194088 (2019년 10월 23일 최종접속).

26) Geoffrey W. A. Dummer, Electronic Inventions and Discoveries: Electronics from its earliest beginnings to the present day, Fourth Edition, Institute of Physics Publishing, 1997, p.47.

27) 이미지 출처: Clary Blair Jr., "Passing of a Great Mind: John von Neumann, a Brilliant, Jovial Mathematician, was a Prodigious Servant of Science and his Country", Life Magazine, Volume 42, Number 8, Time Inc., 1957.2.25., p.89, https://books.google.co.kr/books?id=rEEEAAAAMBAJ&pg=PA89&lpg=PA89&dq=Passing+of+a+Great+Mind++John+von+Neumann++Life+Magazine&source=bl&ots=-sj_DGnaig&sig=ACfU3U30eupAERkZFonBtH8D5UNXrNF39g&hl=ko&sa=X&ved=2ahUKEwishcLbiLzmAhUEGaYKHXF6CRMQ6AEwC3oECAwQAQ#v=onepage&q=Passing%20of%20a%20Great%20Mind%20%20John%20von%20Neumann%20%20Life%20Magazine&f=false (2019년 10월 23일 최종접속).

2) 컴퓨터의 대중화

ABC와 에니악의 등장에 이어서 폰 노이만이 제안한 구조의 컴퓨터가 개발되면서 군사부문뿐만 아니라 민간부문에서도 컴퓨터가 실용화될 수 있는 토대가 마련되었다. 에니악 개발에 참여했던 존 에커트와 존 모클리는 1950년에 천공카드가 아닌 자기테이프로 데이터를 저장하는 최초의 상용 컴퓨터 유니박(Universal Automatic Computer, UNIVAC)을 개발하였고, 상용화를 위해 IBM과 접촉하였다. 그러나 유니박은 당시 전자계산기와 타자기 부문에서 독점적 지위를 가지고 있던 IBM을 통해서는 판매가 불가능했고,[29] 이에 레밍턴 랜드(Remington Rand)사를 통해 한 대당 약 16만 달러에 판매가 이루어졌다.[30][31] 최초의 상업용 컴퓨터를 판매할 기회를 잃은 IBM은 한동안 업무용 컴퓨터 시장에서 고전하였으나 1953년에 유니박보다 작고 유지비가 적게 드는 IBM 650 개발에 성공하였으며,[32] 대량생산 시스템과 영업망을 갖춤으로써 이 분야 1인자로 군림하게 되었다.

---

28) 이미지 출처: "Pioneering Edsac computer to be built at Bletchley Park", BBC News 2011.1.13., https://www.bbc.com/news/technology-12181153 (2019년 10월 23일 최종접속).

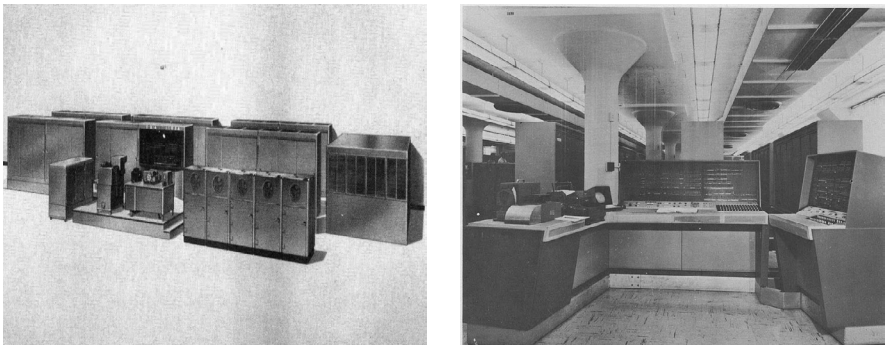
29) "UNIVAC: the troubled life of America's first computer", arsTECHNICA 2011.9.19., https://arstechnica.com/tech-policy/2011/09/univac-the-troubled-life-of-americas-first-computer/ (2019년 10월 23일 최종접속).

30) Harald Sack, "Behold the First Commercial Computer (in the US) – the UNIVAC I", The SciHi Blog, 2018.6.14., http://scihi.org/first-commercial-computer-univac/ (2019년 10월 23일 최종접속).

31) 1951년 6월 미국 인구조사국(U.S.Census Bureau)에 설치되었다. David E. Lundstrom, A Few Good Men From Univac, MIT Press, 1987, pp.5-6, http://tcm.computerhistory.org/exhibits/FewGoodMen.pdf (2019년 10월 23일 최종접속); "The Story Behind America's First Commercial Computer", TIME 2016.3.31., https://time.com/4271506/census-bureau-computer-history/ (2019년 10월 23일 최종접속).

32) IBM, IBM 650, https://www.ibm.com/ibm/history/exhibits/650/650_intro.html (2019년 10월 23일 최종접속); IBM, 650 Applications, https://www.ibm.com/ibm/history/exhibits/650/650_ap1.html (2019년 10월 23일 최종접속).

[그림 2-7] 유니박[33]



[그림 2-8] IBM 650[34]



한편 1947년에 발명된 트랜지스터(Transistor)[35]가 진공관의 한계를 극복하고, 1958년 정보 저장에 이용될 집적회로(Integrated Circuit, IC)가 발명[36]되면서 컴퓨터

33) 이미지 출처: (좌) David E. Lundstrom, Ibid., p.46 Figure 1(Univac Scientific Computer System. Photograph courtesy of the Charles Babbage Institute and Unisys Corporation). (우) U.S. Census Bureau, UNIVAC I, https://www.census.gov/history/img/UNIVAC1105.jpg (2019년 10월 23일 최종접속).

34) 이미지 출처: (좌) IBM, a history of progress, p.30, https://www.ibm.com/ibm/history/interactive/ibm_history.pdf (2019년 10월 23일 최종접속). (우) IBM, IBM 650, https://www.ibm.com/ibm/history/exhibits/650/650_intro.html (2019년 10월 23일 최종접속).

35) Alaina G. Levine, "Bell Telephone Laboratories, New Jersey", APS(American Physical Society) physics, 2008, https://www.aps.org/programs/outreach/history/historicsites/transistor.cfm (2019년 10월 23일 최종접속); Marc A. Shampo/Robert A. Kyle/David P. Steensma, "William Shockley and the Transistor", Mayo Clinic Proceedings, Volume 87, Issue 6, Mayo Foundation for Medical Education and Research, 2012, p.43.

는 점차 소형화되었으나, 그럼에도 불구하고 컴퓨터는 여전히 너무 크고 비싸서 공공기관이나 기업에 의해서만 활용되었다. 이후 하나의 칩에 수천 또는 수백만 개의 전자회로 소자를 집적시키는 고밀도 집적회로(Large Scale Integration, LSI)와 초고밀도 집적회로(Very Large Scale Integration, VLSI) 기술이 개발되자 1971년 인텔(Intel)은 중앙처리장치가 하나의 칩에 들어있는 마이크로프로세서(microprocessor)를 내놓았고,[37] 이로써 개인용 컴퓨터가 대량 생산될 수 있는 획기적인 토대가 마련되었다. 최초의 개인용 컴퓨터는 1975년 MITS(Micro Instrumentation and Telemetry Systems)사의 에드 로버츠(Ed Roberts)가 인텔의 마이크로프로세서를 이용해서 개발한 '알테어(Altair) 8800'이었다.[38] 그러나 이 컴퓨터를 구동시킬 수 있는 운영체제가 없었던바, 당시 하버드대학에 재학 중이던 빌 게이츠(Bill Gates)와 폴 알렌(Paul Allen)이 알테어용 베이식 언어 해석기를 개발하여 판매하였다. 한편 개인용 컴퓨터가 본격적으로 보급되는 계기를 마련한 것은 스티브 잡스(Steve Jobs)와 스티브 워즈니악(Steve Wozniak)이 개발한 애플 컴퓨터였다. 1976년 애플(Apple)사를 설립한 이들은 그 이듬해 '애플 Ⅱ'라는 소형 컴퓨터를 출시하면서 컴퓨터의 대중화 시대를 열었다. 키보드를 통해 입력하고 그 결과를 모니터로 확인할 수 있도록 구현된 이 컴퓨터는 크기가 작고 사용법이 간편했으며, 가격이 1,300달러 정도로 저렴한 편이어서 큰 인기를 끌었다. 이에 중대형 컴퓨터 시장을 독점하며 개인용 컴퓨터에 큰 관심을 두지 않았던 IBM은 애플에 대항하기 위해 1981년 'IBM 퍼스널 컴퓨터(Personal Computer)'를 출시했고,[39] 설계 관련 사항을 공개하여 다른 회사의 제품과 호환될 수 있도록 함으로써 시장의 주도권을 잡게 되었다.[40]

---

36) Vaclav Smil, "July 1958: Kilby Conceives the Integrated Circuit", IEEE Spectrum, 2018.6.27., https://spectrum.ieee.org/semiconductors/devices/july-1958-kilby-conceives-the-integrated-circuit (2019년 10월 23일 최종접속).

37) Intel, The Story of the Intel® 4004: Intel's First Microprocessor, https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html (2019년 10월 23일 최종접속).

38) Forrest M. Mims III, "The Tenth Anniversary of the ALTAIR 8800", Computers & Electronics 1985.1., pp.58-59, http://www.classiccmp.org/dunfield/altair/d/pe0185er.pdf (2019년 10월 23일 최종접속); "Microsoft founders lead tributes to 'father of the PC'", BBC News 2010.4.2., http://news.bbc.co.uk/2/hi/technology/8600493.stm (2019년 10월 23일 최종접속).

39) IBM, The birth of the IBM PC, https://www.ibm.com/ibm/history/exhibits/pc25/pc25_birth.html (2019년 10월 23일 최종접속).

40) 현재 사용되고 있는 PC들의 기본적인 시스템 구조나 설계 방식도 여전히 IBM PC의 호환 규격을 따르고 있다.

[그림 2-9] 애플 II[41]



[그림 2-10] IBM 퍼스널 컴퓨터[42]



나. 컴퓨터를 이용한 범죄와 형사법적 대응 연혁

1) 컴퓨터를 이용한 범죄 대두

컴퓨터 기술이 발전하고 개인용 컴퓨터의 보급이 확대되면서 컴퓨터를 이용한 신종 범죄의 등장이 사회적 문제로 대두되었다.[43] 1967년 우리나라의 경제기획원(현 기획재정부의 전신 중 하나)이 컴퓨터를 들여온 이래로[44] 최초의 컴퓨터범죄로 기록되고 있는 것은 1971년 대구의 미군기지에서 발생했던 군수품유출사건이다.[45] 당시 미군부대에서 일하던 한국인 종업원들이 1천 7백만 달러 상당의 보급품을 빼돌리면서 컴퓨터에 저장된 물품기록을 모두 지워버려서 미국 상원이 발칵 뒤집힌 사건이다.[46] 이후 컴퓨터범죄가 크게 문제된 것은 1973년 10월에 발생한 반포AID차관아파트 부정추첨

41) 이미지 출처: "Apple II celebrates its 35th anniversary", The Verge 2012.4.16., https://www.theverge.com/2012/4/16/2953921/apple-ii-35th-anniversary (2019년 10월 23일 최종접속).
42) 이미지 출처: IBM, The IBM PC's debut, https://www.ibm.com/ibm/history/exhibits/pc25/pc25_intro.html (2019년 10월 23일 최종접속).
43) 이천현/도중진/권수진/신동일/김현우, 형법각칙 개정연구[9]-우리나라 및 주요 국가의 형법개정 동향-, 한국형사정책연구원, 2007, 37-38면.
44) "지금과는 사뭇 다른 '컴퓨터'의 옛 모습", 대한민국 정책브리핑 No.124, 2017년 4월 13일자, http://www.korea.kr/archive/longTimeAgoView.do;JSESSIONID_KOREA=iGc6PVX1HaYjIcS0sKtALMkvKmcBFStSxazJzLD3LJ6ECIF7QhpO!848344954!8614619?bbsKey=25729&themekey=longtimeago&pageIndex=1&rownum=124 (2019년 10월 23일 최종접속).
45) "컴퓨터 범죄(설왕설래)", 세계일보 1993년 2월 20일자, http://www.segye.com/newsView/19930220000015 (2019년 10월 23일 최종접속).
46) "외언내언", 서울신문 1991년 3월 22일자, http://www.seoul.co.kr/news/newsView.php?id=19910322001005 (2019년 10월 23일 최종접속).

사건이다.[47] 대한주택공사가 미국 국제개발국(Agency of International Development, AID)의 차관을 들여와 반포에 건설하는 대단지 아파트에 입주 신청이 몰리자 컴퓨터를 이용한 선정이 이루어졌는데,[48] 이를 담당했던 과학기술처 산하 중앙전자계산소(NCC) 소속 직원이 프로그램 처리과정을 조작해서 특정인을 당첨시킨 일이 드러난 것이다.[49] 반포AID차관아파트 부정추첨사건 이후 1992년 10월까지 발생한 컴퓨터범죄는 총 51건으로 집계되었는데, 그 중 금융기관에서 발생한 사건이 41건으로 전체 범죄의 80.4%를 차지하였다.[50] 일례로 1989년에는 외환은행 전산부 대리가 거래실적이 거래원장에 나타나지 않도록 프로그램을 조작해서 고객이 맡긴 예금을 180여 회에 걸쳐 불법 인출함으로써 총 6,200만원을 가로챈 사건이 발생하였다.[51]

한편 정보화 사회의 기반을 조성하기 위해서 전산망의 개발보급과 이용이 촉진됨에 따라 전산망 자체의 안정성과 정보의 신뢰성을 침해하거나 훼손하는 문제에 대한 경각심이 높아졌다. 정부 각 부처를 비롯하여 학교나 공공기관, 금융기관이나 기업체

---

47) 미군기지는 대한민국의 법률이 적용되지 않는 치외법권 지역인바, 반포AID차관아파트 부정추첨사건이 사실상 한국 최초의 컴퓨터범죄로 언급되기도 한다. 이 철, 컴퓨터범죄와 소프트웨어 보호, 박영사, 1995, 51면; 장영민/조영관, 컴퓨터범죄에 관한 연구, 한국형사정책연구원, 1991, 65면; 조규정, "컴퓨터조작범죄: 유형과 처벌을 중심으로", 형사정책연구 제1권 제2호(통권 제2호), 한국형사정책연구원, 1990, 109면.

48) 애당초 추첨은 안이 보이지 않는 상자 속에 지원자의 번호를 써넣은 은행 알을 넣어둔 후 경찰관이 입회한 가운데 추첨자(주택공사 직원)가 무작위로 은행 알을 뽑아서 그 번호를 외치면, 다른 한 사람(주택공사 직원)이 벽에 걸어둔 게시판에 이를 기록하는 방식이었다. 이후 주택공사 본사가 당첨된 번호들을 정리해 신문사에 넘겨서 이튿날 공시가 이루어졌는데, 추첨 현장에서 게시된 결과와 신문을 통해 보도된 공시 결과가 불일치하는 등 이런저런 문제들이 불거졌다. 이에 추첨에서 떨어진 사람들이 거세게 항의하며 시위를 벌이자 주택공사 측은 그 과정을 점검한 후 문제가 있다고 판단한 150여 세대를 다시 추첨하기로 결정했다. 이미 추첨 과정에 대한 신뢰가 떨어진 상황이라 주택공사 측은 컴퓨터 추첨으로 그 방식을 변경하면서, 당시 도입된 컴퓨터 중에서 가장 성능이 우수했던 '유니백1106'을 보유한 과학기술처 산하 중앙전자계산소에 재추첨을 의뢰하였다. "국민검사 심재륜의 수사일지 ⑤ 국내 최초 컴퓨터 범죄를 밝히다", 월간조선 2012년 5월호, https://monthly.chosun.com/client/news/viw.asp?nNewsNumb=201205100050 (2019년 10월 23일 최종접속); "국내 첫 컴퓨터 범죄 발생… 시행기관 직원이 부정 당첨 조작", 경영과 컴퓨터 2006년 9월호, 한국데이터산업진흥원, https://kdata.or.kr/info/info_03_view.html?field=&keyword=&type=trend&page=309&dbnum=129768&mode=detail&type=trend (2019년 10월 23일 최종접속).

49) 당시 추첨 프로그램은 컴퓨터 성능의 한계로 인해 그 과정을 저장할 수 없었다. 이에 25장의 조작된 프로그램 카드를 끼워 넣어서 무조건 당첨되게 한 다음에 다시 빼내는 수법으로 조작의 증거를 남기지 않았다고 한다(서울형사지방법원 74고합102, 특정범죄가중처벌등에관한법률위반). 이 철, 앞의 책, 51면.

50) 한국전산원, 정보화 역기능 현황 및 분석, 1994.12., 27면.

51) "컴퓨터범죄/대부분 금융기관서 발생", 세계일보 1992년 7월 7일자, http://www.segye.com/newsView/19920707000060 (2019년 10월 23일 최종접속).

등의 전산망이 구축되어 가면서 그 망에 침입하여 정보를 조작하거나 유출하는 사건이 늘어난 것이다. 1993년에는 컴퓨터통신망에 침입해서 청와대 계정의 ID와 비밀번호를 알아낸 후 농협 등 금융기관 전산망에 대한 주요자료를 수집한 뒤 휴면계좌에 있는 돈을 빼돌리려고 했던 대입 3수생이 언론의 주목을 받았고,[52] 1994년에는 16세의 영국 소년이 한국원자력연구소의 컴퓨터에 침입했던 사건이 알려지면서 논란이 일기도 했다.[53] 일련의 전산망 침입 사건들은 컴퓨터범죄 대책 마련의 필요성을 절감하게 만드는 계기가 되었다.[54]

---

52) 「이번 사건은 우리나라가 이제 더 이상 최첨단 컴퓨터범죄의 사각지대가 아님을 분명히 보여주고 있다. 더욱이 김씨가 청와대·재무부 등 국가기관의 컴퓨터통신 사용자 이름과 비밀번호를 도용해 업체와 기관들의 주요 정보를 빼내 대형 금융범죄를 벌이려고 한 것은 지금까지의 컴퓨터범죄 수준을 훨씬 뛰어넘었다는 점에서 충격을 던져주고 있다. 지금까지의 컴퓨터범죄는 금융기관의 내부직원이 단말기를 조작해 예금액을 거짓으로 늘린 뒤 돈을 빼내는 수준에 그쳐왔다. 그러나 이번 사건은 업체나 기관이 권력에 약하다는 속성을 이용해 청와대를 사칭하는 '고전적 수법'과 컴퓨터통신망에 침입해 정보를 빼내려는 '첨단 수법'을 혼합한 컴퓨터범죄라는 점에 문제의 심각성이 있다. 이제 우리나라도 국가기관 전산망의 비밀번호를 해독하거나 빼내 전산망에 침투한 뒤 중요 국가기밀을 수집하고 팔아넘기는 고도의 컴퓨터 스파이 범죄에 안전하다고 할 수 없게 된 것이다.」 "청와대 사칭 컴퓨터범죄 '충격'(현장추적)", 한겨레 1993년 2월 18일자(제1478호), 12면; "청와대 업무인수팀 사칭 컴퓨터사기/범인은 IQ 140 고졸자", 조선일보 1993년 2월 18일자, http://news.chosun.com/svc/content_view/content_view.html?contid=1993021873101 (2019년 10월 23일 최종접속).

53) 「16세 소년으로 알려진 영국의 컴퓨터 해커는 1994년 6월초 한국원자력연구소의 컴퓨터에 침입했던 것으로 알려졌다. 관련기사를 쓴 워싱턴타임스지의 기자는 1994년 11월 4일 원자력연구소(KAERI)가 아니라 영문명칭이 유사한 항공우주연구소(KARI)가 해커의 피해를 입었을 가능성이 있다는 과기처의 발표에 언급, "미공군 컴퓨터범죄 수사반은 분명히 한국원자력연구소에 해커가 침입했다고 밝혔다"고 확인하면서 "그러나 해커는 원자력연구소의 데이터를 복사했을 뿐 데이터자체를 파괴하지 않았기 때문에 데이터들이 그대로 있을 것"이라고 설명했다. 아노드 보그라브(Arnaud de Borchgrave) 기자는 "한국원자력연구소는 분명히 해커의 침범 사실자체를 알지 못했을 것"이라면서 "해커가 미국방부 항공우주국(NASA)의 컴퓨터조차 상대방도 모르게 침범하는 사례가 적지 않기 때문에 한국의 원자력연구소가 해커의 침범사실을 부끄러워할 필요는 없다"고 말했다. 그는 컴퓨터 해커인 문제의 영국소년은 체포됐다가 곧 석방됐고, 현행 영국법상 이 소년을 처벌할 규정이 없어 법률논쟁이 계속되고 있다고 설명하면서 이번 사건이 지난 6월 초에 발생했다고 말했다.」 "South Korea Says Slim Chance Hacker Stole Nuclear Secrets", L.A. Times 1994.11.5., https://www.latimes.com/archives/la-xpm-1994-11-05-mn-58774-story.html (2019년 10월 23일 최종접속); "원자력연구소 컴퓨터침범사건 지난 6월 발생", 매일경제신문 1994년 11월 5일자, https://www.mk.co.kr/news/home/view/1994/11/56605/ (2019년 10월 23일 최종접속).

54) 「1992년 서울대 교육전산망용 컴퓨터시스템에 해커가 침입해 전산망을 휘저어 정보를 모조리 파괴한 사건은 최첨단 컴퓨터범죄가 이미 발등에 떨어진 불처럼 위험수위에 이르렀다는 사실을 그대로 보여주고 있다. 더욱이 지난 89년 일본 도쿄대의 컴퓨터에 한 한국인이 개인용컴퓨터로 하와이를 경유하는 전산망을 통해 침입했던 사건이 일어나 일본이 조사를 요청해왔던 적도 있을 만큼 우리나라 컴퓨터광들의 수준은 이미 컴퓨터시스템의 보안장치를 자유롭게 풀고 들어갈 정도여서 최첨단 컴퓨터범죄에 대한 대책 마련이 시급한 실정이다.」 "청와대 사칭 컴퓨터범죄 '충격'(현장추적)", 한겨레 1993년 2월 18일자(제1478호), 12면.

컴퓨터를 이용한 범죄에 대해서는 문서범죄나 사기죄 및 업무방해죄 등을 적용하려는 시도가 이루어졌으나 그 구성요건해당성이 인정되는 데에는 한계가 있었다. 첫째, 컴퓨터 등 정보처리장치로부터 출력된 기록은 문서에 해당하나 매체에 기록되어 출력되기 전의 전자기록은 가시성과 가독성이 없어서 문서로 인정될 수 없었다. 또한 전자기록의 경우 입력된 정보는 기존의 데이터와 함께 처리되어 만들어지는가 하면 해당 기록에 명의인이 없거나 불분명한 경우가 많아서 문서에서와 같은 명의인을 전제하기가 어려웠던바, 문서범죄로 처벌될 수 없었다.[55] 둘째, 사람이 개입하지 않고 컴퓨터 등 정보처리장치에 의해 자동적으로 처리되는 거래형태가 증가하는 상황에서, 이를 통해 불법한 이익을 취득하는 행위는 재물의 점유이전이 수반되지 않아서 절도죄로 처벌될 수 없고, 사람에 대한 기망행위가 없어서 사기죄로도 처벌될 수 없었다. 셋째, 사람의 신체적 동작에 의해 수행되던 업무처리가 컴퓨터 등 정보처리장치에 의해 이루어지면서 컴퓨터에 대한 가해행위를 수단으로 해서 사람의 업무를 방해할 가능성이 커졌으나, 컴퓨터의 사용방해나 정보의 부정조작 등이 업무방해죄를 구성하는지에 대해서는 해석상 논란이 있었다.[56] 넷째, 종래 비밀침해죄나 공무상비밀표시무효죄의 객체는 봉함 기타 비밀장치한 문서나 도화 등으로 한정되었기 때문에 동 규정들로 이른바 정보탐지나 컴퓨터 스파이를 처벌할 수 없었다. 다섯째, 저장매체에 기록된 정보 자체를 재물로 인정하는 것에 대하여도 의문이 제기되었는바, 사람의 지각에 의하여 인식될 수 없는 방식으로 작성되어 컴퓨터 등 정보처리를 위해 제공된 전자기록 등 특수매체기록의 효용을 해한 경우를 기존의 손괴죄 규정을 적용하여 처벌할 수 없다는 문제가 발생하였다.

2) 형사법적 대응 연혁

전산망의 개발보급 및 이용 등을 촉진함으로써 정보화 사회의 기반을 조성하고자 1986년 5월 12일 법률 제3848호로 「전산망보급확장과이용촉진에관한법률」이 제정

---

55) 자기테이프나 디스크 등 전자적 기록이 법률상 문서의 개념에 포함되지 않는 상황에서 그에 대한 위조·변조를 처벌하는 데에 공백이 발생하였다. "「컴퓨터범죄」 처벌규정 만든다/95년까지/자기테이프·디스크 문서간주", 서울신문 1991년 12월 31일자, http://www.seoul.co.kr/news/newsView.php?id=19911231018001 (2019년 10월 23일 최종접속).

56) 강동범, "컴퓨터범죄에 대한 입법론적 대책", 형사정책 제3호, 한국형사정책학회, 1998, 86-88면; 장영민/조영관, 앞의 보고서, 104-107면; 전지연, "컴퓨터범죄에 대한 형법적 대응방안", 한림법학 FORUM 제5권 제1호, 한림대학교 법학연구소, 1996, 142, 145면.

되어 1987년 1월 1일부로 시행되었다.[57] 동법은 불법 또는 부당한 방법으로 전산망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 침해하거나 훼손하는 행위를 처벌하였고(1986년 5월 12일 시행된 전산망보급확장과이용촉진에관한법률 제29조), 전산망에 의하여 처리·보관·전송되는 타인의 비밀을 침해하거나 누설하는 행위를 처벌하였다(동법 제30조).

[표 2-1] 1986년 5월 12일 시행된 전산망보급확장과이용촉진에관한법률의 벌칙[58]

전산망보급확장과이용촉진에관한법률 [시행 1987.1.1.] [법률 제3848호, 1986.5.12, 제정]
제22조(전산망의 안정성등) ① 전산망을 이용하여 정보를 처리, 보관, 전송하는 사업을 영위하는 자는 전산망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 강구하여야 한다. ② 누구든지 불법 또는 부당한 방법으로 제1항의 규정에 의한 보호조치를 침해하거나 훼손하여서는 아니된다.
제25조(비밀의 보호) 누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 비밀을 침해하거나 누설하여서는 아니된다.
제29조(벌칙) 제22조 제2항의 규정에 위반한 자는 3년 이하의 징역 또는 300만원 이하의 벌금에 처한다.
제30조(벌칙) ① 제25조의 규정에 위반한 자는 3년 이하의 징역 또는 300만원 이하의 벌금에 처한다. ② 전산망사업자가 제1항의 죄를 범한 때에는 5년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

이후 동법은 정보통신의 국제화 및 전산망의 급속한 확산에 따른 변화된 환경에 효과적으로 대처하고자 1991월 12월 14일에 법률 제4439호로 일부 개정되어 같은 날 시행되었는데, 이 개정을 통해 종래의 벌칙 규정이 아래의 [표 2-2]와 같이 상향 조정되었다.[59] 또한 동법은 체신부(정보통신부 이전의 명칭) 장관으로 하여금 전산망의 설계나 구성 및 유지보수가 기술기준에 적합하지 아니할 경우에는 그 시정 등 기타 필요한 조치를 명할 수 있도록 규정하고 있는데(동법 제14조 제3항), 이를 이행하

57) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=573&ancYd=19860512&ancNo=03848&efYd=19870101&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

58) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=573&ancYd=19860512&ancNo=03848&efYd=19870101&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

59) 법제처 국가법령정보센터, 제정·개정이유 및 신구법비교 참조, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=575&ancYd=19911214&ancNo=04439&efYd=19911214&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

지 아니한 경우에는 1년 이하의 징역 또는 300만원 이하의 벌금에 처하도록 하는 벌칙 규정을 신설함으로써 법 집행의 실효성을 도모하였다.[60]

[표 2-2] 1991년 12월 14일 개정된 전산망보급확장과이용촉진에관한법률의 벌칙[61]

전산망보급확장과이용촉진에관한법률 [시행1991.12.11] [법률 제4393호, 1991.8.10, 타법개정]	전산망보급확장과이용촉진에관한법률 [시행1991.12.14] [법률 제4439호, 1991.12.14, 일부개정]
제29조(벌칙) 제22조 제2항의 규정에 위반한 자는 3년 이하의 징역 또는 300만원 이하의 벌금에 처한다.	제29조(벌칙) ----------위반하여 전산망의 보호조치를 침해 또는 훼손----------1천만원 이하----------.
제30조(벌칙) ① 제25조의 규정에 위반한 자는 3년 이하의 징역 또는 300만원 이하의 벌금에 처한다.	제30조(벌칙) ① ---------- 위반하여 타인의 비밀을 침해 또는 누설----------1천만원 이하----------.
② 전산망사업자가 제1항의 죄를 범한 때에는 5년 이하의 징역 또는 500만원 이하의 벌금에 처한다.	② 전산망사업에 종사하는 자----------2천만원 이하----------.
〈신 설〉	제30조의2(벌칙) 제14조 제3항의 규정에 의한 시정등의 명령을 이행하지 아니한 자는 1년 이하의 징역 또는 300만원 이하의 벌금에 처한다.

나아가 동법은 정보화의 진전에 따라서 점차 중요성이 커져가는 전산망의 안전과 신뢰성을 확보하고, 전자문서의 이용을 촉진하고자 1995년 12월 6일에 법률 제4998호로 또 한 차례 개정된 후 1996년 3월 7일부로 시행되었다.[62] 개정법은 전자문서에 대해 정의하면서[63] 이를 위작·변작하거나 위작·변작된 전자문서를 행사하는 것을

60) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=575&ancYd=19911214&ancNo=04439&efYd=19911214&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

61) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=575&ancYd=19911214&ancNo=04439&efYd=19911214&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

62) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=578&ancYd=19951206&ancNo=04998&efYd=19960307&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

63) "전자문서"라 함은 국가기관, 지방자치단체 및 법령의 규정에 의하여 그 위탁을 받은 자가 전산망을 이용하여 전송·처리 또는 보관하는 문서형식의 자료로서 표준화된 것을 말한다([시행 1996.3.7.] 전산망보급확장과이용촉진에관한법률 제2조 제3호).

금지하였고, 이를 위반한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 하였으며, 그 외의 벌칙 규정들을 정비하였다.[64]

[표 2-3] 1995년 12월 6일 개정된 전산망보급확장과이용촉진에관한법률의 벌칙[65]

전산망보급확장과이용촉진에관한법률 [시행1996.1.1] [법률 제4969호, 1995.8.4, 타법개정]	전산망보급확장과이용촉진에관한법률 [시행1996.3.7] [법률 제4998호, 1995.12.6, 일부개정]
제25조(비밀의 보호) 누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 비밀을 침해하거나 누설하여서는 아니된다.	제25조(비밀등의 보호) ① 누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 정보를 훼손하거나 비밀을 침해·도용 또는 누설하여서는 아니된다.
〈신 설〉	② 누구든지 전자문서를 위작·변작하거나 위작·변작된 전자문서를 행사하여서는 아니된다.
제29조(벌칙) 제22조 제2항의 규정에 위반하여 전산망의 보호조치를 침해 또는 훼손한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.	제29조(벌칙) ① 제25조 제2항의 규정을 위반하여 전자문서를 위작·변작하거나 그 사정을 알면서 위작·변작된 전자문서를 행사한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.
〈신 설〉	② 제1항의 미수범은 처벌한다.
제30조(벌칙) ① 제25조의 규정에 위반하여 타인의 비밀을 침해 또는 누설한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.	제30조(벌칙) 제25조 제1항의 규정에 위반하여 타인의 정보를 훼손하거나 비밀을 침해·도용 또는 누설한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
② 전산망사업에 종사하는 자가 제1항의 죄를 범한 때에는 5년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.	〈삭 제〉
제30조의2(벌칙) 제14조 제3항의 규정에 의한 시정 등의 명령을 이행하지 아니한 자는 1년 이하의 징역 또는 300만원 이하의 벌금에 처한다.	제30조의2(벌칙) 제22조 제2항의 규정에 위반하여 전산망의 보호조치를 침해 또는 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
〈신 설〉	제30조의3(벌칙) 제14조 제3항의 규정에 의한 시정 등의 명령을 이행하지 아니한 자 및 제17조의4 제2항의 규정에 의한 전자문서의 보관의무를 위반한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
〈신 설〉	제30조의4(벌칙) 제17조의5의 규정을 위반하여 전자문서 또는 전자계산조직에 입력되어 있는 기록을 공개한 전산망관리자는 1천만원 이하의 벌금에 처한다.

64) 법제처 국가법령정보센터, 제정·개정이유 및 신구법비교 참조, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=578&ancYd=19951206&ancNo=04998&efYd=19960307&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

65) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=578&ancYd=19951206&ancNo=04998&efYd=19960307&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

한편 사회가 산업화·정보화되는 추세에 따라 컴퓨터범죄 등 신종범죄에 효율적으로 대처함으로써 국민생활의 안정을 도모하고 현행규정의 미비점을 개선·보완하고자 1995년 12월 29일 법률 제5057호로 형법 일부가 개정되어 1996년 7월 1일부터 시행되었다.[66] 컴퓨터 기술의 발전 및 개인용 컴퓨터 보급의 확대에 따라서 컴퓨터 관련 법익침해행위의 처벌 필요성이 증가하였음에도 불구하고 기존의 형법 구성요건만으로는 포섭할 수 없다는 문제를 해결하고자 1995년 형법 개정을 통해 새로운 구성요건을 신설하거나 개정하는 작업이 단행된 것이다.[67]

해당 형법개정을 통해 첫째, 컴퓨터해킹을 포함하여 전자적 기록에 대한 직접적인 위조·변작은 물론이고 타인의 전산망에 침입해서 저장된 기록 등을 조작하는 범죄를 처벌하는 규정이 제·개정되었는바,[68] 공전자기록위작·변작(형법 제227의2)과 사전자기록위작·변작(동법 제232조의2)을 신설하고, 공정증서원본등의 부실기재(동법 제228조)와 위조등 공문서의 행사(동법 제229조), 위조사문서등의 행사(동법 제234조) 규정이 정비되었다. 둘째, 사람에 대한 직접적인 기망행위가 존재하지 않는 경우에 사기죄로 처벌할 수 없는 법적 공백을 해소하고자 "컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자를 처벌"하는 컴퓨터등사용사기죄(동법 제347조의2)[69]가 신설되었다.[70] 셋째, "컴퓨터등 정보처리장치 또는 전자기록등 특수매체

---

66) 법제처 국가법령정보센터, http://www.law.go.kr/lsInfoP.do?lsiSeq=62388&ancYd=19951229&ancNo=05057&efYd=19960701&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

67) 박상기, "개정형법의 내용과 문제점", 형사정책연구 제7권 제1호(통권 제25호), 한국형사정책연구원, 1996, 156면; 장영민, "개정형법의 컴퓨터범죄", 고시계 1996년 2월호(통권 제468호), 고시계사, 1996, 42면.

68) 박상기, 앞의 글, 157면.

69) 1995년 형법 개정을 통해 편의시설부정이용죄(제348조의2)도 신설되었는데, 부정한 방법으로 대가를 지급하지 아니하고 자동판매기, 공중전화 기타 유료자동설비를 이용하여 재물 또는 재산상의 이익을 취득한 자는 3년 이하의 징역, 500만원 이하의 벌금, 구류 또는 과료에 처하도록 했다. 기계를 이용하여 불법한 이익을 취득한 경우에 성립되는 범죄라는 점에서는 편의시설부정이용죄와 컴퓨터사용사기죄가 공통되나, 전자는 자동판매기 등 유료자동설비를 이용한 경우에 적용되는 것에 반해 후자는 컴퓨터를 이용한 경우에 적용된다는 점에서 차이가 있다.

70) 컴퓨터등 사용사기죄는 2001년 12월 29일에 단행된 형법 개정을 통해 다시 정비되었다. 종래에는 일시적으로 취득하였거나 절취한 타인의 신용카드를 이용해서 ATM에서 돈을 인출할 때 정상적인 비밀번호를 입력하면 권한은 없지만 부정한 명령이 아니어서 컴퓨터등 사용사기죄로 처벌할 수 없다는 문제가 지적되었다. '부정한 명령의 입력'이라는 개념에는 '진정한 자료를 권한 없이 입력·변경하는 행위'가 포함되지 않는다는 비판이 제기된 것이다. 이에 동 개정을 통해 컴퓨터등 사용사기죄의 구성요건에 "권한 없이 정보를 입력·변경하여 정보처리를 하게 하는 행

기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자"를 처벌하는 업무방해죄(동법 제314조 제2항)가 신설되었다.[71] 넷째, "봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자"를 처벌하는 비밀침해죄(동법 제316조 제2항)와 공무상비밀표시무효죄(동법 제140조 제3항)가 신설되었다. 마지막으로 재물손괴죄(동법 제366조)와 공용서류등의 무효 및 공용물의 파괴(동법 제141조)에 타인의 재물이나 문서는 물론이고 전자기록등 특수매체기록이 행위의 객체로 추가되었다.[72]

[표 2-4] 1995년 형법 개정을 통한 컴퓨터 관련 범죄 대응[73]

형법 [시행 1988.12.31] [법률 제4040호, 1988.12.31, 일부개정]	형법 [시행 1996.7.1] [법률 제5057호, 1995.12.29, 일부개정]
〈신 설〉	제140조(공무상비밀표시무효) ③ 공무원이 그 직무에 관하여 봉함 기타 비밀장치한 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다.
제141조(공용서류등의 무효, 공용물의 파괴) ① 공무소에서 사용하는 서류 기타 물건을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해한 자는 7년 이하의 징역 또는 3만 5천환 이하의 벌금에 처한다.	제141조(공용서류등의 무효, 공용물의 파괴) ① ---------- 물건 또는 전자기록등 특수매체기록을---------- ----------7년 이하 ----------1천만원 이하 ----------.

위"가 추가되었다. 이천현/도중진/권수진/신동일/김현우, 앞의 보고서, 69-71면; 황만성, "형법상 사기죄 관련규정의 제·개정방안", 형사정책연구 제20권 제1호(통권 제77호), 한국형사정책연구원, 2009, 479-480면 참조.

71) 컴퓨터 등에 대한 사보타주를 처벌하는 규정으로서 물리적 손괴는 물론이고 바이러스에 감염시키는 행위 등 정보처리 과정에 장애를 일으키는 일체의 행위가 포함된다. 박상기, 앞의 글, 159-160면.

72) 1995년 제3차 형법 개정을 통해 ① 컴퓨터조작범죄와 ② 컴퓨터파괴범죄 및 ③ 데이터 스파이범죄와 관련된 구성요건이 정비되었다고 평가하는 견해도 있다. 이 견해에 따르면 우선 공전자기록위작·변작(제227조의2), 공정증서원본부실기재(제228조), 위조공문서등행사(제229조), 사전자기록위작·변작(제232조의2), 위조사문서등행사(제234조) 및 컴퓨터사용사기죄(제347조의2) 등은 컴퓨터조작범죄에 속한다. 한편 컴퓨터 업무방해죄(제314조 제2항)와 컴퓨터 데이터파괴죄(제366조)는 컴퓨터파괴범죄로, 컴퓨터 데이터탐지죄(제316조 제2항)는 데이터 스파이범죄로 각각 분류된다. 장영민, 앞의 글, 43면.

73) 법제처 국가법령정보센터, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=62388&ancYd=19951229&ancNo=05057&efYd=19960701&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

형법 [시행 1988.12.31] [법률 제4040호, 1988.12.31, 일부개정]	형법 [시행 1996.7.1] [법률 제5057호, 1995.12.29, 일부개정]
〈신 설〉	제227조의2(공전자기록위작·변작) 사무처리를 그르치게 할 목적으로 공무원 또는 공무소의 전자기록등 특수매체기록을 위작 또는 변작한 자는 10년 이하의 징역에 처한다.
제228조(공정증서원본등의 부실기재) ① 공무원에 대하여 허위신고를 하여 공정증서원본에 부실의 사실을 기재하게 한 자는 5년 이하의 징역 또는 2만 5천환이하의 벌금에 처한다.	제228조(공정증서원본등의 불실기재) ① ----------공정증서원본 또는 이와 동일한 전자기록등 특수매체기록----------기재 또는 기록하게 ----------1천만원----------.
제229조(위조등의 공문서의 행사) 위조, 변조, 작성, 변작 또는 부실기재한 전4조기재의 문서, 도화, 공정증서원본, 면허장, 감찰 또는 여권을 행사한 자는 위조, 변조, 작성, 변작 또는 부실기재의 각죄에 정한 형에 처한다.	제229조(위조등 공문서의 행사) 제225조 내지 제228조의 죄에 의하여 만들어진 문서, 도화, 전자기록등 특수매체기록, 공정증서원본, 면허증, 허가증, 등록증 또는 여권을 행사한 자는 그 각 죄에 정한 형에 처한다.
〈신 설〉	제232조의2(사전자기록위작·변작) 사무처리를 그르치게 할 목적으로 권리·의무 또는 사실증명에 관한 타인의 전자기록등 특수매체기록을 위작 또는 변작한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제234조(위조등의 사문서의 행사) 위조, 변조 또는 작성한 전3조 기재의 문서 또는 도화를 행사한 자는 위조, 변조 또는 작성의 각죄에 정한 형에 처한다.	제234조(위조사문서등의 행사) 제231조 내지 제233조의 죄에 의하여 만들어진 문서, 도화 또는 전자기록등 특수매체기록을 행사한 자는 그 각 죄에 정한 형에 처한다.
〈신 설〉	제314조(업무방해) ② 컴퓨터등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형과 같다.
〈신 설〉	제316조(비밀침해) ② 봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다.
제323조(권리행사방해) 타인의 점유 또는 권리의 목적이 된 자기의 물건을 취거, 은닉 또는 손괴하여 타인의 권리행사를 방해한 자는 5년 이하의 징역 또는 1만 5천환 이하의 벌금에 처한다.	제323조(권리행사방해)----------물건 또는 전자기록등 특수매체기록 ----------5년 이하 --700만원 이하----------.

형법 [시행 1988.12.31] [법률 제4040호, 1988.12.31, 일부개정]	형법 [시행 1996.7.1] [법률 제5057호, 1995.12.29, 일부개정]
〈신 설〉	제347조의2(컴퓨터등 사용사기) 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제366조(재물 또는 문서의 손괴) 타인의 재물 또는 문서를 손괴 또는 은닉 기타 방법으로 기 효용을 해한 자는 3년 이하의 징역 또는 1만 5천환 이하의 벌금에 처한다.	제366조(재물손괴등) ---------- 재물, 문서 또는 전자기록등 특수매체기록을---------- ---------- ---------- 3년 이하-----700만원 이하----------.

2. 인터넷 상용화와 형사법적 대응

가. 인터넷의 등장과 대중화

1) 인터넷의 등장

컴퓨터가 발전함에 따라서 그 용도는 단순한 계산기에서 벗어나서 종합적인 정보 단말기로 거듭나게 되었다. 컴퓨터로 처리해야 할 데이터가 다양해지고 그 용량이 방대해지면서 두 대 이상의 컴퓨터가 데이터를 주고받을 수 있는 방안이 모색되었다. 디스크(Disc)로 대표되는 초창기 보조기억장치에 데이터를 저장한 후 교환하는 방식은 많은 시간이 소요되었고, 컴퓨터들을 직접 케이블로 연결해서 데이터를 교환하는 방식은 컴퓨터 간 물리적 거리의 제한을 받을 수밖에 없었다.

1960년 미국의 심리학자이자 컴퓨터공학자인 조셉 릭라이더(Joseph Carl Robnett Licklider)는 시간대를 나누어 한 대의 컴퓨터로 여러 작업을 효율적으로 처리할 수 있는 '시분할 시스템(Time Sharing System, TSS)'에 대한 기초 이론을 발표하였다.[74] 이는 사용자가 데이터를 입력하거나 출력하는 속도가 컴퓨터의 연산 속도에 비해 느리다는 점에 착안하였는바, 특정 사용자가 데이터를 입출력하는 사이에 컴퓨터는 그 공백 시간을 이용해서 다른 사용자가 입력한 데이터를 처리할 수 있다는 것이다.[75]

74) Joseph C. R. Licklider, "Man-Computer Symbiosis", IRE(now IEEE) Transactions on Human Factors in Electronics, HFE-1, 1960.3., pp.4-11, http://worrydream.com/refs/Licklider%20-%20Man-Computer%20Symbiosis.pdf (2019년 10월 23일 최종접속).

이러한 시분할 시스템은 이후 등장한 대다수 컴퓨터 네트워크 시스템의 기본 이론이 되었다. 또한 미국의 컴퓨터공학자 레너드 클라인록(Leonard Kleinrock)[76]과 폴 바랜(Paul Baran)[77] 등은 패킷교환(Packet Switching)[78]의 이론적 토대를 제공함으로써 컴퓨터 네트워크상 데이터 통신이 가능할 수 있도록 하였다. 한편 조셉 릭라이더는 1962년에 전 세계의 컴퓨터를 상호 연결하는 구상으로서 "은하 네트워크(Galactic Network)"라는 개념을 제안했고,[79] 1968년에는 로버트 테일러(Robert Taylor)와 함께 "커뮤니케이션 장치로서의 컴퓨터(The Computer as a Communication Device)"라는 논문을 발표해서 큰 반향을 일으켰다.[80]

---

75) Joseph C. R. Licklider, Ibid., pp.5-10.

76) 레너드 클라인록은 1963년 MIT에서 "Message Delay in Communication Nets with Storage"라는 논문으로 박사학위를 취득하였는데, 그가 61년 발표한 "Information Flow in Large Communication Nets"는 컴퓨터를 매개로 한 커뮤니케이션 방식인 패킷교환(Packet Switching) 이론에 관한 최초의 논문으로 평가된다. Andrew Murray, Information Technology Law: The Law and Society, Oxford University Press, 2019, p.24; 이재현, 인터넷, 커뮤니케이션북스, 2013, 15면.

77) 1964년 폴 바랜은 미국의 글로벌 정책 싱크탱크인 RAND(Research ANd Development)에서 "분산 커뮤니케이션에 관한 연구(On Distributed Communication)"를 수행·발표하였다. 이 보고서에서 바랜은 "중복 연결(redundancy of connectivity)"의 원리를 제안하였고, 탈중앙집중적인 명령과 통제 시스템을 구축하면 시스템의 일부가 파괴되더라도 전체 시스템의 손실이 최소화될 수 있다고 보았다. Paul Baran, On Distributed Communications, RM-3420-PR, RAND Corporation, 1964, https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf (2019년 10월 23일 최종접속).

78) 발신단말기에서 송출된 정보를 일단 교환기가 수신해서 기억장치에 축적한 후 착신단말기로 전달하는 축적교환 방식 중 하나이다. 이때 전송되는 정보는 일정 길이의 블록으로 분할되는데, 각각의 블록에는 전송에 필요한 제어정보가 포함된 헤더(header)가 붙여지는바, 이것이 바로 패킷이다. 패킷교환의 경우 송출된 정보가 교환기의 기억장치에 축적되기 때문에 통신의 공백시간을 융통할 수 있고, 이로 인해 1개의 회선을 통해 다중통신이 가능하다. Jim Costello/Paul Dyer/David L. Jeanes, "Packet switching", Fraidoon Mazda(ed.), Telecommunications Engineer's Reference Book, Butterworth-Heinemann, 1993, pp.54/3-54/6; Lawrence G. Roberts, "The Evolution of Packet Switching", Proceedings of the IEEE, Volume 66, Issue 11, IEEE, 1978, p.1307.

79) Joseph C. R. Licklider/Robert W. Taylor, "On-Line Man Computer Communication", G. A. Barnard(ed.), AFIPS(American Federation of Information Processing Societies): Proceedings 1962 Spring Joint Computer Conference, San Francisco, California, May 1-3, Volume 21, National Press, 1962, pp.113-128.

80) Joseph C. R. Licklider/Robert W. Taylor, "The Computer as a Communication Device", Science and Technology, Volume 76, 1968, pp.21-31. 조셉 릭라이더는 오늘날 인터넷의 전신이라고 할 수 있는 '아르파넷(ARPANET)'의 토대를 만든 기여를 높게 평가받아서 이른바 "인터넷의 아버지"라고 불리기도 한다. David Malakoff, "The Real Father of the Internet", Science, Volume 285, Issue 5433, American Association for the Advancement of Science (AAAS), 1999.9.3., p.1478.

1969년 미국의 국방부 산하 고등연구계획국(Advanced Research Project Agency, ARPA)[81]은 최초의 인터넷망이라고 할 수 있는 '아르파넷(Advanced Research Projects Agency Network, ARPANET)'을 구축하였다.[82] 이는 종래 컴퓨터와 컴퓨터를 직접 연결하던 회선교환(Circuit Switching)[83] 방식 대신에 대규모 통신망을 구축한 후 이에 연결된 컴퓨터들 간에 데이터를 주고받을 수 있도록 한 것이다.[84] 첫 가동 당시에는 UCLA(University of California, Los Angeles) 네트워크측정센터(Network Measurement Center), 스탠포드연구소(Stanford Research Institute, SRI), UC 산타바바라(University of California, Santa Barbara), 유타 대학(University of Utah)이 참여하여 총 4개의 호스트 컴퓨터가 연결되었으나, 이후 그 수는 점차 늘어났다.[85]

---

81) 1957년 구 소련이 세계 최초로 인공위성 스푸트니크 1호를 발사하여 지구 궤도에 올려놓는 데 성공하자 미국과 서방 국가들은 충격에 휩싸였고, '스푸트니크 쇼크'라는 신조어까지 등장했다. 미국은 아이젠하워 대통령의 지시로 그 이듬해인 1958년에 국방부 산하에 '고등연구계획국(Advanced Research Projects Agency, ARPA)'을 설립했는데, 이는 오늘날 '방위고등연구계획국(Defense Advanced Research Projects Agency, DARPA)'의 전신이다. '적의 기술적 진보에 놀라지 않고, 적을 기술적 진보로 놀라게 한다.'라는 설립취지에서 알 수 있듯이 이후 미국은 획기적인 국방기술 개발에 도전하였다. 이를 통해 인터넷의 시초가 된 아르파넷(ARPANET)을 필두로 하여 GPS 기술은 물론이고 전자레인지나 탄소섬유 등과 같은 다양한 혁신적 기술의 결과물이 도출되었다. 장용석, "ARPA, DARPA, ARPA-E : 창의적 연구개발 모형", 과학기술정책 제21권 제3호(통권 제184호), 과학기술정책연구원, 2011, 106-108면.

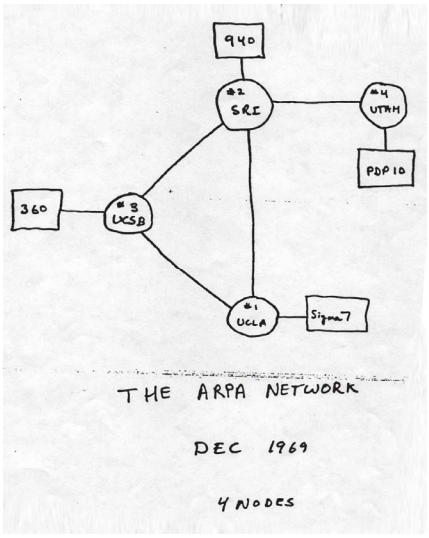
82) 복수의 통신망이 모여 있는 광역 통신망을 뜻하는 일반명사가 '인터네트워크(internetwork)'인데, 미국의 아르파넷은 인터네트워크를 본격적으로 구축한 최초의 사례였다. 이재현, 인터넷과 사이버사회, 커뮤니케이션북스, 2001, 58-59면; 이재현, 앞의 책(인터넷), 19-20면.

83) 회선교환(circuit switching) 방식은 음성전화망에 채택되었던 것으로서 통신을 위해서는 발신자와 착신자 사이에 전용 회선이 설정되어야 했다. 인터넷 이전의 데이터 통신 역시도 송수신자 간에 회선이 확보되어야 하는 접속형 통신이었다. 이 경우 전송로 중 어느 한곳에 문제가 생기면 그 전체가 제 기능을 수행하지 못하게 되는 한계가 있었고, 전송로가 길어질수록 그 취약성은 보다 쉽게 노출되었다. Andrew Murray, Ibid., p.24.

84) 냉전시대에 미국은 구소련이 대륙간탄도미사일(ICBM)을 이용해서 미국의 주요 핵전략 기지를 연결하는 회선 중 일부를 타격하면 그 통신망 전체가 마비될 수 있다는 고민을 가지고 있었다. 아르파넷은 중앙집중적인 명령 및 통제 구조를 극복하기 위해 분산된 네트워크 구조로서 개발되었는바, 핵전쟁이 일어나더라도 신속하게 데이터를 보관 또는 공유하며 분산시킬 수 있는 방안이 모색된 것이다. "[IT강의실] 전세계를 하나로 연결하는 정보의 바다 – 인터넷", IT 동아 2015년 7월 27일자, https://it.donga.com/21932/ (2019년 10월 23일 최종접속); 정지훈, 거의 모든 인터넷의 역사 : 우리가 지금껏 알지 못했던 인터넷 혁명의 순간들, 메디치미디어, 2014, 130면.

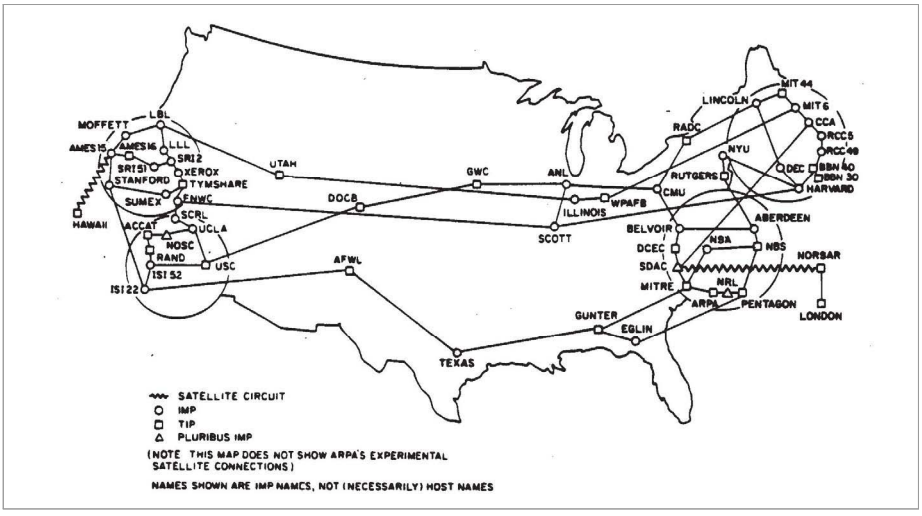
85) Barry M. Leiner/Vinton G. Cerf/David D. Clark/Robert E. Kahn/Leonard Kleinrock/Daniel C. Lynch/Jon Postel/Larry G. Roberts/Stephen Wolff, "A Brief History of the Internet", Computer Communication Review, Volume 39, Number 5, ACM SIGCOMM, 2009, pp.23-24.

[그림 2-11] 아르파넷 개요 및 아르파넷 접속 신호 처리 장치(IPM)[86]





[그림 2-12] 아르파넷[87]



86) 이미지 출처: (좌) DARPA 웹페이지, Paving the Way to the Modern Internet, https://www.darpa.mil/about-us/timeline/modern-internet; https://www.darpa.mil/ddm_gallery/1969%20ARPANET%20290x230.png (2019년 10월 23일 최종접속). (우) Mitch Waldrop, DARPA and the Internet Revolution, 50 Years of Bridging the Gap, DARPA, 2015, p.83, https://www.darpa.mil/attachments/(2015)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf (2019년 10월 23일 최종접속).

87) 이미지 출처: Mitch Waldrop, Ibid., p.85.

1972년 로버트 칸(Robert Kahn)은 "개방형 구조의 네트워크화(Open-Architecture Networking)"라는 아이디어를 제시하였는데, 이는 개별 네트워크들을 상호 연결함으로써 이용자들이 자유롭게 다른 네트워크에도 접근할 수 있는 메타 수준의 "상호네트워킹 구조(Internetworking Architecture)"를 구축하는 것이었다.[88] 이로 인해 제한된 컴퓨터만을 연결하던 아르파넷이 광범위한 네트워크를 연결하는 인터넷으로 발전할 수 있는 계기가 마련되었다. 개방형 구조의 네트워크 환경을 조성하기 위해서는 새로운 프로토콜(Protocol: 컴퓨터 간에 정보를 주고받을 때 적용되는 통신규약)이 필요했고, 이에 미국 국방부는 TCP/IP(Transmission Control Protocol/Internet Protocol)[89]를 개발하여 1983년 1월 1일부터 사용하였다.[90] 또한 1983년 미국 국방부는 종래 인터넷의 기간망 역할을 수행했던 아르파넷을 군사용 네트워크인 밀넷(Military Network, MILNET)과 연구 중심의 민간용 네트워크인 아르파넷으로 분리하였다.[91] 이후 기간망으로서의 역할은 미국 국립과학재단의 네트워크인 'NSFNET(National Science Foundation Network)'이 담당하였으나,[92] 이는 학술 연구와 교육 분야로 그 이용이 제한된다는 한계가 있었다.[93]

---

88) Barry M. Leiner/Vinton G. Cerf/David D. Clark/Robert E. Kahn/Leonard Kleinrock/Daniel C. Lynch/Jon Postel/Larry G. Roberts/Stephen Wolff, Ibid., p.24.

89) 전송 제어 프로토콜인 TCP(Transmission Control Protocol)는 전송할 파일을 작은 패킷들로 나누어 인터넷 네트워크를 통해 전송하는 일과 수신된 패킷을 원래의 메시지로 조립하는 일을 담당하는데, 데이터의 흐름이나 오류를 조절하는 기능을 수행한다. IP(Internet Protocol)는 주소를 기반으로 각 패킷이 목적지까지 정확하게 도달할 수 있도록 하는 기능을 수행한다.

90) 인터넷을 정의함에 있어서 "TCP/IP라는 고유한 프로토콜을 기반으로 구축된 전 세계적인 네트워크들의 네트워크 또는 이를 통해 구성되는 전 세계적인 사람들과 자원들의 집합체"라고 보는 입장도 있다. 이재현, 앞의 책(인터넷과 사이버사회), 21면; 이재현, 앞의 책(인터넷), 2-3면.

91) Barry M. Leiner/Vinton G. Cerf/David D. Clark/Robert E. Kahn/Leonard Kleinrock/Daniel C. Lynch/Jon Postel/Larry G. Roberts/Stephen Wolff, A Brief History of the Internet, Internet Socity, 1997, p.9; John Naughton, "The evolution of the Internet: from military experiment to General Purpose Technology", Journal of Cyber Policy, Volume 1, Number 1, Chatham House, 2016, p.11.

92) 1986년 미국 국립과학재단은 프린스턴 대학교, 피츠버그 대학교, UC 샌디에이고, 일리노이대학교 어바나 샴페인(UIUC), 코넬 대학교에 각각 슈퍼컴퓨터센터(National Supercomputer Centers)를 설치하고 이들을 상호 연결한 네트워크를 구축하였다. TCP/IP 기반의 통신망인 NSFNET은 학술 연구 분야를 중심으로 큰 인기를 끌었다. 1988년에는 아르파넷이 NSFNET에 흡수되면서 거대한 망이 형성되었다. Janet Abbate, Inventing the Internet, MIT Press, 1999, pp.192-195; 이재현, 앞의 책(인터넷), 23면; 정지훈, 앞의 책, 113면.

93) Jeffrey A. Hart/Robert R. Reed/Francois Bar, The Building of the Internet: Implications for the Future of Broadband Networks, Berkeley Roundtable on the International Economy, UC Berkeley, 1992, pp.22-23, https://brie.berkeley.edu/sites/default/files/wp_60.pdf (2019년 10월 23일 최종접속); 권오상/남승용/조대근/김유석/이수연, 인터넷전용회선 및 IDC 요금에 대한 사후규제 방안 연구, 방송통신위원회, 2018, 6면.

2) 인터넷의 대중화

국가 주도로 구축된 네트워크의 이용 목적이 학술 연구 등으로 제한되면서 민간부문에서 일반인을 대상으로 인터넷 서비스를 제공해야 할 필요성이 대두되었다.[94] 1987년에 최초의 인터넷 서비스업체인 UUNET이 설립[95]된 이래로 전자우편이나 채팅 서비스 등을 제공하는 회사들이 잇따라 설립되었다.[96] 그러나 인터넷의 대중화 및 상업화의 결정적 전기를 맞이한 것은 'WWW'로 불리는 월드와이드웹(World Wide Web)이 개발·배포되면서 부터이다. 1989년에 스위스 제네바에 위치한 유럽입자물리연구소(Organisation Européenne pour la Recherche Nucléaire, CERN[97])의 팀 버너스 리(Tim Berners-Lee) 박사는 다양한 형태의 정보가 포함된 방대한 규모의 데이터베이스를 구축한 후 이를 검색할 수 있는 시스템을 고안하였다.[98] WWW 서비스는 1991

---

94) 1980년대 말과 1990년대에 상용 인터넷 서비스 제공자(ISP)들이 병합을 시작하였다. 아르파넷은 1990년에 서비스가 종료되었다. 인터넷은 NSFNET이 서비스 종료된 1995년 시장에 진입하였으며, 이로써 상용 트래픽의 전달을 위한 인터넷 사용의 마지막 제한이 제거되었다. 이에 따라 인터넷을 상용화 하고자 했던 미국의 통신 사업자들은 1991년 킥스(Commercial Internet eXchange, CIX)라는 협회를 구성하여 상업적 목적으로 이용할 수 있는 인터넷 기간 통신망을 구축하였다. 시간의 경과에 따라 킥스에는 미국 외에도 여러 국가의 기업들이 참여하기 시작했고, 그로 인해 인터넷의 상업화는 급격히 진행된다. K. G. Coffman/A. M. Odlyzko, Growth of the Internet, AT&T Labs - Research, 2001, p.16, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.23.7962&rep=rep1&type=pdf (2019년 10월 23일 최종접속).

95) Ronald A. Asherson/Ricard Cervera/Jean-Charles Piette/Yehuda Shoenfeld, The Antiphospholipid Syndrome II: Autoimmune Thrombosis, Elsevier Science, 2002, p.432.

96) Anna DiStefano/Kjell Erik Rudestam/Robert Silverman, Encyclopedia of Distributed Learning, SAGE Publications, 2004, p.259.

97) 유럽입자물리연구소의 구 명칭인 유럽원자핵공동연구소(Conseil Européenne pour la Recherche Nucléaire)의 약자 형태로 사용되고 있는데, 변경된 공식 명칭의 약자 발음이 불편하던 차에 당시 중요한 역할을 담당하던 세계적 과학자 베르너 하이젠베르크(Werner Karl Heisenberg)가 계속 CERN으로 하자는 의견을 제안하였고, 이를 받아들여 그 의미와 관계없이 CERN으로 표기하고 있다. 정지훈, 앞의 책, 144면.

98) 팀 버너스 리는 하이퍼텍스트(Hypertext: 서로 연결되는 문서) 방식의 인터넷 표준문서인 'HTML (HyperText Markup Language)'의 개념을 제시했고, 인터넷 데이터의 위치를 표시하는 기준인 'URL(Uniform Resource Locator)', 월드와이드웹 상에서 하이퍼텍스트를 교환하는 프로토콜인 'HTTP(HyperText Transfer Protocol)', 그리고 세계 최초의 웹 브라우저인 '넥서스(NEXUS)' 등의 설계 및 규격 제정에 참여하였다. 팀 버너스 리는 월드와이드웹의 발명으로 인한 로열티를 포기하고 이를 일반에 공개하였는바, 오늘날 '웹의 아버지'로 불리고 있다. Andrew Murray, Ibid., pp.33-35; Tim Berners-Lee/Mark Fischetti, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor, Harper Collins Publishers, 1999, pp.30-32, pp.129-130; "The Father Of The Web Is Worried About How Ugly It's Become", npr 2017.4.4., https://www.npr.org/sections/alltechconsidered/2017/04/04/522593360/the-father-of-the-web-is-worried-about-how-ugly-its-become (2019년 10월 23일 최종접속); 정지훈, 앞의 책, 149면.

년 8월 6일부터 제공되었고, 같은 날 세계 최초의 홈페이지도 공개되었다.[99] 이후 월드와이드웹은 1993년에 일리노이 대학의 국립 슈퍼컴퓨팅 어플리케이션 센터(National Center for Supercomputing Applications, NCSA)의 마크 앤드리슨(Mark Andreesen)과 에릭 비나(Eric Bina)가 그래픽 기반의 웹 브라우저(Web Browser)[100]인 '모자이크(Mosaic)'를 개발하면서 급속도로 확산되었다.[101][102]

[그림 2-13] 팀 버너스 리[103]



[그림 2-14] 마크 앤드리슨[104]



한국에서는 1982년 전길남 교수의 주도로 서울대학교와 한국전자기술연구소(현재 '한국전자통신연구원'의 전신) 간에 구축된 SDN(System Development Network)이

99) CERN 웹페이지, http://info.cern.ch/hypertext/WWW/History.html (2019년 10월 23일 최종접속).
100) 'browse'는 '가게 안의 물건들을 둘러보거나 책이나 신문 등을 훑어보다'라는 의미를 가지고 있으며, 웹 브라우저는 인터넷 서비스나 자료에 접근할 수 있도록 지원하는 프로그램을 말한다.
101) 모자이크는 그 설치 및 이용이 편리하고 그래픽 처리 능력도 우수해서 이용자와 웹 사이트들의 수를 비약적으로 증가시켰다. John Naughton, Ibid., p.14; National Research Council, Funding a Revolution: Government Support for Computing Research, The National Academies Press, 1999, pp.180-181, https://www.nap.edu/read/6323/chapter/1 (2019년 10월 23일 최종접속).
102) 종래 인터넷이 제공해 온 개별적인 서비스들은 대부분 월드와이드웹에 이전되거나 통합되었다. Marjie T. Britz, Ibid., p.40; 정지훈, 앞의 책, 161-165면.
103) 이미지 출처: "What is Sir Tim Berners-Lee's net worth as the World Wide Web celebrates its 30th anniversary?", METRO 2019.3.12., https://metro.co.uk/2019/03/12/tim-berners-lees-net-worth-world-wide-web-celebrates-30th-anniversary-8887298/ (2019년 10월 23일 최종접속).
104) 이미지 출처: "Marc Andreessen on the Future of Silicon Valley(s), and the Next Big Technology", The New York Times Bits 2014.5.18., https://bits.blogs.nytimes.com/2014/05/18/marc-andreessen-on-the-future-of-silicon-valleys-and-the-next-big-technology/ (2019년 10월 23일 최종접속).

최초의 컴퓨터 통신망으로 파악되고 있다.[105][106] 1986년 7월 국내 컴퓨터 네트워크에 처음으로 IP 주소가 할당되었고,[107] 1986년 9월에는 한국데이터통신(1991년 '데이콤'으로 변경되기 이전의 명칭)[108]이 PC통신 서비스인 '천리안'을 개시하면서 한국에서도 인터넷 서비스의 기반이 마련되었다.[109][110] 이후 1994년 한국통신(현재 'KT'의 전신)이 일반인들을 대상으로 월드와이드웹 기반의 인터넷 접속 및 계정 서비스를 제공하면서 인터넷 대중화는 본격적으로 시작되었다.[111] 1990년대 후반 인터넷 속도가 비약적으로 향상되고, PC 보급이 늘어나면서 인터넷 이용자는 폭발적으로 증가하였다.[112]

---

105) SDN의 교신에는 유닉스 시스템과 1,200bps 전용회선 및 TCP/IP 프로토콜이 사용되었다. SDN은 1980년대 중반 구축되는 국가기간전산망의 토대가 되었고, 우리나라가 인터넷 강국으로 도약할 수 있었던 밑거름이 된 것으로 평가된다. 안정배, 한국인터넷의 역사 - 되돌아보는 20세기, 블로터앤미디어, 2014, 35-37면; 전길남, "초기 한국 인터넷 역사(1982년-2004년)", The e-Bridge 제12호, 한국정보처리학회, 2011, 11-12면.

106) 이후 1983년에는 과학기술원의 주도 하에 UUCP(Unix-to-Unix Copy Program)를 이용해서 접속되는 HANAnet이 탄생하였고, 1985년에는 전자우편서비스가 시작되었다. 1987년에는 국가기간전산망으로서 교육연구망 프로그램이 시작되었는데, 이는 IBM 컴퓨터 기반의 미국 대학 인터넷망인 BITnet과 연동되었고, SDN 역시 TCP/IP를 통해 미국의 CSNET과 연결되었다. 박현제, "한국 인터넷 역사와 표준", TTA Journal 제143호, 한국정보통신기술협회, 2012, 31-32면.

107) 전길남, 앞의 글, 15면.

108) 데이터통신을 육성하여 정보화 사회를 촉진시키고자 정부와 민간이 합동으로 출자하여 상법상 주식회사인 한국데이터통신(이하 '데이콤'이라고 함)을 1982년 3월 29일에 설립하였다. 데이콤은 공공정보통신망(PSDN) 건설 및 운용을 주도적으로 담당하면서 정보 전송 및 처리 서비스 등을 제공하였다. 성낙일/이명호/김도환/성극제/손상영/강인수, 한국정보통신 20세기사 : 정책/산업부문 조사, 집필-제5편 도약 발전시기(1980년-2000년)-, 정보통신정책연구원, 2001, 8-9면.

109) PC통신의 효시인 천리안 서비스는 1986년 시작되어 1988년에 상용화되었고, 1991년에는 데이콤이 하이텔을 만들어 서비스를 제공하였다. 이후 PC통신 사용자가 증가하자 1994년에는 나우콤의 나우누리, 1996년에는 유니텔 등의 PC통신 서비스가 제공되었다. 노명우/윤명희, 탈근대사회에서의 개인과 공동체 관계의 변화, 정보통신정책연구원, 2008, 60면; 안정배, 앞의 책, 91면.

110) 1982년에서 1993년까지는 국내에 인터넷이 도입된 시기로서 정부부처나 연구기관이 중심이 되어 인터넷 발전의 기반이 조성되었다. 박현제, 앞의 글, 35면.

111) 1994년 6월 한국통신이 KORNET를 구축하여 인터넷 상용화 서비스에 들어갔고, 같은 해 10월부터는 데이콤의 DACOM InterNet/BORANET, 11월부터는 아이네트기술(현재 'PSINet'의 전신)의 NURINET이 인터넷 서비스 제공을 시작하였는바, 1994년은 국내 인터넷 대중화의 원년으로 평가된다. 박현제, 앞의 글, 35면; 이효은/홍승표, "한국 IT 산업의 발자취", 주간기술동향 제1500호 특집, 정보통신산업진흥원, 2011.6.17., 39면; 전길남, 앞의 글, 23면.

112) 우리나라는 1998년에 두루넷(2005년 하나로 텔레콤에 합병)이 광케이블 백본망과 케이블 TV망 기반의 초고속 인터넷(Broadband) 서비스를 최초로 시작하였고, PC보급의 증가 시기와 맞물리면서 2000년대에 이르러서는 약 1,900만 명의 국민이 인터넷을 이용하게 되었다. 박현제, 앞의 글, 35면, 안정배, 앞의 책, 173-179면; 이효은/홍승표, 앞의 글, 39면; 전길남, 앞의 글, 26-27면.

나. 인터넷을 이용한 범죄와 형사법적 대응 연혁

1) 인터넷을 이용한 범죄 대두

종래 컴퓨터범죄는 전산망을 침해하거나 관련 정보를 조작하는 양상을 보였고, 컴퓨터를 이용하는 사람 자체가 한정적이었기 때문에 은행 등 금융기관을 중심으로 벌어지는 화이트칼라 범죄로 간주되는 경향이 있었다.[113] 그러나 개인용 컴퓨터가 보급되고, 인터넷을 통한 네트워크화가 본격적으로 진행되면서 정보통신망에 대한 침해로 인한 파급효는 막대해졌다.[114] 전자메일이나 채팅은 물론이고, 정보 검색과 온라인 쇼핑 및 소셜 네트워크 등 다양한 서비스를 제공하는 사이버 공간이 일상의 중요한 부분으로 자리매김하면서 정보통신망을 통해 수집·처리·보관·유통되는 개인정보의 오·남용에 대한 우려의 목소리도 커졌다.[115] 특히 인터넷은 익명성과 개방성 및 높은 전파성을 가지고 있고, 시간적·공간적인 제약을 받지 않는다는 특징[116]으로

113) 임종률, "컴퓨터범죄와 형법적 대응", 법학논총 제5집, 숭실대학교 법학연구소, 1989, 65면.

114) 강동범, "사이버범죄와 형사법적 대책", 형사정책연구 제11권 제2호(통권 제42호), 한국형사정책연구원, 2000, 39-40면; 오영근, "인터넷범죄에 관한 연구", 형사정책연구 제14권 제2호(통권 제54호), 한국형사정책연구원, 2003, 301-302면; 전지연, "인터넷 피싱의 형사법적 책임", 형사정책연구 제20권 제4호(통권 제80호), 한국형사정책연구원, 2009, 98면.

115) 「1994년 지존파 일당이 서울 압구정동 현대백화점 고객 1천 2백 65명의 명단이 적힌 컴퓨터 자료를 입수, 범행한 것으로 드러나 충격을 던져줬다. 이들이 입수한 자료는 고액 물품을 구입한 백화점 고객의 주소, 전화번호, 거래액 등이 기록된 A3용지 39장 분량으로 극비에 부쳐져야 할 개인정보가 쉽게 범죄자들의 손에까지 넘어가고 있음을 보여줬다. 심지어 경찰등 행정기관에 전산망이 완비된 뒤 일부공무원들까지 악덕업자와 연결고리를 맺고 개인의 재산상태·신상정보를 빼내 팔아먹는 사례도 있었다. 개인정보의 경우 전산실컴퓨터에 저장돼 있어 관련 일부 직원이 마음만 먹으면 얼마든지 빼낼 수 있어 무방비로 노출돼 있다. 특히 최근 일상생활에 컴퓨터통신기술이 접목되면서 개인정보의 유출문제가 크게 부각되고 있으며 「정보화 사회의 복병」으로 인식되고 있다. 행정전산망, 금융전산망 등 대규모 국가기간전산망이 본격 가동되면서 전산망에 입력된 각 개인의 정보가 유출되거나 고의로 조작돼 이들 정보가 각종 범죄 등에 활용되는 등 정보 유통의 부작용이 속출하고 있는 것이다. 국내에서는 개인의 주민등록번호만 있으면 국내외의 신용카드 사용실적을 뽑아 그 사람의 사생활 추적은 물론 탈세여부 등도 곧바로 밝혀낼 수 있다. 국가기간전산망에는 전 국민의 신상명세서가 이미 입력완료돼 이를 활용하면 누구든지 개인정보를 훤히 들여다 볼 수 있다. 더욱이 공안망에는 17세 이상 성인남녀의 주민등록사항은 물론 전과유무, 조직폭력계의 계보 등 종합적인 방대한 개인정보가 낱낱이 담겨 있다. 민간기업이 자체보유하고 있는 개인정보까지 치면 전 국민 어느 누구도 이 같은 「정보은행」에서 벗어날 수 없는 처지이다. 그러나 이 같은 개인정보유출을 사전에 예방하거나 단속·처벌할 법적·행정적 규제가 제대로 갖춰져 있지 않아 문제의 심각성을 더해주고 있다. 전문가들은 『정보사회에서 사생활침해를 예방하고 그 피해를 최소화하기 위해 관련법의 제정 및 개정도 필요하고 법규위반자에 대한 엄격한 법집행과 관련공무원들의 철저한 윤리의식이 뒤따라야 한다』고 지적하고 있다.」 "정보유출(사이버문화 이대론 안된다: 8)", 국민일보 1996년 9월 2일자, http://news.kmib.co.kr/article/viewDetail.asp?newsClusterNo=01100201.19960902000001903 (2019년 10월 23일 최종접속).

인하여 온라인에서의 명예훼손[117]이나 모욕[118] 및 정보통신망을 이용한 음란물 유통[119] 등을 강력하게 처벌해야 한다는 주장이 제기되었다.[120] 또한 이동통신이나 이메일, 인터넷 게시판이나 대화방 등 정보통신망을 이용해서 공포심이나 불안감을 유

---

116) 강동범, 앞의 글, 2000, 41-42면.

117) 「사이버 스페이스에서 명예훼손 문제는 더 이상 '강건너 불'이 아니다. 최근 컴퓨터 통신망에 검찰이 강압 편파수사를 했다는 글을 올린 가정주부가 무고 및 명예훼손 혐의로 검찰에 구속됐다. 그러자 네티즌들이 컴퓨터 통신망에 연일 검찰을 비난하는 성명을 띄우고 있다. 인터넷의 출현과 함께 명예훼손 문제가 새로운 전기를 맞고 있으나 한국 법조계는 아직 무방비 상태.」 "[리걸 스탠더드④] 법조계, 인터넷 명예훼손 무방비", 동아일보 1999년 4월 22일자, http://www.donga.com/news/article/all/19990422/7435703/1 (2019년 10월 23일 최종접속).

118) 「사회생활에서 컴퓨터의 의존도가 높아지면서 컴퓨터를 악용한 범죄도 늘고 있어 심각한 사회문제가 되고 있다. 특히 정부 각 부처의 행정전산망과 금융기관을 비롯한 각 기업체등의 전산망이 완비되면 여기에 병행하여 더욱 지능화된 컴퓨터범죄도 갈수록 기승을 부릴 것으로 전문가들은 내다보고 있다. 지난 (1992년) 6월 14일 서울 도봉구 미아4동 이모양(13·Y여중2)이 역시 BBS의 전자사서함프로그램인 「대화마당」에서 회원들과 컴퓨터로 대화를 해오던 중 자신에게 「걸레」 운운하는 성폭언에 충격을 받고 스스로 목숨을 끊은 사건은 컴퓨터를 이용한 또 다른 반윤리적 행위가 확산되고 있음을 드러낸 것이었다.」 "컴퓨터범죄/대부분 금융기관서 발생", 세계일보 1992년 7월 7일자, http://www.segye.com/newsView/19920707000060 (2019년 10월 23일 최종접속).

119) 「"야한 사진을 보여주세요" 동영상을 제공할 수 있는 신종채팅 사이트인 태그채팅을 통해 음란물이 공개적으로 유포되고 있어 심각한 사회문제로 지적되고 있다. 태그채팅은 본래 채팅을 즐기는 네티즌들에게 새로운 재미를 주기 위해 만들어졌지만 실제로 다수의 네티즌들이 음란물을 유통하는 방법으로 활용하고 있다. ... 특히 이 채팅방은 클릭 한번으로 음란영상을 다운로드 받을 수 있어 청소년들에게 음란물이 무차별적으로 유포될 수 있다. 이를 본 회사원 배모씨는 청와대 자유게시판에 "태그채팅방에서는 14, 15살의 어린 학생들이 있는데도 포르노 사진과 포르노 동영상이 펼쳐지고 있었다"면서 "누구나 참여할 수 있는 채팅방에 어떻게 아무런 규제도 없이 음란물이 게재될 수 있느냐"며 단속을 호소했다.」 "'태그채팅' 사이트 음란영상물 '홍수'", 국민일보 2000년 5월 16일자, http://news.kmib.co.kr/article/viewDetail.asp?newsClusterNo=01100201.20000516000002601 (2019년 10월 23일 최종접속).

120) 「K대학교에 다니는 김모씨(21·여)는 한 대화방에 들어가 채팅을 하던 중 한 남성으로부터 신음소리와 함께 "너랑 잤던 기억이 잊혀지지 않는다"는 등 성과 관련된 모욕을 당한 데 이어 급기야 상대방이 자신의 ID를 매춘여성으로 둔갑시켜 인터넷 상에 올리는 피해를 입었다. 또 인터넷의 대화방 외에 게시판, 독자투고, 자유토론 등 각종 공간에서도 욕설과 언어 성폭력이 난무하고 있는 것은 물론 확인되지 않은 정보나 사실이 마구 게재돼 당사자를 혼란에 빠트리는 경우도 속출하고 있다. 인터넷 공간이 아닌 공공장소나 인쇄물 또는 방송매체를 통해 공개된다면 처벌이 쉬운 내용들이 대부분이다. 그러나 네티즌들에게 이런 모멸감이나 명예훼손은 인터넷이라고 하는 특수성 때문에 법적 해결책을 찾기 쉽지 않다. 인터넷에 저질 글을 올리는 사람 대다수가 익명이나 가명을 사용하고 있는데다 상대방의 ID를 안다고 해도 다시 ID도용 등의 문제점에 부딪혀 끝까지 추적하기 불가능하기 때문이다. 실제로 춘천에서 발생한 욕설과 음란물 전자메일 고소사건의 경우 상대방의 전자메일주소와 ID는 밝혀졌지만 당사자가 ID와 비밀번호를 도용당했다고 주장, 경찰이 수사에 큰 어려움을 겪고 있다. PC통신업체 관계자들은 "사이버 공간상에서 이뤄지는 욕설과 음란물 게재에 대한 제재조치는 개인 ID를 없애고 사용을 중지시키는 것 외에 다른 방법이 없다"며 "컴퓨터 범죄를 예방할 수 있는 다각적인 제도적 장치 마련이 시급하다"고 입을 모으고 있다.」 "정보의 바다, 범죄의 바다 우려", 강원도민일보 1999년 3월 4일자.

발하는 문언이나 음향 또는 영상 등을 반복적으로 전송하는 이른바, 사이버 스토킹의 심각성도 대두되었다.[121]

한편 네트워크의 발달로 인해 악성 프로그램의 유포 양상도 변화되었는데, 종래에는 USB와 같은 저장매체를 통해 악성 프로그램이 전파되었다면, 인터넷이 대중화되면서 컴퓨터 바이러스,[122] 웜,[123] 트로이목마[124] 등으로 악성프로그램이 고도화되면서 그로 인한 피해도 막대해졌다.[125] 또한 사이버 공간을 통해 얻을 수 있는 경제적

---

121) 「컴퓨터통신을 통한 신종범죄인 '사이버 스토킹'이 국내서도 빠르게 확산되면서 피해자들이 속출하고 있다. 현재 천리안 등 국내 PC통신 업체에는 전자우편이나 게시판 등을 이용한 사이버 스토킹 피해사례가 업체별로 월 40-50건씩 접수되고 있다. 정보통신윤리위원회에 따르면 사이버 스토킹은 보통 채팅을 하는 과정에서 발생한다. 스토커들은 채팅 도중 마음에 드는 여성 상대를 정하면 노골적으로 성적 표현을 써가며 접촉을 시도한다. 또 접속자명(ID)을 기억한 후 '마음에 든다, 한번 만나자'는 전자우편을 보내다 거절당하면 병적인 사이버 스토킹 증세를 보인다. 실례로 대구에 사는 박모양(23)은 최근 PC통신 하이텔의 대화방을 이용하다 이와 비슷한 경험을 당했다. 박양은 대화중 이모씨로부터 '죽여주꾸마', '번섹(번개섹스의 줄임말로 섹스를 목적으로 특정한 시간과 장소를 정해 만나는 것을 의미하는 통신속어) 한번 할까' 등 저속한 용어의 성희롱을 받았다. 박모양은 이후에도 전자우편을 통한 병적인 구애에 시달리다 정보통신윤리위원회에 신고했다. 하이텔은 이에 따라 지난 11일 스토킹 문제로 고통받는 네티즌을 위해 스토커 대처방안, 스토커 예방법 등을 알려주고 토론도 하는 등의 서비스인 '스토커 출입금지'(go STALK)를 개설하기도 했다.」 "사이버공간 인간진드기 '경계경보'", 국민일보 1999년 8월 17일자, http://news.kmib.co.kr/article/viewDetail.asp?newsClusterNo=01100201.19990817000003101 (2019년 10월 23일 최종접속).

122) 컴퓨터 바이러스(Computer Virus)는 생물학적인 바이러스가 생물체에 침투하여 병을 일으키는 것처럼 컴퓨터를 동작시키는 운용 체제나 소프트웨어에 몰래 들어가서 자기 자신을 시스템이나 프로그램 및 데이터 파일에 복제하여 감염시킴으로써 그것들을 손상시키는 프로그램이다. "What is a computer virus?", Norton by Symantec, https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html (2019년 10월 23일 최종접속); 김태석, "컴퓨터 바이러스의 제작유포행위에 대한 형사법적 규제", 중앙법학 제4집 제3호, 중앙법학회, 2002, 114-115면.

123) 감염의 대상(숙주)이 필요한 바이러스와 달리 웜(Worm)은 네트워크를 통해서 스스로 전파되어 컴퓨터 작업을 지연 내지는 방해하는 악성프로그램이다. "What Is A Worm Virus?", VIPRE, https://www.vipre.com/resource/what-is-a-worm-virus/ (2019년 10월 23일 최종접속); 김형석/전용태, "컴퓨터 바이러스 등 유해 프로그램의 법적 규제 검토 - 미국의 제정법과 판례를 중심으로 -", 법이론실무연구 제7권 제2호, 한국법이론실무학회, 2019, 122면.

124) 트로이 목마(Trojan Horse)는 정상적인 프로그램으로 보이지만, 막상 실행되면 컴퓨터의 속도를 저하시키거나 파일을 삭제할 수 있고, 해킹 기능을 가지고 있어서 컴퓨터 사용자의 정보를 유출시킬 수 있는 등 보안에 큰 위협을 가하는 악성프로그램이다. "What is a Trojan? Is it a virus or is it malware?", Norton by Symantec, https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (2019년 10월 23일 최종접속); 정연덕, "악성프로그램의 정의와 해석에 관한 법적 문제", 동아법학 제53호, 동아대학교 법학연구소, 2011, 695면; 최준혁, "효과없는 악성코드 제거프로그램 배포에 관한 형법의 쟁점", 법학연구 제42집, 전북대학교 법학연구소, 2014, 110면.

125) 「경찰청 컴퓨터범죄수사대는 (1999년) 3월 5일 인터넷, 컴퓨터 통신망을 통해 각종 바이러스 재료들을 모아 직접 제작한 컴퓨터 바이러스를 사설 전자게시판(BBS)을 통해 유포한 김모(15. 고교 1년)군과 조모(24.대학교 1년), 한모(26.무직)씨를 컴퓨터 등 장애업무방해 혐의로 불구속입건했다. 김군은 97년 7월부터 가명으로 10여개의 ID를 만든 뒤 지난해 국내 10대 악성

이익의 규모가 커지고, 인터넷의 파급 효과가 확대되면서 청소년유해매체물 등에 대한 불법광고나 수신인의 의사와 관계없이 대량으로 발송되는 스팸(spam)[126]이 새로운 사회적 문제로 등장하였다.[127] 근래에는 인터넷을 통한 신종 사기수법이 사회적 우려를 야기하였는바, 금융기관 등의 웹사이트나 그로부터 전송된 메일로 위장하여 개인정보를 불법적으로 알아내서 이용하는 피싱(Phishing),[128][129] 금융기관 등이 공

바이러스 프로그램으로 뽑힌 「까마귀」「에볼라」「남벌」 등 22종의 컴퓨터 바이러스를 제작, 각종 사설통신망을 통해 유포했다. 또 조씨는 지난해 3월부터 실행파일을 감염시키는 「PS-MPC675」 등 10여종의 바이러스를, 한씨는 컴퓨터 하드디스크가 완전히 파괴되는 「ALT-X 버전 13」 등 10여종의 프로그램을 만들어 퍼뜨렸다. 김군 등은 바이러스 프로그램을 「백신 프로그램」「이야기 7.3」 같은 유용한 프로그램이나 「○○누드 사진」 같은 프로그램으로 속여 이용자들이 다운받도록 했다. 경찰은 이들로 인한 피해자가 수천명에 이를 것으로 추산하고 있다.」 "악성 컴퓨터바이러스 유포..10대포함 3명 검거", 연합뉴스 1999년 3월 5일자, https://news.v.daum.net/v/19990305135100682?f=o (2019년 10월 23일 최종접속).

126) 스팸(spam)은 미국 호멜(Hormel)사의 통조림 햄의 상표명인데, 한때 통조림 햄에 대한 광고가 지나치게 많았던 것에 착안하여 사용자의 의사와 무관하게 대량으로 발송되는 이메일이나 문자메시지를 일컫는 용어로 사용되고 있다. "Why do we call it spam? Blame spiced ham shoulder, Monty Python and Usenet", Digital Trends 2015.2.8., https://www.digitaltrends.com/web/why-junk-email-is-spam/ (2019년 10월 23일 최종접속); 김상겸, "스팸규제에 관한 헌법적 연구", 공법학연구 제5권 제3호, 한국비교공법학회, 2004, 302면; 윤창술, "스팸메일(Spam Mail)에 대한 규제방안", 기업법연구 제12집, 한국기업법학회, 2003, 459면.

127) 「PC통신과 인터넷 이용인구가 급증하면서 국내에도 스팸(spam) 메일이 난무하고 있다. ... 얼마전 삼성그룹 미국 현지법인은 익명의 스패머가 삼성의 인터넷 웹호스트서비스인 「세일러헤드」라는 이름으로 6백만-2천만명의 인터넷 이용자들에게 보낸 메일 때문에 곤욕을 치렀다. 메일 수신자 수천명이 삼성측에 항의전화를 걸었고 이로 인해 업무가 마비될 지경이었다. 삼성 관계자는 『스팸 메일로 입은 이미지 손상 때문에 수백만달러를 날리게 된 것으로 추산하고 있다』고 털어놨다. 스팸 메일은 통신망에 과도한 부하를 발생시켜 통신업체들의 시스템을 다운시킨다. 또 건전한 네티즌들을 메일 홍수 속에 빠뜨려 통신 노이로제에 걸리게 하기도 한다. 자영업자인 ㅇ씨는 『스팸 메일을 받을 때마다 개인정보가 유출된 것 같아 불쾌하다』며 『쓸데없는 전자우편을 열어보고 정리하는 데 드는 시간과 통화료를 생각하면 울화통이 터진다』고 말했다. 스팸 메일의 폐해가 심각한 수준에 이르자 천리안과 하이텔 나우누리 등 PC통신업체들은 ID를 등록하면 전자우편 발송을 자동으로 차단하는 「메일통제 서비스」를 제공하고 있지만 역부족이다. 숙명여대 윤종필 교수(전산학)는 『미국을 비롯한 선진국에서도 스팸 메일 피해로 정보화가 심각한 부작용을 낳고 있다』며 『정부차원에서 반드시 근절책을 마련해야 한다』고 강조했다.」 "〈변화 가로막는 네오 러다이트族〉통신公害유발 사이버광고", 경향신문 1999년 5월 28일자.

128) 피싱(Phishing)은 '개인정보(private data)'와 '낚시(fishing)'의 합성어로 파악되는가 하면, 어원이 '낚시(fishing)'라는 점은 일치하나 위장의 수법이 '세련되었다(sophisticated)'라는 뜻에서 그 철자를 'phishing'으로 쓰게 되었다고 보는 입장도 있다. 한편 피싱이라는 용어는 그 원조라 할 수 있는 '프리킹(phreaking: phone + freaking)'의 영향을 받아 만들어진 것이라는 설도 있는데, 프리킹은 요금을 내지 않고 전화를 사용하기 위해 원격 통신 시스템을 해킹하는 것을 칭한다. 애당초 phishing이라는 말은 미국의 유명해커인 칸 스미스(Khan C. Smith)가 만든 것으로 알려졌는데, 온라인 서비스망인 AOL(America Online)을 이용하던 해커들 사이에서 불법행위를 가리키는 기호로 쓰이던 '◇<'의 모습이 물고기를 닮았다고 해서 fishing이 나왔고, 당시에 인기가 높던 phreaking을 염두에 두고 phishing으로 변형시켰다는 것이다. "History of Phishing: Then and Now", Cybrary 2017.3.23., https://www.cybrary.it/2017/03/history-phishing-now/ (2019년 10월 23일 최종접속).

식적으로 운영하는 도메인을 탈취하여 사용자들로 하여금 의심 없이 접속하도록 한 뒤에 개인정보를 훔쳐내는 파밍(Pharming)[130][131] 등이 대표적이다.[132] 그 이외에도 인터넷이 대중화되면서 온라인상에서 지적재산권 등을 침해[133]하거나 주요정보통신기반시설을 교란·마비 또는 파괴하는 행위[134]에 대한 별도의 처벌 규정이 마련되어야 한다는 필요성도 제기되었다.

---

129) 통상적으로 피싱은 ① 금융기관을 가장한 이메일 발송 → ② 이메일에서 안내하는 인터넷주소 클릭 → ③ 가짜 은행사이트로 접속 유도 → ④ 보안카드 번호 전부 입력 요구 → ⑤ 금융정보 탈취 → ⑥ 범행계좌로 이체 등의 과정을 거쳐 피해가 발생한다. 경찰청 웹페이지, https://www.police.go.kr/portal/main/contents.do?menuNo=200569 (2019년 10월 23일 최종접속).

130) 파밍(Pharming)은 넓은 의미의 피싱(Phishing)으로서 보다 진화한 형태의 기법이다. 피싱은 금융기관 등이 보낸 이메일로 위장해서 사용자로 하여금 웹사이트에 접속하도록 한 뒤 개인정보를 빼내는 방식인데 비하여, 파밍은 해당 사이트가 공식적으로 운영하던 도메인 자체를 중간에서 탈취하거나 변조하는 수법이다.

131) 통상적으로 파밍은 ① 사용자 PC가 악성코드에 감염 → ② 정상 홈페이지에 접속하여도 피싱(가짜)사이트로 유도 → ③ 금융정보 탈취 → ④ 범행계좌로 이체 등의 과정을 거쳐 피해가 발생한다. 경찰청 웹페이지, https://www.police.go.kr/portal/main/contents.do?menuNo=200568 (2019년 10월 23일 최종접속).

132) 스미싱(Smishing)도 신종금융범죄로 주목받고 있다. '문자메시지(SMS)'와 '피싱(Phishing)'의 합성어인 스미싱은 통상적으로 ① '무료쿠폰 제공', '돌잔치 초대장', '모바일 청첩장' 등을 내용으로 하는 문자메시지내 인터넷주소 클릭하면 → ② 악성코드가 스마트폰에 설치되어 → ③ 피해자가 모르는 사이에 소액결제 또는 개인·금융정보 탈취 등의 과정을 거쳐 피해가 발생한다. 경찰청 웹페이지, https://www.police.go.kr/portal/main/contents.do?menuNo=200567 (2019년 10월 23일 최종접속).

133) 「최근 PC통신과 인터넷 사용이 일반화되면서 디지털정보에 대한 저작권 침해 행위가 곳곳에서 일어나고 있으며 이에 대한 관심이 고조되고 있다. 디지털정보는 복제나 배포가 손쉽게 이뤄진다. 책이나 문서를 복제하려면 상당한 시간과 비용이 필요하지만 디지털화된 텍스트 이미지 동영상파일들은 별다른 노력이나 시간, 비용을 들이지 않아도 복제, 가공이 쉽다. 또 인터넷의 폭발적 성장에 따라 모든 형태의 저작물을 안방에서 누구나 받아 볼 수 있다. 이는 저작권법이 보호하는 창작물에 대한 복제권과 배포권의 침해가 쉬워졌다는 것을 의미한다. ... PC통신과 인터넷 이용자들이 범하는 저작권 침해 행위도 비일비재하다. 마음에 드는 홈페이지의 사진이나 아이콘 등 문서 일부를 다운로드 받아 자신의 홈페이지를 만드는 것은 주위에서 쉽게 볼 수 있다. 전문가들은 IP들의 불법복제 서비스, 불법복제물 자료실 유통, 교묘한 링크, 인터넷문서 복제 등은 명백한 저작권 침해라며 디지털정보에 대한 이해부족과 규제장치가 미흡하기 때문에 저작권 침해행위가 난무한다고 지적한다.」 "〈열린마당〉 MP3파일과 저작권", 전자신문 1997년 3월 26일자, http://www.etnews.com/199703260019 (2019년 10월 23일 최종접속).

134) 「최근의 해킹 및 바이러스 유포는 자신의 컴퓨터 실력을 과시하는 수준에서 벗어나고 있다. 즉, 전자상거래 환경에서의 금전적 이익을 노리거나, 기업 등의 산업정보를 노리는 해킹과 정치적이고 무정부적인 「핵티비즘(Hacktivism)」으로 변화하고 있다는 것이다. 따라서 해킹과 바이러스의 유포는 인터넷 웹사이트를 단순히 침해하는 것뿐만 아니라 국민의 일상생활을 위협할 수 있다. 프라이버시를 침해할 수 있으며, 심지어는 국가기간산업의 마비와 정보전을 통한 국가안보체계까지도 무너뜨릴 수 있다. 이러한 상황에서 해킹 및 바이러스에 대한 대비의 필요성이 절실히 요구되고 있다.」 "《사이버 칼럼》...해킹과 바이러스", 국제신문 2000년 8월 2일자, http://www.kookje.co.kr/news2011/asp/newsbody.asp?code=0300&key=20000802.010223821 56 (2019년 10월 23일 최종접속).

2) 형사법적 대응 연혁

인터넷의 상용화로 인해 변화된 범죄 양상에 대한 법적 대응은 형법이 아닌 특별법 개정을 통해 이루어졌다. 우선 정보통신망을 통해 수집·처리·보관·유통되는 개인정보의 오·남용에 대한 우려가 커지자 1999년 2월 8일에 종래의 「전산망보급확장과이용촉진에관한법률」이 「정보통신망이용촉진등에관한법률」로 전부개정되면서[135] 개인정보에 대한 보호규정이 신설되었다.[136] 이후 정보통신망을 통한 명예훼손이나 음란물 배포·판매 행위에 대한 처벌 강화의 목소리가 높아지는 등 법률 정비의 필요성이 대두되자 2001년 1월 16일에 「정보통신망이용촉진등에관한법률」은 또 다시 「정보통신망이용촉진및정보보호등에관한법률」(이하 '정보통신망법'이라고 함)로 전부개정되어 2001년 7월 1일부로 시행되었다.[137] 정보통신망법은 2001년 전부개정 이래로 무려 48차에 걸쳐 개정되었는데,[138] 16차례의 타법 개정을 제외하더라도 총 23회의 일부개정이 단행되었다. 이러한 법률 개정을 통해 새로운 구성요건이 추가되는가 하

---

135) 법률 제5835호로 전부개정되어 1999년 7월 1일부로 시행되었다. 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=581&ancYd=19990208&ancNo=05835&efYd=19990701&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

136) 동법상 개인정보 보호 관련 규정을 위반하여 이용자의 개인정보를 수집목적·이용목적 또는 제공목적외의 용도로 이용하거나 제3자에게 제공한 자, 이용자의 개인정보를 타인에게 누설하거나 제공한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(정보통신망이용촉진등에관한법률 제30조 제1호, 제2호). 다만 개인정보 보호 관련 규정을 위반하여 개인정보를 수집한 자, 이용자에게 고지하지 아니하거나 이용약관에 명시하지 아니한 자, 목적을 달성한 개인정보를 파기하지 아니한 자 및 개인정보 관리책임자를 지정하지 아니한 자에 대해서는 500만원 이하의 과태료에 처한다(동법률 제32조 제1항).

137) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=51505&ancYd=20010116&ancNo=06360&efYd=20010701&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

138) 2018년 6월 12일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제15628호[시행 2019. 6. 13.], 2018년 12월 4일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제16021호[시행 2019. 6. 13], 2016년 3월 22일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제14080호[시행 2017. 3. 23.], 2016년 3월 22일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제14080호[시행 2017. 7. 25.], 2016년 3월 22일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제14080호[시행 2016. 3. 22], 2015년 12월 1일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제13520호[시행 2015. 12. 1.], 2014년 5월 28일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제12681호[시행 2014. 5. 28.], 2012년 2월 17일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제11322호[시행 2013. 2. 18.], 2004년 1월 29일 일부개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제7139호[시행 2004. 7. 30.]와 같이 개정일은 동일하나 시행일이 다른 경우는 제외하였다.

면, 형사처벌의 수위가 조절되기도 하였는바, 현행 정보통신망법상 형사법적 금지행위와 그에 대한 벌칙 규정은 다음의 [표 2-5]와 같다.

[표 2-5] 현행 정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 벌칙 규정[139)]

조문	처벌대상	벌칙
제70조 ①	사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제70조 ②	사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자	7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.
제70조 ③	제1항과 제2항의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.	
제70조의2	제48조 제2항을 위반하여 악성프로그램을 전달 또는 유포하는 자	7년 이하의 징역 또는 7천만원 이하의 벌금에 처한다.
제71조 ① 1	제22조 제1항(제67조에 따라 준용되는 경우를 포함)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 2	제23조 제1항(제67조에 따라 준용되는 경우를 포함)을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 3	제24조, 제24조의2 제1항 및 제2항 또는 제26조 제3항(제67조에 따라 준용되는 경우를 포함)을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 4	제25조 제1항(제67조에 따라 준용되는 경우를 포함)을 위반하여 이용자의 동의를 받지 아니하고 개인정보 처리위탁을 한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 5	제28조의2 제1항(제67조에 따라 준용되는 경우를 포함)을 위반하여 이용자의 개인정보를 훼손·침해 또는 누설한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 6	제28조의2 제2항을 위반하여 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 7	제30조 제5항(제30조 제7항, 제31조 제3항 및 제67조에 따라 준용되는 경우를 포함)을 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

139) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=206009&efYd=20190625#0000 (2019년 10월 23일 최종접속).

조문	처벌대상	벌칙
제71조 ① 8	제31조 제1항(제67조에 따라 준용되는 경우를 포함)을 위반하여 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 9	제48조 제1항을 위반하여 정보통신망에 침입한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 10	제48조 제3항을 위반하여 정보통신망에 장애가 발생하게 한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ① 11	제49조를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자	5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
제71조 ②	제1항 제9호의 미수범은 처벌한다.	
제72조 ① 2	제49조의2 제1항을 위반하여 개인정보를 수집한 자	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제72조 ① 2의2	「재난 및 안전관리 기본법」 제14조 제1항에 따른 대규모 재난 상황을 이용하여 제50조의8을 위반하여 광고성 정보를 전송한 자[140]	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제72조 ① 3	제53조 제1항에 따른 등록을 하지 아니하고 그 업무를 수행한 자	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제72조 ① 4 가	재화등의 판매·제공을 가장하거나 실제 매출금액을 초과하여 통신과금서비스에 의한 거래를 하거나 이를 대행하게 하는 행위를 통하여 자금을 융통하여 준 자 또는 이를 알선·중개·권유·광고한 자	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제72조 ① 4 나	통신과금서비스이용자로 하여금 통신과금서비스에 의하여 재화등을 구매·이용하도록 한 후 통신과금서비스이용자가 구매·이용한 재화등을 할인하여 매입하는 행위를 통하여 자금을 융통하여 준 자 또는 이를 알선·중개·권유·광고한 자	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제72조 ① 5	제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자	3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
제73조 1	제28조 제1항 제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 1의2	제29조 제1항을 위반하여 개인정보를 파기하지 아니한 자(제67조에 따라 준용되는 경우를 포함)	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 2	제42조를 위반하여 청소년유해매체물임을 표시하지 아니하고 영리를 목적으로 제공한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 3	제42조의2를 위반하여 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

조문	처벌대상	벌칙
제73조 4	제44조의6 제3항을 위반하여 이용자의 정보를 민·형사상의 소를 제기하는 것 외의 목적으로 사용한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 5	제44조의7 제2항 및 제3항에 따른 방송통신위원회의 명령을 이행하지 아니한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 6	제48조의4 제3항에 따른 명령을 위반하여 관련 자료를 보전하지 아니한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 7	제49조의2 제1항을 위반하여 개인정보의 제공을 유인한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 7의2	제58조의2(제59조 제2항에 따라 준용되는 경우를 포함)를 위반하여 제공받은 정보를 본인 여부를 확인하거나 고소·고발을 위하여 수사기관에 제출하기 위한 목적 외의 용도로 사용한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제73조 8	제61조에 따른 명령을 이행하지 아니한 자	2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
제74조 ① 1	제8조 제4항을 위반하여 비슷한 표시를 한 제품을 표시·판매 또는 판매할 목적으로 진열한 자	1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제74조 ① 2	제44조의7 제1항 제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자	1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제74조 ① 3	제44조의7 제1항 제3호를 위반하여 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자	1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제74조 ① 4	제50조 제5항을 위반하여 조치를 한 자	1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제74조 ① 6	제50조의8을 위반하여 광고성 정보를 전송한 자	1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제74조 ① 7	제53조 제4항을 위반하여 등록사항의 변경등록 또는 사업의 양도·양수 또는 합병·상속의 신고를 하지 아니한 자	1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제74조 ②	제1항 제3호의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.	
제75조 (양벌규정)	법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지 또는 제74조 제1항의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.	
제75조의2 (몰수·추징)	제71조 제1항 제1호부터 제8호까지, 제72조 제1항 제2호 및 제73조 제1호·제1호의2·제7호의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.[141]	

형법상 명예훼손죄는 "사실의 적시인 경우 '2년 이하의 징역이나 금고 또는 500만원 이하의 벌금', 허위사실의 적시인 경우 '5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금'"에 처하고,[142] 출판물 등에 의한 명예훼손의 경우 "사실일 경우 '3년 이하의 징역이나 금고 또는 700만원 이하의 벌금', 허위사실인 경우 '7년 이하의 징역, 10년 이하의 자격정지 또는 1천 500만원 이하의 벌금'"에 처한다.[143] 후자는 전자에 비해 초과주관적 요소인 비방의 목적을 필요로 하고, 출판물을 이용함으로써 명예훼손의 위험성이 커진다는 점에 근거하여 그 처벌이 가중되어 있다. 정보통신망법상 사이버 명예훼손의 경우에도 사람을 비방할 목적으로 전파성이 높은 정보통신망을 통해 명예훼손이 이루어진다는 점을 고려해서 가중적 구성요건으로 규정되어 있는바, 사실을 적시한 경우에는 '3년 이하의 징역 또는 3천만원 이하의 벌금', 허위사실을 적시한 경우에는 '7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금'에 처하도록 규정되어 있다(정보통신망법 제70조 제1항, 제2항). 인터넷

---

140) 국가적 재난사태인 세월호 침몰 참사를 이용하여 잘못된 정보 또는 광고성 정보를 전송하여 재산상의 이익을 취득하려는 범죄가 발생하여 국민적 분노를 유발하였으나, 그 처벌수준은 미미하다는 비판이 제기되었다. 이에 2015년 3월 27일 법률 제13280호로 정보통신망법을 개정하여 「재난 및 안전관리 기본법」 제14조 제1항에 따른 대규모 재난 상황을 이용하여 이 법 또는 다른 법률에서 금지하는 불법행위를 위한 광고성 정보를 전송하는 자에 대해서 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 하였다. 법제처 법령정보센터 웹페이지, 법률 제13280호 제정·개정이유 참조, http://www.law.go.kr/lsInfoP.do?lsiSeq=169551&ancYd=20150327&ancNo=13280&efYd=20150327&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

141) 종래 개인정보 유출에 대한 법정손해배상제만으로는 재산적 피해 보전이 어렵고 피해방지의 실효성도 떨어진다는 의문이 제기되었다. 이에 정보통신서비스 제공자의 책임성을 강화하기 위해서는 징벌적 손해배상제가 도입되어야 한다는 목소리가 커졌다. 이에 정보통신서비스 제공자 등의 개인정보 분실·도난·유출·위조·변조 또는 훼손 행위에 대한 징벌적 손해배상 및 개인정보 관련 범죄로 인한 이익을 환수하기 위한 몰수·추징 규정을 도입하는 내용이 포함된 정보통신망법 개정이 2016년 3월 22일 법률 제14080호로 단행되어 9월 23일부터 시행되었다. 법제처 법령정보센터 웹페이지, 법률 제14080호 제정·개정이유 참조, http://www.law.go.kr/lsInfoP.do?lsiSeq=181842&ancYd=20160322&ancNo=14080&efYd=20160923&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

142) 형법 제307조(명예훼손) ① 공연히 사실을 적시하여 사람의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
② 공연히 허위의 사실을 적시하여 사람의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처한다.

143) 형법 제309조(출판물 등에 의한 명예훼손) ① 사람을 비방할 목적으로 신문, 잡지 또는 라디오 기타 출판물에 의하여 제307조 제1항의 죄를 범한 자는 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에 처한다.
② 제1항의 방법으로 제307조 제2항의 죄를 범한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 1천 500만원 이하의 벌금에 처한다.

을 이용한 음란물의 배포·판매 등에 대해서도 정보통신망이라는 매체의 특수성을 고려해서 형법상 음화반포 등[144]에 비해 처벌 수위를 높여 두었다(동법 제74조 제1항 제2호).[145]

통상적인 스토킹의 경우 경범죄 처벌법상 '지속적 괴롭힘'[146]으로 보아 10만원 이하의 벌금, 구류 또는 과료의 형으로 처벌할 수 있을 뿐이고, 이에 대해서는 그 처벌 수준이 경미하다는 비판이 제기되고 있다.[147] 사이버 스토킹의 경우 가해자와 직접 대면함으로써 생길 수 있는 위험은 감소되지만, 언제 어디서든 손쉽게 상대방을 괴롭힐 수 있다는 점에서 사회적 문제가 되었고,[148] 이에 정보통신망법은 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 하는 자에 대해서는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하였다(동법 제74조 제1항 제3호).

2001년 단행된 정보통신망법 전부개정을 통해서 컴퓨터 바이러스 등 악성프로그램을 전달·유포하는 행위에 대한 처벌 규정도 마련되었다. 이후 인터넷 보급이 확산되고 악성프로그램이 진화함에 따라서 그 피해 규모가 증대하자 법정형이 상향조정되었다. 즉 해당 행위에 대해서는 종래 '5년 이하의 징역 또는 5천만원 이하의 벌금'에 처해질 수 있었으나, 2016년 3월 22일에 이루어진 동법 개정을 통해서 '7년 이하의 징역 또는 7천만원 이하의 벌금'에 처해지도록 변경된 것이다(동법 제70조의2). 또한 사이버 공간에서 불법·유해정보가 확산되고 있는 상황에서 무차별적인 광고성 정보 전송

144) 형법 제243조(음화반포등) 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

145) 사이버 모욕죄나 도박죄에 대해서는 정보통신망법상 별도의 구성요건이 존재하지 않고, 형법상 모욕죄(형법 제311조)나 도박·상습도박죄(형법 제246조) 및 도박개장죄(형법 제247조) 등이 적용된다.

146) '지속적 괴롭힘', 즉 상대방의 명시적 의사에 반하여 지속적으로 접근을 시도하여 면회 또는 교제를 요구하거나 지켜보기, 따라다니기, 잠복하여 기다리기 등의 행위를 반복하여 하는 사람은 10만원 이하의 벌금, 구류 또는 과료의 형으로 처벌한다(경범죄 처벌법 제3조 제1항 제41호).

147) 송란희, "한국의 스토킹 피해 실태 및 특징", 한일 심포지엄「스토킹 피해 실태 및 법적 대응」자료집, 한국여성정책연구원/남인순 국회 여성가족위원장실/교토여자대학교, 2016.8.25., 27, 29면; 이원상, "스토킹 처벌규정 도입에 대한 고찰", 형사정책연구 제24권 제2호(통권 제94호), 한국형사정책연구원, 2013, 166-167면.

148) 백광훈, 인터넷범죄의 규제법규에 관한 연구, 한국형사정책연구원, 2000, 74-75면; 양성은, "사이버범죄의 동향과 이에 대한 형사법적 책임", Internet & Security Focus 2013 9월호, 한국인터넷진흥원, 2013, 62면; 이원상/채희정, 사이버범죄의 새로운 유형과 형사정책적 대안연구, 한국형사정책연구원, 2010, 53면.

문제를 해소하기 위한 대응 입법도 마련되었다. 현행 정보통신망법은 불법행위를 위한 광고성 정보 전송을 금지하면서 (동법 제50조의8), 이를 위반한 경우에는 '1년 이하의 징역 또는 1천만원 이하의 벌금'에 처하도록 하고(동법 제74조 제1항 제6호), 대규모 재난 상황을 이용하여 불법행위를 위한 광고성 정보를 전송한 경우에는 '3년 이하의 징역 또는 3천만원 이하의 벌금'에 처하도록 규정하고 있다(동법 제72조 제1항 제2의2호). 또한 스팸 발송으로 인한 피해를 최소화하기 위한 벌칙 규정도 마련하고 있는바, "전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자"가 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 등 일정한 조치를 취하는 것을 금지하면서(동법 제50조 제5항),[149] 이를 위반한 자는 '1년 이하의 징역 또는 1천만원 이하의 벌금'에 처하도록 한다(동법 제74조 제1항 제4호). 아울러 청소년유해매체물 광고를 청소년에게 전송하거나 청소년의 접근을 제한하는 조치 없이 공개적으로 전시하는 행위를 금지하면서(동법 제42조의2), 이를 위반한 경우에는 '2년 이하의 징역 또는 2천만원 이하의 벌금'에 처하도록 규정하고 있다(동법 제73조 제3호).[150]

피싱 등의 수법을 이용한 금융사기로 인한 피해가 늘어나자 이에 대응하기 위해 2005년 12월 30일 정보통신망법 개정을 통해 정보통신망을 통하여 속이는 행위에 의한 개인정보의 수집을 금지하는 조문이 도입되었다. 피싱이나 파밍 등을 통해 수집된 개인정보나 금융정보를 이용하여 사람을 기망하여 재물의 교부를 받거나 재산상의

---

149) 정보통신망법 제50조(영리목적의 광고성 정보 전송 제한) ⑤ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 다음 각 호의 어느 하나에 해당하는 조치를 하여서는 아니 된다.
1. 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 조치
2. 숫자·부호 또는 문자를 조합하여 전화번호·전자우편주소 등 수신자의 연락처를 자동으로 만들어 내는 조치
3. 영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 조치
4. 광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 조치
5. 영리목적의 광고성 정보를 전송할 목적으로 수신자를 기망하여 회신을 유도하는 각종 조치

150) 종래 정보통신서비스 제공자가 인지능력 등이 부족할 수 있는 만 14세 미만 아동의 개인정보 처리에 대한 동의를 받아야 할 때에는 법정대리인의 동의를 받도록 하였으나 이에 대한 동의가 형식적으로 이루어지거나 동의를 받지 않는 사례가 다수 있어 아동의 개인정보 보호를 보다 강화하고 법정대리인 동의 제도를 개선할 필요가 있다는 지적이 있었다. 이에 2018년 12월 24일에 동법을 개정하여 정보통신서비스 제공자로 하여금 만 14세 미만 아동의 개인정보 처리에 관하여 법정대리인의 동의를 받을 때에는 대통령령이 정하는 바에 따라 법정대리인이 동의하였는지를 확인하도록 하고(정보통신망법 제31조 제1항), 그 위반 시에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하였다(동법 제71조 제1항 제8호).

이익을 취득한 자는 형법상 사기죄로 처벌될 수 있고(형법 제347조), "컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자"는 형법상 컴퓨터등 사용사기죄로 처벌될 수 있다(형법 제347조의2). 그러나 은행과 같은 금융기관의 담당자에 대하여 편취의 의사로 기망행위를 개시하지 않은 경우 또는 컴퓨터등 정보처리장치에 허위의 정보나 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하지 않은 경우에는 (컴퓨터등 사용)사기죄의 실행의 착수가 인정되지 않는바, 형법상 사람을 기망하여 정보를 수집하거나 그 제공을 유인한 행위 자체를 처벌할 수 있는 규정이 존재하지 않는다.[151] 이에 현행 정보통신망법은 "누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인"하는 행위를 금지하면서(정보통신망법 제49조의2 제1항),[152] 이를 위반하여 개인정보의 제공을 유인한 자는 '2년 이하의 징역 또는 2천만원 이하의 벌금'에 처하도록 규정하고 있다(동법 제73조 제7호).

인터넷 상용화에 따라서 드러났던 형법상 구성요건의 한계는 주로 정보통신망법 정비를 통해 극복되었으나 그 이외의 형사특별법을 통해서도 일정 부분 보완이 이루어졌다.[153] 우선 정보화 사회가 진전되고 개인정보의 경제적 가치가 증대함에 따라서 개인정보의 수집이나 이용이 보편화되고 있으나 종래의 법규만으로 규제될 수 없는 개인정보 보호의 사각지대가 존재한다는 비판의 목소리가 나왔다. 개인정보의 유출·

---

151) 형법은 사기죄의 예비·음모를 처벌하지 않는다.

152) 정보통신망법 제49조의2(속이는 행위에 의한 개인정보의 수집금지 등) ① 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다.
② 정보통신서비스 제공자는 제1항을 위반한 사실을 발견하면 즉시 과학기술정보통신부장관, 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.
③ 과학기술정보통신부장관, 방송통신위원회 또는 한국인터넷진흥원은 제2항에 따른 신고를 받거나 제1항을 위반한 사실을 알게 되면 다음 각 호의 필요한 조치를 하여야 한다.
1. 위반 사실에 관한 정보의 수집·전파
2. 유사 피해에 대한 예보·경보
3. 정보통신서비스 제공자에게 접속경로의 차단을 요청하거나 이용자에게 제1항의 위반행위에 노출되었다는 사실을 알리도록 요청하는 등 피해 예방 및 피해 확산을 방지하기 위한 긴급조치
④ 과학기술정보통신부장관 또는 방송통신위원회는 제3항 제3호의 조치를 취하기 위하여 정보통신서비스 제공자에게 정보통신서비스 제공자 간 정보통신망을 통하여 속이는 행위에 대한 정보 공유 등 필요한 조치를 취하도록 명할 수 있다.

153) 오영근, 앞의 글, 306-307면.

오용·남용 등으로 인한 프라이버시 침해는 물론이고 이를 이용한 명의도용이나 전화 사기 등으로 인해 정신적·금전적 피해가 발생하는 것이 사회적 문제로 대두된 것이다. 이에 공공부문과 민간부문을 망라하여 적용될 수 있는 개인정보 처리 원칙이 규정될 필요성이 제기되었는바, 2011년 3월 29일에 「개인정보 보호법」이 제정되어 같은 해 9월 30일부터 시행되고 있다.[154] 현행 개인정보 보호법은 총칙(제1장)과 개인정보 보호정책의 수립 등(제2장), 개인정보의 처리(제3장), 개인정보의 안전한 관리(제4장), 정보주체의 권리 보장(제5장), 개인정보 분쟁조정위원회(제6장), 개인정보 단체소송(제7장), 보칙(제8장) 및 벌칙(제9장)으로 구성되어 있다.[155] 「정보통신망법」이 정보통신서비스 이용자의 개인정보 보호에 초점을 맞추고 있다면, 「개인정보 보호법」은 개인정보의 처리 및 보호에 관한 사항을 규정하는 일반법으로서 그 역할을 한다는 점에서 차별화된다.

다음으로 전화나 컴퓨터를 이용하여 음란한 행위를 하는 등 새로운 유형의 성폭력 범죄가 발생함에도 불구하고 기존의 법체계로는 적절한 대처가 어렵다는 문제가 제기되었고, 이에 1994년 1월 5일 (구)「성폭력범죄의처벌및피해자보호등에관한법률」[156]이 제정되면서 통신매체를 이용한 음란행위에 대한 처벌 규정이 마련되었다. 해당 규정은 현행 「성폭력범죄의 처벌 등에 관한 특례법」(이하 '성폭력처벌법'이라고 함)을 통해 규정되고 있는바, "자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화, 우편, 컴퓨터, 그 밖의 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말, 음향, 글, 그림, 영상 또는 물건을 상대방에게 도달"하게 한 사람은 2년 이하의 징역 또는 500만원 이하의 벌금에 처한다(성폭력처벌법 제13조). 형법상 강제추행죄는 폭행 또는 협박으로 사람을 추행한 자를 '10년 이하의 징역 또는 1,500만원 이하의 벌금'에 처하는데(형법 제298조), 가해자와 피해자가 직접 대면하지 않는 경우에 동 규정을 적용하는 데에는 어려움이 있었다. 이에 법적 공백을 해소하고자 형사특

154) 「개인정보 보호법」은 종래 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」이나 「신용정보의 이용 및 보호에 관한 법률」 등 개별 법령에서 다루고 있던 개인정보와 관련된 사항을 통합하여 규정한 법이다.

155) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=173223#0000 (2019년 10월 23일 최종접속).

156) 2010년 4월 15일에 「성폭력범죄의 처벌 등에 관한 특례법」과 「성폭력범죄의 피해자보호 등에 관한 법률」이 제정되면서 「성폭력범죄의처벌및피해자보호등에관한법률」은 폐지되었다.

별법을 통해 통신매체를 이용한 음란행위를 처벌하는 규정이 마련된 것이다.

또한 정보화가 진전됨에 따라서 주요사회기반시설들이 정보통신시스템에 대해 가지는 의존도가 심화되었고, 해킹이나 컴퓨터 바이러스 등을 이용한 전자적인 침해행위가 국가안보를 위협하는 새로운 요소로 등장하였다. 그러한 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위한 대응체계를 구축하고자 2001년 1월 26일「정보통신기반 보호법」이 제정되었다.[157] 동법은 주요정보통신기반시설[158]에 대한 침해행위 등을 금지하고 있으며,[159] 이를 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 '10년 이하의 징역 또는 1억원 이하의 벌금'에 처하도록 한다(정보통신기반 보호법 제28조 제1항). 형법상 타인의 재물이나 문서 또는 전자기록등 특수매체기록을 손괴한 자는 '3년 이하의 징역 또는 700만원 이하의 벌금'에 처하고(형법 제366조), 공익에 공하는 건조물을 파괴한 자는 '10년 이하의 징역 또는 2천만원 이하의 벌금'에 처하고 있으나(형법 제367조), 주요정보통신기반시설의 중요성과 그 침해로 인한 파급 효과를 고려하여 법정형이 상향 조정된 것이다.

나아가 정보화 시대에 발맞추어 전자거래의 안정성과 신뢰성을 확보하고 거래의 공정을 제고하기 위하여 1999년 2월 8일「전자거래기본법」이 제정되었고,[160] 동법은 2012년 6월 1일에 그 제명이「전자문서 및 전자거래에 관한 기본법」(이하 '전자문서법'이라고 함)으로 변경되었다.[161] 전자문서법은 전자문서 등과 관련된 정보의 보

---

157) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=61565&ancYd=20010126&ancNo=06383&efYd=20010701&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

158) "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항 제1호의 규정에 의한 정보통신망을 말한다(정보통신기반 보호법 제2조 제1호).

159) 정보통신기반 보호법 제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니 된다.
1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

160) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=8789&ancYd=19990208&ancNo=05834&efYd=19990701&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

161) 이 법은 공공기관과 민간기관 사이, 개인과 민간기관 사이 또는 이들 상호간에 이루어지는 전자문서 유통에 대한 일반적 사항을 규정하고 있고, 개정안의 대부분 조문에서 종래의 "전자

안[162]이나 비밀 유지[163] 규정을 두면서, 이에 위반하여 공인전자문서센터에 보관된 전자문서 등을 위조·변조 및 거짓 발급되게 한 자는 '10년 이하의 징역 또는 1억원 이하의 벌금'에 처하도록 한다(전자문서법 제43조).[164] 또한 해당 전자문서 등을 멸실·훼손하거나 직무상 알게 된 전자문서의 내용이나 비밀 등을 누설한 자는 '5년 이하의 징역 또는 5천만원 이하의 벌금'에 처한다(전자문서법 제44조).[165] 형법상 공문서 위조·변조, 공전자기록 위작·변작죄 및 동 행사죄는 '10년 이하의 징역'에 처하고(형법 제225조, 제227조의2, 제229조), 사문서 위조·변조, 사전자기록 위작·변작죄 및 동 행사죄는 '5년 이하의 징역 또는 1천만원 이하의 벌금'에 처한다(형법 제231조, 제232조의2, 제234조). 공인전자문서센터에 보관된 전자문서의 경우 형법상

거래"라는 용어가 "전자문서 및 전자거래"로 변경된다는 점 등이 고려되어 그 제명이 바뀌었다. 법제처 국가법령정보센터 웹페이지, 법률 제11461호 제정·개정이유 참조, http://www.law.go.kr/lsInfoP.do?lsiSeq=125865&ancYd=20120601&ancNo=11461&efYd=20120902&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

162) 전자문서법 제31조의12(전자문서 등 관련 정보의 보안) ① 누구든지 공인전자문서센터에 보관된 전자문서나 그 밖의 관련 정보를 위조 또는 변조하거나 위조 또는 변조된 정보를 행사하여서는 아니 된다.
② 누구든지 공인전자문서센터의 정보처리시스템에 거짓 정보나 부정한 명령을 입력하는 등의 방법으로 제31조의7 제2항에 따른 증명서가 거짓으로 발급되게 하여서는 아니 된다.
③ 누구든지 공인전자문서센터에 보관된 전자문서나 그 밖의 관련 정보를 멸실 또는 훼손하거나 그 비밀을 침해하여서는 아니 된다.
④ 공인전자문서센터의 임원 또는 직원이거나 임원 또는 직원이었던 사람은 직무상 알게 된 전자문서의 내용이나 그 밖의 관련 정보의 내용을 누설하거나 자신이 이용하거나 제3자로 하여금 이용하게 하여서는 아니 된다.

163) 전자문서법 제37조의2(비밀 유지) 위원회의 분쟁조정 업무에 종사하는 자 또는 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외의 용도로 사용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

164) 전자문서법 제43조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.
1. 제31조의12 제1항을 위반하여 공인전자문서센터에 보관된 전자문서나 그 밖의 관련 정보를 위조 또는 변조하거나 위조 또는 변조된 정보를 행사한 자
2. 제31조의12 제2항을 위반하여 공인전자문서센터의 정보처리시스템에 거짓 정보나 부정한 명령을 입력하는 등의 방법으로 제31조의7 제2항에 따른 증명서가 거짓으로 발급되게 한 자
② 제1항의 미수범은 처벌한다.

165) 전자문서법 제44조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
1. 제31조의12 제3항을 위반하여 공인전자문서센터에 보관된 전자문서나 그 밖의 관련 정보를 멸실 또는 훼손하거나 그 비밀을 침해한 자
2. 제31조의12 제4항을 위반하여 직무상 알게 된 전자문서의 내용이나 그 밖의 관련 정보의 내용을 누설하거나 자신이 이용하거나 제3자로 하여금 이용하게 한 공인전자문서센터의 임원 또는 직원이거나 임원 또는 직원이었던 자
3. 제37조의2를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외의 용도로 사용한 자

공문서라고 할 수는 없지만,[166] 그에 준하여 안정성과 신뢰성이 확보되어야 한다는 점에서 법정형이 조정되어 있다. 또한 형법상 타인의 문서나 전자기록등 특수매체기록을 손괴한 경우에는 '3년 이하의 징역 또는 700만원 이하의 벌금'에 처할 수 있으나(형법 제366조), 전자문서법을 통해 공인전자문서센터에 보관된 전자문서 등을 멸실·훼손한 경우에는 '5년 이하의 징역 또는 5천만원 이하의 벌금'에 처하도록 법정형이 상향 조정되었다.

그 이외에도 온라인상에서 이루어지는 지적재산권 침해에 대응하고자 「저작권법」 등이 정비되었다.[167] 정보통신망을 통해 지적재산권과 그 밖에 동법을 통해 보호되는 재산적 권리를 복제하거나 공연, 공중송신, 전시 및 배포하는 자[168]는 물론이고, 정당

---

166) 미래창조과학부/법무부, 전자문서법 해설서-전자문서 효력의 일반적 인정과 예외 및 전자문서 활용-, 2017, 17면.

167) 2000년 1월 12일에는 저작권법 개정을 통해 저작재산권에 전송권을 추가함으로써 컴퓨터통신 등을 통한 저작물 전송 시에도 저작자의 이용허락을 받도록 하였다. 2003년 5월 27일에는 온라인서비스제공자가 안정적인 영업활동을 도모할 수 있도록 일정한 요건을 갖춘 경우에는 인터넷을 통한 제3자의 저작권 침해에 대해 면책되는 규정을 마련하였고, 2004년 10월 16일에는 실연자와 음반제작자에게 전송권을 부여해서 인터넷 등을 활용한 실연이나 음반의 이용에 관한 권리를 명확히 하는 개정이 이루어졌다. 또한 2009년 4월 22일에는 「저작권법」과 「컴퓨터프로그램 보호법」을 통합하는 한편, 온라인상에서 이루어지는 불법복제를 효과적으로 근절하고자 온라인서비스제공자와 불법 복제자 및 전송자에 대한 규제를 강화하였고, 2009년 3월 25일에는 국립중앙도서관이 온라인 자료를 체계적으로 수집 및 관리할 수 있도록 복제근거를 마련하였으며, 2011년 6월 30일에는 온라인서비스제공자의 면책범위를 유형별로 세분화하는 내용의 개정이 단행되었다. 법제처 국가법령정보센터 웹페이지, 법률 제6134호, 법률 제6881호, 법률 제7233호, 법률 제9625호, 법률 제9529호, 법률 제10807호 제정·개정이유 참조, http://www.law.go.kr/lsInfoP.do?lsiSeq=204802&efYd=20190417#0000 (2019년 10월 23일 최종접속).

168) 저작권법 제136조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있다.
1. 저작재산권, 그 밖에 이 법에 따라 보호되는 재산적 권리(제93조에 따른 권리는 제외한다)를 복제, 공연, 공중송신, 전시, 배포, 대여, 2차적 저작물 작성의 방법으로 침해한 자
2. 제129조의3 제1항에 따른 법원의 명령을 정당한 이유 없이 위반한 자

② 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하거나 이를 병과할 수 있다.
1. 저작인격권 또는 실연자의 인격권을 침해하여 저작자 또는 실연자의 명예를 훼손한 자
2. 제53조 및 제54조(제90조 및 제98조에 따라 준용되는 경우를 포함한다)에 따른 등록을 거짓으로 한 자
3. 제93조에 따라 보호되는 데이터베이스제작자의 권리를 복제·배포·방송 또는 전송의 방법으로 침해한 자

3의2. 제103조의3 제4항을 위반한 자

3의3. 업으로 또는 영리를 목적으로 제104조의2 제1항 또는 제2항을 위반한 자

3의4. 업으로 또는 영리를 목적으로 제104조의3 제1항을 위반한 자. 다만, 과실로 저작권 또는 이 법에 따라 보호되는 권리 침해를 유발 또는 은닉한다는 사실을 알지 못한 자는 제외한다.

3의5. 제104조의4 제1호 또는 제2호에 해당하는 행위를 한 자

한 권리 없이 고의로 복제·전송의 중단이나 재개요구를 해서 온라인서비스제공자의 업무를 방해하는 자[169] 등에 대한 처벌 규정이 마련되어 있다.

제2절 | 정보통신 기술의 고도화에 따른 형사법적 과제

1. 모바일 디바이스의 발전과 형사법적 과제

가. 모바일 디바이스의 발전

1) 휴대전화의 대중화

모바일폰(Mobile phone)이나 셀폰(Cell phone)으로 불리는 휴대전화는 이동통신 서비스를 이용하기 위한 목적으로 개발된 무선 전화기를 말한다. 무선통신 분야를 선도했던 회사인 미국의 모토로라(Motorola)는 1939년에 차량용 모바일 송신기(AM mobile transmitter)를 개발하였고,[170] 1955년에 세계 최초로 이른바 '삐삐(Handie-Talkie

---

3의6. 제104조의5를 위반한 자
3의7. 제104조의7을 위반한 자
4. 제124조 제1항에 따른 침해행위로 보는 행위를 한 자
5. 삭제
6. 삭제

169) 저작권법 제137조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
1. 저작자 아닌 자를 저작자로 하여 실명·이명을 표시하여 저작물을 공표한 자
2. 실연자 아닌 자를 실연자로 하여 실명·이명을 표시하여 실연을 공연 또는 공중송신하거나 복제물을 배포한 자
3. 제14조 제2항을 위반한 자
3의2. 제104조의4 제3호에 해당하는 행위를 한 자
3의3. 제104조의6을 위반한 자
4. 제105조 제1항에 따른 허가를 받지 아니하고 저작권신탁관리업을 한 자
5. 제124조 제2항에 따라 침해행위로 보는 행위를 한 자
6. 자신에게 정당한 권리가 없음을 알면서 고의로 제103조 제1항 또는 제3항에 따른 복제·전송의 중단 또는 재개요구를 하여 온라인서비스제공자의 업무를 방해한 자
7. 제55조의2(제90조 및 제98조에 따라 준용되는 경우를 포함한다)를 위반한 자
② 제1항 제3호의3의 미수범은 처벌한다.

170) Motorola Solutions 웹페이지, Calling All Cars, Motorola Milestones, https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/calling-cars.html (2019년 10월 23일 최종접속).

pagers)'라고 불리는 무선호출기를 개발하여 병원 내 의료인들에게 보급하였다.[171] 1966년에 방영되었던 미국의 공상과학(Science Fiction, SF) TV 드라마인 스타트렉(Star Trek)에서는 우주선 승무원들이 현대의 휴대전화인 폴더폰과 유사한 통신기기(Communicator)를 이용하는 모습이 그려졌으나,[172] 이는 어디까지나 상상 속의 산물에 불과했다. 그로부터 10년이 채 지나지 않은 1973년에 모토로라 소속의 마틴 쿠퍼(Martin Cooper) 박사 연구팀은 인류 최초로 휴대폰을 개발하였고,[173] 이는 경찰에 보급되어 경찰차에 장착된 카폰 형태로 이용되었다. 이후 모토로라는 1983년에 전 세계 최초로 상업용으로 승인된 휴대전화 다이나택(DynaTAC) 8000X[174]를 출시하면서 휴대전화 상용화의 포문을 열었다.

[그림 2-15] 스타트렉 속 통신장치[175]



[그림 2-16] 모토로라 다이나택 8000X[176]



171) Motorola Solutions 웹페이지, Handie-Talkie Paging System, https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/handie-talkie-paging-system.html (2019년 10월 23일 최종접속).

172) Motorola Solutions 웹페이지, Cell Phone Development, https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/cell-phone-development.html (2019년 10월 23일 최종접속).

173) Motorola Solutions 웹페이지, Cell Phone Development, https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/cell-phone-development.html (2019년 10월 23일 최종접속).

174) Motorola Solutions 웹페이지, https://www.motorolasolutions.com/en_us/about/company-overview/history/timeline.html (2019년 10월 23일 최종접속).

175) 이미지 출처: "[과학으로 본 드라마 '시그널'] '시그널' 속 타임슬립 도구가 '무전기'인 이유는?", 동아사이언스 2016년 2월 19일자, http://dongascience.donga.com/news/view/10388 (2019년 10월 23일 최종접속).

176) 이미지 출처: Motorola Solutions 웹페이지, Cell Phone Development, https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/cell-phone-development.html (2019년 10월 23일 최종접속).

1900년대 초부터 무선통신(Wireless Communications)이 시작되었으나,[177] 선이 없는 전화기가 등장한 것은 1921년 미국 디트로이트(Detroit) 경찰이 차량에 무선이동통신 시스템을 설치·이용하면서 부터이다.[178] 그러나 당시의 기술로는 교환이 필요한 일방통신만 가능했고, 실시간 양방향 통화는 이루어지지 못했다. 1946년 미국 세인트루이스(Saint Louis)에서는 처음으로 일반인을 대상으로 한 이동전화 서비스가 제공되었으나 이 역시 수동교환 방식이었다.[179] 사용자가 직접 다이얼을 돌려서 상대방과 접속하는 양방향 통화 서비스는 1964년에 이르러서 제공되었다.[180] 1973년 미국 모토로라의 마틴 쿠퍼 박사팀이 셀룰러 시스템(Cellular System)[181]을 활용한 휴대전화를 개발하면서, 이 시스템은 1970년대 후반부터 보편적인 이동통신의 방식으로 자리매김하였다.[182] 1977년 미국 연방통신위원회(Federal Communication Commission, FCC)가 셀룰러 전화를 차량 전화로만 사용되도록 했던 기존의 정책을 바꾸어 셀룰러 시스템이 본격적으로 시험 운영되도록 하였는바, 이때부터 1세대 이동전화 시대가

177) 우동진/이동철/백광천, 우리나라 전기통신기술 발달사에 관한 연구, 한국전기통신연구소, 1989, 33면.

178) 우동진/이동철/백광천, 앞의 보고서, 34면; 이재현, 멀티미디어, 커뮤니케이션북스, 2013, 63면.

179) 이용수, "세계의 이동통신현황과 경쟁도입", 통신정책연구 1991년 여름호, 정보통신정책연구원, 1991.7., 131면; 정선종/박세경, UHF대역 셀룰러 이동 무선전화 시스템을 위한 채널 최적 할당방식에 관한 연구, 한국전기통신연구소, 1987, 37면.

180) Mingtao Shi, Technology Base of Mobile Cellular Operators in Germany and China: A Comparative Study from the Perspective of the Resource-based View, Univerlagtuberlin, 2007, pp.55-56; Robert Curley, Breakthroughs in Telephone Technology: From Bell to Smartphones, Britannica Educational Publishing, 2012, p.97.

181) 현재와 같은 셀룰러 시스템은 1947년 미국 벨연구소(Bell Labs)의 연구팀에 의해 기본개념이 제안되며 개발이 시작되었다. 셀룰러 시스템은 일반공중통신망(PSTN)과 이동통신 간의 교환기능을 수행하는 무선 교환국, 셀이라는 일정한 범위의 크기를 갖는 무선 구역, 무선 구역에서 무선 교환국과 이용자 단말기 상호 간의 송수신 기능을 담당하는 기지국 및 이용자가 몸에 휴대하거나 이동체 내에서 통신을 할 수 있게 해 주는 모바일 단말기로 구성되며, 서비스 지역을 셀 단위로 분할한 후 각 셀마다 기지국을 설치하여 서비스 영역을 담당하도록 하는 시스템을 말한다. 동 시스템은 일정한 거리를 두고 동일 주파수를 재사용하며 통화 중인 이용자가 새로운 지역으로 진입할 때 통화의 단절 없이 계속해서 통화를 할 수 있도록 통화 채널을 자동전환한다. 또한 서로 다른 통신사업자의 서비스 지역 내에서도 통신할 수 있도록 연결해주는 서비스로써, 이러한 셀룰러 시스템은 휴대전화를 포함하여 대부분의 이동통신 분야에서 활용되고 있다. 이재현, 모바일 미디어, 커뮤니케이션북스, 2013, 89-94면; Gerard O'Regan, World of Computing: A Primer Companion for the Digital Age, Springer, 2018, pp.230-232.

182) Imar De Vries, Tantalisingly Close: An Archaeology of Communication Desires in Discourses of Mobile Wireless Media, Amsterdam University Press, 2012, pp.132-133; Motorola Solutions 웹페이지, Cell Phone Development, https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/cell-phone-development.html (2019년 10월 23일 최종접속).

열린 것이다.[183] 이후 1990년대부터 아날로그 방식이 디지털 방식으로 변경되면서 2세대 이동전화 시대가 개막되었고,[184] 휴대전화 단말기의 가격이 대폭 떨어지면서[185] 이동통신시장은 무선호출기에서 휴대전화를 중심으로 급격히 재편되었다. 2000년부터 현재와 같은 3세대 이동전화 시대가 시작되었는데, 휴대전화 단말기를 이용해서 전화통화는 물론이고 사진촬영이나 무선인터넷 사용 등이 가능해졌다.[186]

2) 스마트폰을 통한 혁신

휴대전화 단말기에 개인용 컴퓨터와 같은 전용 운영 체제(Operating System)를 탑재해서 다양한 콘텐츠와 어플리케이션을 이용할 수 있도록 구현된 스마트폰(Smart Phone)이 등장하면서, 정보통신산업의 패러다임은 물론이고 인간의 생활 방식까지 바꾼 혁신이 이루어졌다. 종래에도 이메일 확인이나 오피스 기능이 탑재된 개인용 정보 단말기(Personal Digital Assistant, PDA)가 있었고, 여기에 이동전화 기능이 결합되기도 했지만 비싼 가격 등을 이유로 하여 대중적으로 이용되지는 못했다.[187] 그러나 2007년 애플이 출시한 '아이폰(iphone)'이 돌풍을 일으키면서 스마트폰 이용자가 급증하였고,[188] 스마트폰을 중심으로 이동통신 시장은 또 한 번 재편되었다. 현재 우리

---

183) 박철순/김성훈, 한국 이동통신 서비스 및 단말기 산업의 변천과 발전방향, 서울대학교 출판부, 2007, 25면, 이재현, 앞의 책(멀티미디어), 63면.

184) 1992년 전 세계 이동전화 가입자 수가 1,000만 명을 돌파했으며, 우리나라는 1996년 한국이동통신(현 SK텔레콤)이 세계 최초로 2세대 기술 중 미국 퀄컴(Qualcomm)사가 개발한 CDMA 방식의 디지털 이동통신 서비스를 개시하였다. 장여경/김지성, "한국의 이동통신 도감청과 통신비밀보호법", 계간 정보운동 액트온(Act On) 2009년 제1호(통권 제5호), 진보네트워크센터, 2009, 5면.

185) 우리나라에서는 차량 이동전화 형태의 휴대전화(삼성 SC-1000)를 1986년 개발 및 생산하였고 이후 1988년에 최초의 휴대전화(삼성 SCH-100)를 출시하였는데, 당시 평균 임금이 64만원이던 시절에 휴대전화의 가격이 무려 165만원에 달했다고 한다. "이것이 한국 최초의 국산 휴대폰", ZDNet korea 2013년 3월 30일자, http://www.zdnet.co.kr/view/?no=20130330112907 (2019년 10월 23일 최종접속); "[뉴스CAFE] 30년 전 휴대폰은 어떤 모습?", 삼성전자 뉴스룸 2018년 7월 19일자, https://news.samsung.com/kr/%EB%89%B4%EC%8A%A4-cafe-%EC%82%BC%EC%84%B1%EC%A0%84%EC%9E%90-%ED%9C%B4%EB%8C%80%EC%A0%84%ED%99%94-30%EB%85%84 (2019년 10월 23일 최종접속).

186) 장여경/김지성, 앞의 글, 5면.

187) 최초의 스마트폰은 'IBM 사이먼'인데, 이는 1992년에 IBM과 벨사우스(Bellsouth)가 공동으로 개발한 것으로서 1994년 8월 공식 판매되었다. "First Smartphone Turns 20: Fun Facts About Simon", TIME 2014.8.18., https://time.com/3137005/first-smartphone-ibm-simon/ (2019년 10월 23일 최종접속).

188) 최초의 아이폰은 이전에 애플이 출시했던 휴대형 음악재생기기인 '아이팟(iPod)'에 통화와 인터넷 기능을 추가한 것이었다. 200만 화소의 카메라와 손가락 전기를 인식하는 '정전식 터치스크린'이 최초로 장착되었던 아이폰은 큰 인기를 얻었으나 당시 우리나라에서는 통신망과 호환이 되지 않아서 출시되지 못하였다.

가 사용하는 스마트폰은 통화와 문자서비스는 물론이고, 사진이나 동영상 촬영 및 영상통화, 인터넷 접속, 멀티미디어 파일 재생 등 다양한 기능을 제공하고 있는바, 스마트폰은 궁극의 디지털 제품으로 변모하였다. 2019년 기준으로 전 세계 76억 인구 중 67% 이상이, 우리나라의 경우 국민의 95%가 스마트폰을 사용하고 있는 것으로 알려져 있는데,[189] 오늘날 모바일 기기를 일상적으로 사용하고 있는 인류를 두고 '호모 모빌리쿠스(Homo Mobilicus)'라고 칭하기도 한다.[190]

[그림 2-17] IBM 사이먼[191]



[그림 2-18] 2007년 애플 아이폰[192]



189) "The Global State of Digital in October 2019", We Are Social 2019.10.23., https://wearesocial.com/us/blog/2019/10/the-global-state-of-digital-in-october-2019 (2019년 10월 23일 최종접속); "국민 95%가 스마트폰 사용…보급률 1위 국가는?", KBS NEWS 2019년 2월 11일자, http://mn.kbs.co.kr/news/view.do?ncd=4135732 (2019년 10월 23일 최종접속).

190) 김성도, 호모 모빌리쿠스: 모바일 미디어의 문화생태학, 삼성경제연구소, 2008, 13면. 이와 유사한 용어로 '호모 모빌리언(Homo Mobilian)' 또는 '호모 모빌리티언(Homo Mobilitian)'이 사용되기도 한다.

191) 이미지 출처: Microsoft Research 웹페이지, https://www.microsoft.com/buxtoncollection/detail.aspx?id=40 (2019년 10월 23일 최종접속).

192) 이미지 출처: "The Apple iPhone", engadget 2007.9.1., https://www.engadget.com/2007/01/09/the-apple-iphone/ (2019년 10월 23일 최종접속).

나. 모바일 디바이스 관련 형사법적 과제

1) 범죄수사를 위한 통신감청 및 통신자료 수집

과학기술의 발전에 따라 등장한 감청이라는 수사방법은 체포·구속·압수·수색과 같은 전통적인 강제수사 방법과 달리 물리력을 행사하거나 상대방에게 의무를 부과하지 않았다. 그러나 이로 인해 개인의 프라이버시가 침해되면서 종래 감청은 임의수사와 강제수사의 한계선에 있게 되었다. 감청의 법적 성격을 두고 벌어진 논쟁은 1994년 「통신비밀보호법」이 제정되면서 일단락되었는바, 감청은 법원의 허가를 받아 이루어지는 강제수사로 규정된 것이다.[193] 점차 지능화·첨단화되는 범죄를 밝혀내는 데에 감청은 효율적 수단이다. 그러나 전기통신 감청에 대한 근거법이 마련되어 있음에도 불구하고, 이동전화에 대한 감청은 제대로 이루어지지 못한다는 문제가 지적되었다.[194] 실제로 2019년 5월 10일 과학기술정보통신부가 발표한 자료에 의하면 이동전화에 대한 감청은 수년째 0건으로 집계되고 있다.

[표 2-6] 통신수단별 통신제한조치 현황[195]

(단위 : 문서수)

구 분	2016년		2017년		2018년	
	상반기	하반기	상반기	하반기	상반기	하반기
유선전화	82	48	56	28	59	46
이동전화	-	-	-	-	-	-
인터넷 등*	93	88	81	54	96	60
합 계	175	136	137	82	155	106

* 인터넷 등 : 인터넷접속, 이메일 등

193) 이재상/조균석, 형사소송법[제12판], 박영사, 2019, 228면.

194) "감청 건수 늘었는데…이동전화 감청은 '0'건", 이데일리 2017년 6월 5일자, https://www.edaily.co.kr/news/read?newsId=02643686615958768&mediaCodeNo=257&OutLnkChk=Y (2019년 10월 23일 최종접속).

195) 과학기술정보통신부 보도자료, "2018년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 발표", 2019.5.10., https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1946094 (2019년 10월 23일 최종접속); 과학기술정보통신부 보도자료, "2018년 상반기 통신자료 및 통신사실확인자료 제공 등 현황 발표", 2018.11.9., https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1413917 (2019년 10월 23일 최종접속); 과학기술정보통신부 보도자료, "2017년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 발표", 2018.5.18., https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1382927 (2019년 10월 23일 최종접속) 참조.

유선전화의 경우 전화국이 개별 전화선을 연결해주면 감청이 가능했으나 이동전화에 대한 감청에는 별도의 설비가 요구된다. 2005년 국가정보원의 불법도청 사건[196]이 문제된 바 있는데, 당시에 사용되었던 2세대 휴대전화에 대해서는 종래의 유선전화 감청장비로 도청이 가능하다고 한다.[197] 그러나 3세대 휴대전화부터는 단말기의 고유번호 복제를 방지하기 위해 유심(Universal Subscriber Identity Module, USIM)칩이 도입되면서 별도의 감청설비 없이는 통신감청이 어려운 실정이다.[198] 설령 정보기관이나 수사기관이 자체적으로 감청설비를 갖출 수 있다고 하더라도 그것은 정보통신기술 변화의 짧은 주기를 고려할 때 비합리적이라는 평가가 내려진다. 현행법상 정보기관이나 수사기관은 통신기관 등에 대하여 통신제한조치 집행을 위탁하거나 협조를 요청할 수 있으나(통신비밀보호법 제9조), 그 이행을 강제할 수는 없다. 이에 미국[199]이

196) 국가정보원에서 정치인 및 민간인 등을 대상으로 도·감청한 사건으로, 2002년 한나라당 정형근 의원에 의해 의혹이 제기되었고 언론의 관련기사 보도를 통해 증폭되며 대선 전 정치 쟁점으로 비화되었으나, 구체적 확증이 없다는 이유로 2005년 5월 국정원장 등 관련자를 무혐의 처분하였다. 이후 언론이 비밀도청팀인 미림팀 운영 등을 폭로하고 안기부 X 파일 사건 등이 드러나며 검찰이 재수사한 끝에 국정원의 감청장치를 이용한 불법 도·감청 사실이 밝혀지며 전직 국정원장 등 관련자들은 체포·구속 및 처벌을 받았다.

197) "[궁금한 화요일] 국정원 감청 논란 … 내 휴대폰 안전할까", 중앙일보 2015년 8월 4일자, https://news.joins.com/article/18379020 (2019년 10월 23일 최종접속); 장여경/김지성, 앞의 글, 10-13면.

198) "간첩의 휴대전화 감청 못하는 국정원, 정보기관 맞나?", 미래한국 2015년 6월 4일자, http://www.futurekorea.co.kr/news/articleView.html?idxno=27940 (2019년 10월 23일 최종접속).

199) 미국의 법집행통신지원법(The Communications Assistance for Law Enforcement Act, CALEA)은 통신사업자 협조의무에 관한 사항을 규정하고 있는데 유선·전기통신사업자는 법원명령이나 기타 합법적인 허가를 받아 서비스를 제공하는 권역 내에서 가입자의 통신 내용을 감청하고, 정보기관이나 수사기관 등에 통신사실확인자료를 제공할 수 있는 통신설비를 갖추어야 한다(47 U.S.C. § 1002 (a)). 다만, 정부는 전기통신사업자에게 특정 통신설비를 갖추도록 요구할 수는 없고, 정보서비스 제공이나 개인 간 통신을 목적으로 구축된 네트워크에 대해서는 이러한 의무를 부여할 수 없다(47 U.S.C. § 1002 (b)). 또한 전기통신사업자로 하여금 동 사업자가 보유한 통신설비시스템으로 감청할 수 있는 최대 건수 등을 일정 기간 내에 보고하도록 하였고, 법무부장관이 해당 보고서의 검토 후 감청설비 구축 시 필요한 직접 경비를 보상하도록 규정하고 있다(47 U.S.C. § 1003). 감청명령을 행한 법원은 전기통신사업자 또는 제조업체가 감청에 필요한 설비를 갖추지 않거나 감청 내용을 제공하지 않은 경우에, 동법에 의해 감청설비를 구축하고 통신 내용을 제공하도록 명할 수 있다(18 U.S.C. § 2522 (a)). 또한 법무부장관은 전기통신사업자 등이 동법에 규정된 감청설비를 갖추도록 요하는 민사소송을 제기할 수 있는데(18 U.S.C. § 2522 (b)), 법원이 전기통신사업자 또는 제조업체에 대하여 해당 설비를 갖추도록 명령하면, 특정일을 정하지 않은 이상 그 명령이 있은 날의 익일부터 1일당 10,000달러까지 민사제재금(Civil monetary penalty)을 부과할 수 있다(18 U.S.C. § 2522 (c)). 이원상, 프라이버시와 범죄통제의 균형을 위한 통신수사 법체계 마련, 대검찰청, 2015, 59-60면; U.S. Government Publishing Office 웹페이지, https://www.govinfo.gov/content/pkg/USCODE-1998-title47/pdf/USCODE-1998-title47.pdf (2019년 10월 23일 최종접속).

나 독일[200]과 같이 우리나라도 전기통신사업자가 감청에 협조할 수 있는 설비를 구축하도록 의무 규정을 신설해야 한다는 필요성이 제기되었고, 이러한 내용을 담은 통신비밀보호법 개정안이 지속적으로 발의되었으나[201] 입법화는 이루어지지 못하고 있다.

한편 2014년에는 모바일 메신저 서비스 '카카오톡(Kakao Talk)' 사찰 논란이 야기되면서 이용자들의 사이버 망명이 이어졌다.[202] 사건 직후 카카오톡의 대표는 회사가 수사기관에게 통신내용 및 자료를 제공했다고 시인하면서 향후 이용자들의 신뢰를 회복할 수 있도록 감청영장에 불응하겠다는 입장을 밝혔는데, 이 발언으로 인해 실정법 위배 논란이 또다시 야기되었다.[203] 비록 '감청'이라는 용어가 사용되었으나 카카오톡 대화를 실시간 감청할 수 있는 설비는 존재하지 않았고, 해당 회사는 서버에 저장되어 있는 대화 내용을 정기적으로 추출해서 수사기관에 제출했던 것으로 알려졌다.[204] 이는 송수신이 완료되어 서버에 보관되어 있던 것으로서 통신비밀보호법상 감청의 대상이 되지 않으며,[205] 필요한 경우 수사기관은 압수·수색을 통해 자료를

---

200) 독일의 통신비밀제한법(Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz - G 10)은 국가안보, 범죄수사 등을 위해 합법적 감청이 가능한데 전기통신사업자에게 통신제한조치가 가능하도록 기술적 부분의 협조나 관련 조치를 위탁 받아 이행가능한 자를 지체 없이 선정하도록 하는 등 통신사업자의 협조의무를 규정하고 있고(§ 2 G 10), 그 이행을 강제하기 위해 과태료 부과 규정을 두고 있다(§ 19 G 10). 이원상, 앞의 보고서, 2015, 40면; Gesetze im Internet 웹페이지, https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html (2019년 10월 23일 최종접속).

201) 의안번호 1650. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_Q0H8K1M0Y3E0A1I8G0Y7Z3R8U3G6T6 (2019년 10월 23일 최종접속).

202) 검찰이 온라인 허위사실 유포 및 사이버 명예훼손을 막기 위한 대응책으로 인터넷이나 SNS를 상시 모니터링하기 위한 수사팀을 설치하겠다고 언급하면서 카카오톡의 검열 문제가 대두되었는바, 검찰 발표 1주일 만에 100만 명 이상의 카카오톡 이용자들이 메시지가 암호화되어 보안이 강력한 독일 기반 메신저 프로그램인 텔레그램(Telegram)으로 옮겨가는 일이 벌어진 것이다. "검찰, 사이버 명예훼손 전담수사팀 신설...여론 통제 우려도", 전자신문 2014년 9월 21일자, http://www.etnews.com/20140921000046?m=1 (2019년 10월 23일 최종접속); "카카오톡 사찰 논란에 '사이버 망명' 늘어", YTN 2014년 10월 1일자, https://www.ytn.co.kr/_ln/0103_201410011709105280 (2019년 10월 23일 최종접속).

203) "[현장에서] '사이버 사찰' 논란에 휘말린 검찰", 헤럴드경제 2014년 10월 14일자, http://news.heraldcorp.com/view.php?ud=20141014000458&md=20141015003557_BL (2019년 10월 23일 최종접속).

204) 대법원 2016. 10. 13. 선고 2016도813 판결; "카카오, '감청' 협조 중단...사이버 검열 논란 재점화", 디지털타임스 2016년 10월 16일자, http://www.dt.co.kr/contents.html?article_no=2016101702101131033001 (2019년 10월 23일 최종접속).

205) 통신비밀보호법에 규정된 '감청'은 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독(共讀)하여 그 내용을 지득(知得) 또는 채록(採錄)하거나 전기통신의 송·수신을 방해하는 것을 말한다(제2조 제7호). 따라서 '전기통신의 감청'은 위 '감청'의 개념 규정에 비추어 현재 이루어지고 있는 전기통신의 내용을 지득·

취득해야 한다. 통신비밀보호법에 의할 때 수사기관이 송수신이 완료된 전기통신에 대해서 압수·수색·검증을 집행한 경우에 그 사건에 관해 공소제기를 하거나 공소제기 또는 입건을 하지 않는 처분(기소중지결정 제외)을 하면 해당 처분이 있은 날로부터 30일 이내에 당해 수사 대상이 되었던 가입자에게 서면으로 압수·수색·검증의 집행 사실을 통지해야 한다(통신비밀보호법 제9조의3).

또한 수사기관은 수사나 형의 집행을 위하여 필요한 경우 관할 지방법원 또는 지원의 허가를 받아서 전기통신사업자에게 통신사실 확인자료[206]의 열람 내지는 제출을 요청할 수 있다(동법 제13조).[207][208] 범죄수사를 위하여 통신사실 확인자료제공을

채록하는 경우와 통신의 송·수신을 직접적으로 방해하는 경우를 의미하는 것이지 전자우편이 송신되어 수신인이 이를 확인하는 등으로 이미 수신이 완료된 전기통신에 관하여 남아 있는 기록이나 내용을 열어보는 등의 행위는 포함하지 않는다(대법원 2012. 7. 26. 선고 2011도12407 판결).

206) "통신사실 확인자료"라 함은 ㉮ 가입자의 전기통신일시, ㉯ 전기통신개시·종료시간, ㉰ 발·착신 통신번호 등 상대방의 가입자번호, ㉱ 사용도수, ㉲ 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, ㉳ 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, ㉴ 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료 중 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다(통신비밀보호법 제2조 제11호).

207) 통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차) ① 검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다.
② 제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다.
③ 제2항 단서의 규정에 의하여 긴급한 사유로 통신사실 확인자료를 제공받았으나 지방법원 또는 지원의 허가를 받지 못한 경우에는 지체 없이 제공받은 통신사실 확인자료를 폐기하여야 한다.
④ 삭제 〈2005. 5. 26.〉
⑤ 검사 또는 사법경찰관은 제2항의 규정에 따라 통신사실 확인자료제공을 받은 때에는 당해 통신사실 확인자료제공요청사실 등 필요한 사항을 기재한 대장과 통신사실 확인자료제공요청서 등 관련자료를 소속기관에 비치하여야 한다.
⑥ 지방법원 또는 지원은 제2항의 규정에 따라 통신사실 확인자료제공 요청허가청구를 받은 현황, 이를 허가한 현황 및 관련된 자료를 보존하여야 한다.
⑦ 전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실 확인자료를 제공한 때에는 자료제공현황 등을 연 2회 과학기술정보통신부장관에게 보고하고, 당해 통신사실 확인자료 제공사실등 필요한 사항을 기재한 대장과 통신사실 확인자료제공요청서 등 관련자료를 통신사실확인자료를 제공한 날부터 7년간 비치하여야 한다.
⑧ 과학기술정보통신부장관은 전기통신사업자가 제7항의 규정에 의하여 보고한 내용의 사실여부 및 비치하여야 하는 대장등 관련자료의 관리실태를 점검할 수 있다.

받은 사건에 대해서 공소제기를 하거나, 공소의 제기 또는 입건을 하지 않는 처분을 한 경우에는 해당 처분이 있은 날로부터 30일 이내에 서면으로 통신사실 확인자료제공을 받은 사실과 제공요청기관, 그 기간 등을 통지해야 한다(동법 제13조의3 제1항).[209] 범죄수사를 위해 통신사실 확인자료제공 절차에 관여했던 공무원이나 그 직에 있었던 자, 통신기관의 직원이나 그 직에 있었던 자는 관련 사항을 외부에 공개 또는 누설해서는 안 되고, 누구든지 동법에 의한 통신제한조치로 인하여 알게 된 내용을 동법에 따라 사용하지 않고 외부로 공개 또는 누설해서는 안 된다(동법 제13조의5). 나아가 전기통신사업자는 이 법에 의해 수사기관이 집행하는 통신제한조치나 통신사실 확인자료제공의 요청에 대해 협조하여야 하는바, 전기통신사업자가 협조할 사항과 통신사실 확인자료의 보관기간 및 그 밖에 필요한 사항에 대해서는 대통령령[210]으로 정한다(동법 제15조의2).[211]

---

⑨ 이 조에서 규정된 사항 외에 범죄수사를 위한 통신사실 확인자료제공과 관련된 사항에 관하여는 제6조(동조 제7항을 제외한다)의 규정을 준용한다.

208) 통신비밀보호법 시행령 제37조(통신사실 확인자료제공의 요청 등) ① 법 제13조 제2항 본문 및 단서에서 "관할 지방법원 또는 지원"이란 피의자 또는 피내사자의 주소지·소재지, 범죄지 또는 해당 가입자의 주소지·소재지를 관할하는 지방법원 또는 지원을 말한다.
② 동일한 범죄의 수사 또는 동일인에 대한 형의 집행을 위하여 피의자 또는 피내사자가 아닌 다수의 가입자에 대하여 통신사실 확인자료제공의 요청이 필요한 경우에는 1건의 허가청구서에 의할 수 있다.
③ 범죄수사 또는 내사를 위한 통신사실 확인자료제공 요청 및 그 통지 등에 관하여는 제11조부터 제13조까지, 제17조부터 제21조까지의 규정을 준용한다. 다만, 제17조 제2항 본문의 규정은 그러하지 아니하다.
④ 국가안보를 위한 통신사실 확인자료제공 요청 및 그 통지 등에 관하여는 제5조부터 제13조까지, 제16조부터 제18조까지, 제20조 및 제21조를 준용한다. 다만, 제17조 제2항 본문의 규정은 그러하지 아니하다.
⑤ 검사, 사법경찰관 또는 정보수사기관의 장(그 위임을 받은 소속 공무원을 포함한다)은 제3항 및 제4항에서 준용하는 제12조에 따라 전기통신사업자에게 통신사실 확인자료제공 요청 허가서 또는 긴급 통신사실 확인자료제공요청서 표지의 사본을 발급하거나 신분을 표시하는 증표를 제시하는 경우에는 모사전송의 방법에 의할 수 있다.

209) 그 이외에 통신사실 확인자료제공을 받은 사실 등에 관하여는 통신비밀보호법 제9조의2(동조 제3항을 제외한다)의 규정을 준용한다(통신비밀보호법 제13조의3 제2항).

210) 통신비밀보호법 시행령 제41조(전기통신사업자의 협조의무 등) ① 법 제15조의2에 따라 전기통신사업자는 살인·인질강도 등 개인의 생명·신체에 급박한 위험이 현존하는 경우에는 통신제한조치 또는 통신사실 확인자료제공 요청이 지체없이 이루어질 수 있도록 협조하여야 한다.
② 법 제15조의2 제2항에 따른 전기통신사업자의 통신사실확인자료 보관기간은 다음 각 호의 구분에 따른 기간 이상으로 한다.
1. 법 제2조 제11호 가목부터 라목까지 및 바목에 따른 통신사실확인자료: 12개월. 다만, 시외·시내전화역무와 관련된 자료인 경우에는 6개월로 한다.
2. 법 제2조 제11호 마목 및 사목에 따른 통신사실확인자료: 3개월

211) 전기통신사업자는 통신비밀보호법 제13조 제1항, 동법 제13조의2 및 동법 제13조의4 제1항

2) 범죄수사를 위한 실시간 위치추적 및 위치정보 수집

종래 수사기관은 범죄 용의자의 행적을 파악하기 위해 잠복이나 미행을 하면서 많은 시간과 노력을 기울여야 했다. 그러나 GPS(Global Positioning System)[212]로 대표되는 위성기반항법 시스템이 등장하면서 용의자의 차량에 GPS 수신기를 부착해서 그 위치를 추적하는 것이 가능해졌다. 이동통신망 시스템이나 무선인터넷망도 위치추적에 이용될 수 있는바, 오늘날 수사기관은 모바일 디바이스의 위치를 통해 용의자의 소재지나 이동경로를 파악할 수 있다. 정보통신 기술이 발전함에 따라서 위치정보의 파악이 용이해졌고, 이를 이용한 다양한 서비스가 등장하였으나 해당정보의 유출이나 오·남용으로 인해 개인의 사생활이 침해될 우려가 커졌다. 이에 위치정보의 유출이나 오·남용으로부터 프라이버시를 보호하고 위치정보의 안전한 이용환경을 조성함으로써 위치정보 이용을 활성화시키고자 2005년 1월 27일에 「위치정보의 보호 및 이용 등에 관한 법률」(이하 '위치정보법'이라고 함)이 제정되었다.[213] 동법에 의할 때 누구든지 개인위치정보주체의 동의 없이 해당 개인위치정보[214]를 수집·이용·제공해서는 안 되나, 긴급구조기관의 긴급구조요청이나 경보발송요청이 있는 경우, 긴급구조를 위해 경찰관서의 요청이 있거나 다른 법률에 특별한 규정이 있는 경우에는

에 따라 통신사실확인자료를 제공한 경우에는 통신사실확인자료 제공대장에 그 제공사실을 기록하여야 하고(통신비밀보호법 시행령 제38조), 동법 제13조 제7항에 따라 자료제공현황 등을 매 반기 종료 후 30일 이내에 과학기술정보통신부장관에게 보고하여야 한다(동 시행령 제39조).

212) GPS는 미국 국방부가 개발한 범세계적인 위성기반 항법시스템으로서 우주 부분(space segment), 제어 부분(control segment), 사용자 부분(user segment)으로 구분되며, 지구 궤도상 배치된 인공위성과 그러한 인공위성을 통제하는 지상관제국 및 사용자의 GPS 수신기 등으로 구성되는데, 지구 궤도를 회전하고 있는 위성을 이용해서 GPS 수신기가 위치한 곳 주변에 대한 정보를 추적한 후 3개의 위성을 이용해서 그 위치를 측정하는 것으로, 미국은 2019년 4월 현재 31개의 인공위성을 운용하고 있다. GPS.GOV(Official U.S. Government information about the Global Positioning System (GPS) and related topics), http://www.gps.gov/systems/gps/, http://www.gps.gov/systems/gps/space (2019년 10월 23일 최종접속).

213) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=66566&ancYd=20050127&ancNo=07372&efYd=20050728&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

214) "위치정보"란 이동성이 있는 물건이나 개인이 특정 시간에 존재하거나 존재했던 장소에 관한 정보로서 전기통신설비 및 전기통신회선설비를 이용해서 수집된 것을 말한다(위치정보법 제2조 제1호). 특정 개인의 위치정보를 "개인위치정보"라 부르는데, 위치정보만으로는 특정 개인의 위치를 파악할 수 없다 하더라도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 경우도 여기에 해당한다(동조 제2호).

예외가 인정된다(위치정보법 제15조 제1항). 범죄피해자나 실종아동 등의 구조를 위해서는 개인위치정보가 이용될 수 있으나 범죄수사는 언급되고 있지 않다.

일반적으로 범죄수사를 위한 위치추적은 통신비밀보호법 제13조에 근거해서 이루어졌다. 이에 의하면 검사나 사법경찰관은 수사를 위해 필요한 경우 전기통신사업자에게 통신사실 확인자료제공을 요청할 수 있는데, 해당 자료를 근거로 기지국 수사[215]나 위치추적이 가능했다. 그러나 2018년 6월 28일 헌법재판소는 기지국 수사를 허용한 통신비밀보호법 제13조 제1항 중 "검사 또는 사법경찰관은 수사를 위해 필요한 경우에 전기통신사업자에게 동법 제2조 제11호 '가목 내지 라목'[216]의 통신사실 확인자료의 열람이나 제출을 요청할 수 있다"라는 부분은 헌법에 합치되지 않는다고 결정하였다.[217] 먼저 범죄예방과 사건의 조기해결을 위해서는 수사기관이 기지국 수사를 할 필요성이 있고, 통신사실 확인자료의 제공을 요청하기 위해서는 법원의 허가를 얻어야 하므로 입법목적의 정당성과 수단의 적정성은 인정되었다. 그러나 헌법재판소는 비록 통신사실 확인자료가 비내용적인 정보이지만, 여러 정보들의 결합 및 분석을 통해 정보주체에 대한 정보를 유추할 수 있는 민감한 정보라는 점에 주목하였다. 또한 통신사실 확인자료 제공 요청을 위해서는 법원의 허가를 거쳐야 하지만 그 요건이 '수사의 필요성'에 한정되어 있는바, 범죄의 경중 없이 요청될 수 있고, 범죄의 의혹만으로 불특정 다수의 통신사실 확인자료가 제공될 수 있다는 점에서 침해의 최소성은 부정되었다.[218] 나아가 이 사건 조항으로 달성하고자 하는 '수사의 효율성

---

215) "기지국 수사"란 특정 시간대에 특정 기지국에서 발신된 모든 전화번호 등을 통신사실 확인자료로 제공받는 수사방식으로서 주로 용의자를 특정하기 어려운 연쇄범죄가 발생하거나 동일 사건의 단서가 여러 지역에서 시차를 두고 발견된 경우에 사건이 발생한 지역의 기지국에서 발신된 전화번호들을 추적하여 용의자의 범위를 좁혀나가기 위해 활용된다. 헌법재판소 2018. 6. 28. 선고 2012헌마538 결정문 중 '통신사실 확인자료 제공요청 및 집행사실 통지 제도 개관' 부분 참조.

216) 통신비밀보호법 제2조 제11호 가. 가입자의 전기통신일시, 나. 전기통신개시·종료시간, 다. 발·착신 통신번호 등 상대방의 가입자번호, 라. 사용도수

217) 헌법재판소 2018. 6. 28. 선고 2012헌마538.

218) 기지국 수사의 허용과 관련해서는 ① 유괴나 납치 및 성폭력 등 강력범죄 또는 국가안보를 위협하는 범죄와 같이 피의자나 피해자의 통신사실 확인자료가 반드시 필요한 범죄로 그 대상을 한정하는 방안이나 ② 중요범죄와 함께 통신을 수단으로 하는 범죄 일반을 포함시키는 방안, ③ 상기의 요건에 더하여 '다른 방법으로는 범죄수사가 어려운 경우(보충성)'를 그 요건으로 추가하거나, 또는 중요범죄 이외의 경우에만 보충성을 요건으로 추가하는 방안, ④ 1건의 허가서로 불특정 다수인에 관한 통신사실 확인자료 제공요청을 못하도록 하는 방안 등을 독립적 내지는 중첩적으로 검토함으로써 수사에 지장을 초래하지 않으면서도 불특정 다수의 기본권을 적게 침해하는 수단을 모색할 수 있다. 헌법재판소 2018. 6. 28. 선고 2012헌마538.

및 신속성'이라는 공익은 그로 인해 침해되는 '정보주체의 개인정보자기결정권 및 통신의 자유'에 비해 중하다고 볼 수 없으므로 법익의 균형성도 인정될 수 없다고 보았다. 이에 헌법재판소는 헌법불합치 결정을 내리면서 다만, 해당 법률조항은 2020년 3월 31일을 시한으로 입법자가 그 위헌성을 제거하고 합리적인 내용으로 법률을 개정할 때까지 계속 적용하도록 했다.[219]

한편 2018년 6월 28일에 헌법재판소는 범죄수사의 목적으로 위치정보를 추적하기 위한 자료의 제공을 요청하고, 수사가 종료된 후에 해당 자료를 제공받은 사실 등을 통지하도록 규정한 통신비밀보호법 조항에 대한 위헌 여부를 판단하였다.[220] 먼저 수사기관이 위치정보 추적 자료의 제공을 요청할 수 있도록 한 통신비밀보호법 제13조 제1항 중 '검사 또는 사법경찰관은 수사를 위해 필요한 경우[221]에 전기통신사업자

---

219) 반면 김창종, 서기석, 조용호 재판관은 이 사건 요청조항이 과잉금지의 원칙에 반하여 개인정보자기결정권과 통신의 자유를 침해하지 않는다는 입장을 내놓았다. 이에 의할 때, 범죄수사를 위해 필요한 경우 수사기관이 법원의 허가를 얻어 전기통신사업자에게 해당 가입자에 관한 통신사실 확인자료의 제공을 요청할 수 있도록 하고 있는 심판대상조항은 입법목적의 정당성과 수단의 적정성이 인정된다. 또한 ① 초동수사 단계에서 활용되는 통신사실 확인자료의 특성상 기지국 수사는 주로 용의자의 범위를 한정하기 위해 사용된다는 점, ② 범죄예방과 사건의 조기해결을 위해서 수사기관으로 하여금 특정 시간대 특정 기지국에 있었던 불특정 다수인의 통신사실 확인자료의 제공을 요청할 수 있도록 허용해야 할 필요성이 있다는 점, ③ 기지국 수사를 통한 통신사실 확인자료는 비내용적인 정보로서 기본권을 제한하는 정도가 심각하지 않다는 점, ④ 다수의견과 같이 대상범죄를 제한하거나 보충성 요건을 추가할 경우 수사의 난항이 예상되고 추가범죄로 연결됨에 따라 국민의 안전에 위험이 초래될 수 있다는 점, ⑤ 관련 규정에 의하면 수사기관이 통신사실 확인자료 제공을 요청하는 경우 그 요청사유, 가입자와의 연관성, 필요한 자료의 범위를 기록한 서면을 통해 법원의 허가를 얻어 실시하도록 하고 있어 필요 최소한의 범위에서 기지국 수사가 허용되고 있다는 점 등을 종합해 볼 때, 침해의 최소성도 인정된다고 판단하였다. 나아가 해당 조항으로 달성하려는 공익은 범죄에 대한 신속한 수사를 통해 범인을 검거하고 추가적인 피해 발생을 방지함으로써 실체적 진실을 발견하고 국가형벌권을 적절하게 행사함과 동시에 궁극적으로는 피해자의 인권을 보호하기 위한 것이라는 점도 강조하였다. 이에 반해 해당 조항으로 인해 제한되는 사익은 특정 장소, 특정 시간대에 있었던 정보주체의 비내용적인 정보에 해당하는 통신사실 확인자료가 수사기관에 제공되는 것으로서, 이러한 사익이 공익보다 크다고 할 수 없으므로 법익의 균형성도 인정된다고 보았다. 아울러 반대의견은 이 사건 요청조항에 일부 개선의 여지가 있다는 점에 동의하였으나, 그러한 개선의 여지가 있다는 것이 곧 위헌임을 의미하지는 않으므로 입법개선을 권고하는 것으로 충분하다는 입장을 밝혔다. 헌법재판소 2018. 6. 28. 선고 2012헌마538 결정문 중 '재판관 김창종, 재판관 서기석, 재판관 조용호의 이 사건 요청조항에 대한 반대의견' 참조.

220) 헌법재판소 2018. 6. 28. 선고 2012헌마191, 2012헌마550, 2014헌마357(병합).

221) "수사를 위하여 필요한 경우"란 위치정보 추적자료가 범인의 발견, 범죄사실의 입증에 기여할 개연성이 있다는 점이 충분히 소명된다는 전제 하에, 범인을 발견하거나 확보하며 증거를 수집 및 보전하는 수사기관의 활동을 위해 그 목적을 달성할 수 있는 범위 내에서 관련성이 있는 자에 대한 위치정보 추적자료 제공요청이 필요한 경우를 의미한다고 해석되므로 이는 명확성의 원칙에 위반되지 않는다고 보았다. 헌법재판소 2018. 6. 28. 선고 2012헌마191 등.

에게 제2조 제11호 '바목, 사목'[222]의 통신사실 확인자료의 열람이나 제출을 요청할 수 있다'라고 규정한 부분은 과잉금지의 원칙에 반해 개인정보자기결정권과 통신의 자유를 침해하고, 적법절차의 원칙에도 위배되어 개인정보자기결정권을 침해한다고 보아 헌법불합치 결정을 내리면서 2020년 3월 31일까지 해당 조항을 잠정적으로 적용하도록 했다.[223]

다음으로 헌법재판소는 수사가 종료된 후에 위치정보 추적 자료를 제공받았다는 사실 등을 통지하도록 규정한 동법 제13조의3 제1항 중 제2조 제11호 '바목, 사목'의 통신사실 확인자료에 관해 헌법불합치 결정을 하면서 2020년 3월 31일을 시한으로 입법자가 법률을 개정할 때까지 해당 조항을 계속 적용하도록 하였다.[224] 이 사안에서는 과연 통지조항이 청구인들의 개인정보자기결정권을 침해하는지가 문제되었다. 헌법재판소는 수사의 밀행성 확보가 요구되지만, 헌법상 적법절차의 원칙을 통해서 수사기관의 권한 남용을 막고, 정보주체의 기본권을 보호하기 위해서는 그 주체에게 위치정보 추적자료 제공에 관한 적절한 고지를 해주어야 하고, 실질적인 의견진술의 기회도 부여해야 한다고 보았다. 그러나 이 사건 통지조항은 공소를 제기하거나, 공소의 제기나 입건을 하지 않는 처분(기소중지결정 제외)을 한 때에만 통지의무를 부과하고 있을 뿐, 수사가 진행 중이거나 기소중지결정이 있는 경우에는 그러한 의무를 규정하지 않고 있다. 이로 인해 수사가 장기간 계속되거나 기소가 중지된 경우에는 정보주체가 그 기간의 장단과 무방하게 자신의 위치정보가 범죄수사에 이용되었다는 사실을 인식할 수 없게 된다. 또한 수사가 종료된 후에 위치정보 제공사실을 통지받은 경우라 할지라도 정보주체로서는 해당 자료가 제공된 사유를 전혀 파악할 수 없다. 나아가 수사기관이 수사의 목적을 달성한 경우라 하더라도 정보주체는 해당 자료의 파기 여부를 확인할 수 있는 방법이 없다. 요컨대 이 사건 통지조항은 정보주체로 하여금 위치정보 추적자료와 관련된 수사기관의 권한남용에 적절히 대응할 수 없도록

---

222) 통신비밀보호법 제2조 제11호 바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, 사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료.

223) 김창종, 서기석, 조용호 재판관은 이 사건 요청조항이 과잉금지의 원칙에 반하여 개인정보자기결정권과 통신의 자유를 침해하지 않는다는 반대의견을 내놓았다. 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정문 중 '재판관 김창종, 재판관 서기석, 재판관 조용호의 이 사건 요청조항에 대한 반대의견' 참조.

224) 헌법재판소 2018. 6. 28. 선고 2012헌마191 등.

하고 있는바,[225] 적법절차의 원칙에 반해 청구인들의 개인정보자기결정권을 침해한 것으로 판단되었다.[226]

2. 프라이버시 보호 기술의 발전과 형사법적 과제

가. 프라이버시 보호 기술의 발전

1) 프라이버시 보호의 요청

정보통신기술의 발전은 시민들에게 다양한 서비스와 편익을 향유할 수 있도록 해주었지만, 그로 인한 프라이버시 침해 가능성은 도처에 존재하고 있다. 인터넷과 휴대전화가 대중화되면서 이용자의 위치정보나 통신사실은 물론이고 이메일이나 문자메시지 등의 내용이 유출될 위험이 커졌다. 이로 인해 조지 오웰(George Orwell)의 '1984'라는 소설 속의 빅브라더가 등장할 수 있다는 우려의 목소리가 나오기도 했다. 그러나 2001년 미국에서 2,990여 명의 생명을 앗아간 9·11 테러를 필두로 하여 세계 곳곳에서 크고 작은 테러가 발생하면서 개별 시민의 프라이버시는 국가안보나 테러예방이라는 대의 앞에 한걸음 뒤로 물러나야 했다.

---

225) 이와 관련해서는 수사가 장기간 계속되거나 기소중지된 경우라도 일정 기간이 경과하면 원칙적으로 정보주체에게 그 제공사실을 통지하도록 하되, 수사에 지장을 초래하는 경우에는 중립적인 기관의 허가를 얻어서 통지를 유예하는 방법, 일정한 조건 하에 정보주체가 그 제공요청 사유의 통지를 신청할 수 있도록 하는 방법, 통지의무를 위반한 수사기관을 제재하는 방법 등이 강구될 수 있다. 헌법재판소 2018. 6. 28. 선고 2012헌마191 등.

226) 김창종, 서기석, 조용호 재판관은 이 사건 통지조항에 대해 반대의견을 제시하였다. 3인의 재판관은 기밀성을 요하는 수사의 진행 과정에서 통신사실 확인자료 제공사실을 정보주체에게 통지한다면 피의자와 그 관련자들이 통신수단을 이용하지 않거나 도주 또는 증거를 인멸할 가능성이 있는 등 범죄수사에 지장이 초래될 수 있다는 우려를 제기하였다. 반면 통신사실 확인자료 제공사실을 공소제기 또는 불기소처분 이후에 통지받는다고 하더라도, 해당 자료는 비내용적인 성격을 가진다는 점을 고려할 때 그로 인해 제한되는 정보주체의 사익은 크지 않다고 평가하였다. 또한 정보주체가 피의자인 경우에는 공소장부본을 송달받거나 불기소처분 결과를 통지받음으로써 통신사실 확인자료 제공요청 사유를 알 수 있고, 정보주체가 피의자가 아닌 경우에는 피의자의 명예와 사생활 보호의 필요성이 있기 때문에 그 제공요청 사유를 통지하지 않는 것이 바람직하다고 보았다. 나아가 이 사건 요청조항이나 허가조항을 위반하여 취득한 통신사실 확인자료에 대해서는 형사절차에서 위법수집증거 배제법칙을 통해 증거능력을 부정할 수 있고, 해당 수사관이나 국가에 대해 손해배상을 청구할 수 있는 등 사후적인 권리구제수단이 마련되어 있다는 점도 고려하였다. 이에 반대의견은 이 사건 통지조항이 수사가 종료된 후에 통신사실 확인자료 제공사실을 통지하도록 하고, 그 사유를 통지사항으로 정하지 않았다고 해서 적법절차의 원칙에 위배되는 것은 아니라고 판단하였다. 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정문 중 '재판관 김창종, 재판관 서기석, 재판관 조용호의 이 사건 통지조항에 대한 반대의견' 참조.

9·11 테러를 계기로 제정된 미국의 애국법(USA Patriot Act)[227]은 감청의 대상이 되는 범죄를 확대하였고,[228] 범죄수사정보를 공유할 수 있는 권한도 확장하였다.[229] 국가정보기관에 대해서는 통신 관련 정보를 제한 없이 공개하도록 했으며,[230] 해외정보감시법(Foreign Intelligence Surveillance Act of 1978, FISA)상 발신번호기록장치나 착신번호추적장치를 이용한 추적과 감시 권한을 강화했다.[231] 애당초 2005년 12월 31일에 만료될 예정이던 동법은 수차례 갱신이 거듭되었는바,[232] 연장된 애국법이 적용되고 있던 2013년에 미국 국가안보국(National Security Agency, NSA) 소속의 요원이던 애드워드 스노든(Edward Joseph Snowden)이 미국 정부의 무차별적인 통신정보 수집 및 도·감청 실태를 폭로하면서 동법에 대한 비판 여론이 거세졌다. 특히 국가안보국이 법원의 허가를 받지 않고 자국민의 전화통화 기록이나 인터넷 검색 내역 등을 대량 수집하는 것이 문제가 되었다. 이를 해결하기 위해 마련된 자유법(USA Freedom Act)[233]은 애국법 만료일 다음날인 2015년 6월 2일에 미 상원에서 통과된 후 같은 해 11월 29일부터 발효되었다.[234] 정보기관의 개혁과 투명성 제고를 위해

227) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001.

228) 주로 컴퓨터를 통해 테러 관련 정보가 전달된다는 점에 주목하여 컴퓨터 사기 및 악용과 관련된 중대 범죄에 대해서도 감청이 가능하도록 규정하였다. USA Patriot Act § 201

229) USA Patriot Act § 203 (a)

230) USA Patriot Act § 204

231) USA Patriot Act § 214

232) 미국은 9·11 테러라는 초유의 사태를 겪은 직후 동법을 제정하였으나, 어느 정도 시간이 경과하여 시민들의 충격과 분노가 잦아드는 시점에 의회가 다시 국가안보와 시민의 자유라는 상충된 가치를 이익형량할 수 있도록 일몰조항(sunset provision)을 두었다(USA PATRIOT ACT § 224). 애당초 2005년 12월 31일부로 만료될 예정이었던 동법은 여러 차례 갱신을 거듭하였는데, 2011년 5월 26일 오바마 대통령이 "2011년 애국법일몰연장법(PATRIOT Sunsets Extension Act of 2011)"에 서명함으로써 동법의 시한은 2015년 6월 1일까지로 연장되었다. "Obama approves extension of expiring Patriot Act provisions", CNN 2011.5.27., http://edition.cnn.com/2011/POLITICS/05/27/congress.patriot.act/index.html (2019년 10월 23일 최종접속).

233) Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015

234) 자유법은 업무기록의 생성이나 전자감시의 시행, 발신 및 송신 관련 정보 기록 장치의 사용 및 대테러나 범죄수사를 목적으로 한 여타의 정보수집 수단을 사용할 수 있는 연방정부의 권한 개혁 차원에서 제정되었다. 총 8개의 절로 구성되어 있는 동법은 해외정보감시법상 전화통화 기록 등 업무 기록의 이용(제1절), 발신·송신 관련 정보 기록 장치의 이용(제2절), 미국시민 이외의 사람에 대한 정보 취득(제3절), 해외정보감시법원(제4절), 국가안보서신(제5절) 등과 관련된 규정을 정비하였고, 해외정보감시법 운영의 투명성 확보를 위한 보고 요건(제6절) 및 보다 강화된 국가안보 조항(제7절)을 마련하였으며, 항해 안전 및 핵 테러 방지 협약의 이행(제8절)에 관한 규정을 두고 있다.

제정된 자유법은 전자통신과 관련된 정보의 대량 수집을 금하고 있다는 점에서 의의가 있다.[235]

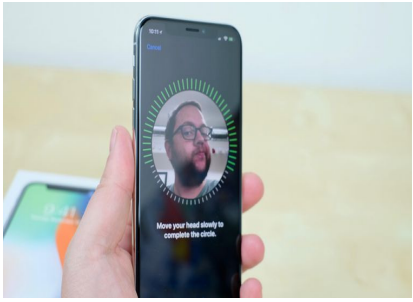
2) 암호화와 익명화 기술 개발

정보통신 사회가 고도화될수록 프라이버시 보호 강화를 요구하는 시민들의 목소리도 높아졌다. 이러한 요구에 법제도의 개선 방안이 모색되는가 하면, 새로운 기술을 개발하고 적용하기도 한다. 스마트폰이 대중화되면서 개별 디바이스는 이용자의 수많은 정보를 담게 되었다. 또한 휴대성이 용이한 스마트폰은 절도나 분실의 위험도 높다. 이용자들은 동의 없이 자신의 기기가 누군가의 손에 들어갔을 때 디바이스가 구동되지 않기를 원한다. 이러한 소비자들의 요구에 부합하고자 스마트폰 제조사들은 보안 수준을 제고시킨 암호화 장치를 구축하기 위해 경쟁적으로 기술을 개발하고 있다. 일례로 단순히 비밀번호를 설정하던 방식은 잘못된 번호를 입력한 횟수에 따라서 일정시간 동안 잠금 해제를 시도하는 것이 불가능한 방식으로 변하였다. 또한 인공지능 기술의 발전에 힘입어 생체정보 인식률이 개선되면서 지문을 비롯해서 홍채나 얼굴을 인식해서 잠금 장치가 해제되는 기술도 이미 적용되었다.

[그림 2-19] 스마트폰 지문인식[236]

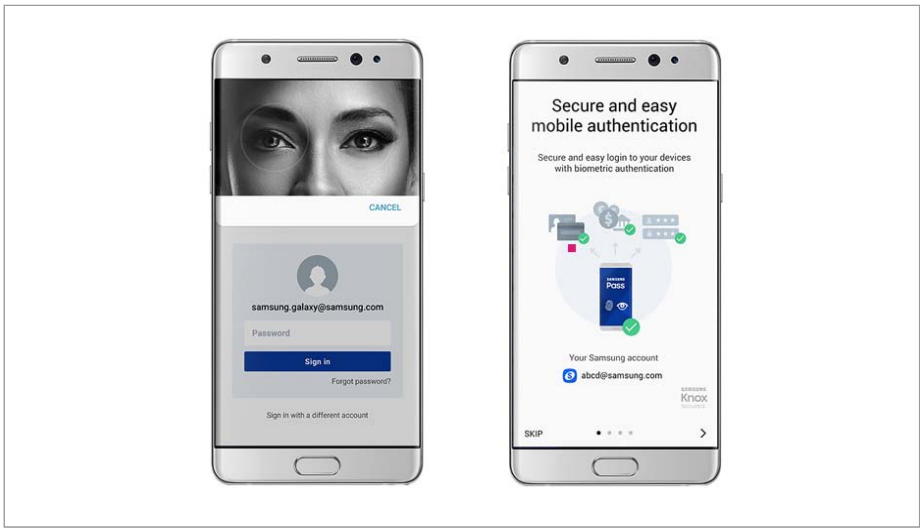


[그림 2-20] 스마트폰 얼굴인식[237]



235) 그러나 여전히 연방수사국은 사법부의 통제 하에 상세통화기록이나 유형화된 정보가 포함된 업무기록의 생성을 요구할 수 있다. 또한 동법은 종래 애국법상의 이동식 전자감시 명령(roving electronic surveillance orders) 조항과 함께 미국 국적 여하를 불문하고 국제테러나 그 준비활동에 관여하고 있는 자를 외국세력의 대리인(agent of a foreign power)으로 포섭시킬 수 있는 소위 "외로운 늑대(lone wolf)" 조항에 대한 일몰기한을 2019년 12월 15일까지로 연장하였다. 요컨대, 자유법은 9·11 테러가 발생한지 15년가량이 경과한 시점에서 미국 의회가 국가안보와 프라이버시라는 상충된 가치 사이의 균형점을 다시 모색한 결과물이라고 평가된다.

[그림 2-21] 스마트폰 홍채인식[238]



한편 접속 기록이 남고, 추적이 가능한 통상의 인터넷과 달리 익명화가 보장되는 기술도 개발되었다. 1990년대 중반 미국의 해군연구소(Naval Research Laboratory, NRL)는 'The Onion Routing(TOR)' 프로젝트를 통해 웹사이트를 방문해도 익명성이 보장되는 '어니언 라우팅(Onion Routing)'이라는 기술을 개발했고,[239] 이후 무상으로 소스코드가 일반에 공개되었다.[240] 이는 인터넷과 같은 일반적 네트워크가 아닌, 가상의 오버레이 네트워크(Overlay Network)[241]를 통해서 같은 웹페이지를 방문할 때

236) 이미지 출처: 삼성디스플레이 뉴스룸 웹페이지, http://news.samsungdisplay.com/18221 (2019년 10월 23일 최종접속).

237) 이미지 출처: "Apple Face ID: Everything you need to know", CNET 2018.10.26., https://www.cnet.com/how-to/apple-face-id-everything-you-need-to-know/ (2019년 10월 23일 최종접속).

238) 이미지 출처: 삼성 뉴스룸 웹페이지, https://news.samsung.com/kr/%EC%8B%AC%E2%88%99%EC%B8%B5%E2%88%99%EB%B6%84%E2%88%99%EC%84%9D-%EA%B0%A4%EB%9F%AD%EC%8B%9C-%EB%85%B8%ED%8A%B7-%E2%91%A2%EA%B6%81%EA%B8%88%ED%95%B4-%ED%99%8D%EC%B1%84-%EC%9D%B8%EC%8B%9D-%EB%B3%B4 (2019년 10월 23일 최종접속).

239) Cath Senker, Cybercrime & the Dark Net: Revealing the Hidden Underworld of the Internet, SIRIUS, 2017, p.120, pp.158-159; "International Raids Target Sites Selling Contraband on the 'Dark Web'", The New York Times 2014.11.7., https://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html (2019년 10월 23일 최종접속).

240) The Tor Project 웹페이지, https://www.torproject.org/about/overview.html.en (2019년 10월 23일 최종접속).

241) 오버레이 네트워크(Overlay Network)는 기존의 네트워크를 바탕으로 다른 필요에 의해 그 위

완벽한 익명성을 보장해주는 기술이다. 일반적인 인터넷 통신의 경우에는 사용자 PC가 ISP를 통해서 목적지(서버나 다른 PC)와 연결한 후 데이터를 주고받는다. 이때 트래픽[242]을 전달하는 중계자인 '망'은 주로 국가기관이기 때문에 검열이나 감청이 용이하게 이루어질 수 있다. 그러나 TOR는 한 번에 목적지로 통신하지 않고, 그 중간에 TOR 라우터를 실행 중인 여러 개의 노드(Node)[243]들을 거쳐서 데이터를 보낸다. 즉 A에서 Z로 바로 가는 것이 아니라 A→B→C…→Z로 우회하는 방식이다.[244] 또한 이름과 같이 양파 껍질처럼 겹겹이 암호화를 해서 패킷을 보내는데, 이때 암호화는 개별 노드(Node)의 공개키를 통해서 이루어지기 때문에 패킷의 출발지와 최종 목적지를 알려면 거의 모든 노드를 장악해야만 한다. 예컨대 국가기관이 B노드를 장악했다고 하더라도 파악할 수 있는 정보라고는 'B에서 왔고, D로 보내라'는 것밖에 없다. 더욱이 노드는 전 세계에 걸쳐서 흩어져 있기 때문에 수많은 PC를 장악하지 못하는 이상 TOR를 이용한 통신을 추적하기란 사실상 불가능하다.[245] TOR 이용자만 접속 가능한 일종의 인트라넷이 형성되어 있는데, 이는 ".onion" 형식의 도메인을 쓴다.[246]

에 재구성되는 또 다른 가상의 컴퓨터 네트워크이다. 기존의 네트워크 위에 별도의 노드(node)와 논리적 링크(logical link)를 구성하므로 기존의 네트워크를 활용하여 성능을 개선하고 효율성을 높인 네트워크 서비스를 제공할 수 있다. ScienceDirect 웹페이지, Overlay Network, https://www.sciencedirect.com/topics/computer-science/overlay-network (2019년 10월 23일 최종접속); 정태진/이광민, "다크웹 범죄활동 동향: 국제공조 및 대응전략", 한국경찰연구 제17권 제1호, 한국경찰연구학회, 2018, 215면.

242) 트래픽(Traffic)이란 전화나 컴퓨터 통신을 위한 특정 전송로에서 일정 시간 내에 흐르는 정보의 양, 즉 전송량을 말한다.

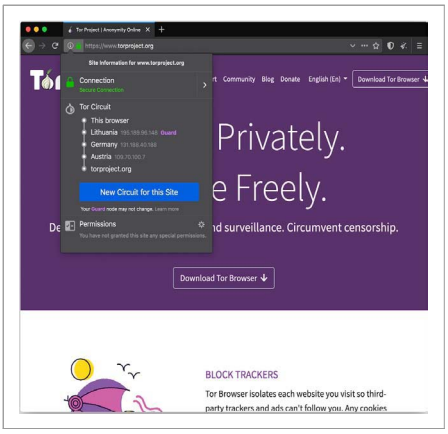
243) 노드(Node)란 네트워크의 연결점 내지는 재분배 지점이다. 통상적으로 네트워크에 연결된 컴퓨터와 그 안에 속한 장비들을 통틀어 하나의 노드라고 한다. techopedia 웹페이지, https://www.techopedia.com/definition/5307/node (2019년 10월 23일 최종접속).

244) 이로 인하여 TOR는 일반 브라우저에 비해 그 처리속도가 심각하게 느리다.

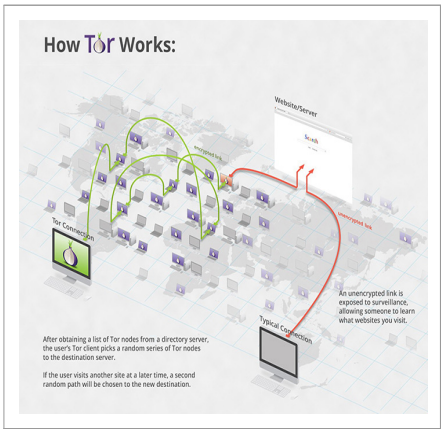
245) Roger Dingledine/Nick Mathewson/Paul Syverson, "Tor: The Second-generation Onion Router", Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13, 2004, pp.4-7, https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/Dingledine%20etal2004.pdf (2019년 10월 23일 최종접속).

246) Roger Dingledine/Nick Mathewson/Paul Syverson, Ibid., pp.7-8.

[그림 2-22] 토르 브라우저[247]



[그림 2-23] 토르 작동 방식[248]



나. 프라이버시 보호 기술 관련 형사법적 과제

1) 디지털 포렌식

정보통신 기술과 디지털 매체의 사용이 일상화되면서 범죄수사에서 컴퓨터나 휴대전화와 같은 디지털 기록 매체에 남아있는 증거를 확보하는 것이 중요해졌다. '디지털 포렌식(Digital Forensic)'이란 디지털 기기를 매개체로 한 정보의 흐름을 조사해서 범죄의 사실관계를 규명하기 위한 절차나 방법을 일컫는다.[249] 수사기관을 중심으로 디지털 포렌식을 담당하는 기관이 설립되고, 관련 정책의 수립 및 신기술 연구가 진행되고 있으나,[250] 2010년대에 들어서는 고도의 은닉 기술과 안티 포렌식 기법이 사용되면서 범죄수사는 어려움에 부딪히고 있다.[251] 분석 대상이 되는 디지털 기기가

247) 이미지 출처: The Tor Project Blog 웹페이지, https://blog.torproject.org/new-release-tor-browser-90 (2019년 10월 23일 최종접속).
248) 이미지 출처: Visual Capitalist 웹페이지, how tor works, https://www.visualcapitalist.com/dark-web/how-tor-works/ (2019년 10월 23일 최종접속).
249) 김종호, "디지털 포렌식의 원리와 소송에서의 증거평가 방식", 경희법학 제52권 제1호, 경희대 법학연구소, 2017, 105면; 양근원, "디지털 포렌식과 법적 문제 고찰", 형사정책연구 제17권 제2호(통권 제66호), 한국형사정책연구원, 2006, 205면; 정익래/홍도원/정교일, "디지털 포렌식 기술 및 동향", 전자통신동향분석 제22권 제1호, 한국전자통신연구원, 2007, 98면.
250) 이상복, "디지털 포렌식 업무의 법·제도적인 개선방향", 서강법학 제10권 제2호, 서강대학교 법학연구소, 2008, 8면.
251) 신 원, "안티포렌식 기법 분석을 통한 안티포렌식 대응 방안", 보안공학연구논문지 Vol.11 No.6, 보안공학연구지원센터, 2014, 606면.

다양해지고 있고, 프라이버시 보호 기술이 발전하면서 디지털 포렌식은 새로운 도전에 직면하고 있는 것이다.

특히 모바일 디바이스나 그 운영체제에 암호화 장치가 구축되면서 범죄수사나 기소를 담당하는 사법당국이 전자통신 기기나 시스템에 접근하는 것 자체가 어려워지고 있다. 실제로 2016년 미국에서는 연방수사국(FBI)과 애플이 아이폰 잠금 해제를 두고 첨예하게 대립한 바 있다.[252] 당시 아이폰은 잘못된 비밀번호를 입력한 횟수에 따라서 일정시간 동안 잠금 해제의 시도가 불가능했다. 만약 비밀번호가 6자리 수에 대문자, 소문자 및 숫자로 구성되었다면 총 568억 개의 조합수를 입력해야 했기 때문에 잠금장치 해제에 소요되는 시간이 최장 144년에 이른다고 계산된 것이다.[253]

2015년 12월 2일에 발생했던 '샌 버나디노(San Bernardino) 총격 사건'[254]에서 연방수사국(FBI)은 용의자의 아이폰을 입수했고, 고속입력기를 이용해 단말기의 암호를 풀려고 하였으나 실패했다. 이에 연방수사국은 애플을 상대로 이른바 '백도어(Backdoor)'[255]를 열어 줄 것을 요구했으나, 개인정보 보호를 이유로 애플이 이를 거부하자 연방수사국이 법원에 소송을 제기하였다. 이 사건을 맡은 미국 캘리포니아주 리버사이드(Riverside) 연방지방법원은 2016년 1월 16일 애플에게 총기 테러 용의자의 스마트폰 잠금장치 해제를 지원하라고 명령했고,[256] 애플은 항소를 제기하였다.[257] 이에 반해 연방수사국이 애플에게 마약거래 용의자의 아이폰 잠금장치 해제를

---

252) "Apple opposes order to help FBI unlock phone belonging to San Bernardino shooter", L.A. Times 2016.2.17., https://www.latimes.com/local/lanow/la-me-ln-fbi-apple-san-bernardino-phone-20160216-story.html (2019년 10월 23일 최종접속).

253) "Why even the FBI can't hack the iPhone", The Washington Post 2016.2.17., https://www.washingtonpost.com/news/wonk/wp/2016/02/17/how-long-it-takes-to-crack-an-iphone/ (2019년 10월 23일 최종접속).

254) 미국 캘리포니아주 샌 버나디노의 발달장애인 복지·재활시설인 인랜드 리저널 센터에서 사예드 리즈완 파루크(Syed Rizwan Farook)와 타슈핀 말리크(Tashfeen Malik)가 총기를 난사해 14명을 숨지게 했으며, 범행 후 도주하다가 경찰에게 사살되었다.

255) '백도어(Backdoor)'란 정상적인 인증절차를 우회하여 시스템에 접근할 수 있도록 하는 프로그램을 말한다. "[카드뉴스] 왕초보를 위한 용어 풀이, 백도어란?", 보안뉴스 2017년 12월 13일자, https://www.boannews.com/media/view.asp?idx=58568 (2019년 10월 23일 최종접속).

256) "Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman", The New York Times 2016.2.16., https://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html (2019년 10월 23일 최종접속).

257) "'Too dangerous': Apple blasts court order over San Bernardino shooter's iPhone", RT News 2016.2.17., https://www.rt.com/usa/332707-judge-orders-apple-unlock-iphone/ (2019년 10월 23일 최종접속).

지원해달라고 요청한 사건에서 2016년 2월 29일 뉴욕 주 브루클린(Brooklyn) 연방지방법원은 애플이 그 요청에 응하지 않아도 된다고 판단했다.[258] 제임스 오렌스타인(James Orenstein) 판사는 이 판결을 통해서 당국이 잠금장치 해제 지원을 요청하는 것은 기업에게 지나친 부담을 지우는 것인바, 기술의 발전 현황을 고려해서 안보와 개인정보 보호 간에 균형점을 어떻게 설정할 것인지는 향후 의회에서 다루어져야 할 문제라고 밝혔다.[259] 용의자의 범죄 유형을 고려하지 않고 두 사건을 평면적으로 비교하는 것은 적절하지 않을 수 있다. 그럼에도 불구하고 연방수사국이 애플을 상대로 범죄 용의자의 아이폰 잠금장치 해제 지원을 요청했다는 점에서는 동일한 두 사건에서 상반된 입장의 판결이 내려지면서 이후 상급심 법원의 논리 전개에 이목이 집중되었다. 2016년 3월 28일에 연방수사국이 아이폰 잠금장치를 성공적으로 해제하면서 애플을 상대로 제기한 소송을 취하하였고, 이에 양측 간의 법적 공방은 일단락되었다. 그러나 프라이버시 보호를 위한 기술적 조치를 두고 벌어지는 수사당국과 기업의 갈등 양상은 언제라도 재현될 것이다.

2) 다크넷 수사

우리가 일상적으로 마주하는 인터넷 세상은 빙산의 일각에 불과하다. 구글이나 네이버와 같은 검색엔진을 통해서 찾을 수 있는 '서피스웹(Surface Web)'과 달리 일반적인 검색엔진을 이용해서는 접근하기 어려운 엄청난 규모의 '딥웹(Deep Web)'이 존재하는데, 딥웹에는 개인의 이메일이나 의료 기록, 기업의 내부망이나 넷플릭스와 같이 유료화 장벽에 의해 막혀 있는 방대한 양의 콘텐츠 등이 있다.[260] 딥웹에 포함되면서도 구분되는 개념으로서 '다크넷(Dark Net)'[261]이 있는데, 이는 표준화되지 않은

---

258) "Apple Wins Ruling in New York iPhone Hacking Order", The New York Times 2016.2.29., https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html (2019년 10월 23일 최종접속).

259) "Magistrate Judge James Orenstein's Order", The New York Times 2016.2.29., https://www.nytimes.com/interactive/2016/02/29/technology/document-Orenstein-Order.html (2019년 10월 23일 최종접속).

260) 나유진, "딥웹으로 퍼져나가는 네덜란드 대마초", Barun ICT newsletter, 연세대학교 바른ICT연구소, 2019.11., 8면; Robert Koch, "Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?", 2019 11th International Conference on Cyber Conflict (CyCon), IEEE(Institute of Electrical and Electronics Engineers), 2019.5.28-31, p.3; "What is Dark Web?", IP Location 2018.8.28., https://www.iplocation.net/dark-web (2019년 10월 23일 최종접속).

프로토콜과 포트를 사용하는 것으로서 특정 소프트웨어나 네트워크의 허가 또는 설정이 있어야만 접근할 수 있는 가상의 네트워크이다. 다크넷 중에서도 웹(Web)만을 일컬어 '다크웹(Dark Web)'이라고 부른다. 그리고 앞서 살펴보았던 토르(TOR)는 가장 유명하고 많이 사용되고 있는 다크넷이다.[262]

강력한 익명성 보장을 특징으로 하는 다크넷은 첩보 작전 등의 군사활동이나 내부고발 등에 이용될 수 있다. 그러나 현재 다크넷은 마약이나 총기 등 불법제품의 거래, 아동 성착취 영상이나 불법 또는 위조 소프트웨어 등의 공유, 테러모의나 살인청부 등이 이루어지는 범죄의 온상이 되고 있다. 이러한 다크넷의 실상은 2013년 미국의 연방수사국이 마약 암거래 웹사이트인 '실크로드(Silk Road)'를 수사하면서 널리 알려졌다.[263][264]

2017년에는 독일 연방형사청(Bundeskriminalamt, BKA)이 이용자 수나 상품거래의 규모 면에서 전 세계 상위 세 손가락 안에 들던 '한자마켓(Hansa Market)'에 대한 대대적인 수사를 하였는데, 해당 사이트에서는 인신매매, 마약, 신용카드 데이터, 신분증 위조 및 불법총기 등 무기와 아동음란물 등 약 40,000종 이상의 불법 상품 및 범죄 서비스가 제공되고 있었다.[265] 한편 우리나라에서도 2018년 아동 성착취 영상물

---

261) 다크넷은 1970년대 보안을 목적으로 아르파넷에서 분리하여 정부 기반의 군사 및 의료 네트워크를 운영하기 위해 만들어졌다. 정태진/이광민, 앞의 글, 216-217면.

262) 그 이외에도 I2P(Invisible Internet Project), 프리넷(Freenet), 지엔유넷(GNUnet), 아노넷(anoNet), 레트로쉐어(RetroShare), 라이플(Riffle), 원스웜(OneSwarm) 등이 있다.

263) "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website", FBI 2013.10.25., https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (2019년 10월 23일 최종접속).

264) 실크로드는 마약, 무기, 위조문서나 위조지폐의 매매·사용, 살인청부, 아동 포르노그라피, 불법 소프트웨어 및 기타 저작권 자료, 악성 소프트웨어, 컴퓨터 해킹도구 등을 익명의 구매자와 판매자가 교환하는 밀거래 시장으로, 운영자인 로스 윌리엄 울브리히트(Ross William Ulbricht)는 2013년 부하직원에 대한 살인 청부를 시도 중 FBI 잠입수사관에 체포되었다. 미국 뉴욕시 남부지방법원은 2015년 5월 해킹, 밀거래, 돈세탁 및 마약 판매와 불법 수익 사업 혐의로 울브리히트에게 종신형을 선고하였다. "Silk Road operator Ross Ulbricht sentenced to life in prison", The Guardian 2015.5.29., https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced (2019년 10월 23일 최종접속).

265) 2017년 7월 기준으로 약 420,000명의 이용자와 1,600여개의 공급 업체 및 30,000여명의 구매자가 파악되었다고 한다. Christian Rückert, "Erlanger Cybercrime Tag 2018: Darknet und Underground Economy", KriPoZ 4/2018, 2018, S.250 참조.

을 거래하는 다크웹 사이트인 '웰컴 투 비디오(W2V)'에 대한 수사가 진행되었다. 한국, 미국, 영국 등 32개국이 공조했던 수사를 통해서 세계 최대 규모의 아동음란물 사이트 운영자가 한국인이라는 사실이 드러났고, 지난 2019년 10월 미국 법무부가 이 사건에 대한 최종 수사결과를 발표하면서 검거된 337명의 이용자 중 223명이 한국인이라고 밝히면서 사회적 파장이 일고 있다.[266]

그러나 상기의 사건들은 관련자들의 실수에 기인하여 범죄자를 특정해서 추적할 수 있었던 매우 이례적인 사례이며, 암호화·익명화라는 다크넷의 기술적 특징으로 인해 웹사이트 운영자나 이용자를 찾아내기란 불가능에 가깝다. 이로 인해 중국이나 러시아 등 권위주의 국가에서는 다크넷 접속을 금지하고 있으나, 다크넷이 범죄에 악용된다고 해서 접속 자체를 막을 수는 없는 노릇이다. 다크넷 상에서 벌어지고 있는 범죄에 대응하는 것은 오늘날 전 세계 수사기관이 직면한 과제인바, 우리나라도 잠입수사나 온라인 수색 등의 도입을 전향적으로 검토할 필요가 있다.

---

266) Department of Justice, Office of Public Affairs, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin", Justice News 2019.10.16., https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child (2019년 10월 23일 최종접속).

사물인터넷(IoT)

윤지영·이병욱

제3장

사물인터넷(IoT)

제1절 | 사물인터넷(IoT)의 기술적 이해와 특징

1. 사물인터넷의 기술적 이해

가. 사물인터넷의 등장 배경

1946년 2월, 펜실베니아 대학에 등장한 전자식 컴퓨터인 ENIAC은 높이가 2.5m였으며 길이는 25m, 무게는 무려 30여톤에 달했다. 이 넓은 공간에 배치된 진공관 개수는 고작 18,000여 개 불과했고 당시에 처리할 수 있는 데이터는 고작 300개 정도의 정수가 전부였다.[267] 과거에는 연산능력을 가진 컴퓨터를 구성하는 것은 엄청난 비용은 물론, 상당한 공간이 있어야만 가능한 일이었다. 그러나 인류가 반도체와 이를 이용한 트랜지스터를 개발하고 나서는 상황이 크게 달라졌다. 현재 가장 보편적으로 사용하고 있는 것은 금속 산화물 반도체전계 트랜지스터(MOSFET)인데, 이는 1959년에 미국 벨 연구소에서 모하메드 아탈라(Mohamed Atalla)와 우리나라의 강대원 박사가 세계 최초로 개발한 것이다. MOSFET은 진공관보다 훨씬 싸고 작지만, 더 뛰어난 기능을 제공해 주었다. 더 적은 공간에 더 적은 비용으로 트랜지스터를 집적하는 것이 가능해지자, 연산능력을 가진 컴퓨터를 구성하는데 필요한 요구조건도 크게 바뀌었다. 비용과 공간상의 제약이 사라지면서 전용 컴퓨터는 물론, 그렇지 않은 다른 장비에도 연산이나 데이터 처리 기능을 추가하는 것이 보편화 된 것이다. 이에 따라

267) "세계 첫 전자식 컴퓨터 '애니악' 탄생 60주년", 전자신문 2006년 2월 15일자, http://www.etnews.com/200602140150?m=1 (2019년 11월 4일 최종접속) 참조.

다양한 형태의 장비들에 여러 기능이 추가되면서 자동차, 가전 등에까지 데이터 처리와 연산 기능을 비교적 용이하게 추가할 수 있게 되었다.

현대의 반도체 기술은 한발 더 나아가 트랜지스터의 크기를 적혈구의 1/5 이하로 줄였다. 2019년 현재, 트랜지스터의 집적 기술은 10나노미터 미만의 크기에 도전하고 있으며, 이제 더 이상 뉴턴 물리학이 통하지 않는 소위 양자 역학의 세계로 한발 더 다가서고 있다.[268] 이러한 기술의 발전은 개인용 노트북에 10억개 이상의 트랜지스터가 손쉽게 탑재될 수 있을 정도로 놀라운 집적도를 성취했고, 작은 공간에도 대규모 연산장치를 충분히 장착할 수 있을 정도로 소형화 되었다. 또 이를 구현하기 위한 비용 역시 충분히 저렴해졌다.

한편, 통신을 위해 필수적인 주소체계에서도 획기적인 확장이 있었다. 근거리나 동일 네트워크 내의 통신의 주류는 MAC 주소나, RFID의 Tag 등을 통해 이루어진다. 이러한 기기들이 외부 인터넷과 연결되기 위해서는 독자적인 IP 주소를 가지거나 NAT[269] 기능을 갖춘 게이트웨이에 의존해야 한다. 과거 IPv4 체계의 IP 주소로는 2^{32}개 즉, 고작 43억개 정도의 주소 개수만 가능했기 때문에 기하급수적으로 늘어나는 각 통신 기기에 별도의 IP를 부여한다는 것이 불가능했다. 이 때문에 IPv4를 사설 IP와 공인 IP로 그 체계를 나누고, 사설 IP에 포트번호를 사용하여 기기에 부여하는 등 편법과 고육지책으로 부족한 IP 주소를 극복해 왔었다. 그러나 IPv4 체계로는 더 이상 감당할 수 없을 정도로 빠르게 '통신이 가능한' 기기가 급증하고 있다.

또한 새로운 주소 체계인 IPv6가 1988년에 제안되었고, 이는 2000년 중반부터 본격적으로 보급되기 시작하였는데, 구글에 따르면 2019년 현재 구글에 접속하는 기기의 약 30% 정도가 IPv6를 사용하고 있다.[270] IPv6는 모두 2^{128}개의 주소를 공급할 수 있으며, 이는 지구상의 모든 해변에 존재하는 모래알 개수를 제곱한 수보다도 훨씬 더 많은 개수다. 따라서 이론적으로는 지구상에 존재하는 모든 사물에 개별적으로 고유한 IP 주소를 하나씩 할당하더라도 넉넉히 남을 정도의 주소공간체계가 마련된 셈이다. 이는 향후 IoT가 통신을 하는 데에 필요한 식별이나 주소체계 등의 기본

268) IEEE, Spectrum, https://spectrum.ieee.org/nanoclast/semiconductors/devices/onenanometer-gate-dimensions-for-transistors-have-been-achieved (2019년 11월 4일 최종접속) 참조.
269) Network Address Translation. 사설 IP를 공인 IP로 매핑해주는 역할을 한다.
270) Google IPv6, https://www.google.com/intl/en/ipv6/statistics.html (2019년 11월 4일 최종접속) 참조.

요소가 모두 구축되었다는 것을 의미한다.

이렇듯 트랜지스터의 혁명과 IP 주소체계의 혁신으로 인해, 각 기계는 소형화와 함께 서로 독자적으로 통신망을 구성할 수 있는 충분한 환경이 조성되었고, 경제적 측면에서나 기술적 측면 모두에서, 명실상부하게 사물인터넷의 세상이 열릴 수 있는 발판이 마련되었다. 사물인터넷이란 과연 무엇인가? 사물인터넷이란 단어는 1999년 처음 언급된 이래 지속적으로 그 정의와 개념이 발전해 왔으며, 지금도 그 정의는 조금씩 발전해 나가고 있다. 따라서 사물인터넷을 정확히 이해하기 위해서는 현재의 여러 정의를 단순히 나열하거나 그 중 하나만을 따르기 보다는, 어떠한 속성이 이러한 새로운 용어를 필요로 했는지에 대한 배경과 함께 기본적으로 어떤 속성을 갖춰야 사물인터넷이라 부를 수 있는지에 대한 이해가 필요하다.

나. 사물인터넷의 정의

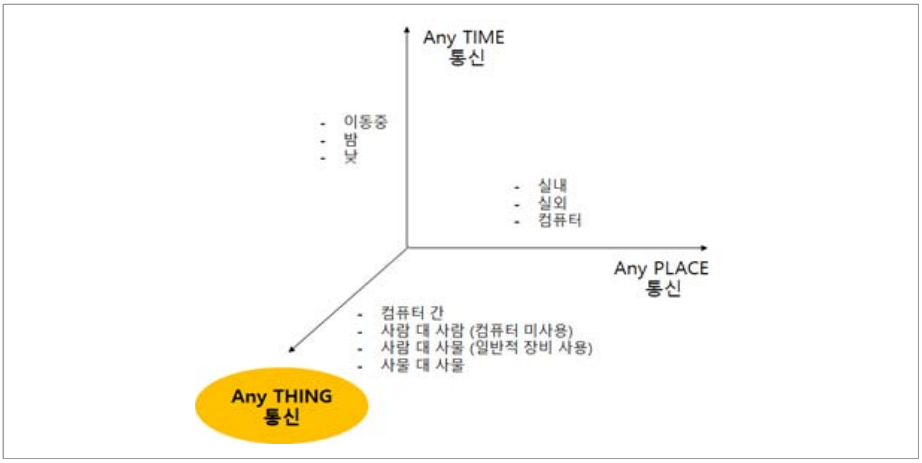
IoT 즉, 사물인터넷(Internet of Thing)이라는 용어를 제일 먼저 사용한 사람은 MIT Auto-ID 센터의 공동 창업자인 케빈 애쉬턴(Kevin Ashton)으로 알려져 있다. 그는 1999년에 자신이 연구 중이던 RFID를 P&G 고위 관리자들에게 설명하는 도중에 이 말을 처음으로 언급했다고 한다.[271] 같은 시기 MIT 교수인 닐 거쉔펠드(Neil Gershenfeld) 역시 그의 저서 “사물이 생각하기 시작할 때(When Things Start to Think)”에서 “생각하는 사물(Things That Think)”이라는 용어로 유사한 내용과 맥락을 언급했지만, 정확히 IoT라는 용어를 쓰지는 않았다.[272] 그로부터 20년이 흐르는 사이, IoT가 무엇인지에 대한 정의는 계속하여 진화돼 왔으며, 많은 사람들이 다양한 방식으로 IoT를 설명하고 정의해 왔다.

UN 전문기구이자 국가 간 정보통신기술 문제를 관장하는 ITU(International Telecommunication Union)에서는 ITU-T Y.2060 문서에서 IoT에 대한 개념을 명확히 기술함과 동시에 그 범위와 핵심 특성, 상위레벨에서의 요구사항 등에 대해 설명하고 있다.[273]

---

271) TechTarget 웹페이지, https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (2019년 11월 4일 최종접속) 참조.
272) Neil Gershenfeld, When things start to think, Henry Holt and Company Inc., 1999, p.199.
273) ITU-T Y.2060, Overview of the Internet of Things, 2012.6, p.1.

[그림 3-1] IoT가 도입한 새로운 차원[274]



[그림 3-1]은 ITU의 문서에서 IoT가 창출한 새로운 통신 차원을 설명한 그림이다. 1988년 제록스의 마크 와이저(Mark Weiser)가 처음 사용했던 유비쿼터스(ubiquitous) 통신의 개념[275]이 주로 시공간에서의 자유로움을 의미했다면, IoT가 포함된 유비쿼터스의 개념은 통신의 주체에 대한 자유로움까지 추가된 새로운 차원으로 해석할 수 있다는 점이 그림에서 강조되고 있다. ITU-T Y.2060 문서에서는 사물에 '디바이스(device)'가 결합돼 기능이 부여되면 IoT가 되는데, 디바이스는 그 필수조건으로 '통신기능'을 갖추어야 하고 부가조건으로 다양한 센서, 데이터 저장, 처리 장치 등을 가진다고 설명하고 있으므로, ITU 문서에 따른 IoT가 되기 위한 최소 요구조건은 '통신기능'으로 볼 수 있다.[276] 그러나 몇 년간 베란다에 방치된 자전거에 어느 날 네트워크 인터페이스 카드만 설치한다고 해서 이를 IoT 기기라고 부를 수 있을까? 사물이 IoT의 형태적인 최소 요구사항을 갖추었더라도 그 자체만으로는 IoT라 할 수 없고, 기능상으로 어떤 역할이 주어지고, 이를 적절히 수행하여 데이터 흐름상에서 일정 이상 기여를 할 때 비로소 IoT라고 분류하는 것이 더 옳을 것이다. 계속해서 ITU-T Y.2060 문서에서 설명하고 있는 최소 요구조건 위에서, IoT가 갖출 수 있는 추가적인 기능으로

274) 이미지 출처: ITU-T Y.2060, p.3 참조.
275) 한국정보통신기술협회 정보통신용어사전, '유비쿼터스 컴퓨팅, ubiquitous computing' 검색결과, http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=058903-1 (2019년 11월 4일 최종접속) 참조.
276) ITU-T Y.2060, p.4.

제시한 10가지[277]를 통해 IoT란 어떤 성질과 기능을 가진 것인지, 그리고 어떠한 잠재적 취약점을 가지고 있는지에 대해 좀 더 구체적으로 알아보자.

① 식별에 기반한 연결
사물과 IoT간의 연결은 사물의 식별자에 기반해 이루어져야 하며, 서로 이질적인 식별절차에 대해서도 통일된 방법으로 이루어져야 한다.[278]

② 상호운영성
여러 이질적이고 분산된 시스템에서 다양한 정보의 생산과 소비를 위한 상호운영성이 보장되어야 한다.

③ 자동 네트워킹
IoT는 서로 다른 응용 분야, 통신 환경, 다양한 유형의 장치에 적응하기 위해 자동적으로 네트워킹이 가능해야 한다. 여기에는 자가-관리, 자가-설정, 자가-최적화, 자가-보호, 자가-치료 등의 기능이 포함된다.

④ 자동 서비스 제공
IoT 장치는 그 설정된 규칙에 따라 데이터를 포착하고, 통신하고, 처리할 수 있어야 한다.

⑤ 위치기반 능력
IoT 기기는 자동으로 지리 정보를 감지하여 위치에 기반한 서비스를 제공할 수 있어야 한다. 위치에 기반한 서비스는 관계 법령과 규정에 의해 제약될 수 있으며 관련 법규를 따라야 한다.

⑥ 보안
모든 IoT 기기들은 데이터와 서비스 모두에 대한 기밀성, 인증, 무결성에 대한 심각한 위협이 될 수 있다. 다양한 기기들 간에 서로 다른 보안 요구조건이 있을 때 이를 통합할 수 있는 방법이 제공되어야 한다.

⑦ 프라이버시 보호
많은 사물에는 그 소유자와 이용자가 있다. 수집된 데이터에는 소유자와 이용자에 대한 프라이버시 정보가 포함될 수 있으므로 데이터 전송, 수집, 저장, 마이닝과 처리 단계에 있어 프라이버시를 보호해야 한다.

⑧ 고품질 고보안의 인체관련 서비스
인체관련 서비스란 사람의 정적인 특징이나 동적인 행동에 대한 데이터를 사람의 개입에 상관없이 수집하고, 통신하고, 처리하는 서비스를 의미한다. 이러한 서비스에는 각 국의 관계 법령이 상이할 수 있으므로, 유관 법규를 잘 준수해야 한다.

⑨ 플러그 앤 플레이
사물이 상호 연결될 때, 문맥에 기반하여 중단 없는 통합과 협업 서비스를 제공하기 위해서는 플러그 앤 플레이 기능이 지원되어야 한다.

⑩ 관리가능성
IoT 응용은 대부분의 시간 동안 사람의 개입 없이 자동으로 작동하지만 전체 운영 프로세스는 관련자에 의해 관리 가능해야 한다.

277) ITU-T Y2060, pp.5-6 참조.
278) 현재 사물의 식별에는 주로 RFID 기술이 다양하게 적용되어 사용되고 있고 주로 수동적인 식별이라는 기능에 국한된다. 이러한 식별은 기기 간에 서로 구분하여 특정하는 것이 가능하다는 의미이며, 이는 통신을 하기 위한 최소요건이기도 하다.

ITU가 제시한 이 10가지 특성을 잘 살펴보면 향후 IoT가 어떤 방향으로 발전해 나갈 것인지와, 보안과 프라이버시 관점에서 어떤 종류의 문제점이 야기될 수 있는지에 대한 여러 정보를 동시에 얻을 수 있다.

ITU의 정의를 요약하자면, IoT란 사물이 장치(device)와 합쳐진 것으로서, 여기서 장치라 함은 통신기능을 필수요소를 갖추고, 선택적으로 센서(Sensor)와 액츄에이터(Actuator)[279], 그리고 데이터 처리를 위한 컨트롤러의 기능을 가지고 있으며, ③번과 ⑩번 항목에서는 특히 사람의 개입 없이도 자율적으로 작동할 수 있어야 한다는 점이 강조되고 있다. 그러나 이 항목들은 IoT 기기의 '바람직한 구현방법'을 위한 지침서 정도로 생각할 수 있지만 IoT의 최소요건이나 IoT의 정의와는 다르다.

한편, 1995년부터 다양한 장치를 인터넷에 연결해 온 창조적 IoT 사업가인 아드리안 맥이웬(Adrian McEwen)은 공저인 "IoT 디자인하기(Designing the Internet of Things)"에서 IoT를 다음과 같은 수식으로 간결하고도 쉽게 표현했다.[280]

IoT = 물리적인 사물 + 컨트롤러, 센서, 액츄에이터 + 인터넷

이 표현식은 물리적인 사물에 어떤 기능이 추가되어야 IoT라 부를 수 있는지 설명하고 있는데, 핵심적으로 통신기능이 반드시 필요하며(인터넷), 컨트롤러, 센서, 액츄에이터 기능 중 하나 또는 그들의 조합으로 결합되면 된다고 설명한다.[281] 이 표현식은 앞서 IoT를 사물과 장치의 결합으로 설명한 ITU-T Y.2060 문서와도 대체로 잘 부합한다. 이 식과 ITU의 문서에서 공통적으로 사물이라고 특히 명시하는 이유는, IoT란 이미 존재하는 객체에 기능을 부가하는 것이며, 이전에 없던 객체를 새로이 생성하는 것은 아니라는 점을 강조하기 위해서이다. 이 점은 뒤에서 다시 자세히 살펴보기로 하자.

---

279) 액츄에이터는 정교한 컨트롤이 가능한 구동장치 정도로 생각하면 된다. 회전 빠르기 외에 회전 각도는 조절할 수 없는 일반 모터와 달리, 액추에이터는 정교한 회전과 운동이 가능하다.

280) Adrian McEwen/Hakim Cassimally, Designing the Internet of Things, Wiley Publishing, 2013, p.11.

281) 사실 책에는 표현식 중 컨트롤러의 역할이나 존재가 다소 모호하게 기술돼 있다. 식의 '인터넷' 항에 통신 처리에 필요한 컨트롤러가 포함된다고 해석하면, IoT = 물리적인 사물 + 인터넷 + (컨트롤러, 센서, 액츄에이터)로 표현할 수 있고 이 표현식이 ITU의 정의에 더 부합해 보인다. 여기서 ( )의 의미는 존재할 수도 있고 하지 않아도 된다는 뜻이다.

한편, 인공지능 기술의 부각과 함께 IoT에 대한 최근의 정의에는 '사람이 개입되지 않는 점'이 많이 부각되기도 한다. 실제로 많은 경우에 IoT가 사람의 개입을 필요로 하지 않는 상태에서도 작동한 것이 사실이지만, 그 특성 자체가 IoT의 필수조건이라 보기는 어렵다. 따라서 본 연구에서 정의하는 IoT에는 자율적 기능을 그 필수특성에 포함시키지 않는다. 그러나 실효적 측면으로 놓고 본다면 향후 대부분의 IoT는 사람의 개입이 없이 스스로 작동할 수 있는 방향으로 제작되어 발전해 나갈 것임은 자명하다.

모든 IoT가 일률적으로 고도의 마이크로 컨트롤러와 다양한 센서를 모두 장착해야 할 필요는 없다. 즉, 고도의 프로세서 없이도 단순히 주변을 인식(센서)하고 이를 전달하거나, 심지어 센서가 없어 독립적으로 데이터를 생산하지 못하더라도 통신기능을 갖추고 일정 역할을 한다면 IoT라 할 수 있는 것이다. 이는 모든 IoT 기기가 일률적으로 고도의 마이크로 컨트롤러를 탑재해 독립적인 컴퓨터처럼 진화하지는 않을 것이라는 의미이기도 하다. 예컨대 자동차 열쇠에 별도의 고성능 마이크로 컨트롤러를 탑재하는 대신, 컨트롤러가 이미 탑재돼 있는 자동차 등의 주변 IoT 기기들과 통신하고 협업하여 소기의 목적을 달성하도록 구성하는 것이 훨씬 더 효율적일 것이다.

> 마이크로 프로세서는 통상 연산 장치를 하는 반도체 칩을 의미하고 마이크로 프로세서에 기본적인 입출력 및 저장 장치 등의 기타 장치까지 포함시킨 것을 마이크로 컨트롤러라고 부른다. 마이크로 컨트롤러는 범용 컴퓨터의 축소판으로 생각할 수 있다. 기술의 발달로 인해 점점 더 많은 IoT 기기들이 마이크로 컨트롤러를 장착하게 되어, 별도의 중앙통제 장치 없이도 자율적인 작동을 하게 될 것이다.

이제, IoT에 대한 여러 정의들을 종합해 보면, IoT에 대한 윤곽을 다음과 같이 정리할 수 있다.

- "IoT"란 사물에 통신기능을 추가한 것으로서, 다음의 세 가지 특성을 가지며, 그 밖의 여러 부가적인 기능으로 확장할 수 있다.
- 사물이다.
- 주변을 인식(센서)하고 스스로 통제(컨트롤러) 또는 구동(액츄에이터)할 수 있는 능력을 가진다.
- 통신할 수 있는 능력을 가지고 있다.

1) 사물이다

"사물이다"라는 특징은 얼핏 당연한 이야기처럼 들리지만, 이 말에는 나름의 의미가 내포돼 있다. 이 말에는 IoT는 이미 존재하는 사물에 기능을 추가하는 것을 의미하는 것이며, 기능의 추가로 인해 존재하는 사물의 용도를 바꾸거나, 존재하지 않던 객체를 새로이 생성하는 것이 아니라는 점이 강조되고 있다. 이는 또한 범용 컴퓨터처럼 연산만을 위한 사물을 특별히 제조하는 것이 아니라는 측면도 포함된다. 따라서 "사물이다"라는 문장이 의미하는 것은 열쇠, 탁자, 냉장고, 세탁기, 청소기 등의 사물이 그 본래의 목적과 기능 및 형태를 그대로 유지해야 하며, IoT가 되기 위한 기능의 추가로 인해 본연의 목적이나 형태가 방해받거나 훼손돼서는 안 된다는 뜻이다. 한편, 앞서 잠시 언급한, ITU-T Y.2060의 문서에서는 이 사물의 개념을 실생활에서의 실물은 물론, 정보 세계에서의 가상의 물체까지로 확대시켜 포함하고 있다.[282]

2) 주변을 인식하고, 스스로 통제하며 구동할 수 있다

센서의 역할은 주위환경으로부터 여러 정보를 감지하는 것이다. 센서는 IoT의 필수 요소에 포함되지 않을 수도 있지만 대부분의 IoT는 센서 혹은 그와 비슷한 장치를 가지고 주변 환경으로부터 유용한 데이터를 직접 생산한다. 센서는 종류에 따라, 영상, 소리, 온도, 위치, 기울기, 거리, 조도, 압력, 습도, 관성, 자기장, 전류, 전압 등 다양한 정보를 수집할 수 있다. 수집된 데이터는 IoT 자체에 보관할 수도 있지만, 대부분 통신을 통해 클라우드 기반의 저장장치에 모은 다음 처리된다.

IoT에는 액츄에이터가 부착될 수 있는데, 이를 통해 스스로 출력을 생성하며, 진동을 전달하거나 움직이거나, 소리를 내거나 빛을 발할 수도 있다. 액츄에이터는 동작을 정교히 조작 가능할 수 있도록 설계된 모터 정도로 개념적으로 생각할 수 있는데, 센서로부터 전달된 정보를 분석하여 사전에 정의된 행동을 수행할 수 있으며 산업 안전에 관련된 IoT 기기에는 핵심 장비가 될 수 있다. 누전시 전원을 차단하거나 가스 누출 시 밸브를 돌려 잠그고, 위험을 감지하면 모터 진동을 통해 경고하는 햅틱(Heptic) 동작 등의 여러 출력을 전달하는 것이 주요예시가 될 수 있다.

282) ITU-T Y.2060, p.3.

컨트롤러는 추가된 장비를 제어하고, 장비가 취득한 데이터를 처리하는 역할을 한다. 컨트롤러는 단순한 장비제어에서부터 복잡한 연산처리 기능을 가진 범용 장치에 이르기까지 매우 다양한 형태로 구현될 수 있다. 자율기능과 인공지능 기능을 위해서는 이 컨트롤러 역할이 핵심이 된다.

3) 통신할 수 있는 능력을 가지고 있다

통신은 IoT의 필수 기능이다. 모든 IoT는 스스로 데이터를 생산하는 능력을 가졌는가의 여부와 상관없이, 주변의 다른 장치와 통신을 할 수 있어야 한다. 통신 기능을 갖추지 않은 어떠한 장치도 IoT로 분류되지 않는다. 따라서 이 기능은 IoT로 분류되기 위한 최소 기준이자, 필수 기준이라고 할 수 있다. 통신 능력은 다양한 방식으로 구현될 수 있다. 주변의 통제 센터에 의존하는 경우에는 RFID 등의 단순한 체계로도 구현이 가능하지만, 자율적으로 스스로 통제하고 통신하는 상황을 위해서는 IPv6 체계를 사용하여, 탄력적으로 구성할 수 있다. 앞서 설명한 것처럼, IPv6 주소 체계를 사용하면, 이론적으로 모든 사물에 고유한 하나의 IP 주소를 할당할 수 있다.

일반적으로 IoT는 생산하는 모든 데이터를 클라우드에 저장한다. 따라서, 데이터를 생산하는 단계, 전송하는 단계, 저장한 단계 각각에서 데이터 침해에 대한 취약점이 존재하며, 이 취약점에 대한 위협을 적절히 통제해야만 프라이버시 보호 등을 적절히 수행할 수 있다.

2. 사물인터넷의 특징

가. 사물인터넷의 응용분야

사물인터넷의 응용분야는 무한하다. 존재하는 사물에 일정 기능을 부가하면 사물인터넷으로 만들 수 있기 때문이다. 그 중에서도 우선적으로 연구가 활발히 일어나고 있는 분야는 존재한다. 윌리엄 스탈링스(William Stallings)는 그의 저서 “현대 네트워크의 기초 이론(Foundations of Modern Networking)”에서 비첨(beechem) 리포트를 인용하여 그 응용분야를 개략적으로 다음과 같은 표로 정리해 두고 있는데, 이를 참고해 볼 만한다.

[표 3-1] 사물인터넷 응용분야[283]

서비스영역	응용 그룹	위치	장치 예시
IT 및 네트워크	공용	서비스, 전자상거래, 데이터 센터	서버, 스토리지, PC, 라우터, 스위치, PBX
	엔터프라이즈	IT/데이터 센터, 사무실, 사설 네트워크	
보안/공공안전	감시장비, 추적	레이더/위성, 군사용 보안, 무인 장비, 무기, 자동차	탱크, 전투기, 전장 통신, 지프
	공공 인프라	사람, 동물, 우편물, 수하물, 음식, 하수처리, 빌딩환경	자동차, 갓길 노동자, 국토보안, 화재, 환경 모니터링
	응급 서비스	장비와 직원, 소방, 단속기관	앰뷸런스, 공공경비 차량
소매	특수제품	주유소, 오락실, 볼링장, 영화관, 특별 이벤트	POS 단말기, 태그, 현금 출납기, 자판기
	접객업	호텔, 레스토랑, 바, 카페	
	상점	슈퍼마켓, 쇼핑센터	
운송	비차량	항공, 철도, 해상	자동차, 가로등, 배, 비행기, 요금소
	차량	개인용, 상업용, 건설 등	
	대중교통 시스템	요금소, 교통량 관리, 내비게이션	
산업	유통	파이프라인, 재로처리, 수송	펌프, 밸브, 통, 컨베이어, 파이프 라인, 모터, 변환, 선박, 탱크
	변환, 개별부품	금속, 종이, 고무, 플라스틱, 전자제품 조립	
	유체/프로세스	석유화학, 탄화수소, 음식, 음료	
	자원 자동화	채굴, 관개, 농업, 삼림	
헬스케어 및 생명과학	보건	병원, 응급실, 클리닉, 실험실, 진료실	MRI, PDA, 임플란트, 외과 수술 장비, 펌프, 모니터, 원격 의료
	생체, 홈	임플란트, 홈 모니터링	
	연구	신약 개발, 진단, 실험실	
소비자 및 가정	인프라	배선, 네트워크, 에너지 관리	디지털 카메라, 전력 시스템, 식기 세척기, 컴퓨터, 세탁기/건조기, 전등, TV, 조명
	안전	보안/경보, 소방, 환경 안전, 경로, 아동, 전력보호	
	편의 및 엔터테인먼트	HVAC/기후, 조명, 가전, 엔터테인먼트	
에너지	공급/수요	발전, 송배전, 에너지 관리	터빈, 풍차, UPS, 배터리, 발전기, 계량기, 드릴, 연료전지
	대체 에너지	태양열, 풍력, 열병합, 전기화학	
	석유/가스	굴착기, 기중기, 갱구, 펌프	
빌딩	상업, 교육	사무실, 학교, 소매점, 점객업	HVAC[284], 운송, 화재 안전, 조명, 보안, 접근성
	산업	무균실, 캠퍼스	

283) 윌리엄 스탈링스(강지양/남기혁 역), 현대 네트워크 기초이론: SDN, NFV, QoE, IoT, 클라우드, 에이콘출판사, 2016, 462-463면 참조.

284) HVAC = Heating, Ventilation and Air Conditioning

[표 3-1]을 살펴보면, 우리 일상의 거의 모든 접점에서 IoT 기기가 특정 역할을 하고 있으며, 그 영역은 빠르게 확대될 것이라 예상할 수 있다. 칩의 크기가 더욱 소형화되고, 구현 가격이 저렴해 질수록 더 많은 사물이 IoT화 되고 기능적인 측면도 더욱 강화될 것이다. 궁극적으로 주변의 거의 모든 사물이 스스로 자료를 수집하며 데이터를 생산하고 이를 저장장소에 축적하는 상황이 보편화 될 것이다.

나. 사물인터넷의 위협

지금까지, 사물인터넷을 정확히 규정하는 과정을 통해 기능면에서는 어떠한 능력을 갖춘 장치인지, 그리고 어떤 분야에서 활발히 적용되고 있는지 개략적으로 살펴보았다. 사물이 방대한 데이터를 생산하고 축적하여 유용한 정보를 끊임없이 생산하면 우리의 삶의 질을 한층 높이는데 도움을 줄 수 있다는 점은 분명해 보인다. 그러나 다른 한편으로는 사물이 주변 상황에 대한 데이터를 끊임없이 생산하는 능력을 갖추게 되면서, 그와 동시에 IoT는 잠재적으로 큰 위험요소가 될 수 있는 가능성도 점점 커지고 있다. 이하에서는 IoT의 발전과 함께 동시에 커져가는 위협요소를 살펴보도록 한다.

앞서 살펴본 사물인터넷의 특징은 통신기능과 함께, 스스로 주변 환경을 감지하는 센서를 (선택적으로) 가졌다는 점이며, 센서의 장착이란 곧 데이터를 생산할 수 있는 능력을 가졌음을 의미한다는 것을 알았다. IoT는 주변의 각종 상황에 대해 끊임없이 데이터를 생산하고, 이는 데이터 처리를 통해 정보로 가공되어 미래의 위협이 될 가능성이 있다. IoT는 스스로 데이터를 생성하고 이를 주변의 다른 장치와 교류할 수 있으므로, 하나의 IoT가 범죄에 개입된다면, 그 유형에 따라 IoT의 소유자, IoT에 대한 침입자, IoT의 제조사, IoT의 판매사 등에 대한 책임소재가 발생할 수 있으며, 동시에 이 IoT와 통신을 통해 연계된 또 다른 모든 장치의 소유자, 침입자, 제조사, 판매사의 책임문제로 파생될 수 있다. IoT가 가진 이러한 위험성은 크게 두 가지로 분류할 수 있는데 첫째는 생산된 데이터에 대한 통제되지 않은 침해이고, 둘째는 IoT 기기의 통제권에 대한 침해이다. 데이터에 대한 침해는 가공을 통해 프라이버시 침해나 기타 정보누출로 이어지는 정보의 생산으로 이어지고, 기기에 대한 통제권

침해는 심각한 물리적 피해로 이어질 수 있다. 바이러스를 통해 제어장치 자체를 공격한 최초의 위협은 2010년 6월 Stuxnet이라 불리는 바이러스가 이라크의 농축 우라늄 제어 시스템을 무력화 시킨 사건이었다.[285] 당시 이라크 제어 시스템은 독일의 지멘스(Siemens) 사가 만든 것이었는데, 바이러스는 지멘스 SCADA[286] 시스템을 공격하여 모터의 동작을 조작해 우라늄 농축 시설의 고장을 일으킨 바 있다. 이와 유사한 공격은 IoT에 대해 광범위하게 발생할 수 있고, 이러한 공격은 IoT 기기가 가지고 있는 제어 통제권한에 따라 심각한 물리적 피해를 유발할 수 있다. 사물인터넷에 대한 이러한 위협은 크게 다음과 같은 네 가지 취약점에 집중되어 발생할 것이다.

1) IoT 기기 자체의 결함

모든 하드웨어와 소프트웨어는 근본적으로 오류가 발생할 수밖에 없다. 모두 사람이 제작하는 것이고, 사람은 실수할 수 있기 때문이다. 이러한 오류는 "근본적 취약점"이 된다. 문제는 이러한 취약점이 발견된 이후부터, 이를 완전히 제거하기 까지는 물리적으로 상당한 시간이 소요된다는 것이다. 기기 자체를 통제하는 제어코드를 담고 있는 소프트웨어는 보통 펌웨어(firmware)라 부르는데, IoT 제조사에서 취약점이 제거된 새로운 펌웨어를 배포하는데 까지도 시간이 소요되지만 이를 다시 기기에 반영하는 것도 오랜 시간이 필요하다. 특히 펌웨어의 업그레이드 절차는 자동화 할 수도 있지만 많은 경우 여전히 사용자의 몫이다. '게으른 사용자'가 펌웨어를 업그레이드 하지 않는다면, 취약점이 노출된 기기는 해커의 주요 목표가 된 상태로 여전히 주변 환경에 대한 데이터를 생산하고 주변 장치를 제어하게 된다. 이렇듯 취약점이 발견되고 이를 완전히 제거할 때 까지 거의 무방비 상태에서 해커들에게 공격당하는 상황을 흔히 제로-데이-공격(zero-day-attack)이라고 한다.

기기 자체의 결함으로 인한 문제는, 통제되지 않은 데이터의 취득, 적절한 제어 실패로 인한 물리적 피해 등 매우 심각하고도 다양한 형태로 나타날 수 있다. 특히, 인공지능 기술을 사용해 자율기능을 장착한 IoT가 가스밸브 제어 등의 물리적 통제를

285) Charles P. Pfleedger/Shari Lawrence Pfleeger/Jonathan Margulies, Security in Computing, 5th Edition, Prentical Hall, 2015, p.368 참조.

286) SCADA는 Supervisory Control And Data Acquisition의 약자로 원격 감시 제어 데이터 수집 시스템을 의미한다.

관할하고 있을 경우, 이 기능의 결함은 잠재적으로 심각한 물리적, 신체적, 재산적 피해로 이어질 수 있다. 앞서 말한 것처럼, 기기 자체의 결함을 완전히 피할 수 있는 방법은 없다. 따라서 기기의 결함을 적절히 통제하기 위한 모니터링과 그에 따른 적절한 대처는 IoT의 안정적 운영을 위해서 필수적인 요인이다.

2) 해킹 또는 악성코드에 의한 침해

IoT에 대한 위협 중 가장 광범위하면서도 파괴적인 것은 해킹이다. IoT가 특히 해킹에 취약한 이유는 개별 IoT 기기 자체의 보안이 상대적으로 약할 수밖에 없기 때문이다. 전통적인 데이터 수집 방식에서는 별도의 컨트롤러를 갖지 않은 주변장치가 단순 센서를 통해 데이터를 수집한 뒤 이를 중앙 서버에 전송하도록 통제 받는다. 아이러니하게도 이러한 더미(dummy) 주변 장치 자체를 직접 해킹하는 것은 거의 불가능하다. 소프트웨어 해킹 공격을 원활히 감행하려면, 공격대상이 마이크로 프로세스 등의 최소한의 장치를 갖춘 지능형 기기여야 하기 때문이다. 따라서 그렇지 않은 기기에 대해서는 직접적인 공격이 아니라, 이를 통제하는 중앙통제 서버를 공격하는 간접적 공격만이 가능하다. 그러나 통상 이러한 중앙통제 장치는 강력한 보안 소프트웨어를 사용해 여러 IoT에 대한 해킹의 위협을 적절히 통제하기 마련이다.

그러나 개별적 IoT가 점점 더 발전하여, 더 많은 기능과 연산 장치, 마이크로 프로세스가 탑재되어 보다 지능적으로 발달하면 상황은 크게 달라진다. 이제 개별 IoT 역시 어느 정도의 지능형 기능을 충분히 갖추게 된 반면, 수많은 개별 기기에 대하여 중앙 서버와 동일한 수준의 보안 소프트웨어를 모두 설치하는 것은 비용문제로 인해 한계에 직면할 수 있다. 따라서 중앙 서버 수준의 보안은 불가능하다.

강력한 보안을 위한 소프트웨어와 하드웨어를 설치하기 위해서는 막대한 비용이 필요하다. 개별 IoT는 이러한 비용을 감당하기 힘든 것은 물론, 계속해서 늘어나는 새로운 공격에 대비해 수많은 IoT 개별 기기를 늘 최신 버전의 소프트웨어로 끊임없이 업데이트 하는 것도 쉽지 않다. 특히, 개인이 소유하고 관리하는 중저가의 IoT 기기의 경우, 강력한 보안 소프트웨어나 하드웨어를 장착하는 비용이 기기 자체의 가격보다 오히려 더 높아, 유지보수 비용이 훨씬 더 커질 수 있으므로 경제적으로도 타당하지 않다. 이런 이유로 인해 상대적으로 성공 가능성이 높은 개별 IoT에 대한 공격시도는

더욱 정교화 될 것이고, 이러한 공격에는 단순히 금전적 이익을 노린 것에서부터, 개인의 사생활 침해는 물론 앞서 이라크의 예처럼, 특정 단체나 국가 간에 상대방의 주요 기간시설을 교란하기 위해 악용될 수도 있다.

한편 IoT 개별 기기에 대한 통제권 침해와 함께 생산된 데이터에 대한 침해 역시 심각하다. IoT의 통제권을 침해당하면 IoT가 생산하는 모든 데이터가 실시간으로 절취될 수 있다. 카메라가 장착된 IoT 기기의 통제권을 침해한 뒤, 타인의 생활을 영상으로 촬영해 절취하는 사건은 이제 빈번히 목격될 정도이다. 그러나 IoT가 수집한 데이터에 대한 침해는 생산단계보다는 주로 데이터가 저장돼 있는 클라우드 저장소에 침입해 데이터를 편취하는 것이 더 심각할 수 있는데, 이에 대한 문제는 뒤에서 다시 자세히 살펴본다.

3) 사용자의 관리상의 문제

IoT 기기의 정상적이고 최적의 작동을 보장하기 위해서는 기기의 최적 작동 환경을 보장할 수 있는 설정을 해주어야 하고, 펌웨어의 변경이 발생할 때마다 이를 적절히 업데이트해야 한다.

기기에 대한 잘못된 설정은 잠재적으로 침해를 방조할 수 있다. 사용자의 잘못된 설정으로 야기될 수 있는 범위는 앞서 설명한 모든 종류의 해킹에 해당되며, 그 외에 기기의 오작동으로 인한 물리적 피해 또한 가능하다. 개인적으로 관리되는 모든 IoT는 궁극적으로 이러한 설정오류의 문제에 노출돼 있다. 이런 종류의 오류는 IoT의 기능이 보다 강화될수록 비례해서 커진다. 설정할 수 있는 자유도가 더 높아지기 때문이다. 이 오류는 전적으로 IoT를 소유하고 관리하는 사람의 책임으로 귀속되는데, 일반적으로 보다 광범위해지고, 보다 심화될 수 있다.

4) 저장장치의 보안

저장장치의 보안은, IoT에서 생산된 데이터가 저장된 공간의 보안을 의미한다. 대개 IoT는 생산한 데이터를 직접 보관하지 않고 통신을 통해 클라우드 저장소로 전송하여 한 곳에서 보관한다. 각 IoT 기기에 방대한 저장소를 두는 것은 비효율성과 보안의 문제가 있어 적절치 않으며, 또한 데이터의 효율적 가공을 위해서는 데이터 일괄

처리 및 보관에 적절한 장소로 옮기는 것이 합리적이기 때문이다.

그러므로 IoT 기기 자체나 전송과정에 있어서 아무런 침해가 발생하지 않았다 하더라도, 최종 저장소의 보안이 침해된다면, IoT 자체의 보안은 무용지물이 된다. 특히, 최종 저장 장소의 침해는, 산재해 있는 다수의 개별 데이터가 서로 결합되어 있어서 보다 강력한 정보유출로 이어질 수 있다. 이렇게 다수의 개별 데이터가 연결되어 생성된 복합 데이터는 우리가 언제 취침하는지, 하루 종일 어디서 어떤 활동을 하였는지 고스란히 드러낼 수 있다. 특히 헬스케어 시계 등의 바이오관련 IoT 장치는 우리의 감정과 건강 상태까지 유추할 수 있다.

협상 테이블에 앉아 긴박한 토론을 이끌고 있는 쌍방을 생각해보자. 이 긴박한 상황에서 손목에 찬 시계 IoT를 통해 상대의 심장박동과 긴장도를 알아내고 카메라에 달린 인공지능 기능을 사용해 얼굴인식으로 심리상태를 고스란히 염탐하는 상황을 생각해 보자. 공상과학 영화에서나 등장할 법한 장면이지만, 이러한 상황은 지금도 가능하며, 가까운 미래에는 보편적인 상황이 될 수도 있다.

한편, 여러 데이터가 복합되어 형성된 정보가 궁극적으로 프라이버시 등을 침해하게 된 경우, 그 개별 데이터가 각각 다른 기기와 다른 소유자가 생산한 것이라면, 귀책 대상이 모호해지고 광범위해 질 수 있다. 복합 데이터를 생산하는데 연루된 IoT 기기들이 매우 많을 경우, 각 IoT 기기의 제작이나 운영에 관련된 모든 사람들이 그 범위에 속할 수 있기 때문이다. 또한, 침해에 연루된 특정 정보의 유출이 데이터의 생산과 통신, 저장 중 어느 단계에서 발생한 것인지 모호할 경우가 발생할 수 있다.

IoT에 대한 해킹은 개별 기기에서 생산된 데이터로부터 원하는 정보를 적절히 조합할 수 있는 효과적인 방법을 얻는 다양한 패턴으로 진화해 나갈 것이다.

제2절 | 사물인터넷으로 인한 범죄 발생 양상의 변화 가능성

1. 사물인터넷과 범죄예방

가. 사물인터넷과 스마트 트랜스폼

1) 제4차 산업혁명 시대의 스마트 트랜스폼

제4차 산업혁명은 현실과 가상을 융합하여 인간의 생활양식을 최적화시킬 것인바, 현실을 데이터화하는 디지털 트랜스폼(Digital Transform)과 데이터를 현실화하는 아날로그 트랜스폼(Analog Transform)이 합쳐진, 이른바 스마트 트랜스폼(Smart Transform)을 통해 구현될 것으로 전망된다.[287] 스마트 트랜스폼은 ① 데이터화, ② 정보화, ③ 지능화, ④ 스마트화라는 4단계 선순환 구조로 이루어진다.[288] 우선 데이터화 단계에서는 사물인터넷(IoT)이나 위치기반서비스(Location Based Service, LBS), 생체인터넷(Internet of Biometry, IoB) 및 사회관계망서비스(Social Network Services, SNS) 등을 통해 현실 세계의 데이터가 수집된다. 다음으로 정보화 단계에서는 수집된 데이터들이 클라우드 등에서 빅데이터로 구축되는데, 여기까지 디지털 트랜스폼이라고 한다. 지능화 단계에서는 다양한 시뮬레이션을 통해 최적의 가치가 창출되며, 이때 인공지능이 이용된다. 마지막 스마트화 단계에서는 인공지능을 통해 분석된 결과가 아날로그 트랜스폼 기술을 통해서 현실화된다.[289] 예컨대 자율주행자동차나 도로에 부착되어 있는 카메라나 각종 센서를 통해서 수집된 데이터는 클라우드를 통해 누적

---

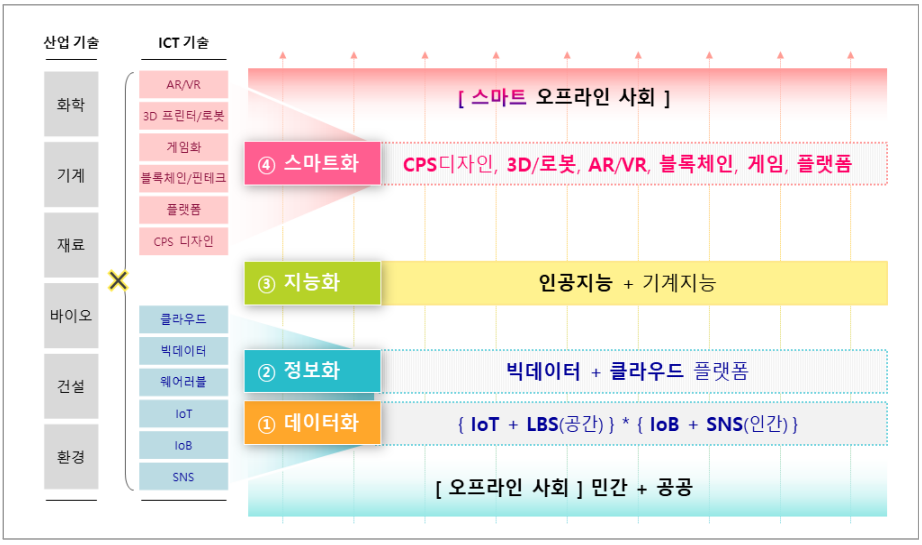
287) 통상 제4차 산업혁명의 특징이 디지털 트랜스폼으로 설명되기도 하나, 이는 현실을 데이터화하는 것으로서 이미 제3차 산업혁명 때부터 시작되었다. 제4차 산업혁명에서는 가상이 데이터를 현실화하는 개념이 추가되어야 하는데, 이것은 아날로그 트랜스폼으로 명명되는 것이 적절하다. 이에 양자가 합쳐진 개념을 스마트 트랜스폼이라고 지칭한다. 이민화/주강진/김애선/김예지/윤예지/장아침/손문영/이명호/차원용/정현호, 4차 산업혁명 국가 로드맵 작성을 위한 정책연구, 국회 4차 산업혁명 특별위원회, 2018.5., 181면.

288) 제4차 산업혁명의 스마트 트랜스폼 과정은 사람의 뇌에서 이루어지는 4단계 작동 과정과 동일하다. 양자 모두 현실 세계의 정보를 수집해서 가상화시켜 저장하고, 이를 구조화한 후 예측이나 맞춤을 통해서 현실로 구현하는 것이다. 이민화/주강진/김애선/김예지/윤예지/장아침/손문영/이명호/차원용/정현호, 앞의 보고서, 181-182면.

289) 이민화/주강진/김애선/김예지/윤예지/장아침/손문영/이명호/차원용/정현호, 앞의 보고서, 170면, 183-184면.

되고, 인공지능은 해당 정보를 분석하여 최적의 경로를 찾아서 개별 차량에 제공할 수 있다. 이러한 스마트 모빌리티가 구현되는 과정에서 다양한 플랫폼이 구축되고 서비스가 제공될 수 있다. 즉 교통정보를 제공받으려는 사람이나 사물로부터 위치정보 등 다양한 데이터를 취득해서 정보화가 이루어지면 이를 토대로 모빌리티 플랫폼이 만들어질 수 있고, 인공지능을 이용해서 지능화를 거치면 새로운 서비스가 구현될 수 있는 것이다.[290]

[그림 3-2] 스마트 트랜스폼 기술과 4단계 융합프로세스[291]



2) 사물인터넷을 이용한 스마트 범죄예방

4단계 스마트 트랜스폼을 통해서 최적화시킬 수 있는 것은 교통만이 아니다. 같은 방법으로 제조업이나 물류, 농업, 교육은 물론이고 도시 자체를 스마트하게 변모시킬 수 있다. 스마트시티(Smart City)란 첨단 정보통신기술을 이용해서 교통이나 주거, 보건, 에너지, 환경, 치안 등 도시 운영이나 서비스의 효율성이 최적화된 도시를 일컫는다.[292] 이러한 스마트시티는 범죄로부터 안전한 곳을 지향하는바, 범죄예방도 데이

290) 이민화/주강진/김애선/김예지/윤예지/장아침/손문영/이명호/차원용/정현호, 앞의 보고서, 171면.
291) 이미지 출처: 이민화/주강진/김애선/김예지/윤예지/장아침/손문영/이명호/차원용/정현호, 앞의 보고서, 184면.
292) 나채준/이준호/김현희/양태건/라정일/정재도, 스마트시티 조성확산을 위한제도개선 연구, 한

터화, 정보화, 지능화, 스마트화를 통해 최적화될 것이 요청된다.

범죄예방 분야의 디지털 트랜스폼 제1단계는 데이터화로서, 112 및 119 신고는 물론이고 CCTV나 드론 등 다양한 사물인터넷 디바이스를 통해서 정보가 수집될 수 있다. 제2단계 정보화 과정에서는 성범죄자 신상정보와 같은 범죄이력은 물론이고 세금 체납 정보나 금융거래 정보 등이 모여서 빅데이터가 된다. 제3단계 지능화는 인공지능을 이용해서 수집된 정보가 분석되는데, 과거 발생했던 범행 장소나 시간, 수법 등이 통합·분석된 후 향후 범죄 발생 가능성이 높은 지역이나 시간이 도출될 수 있다. 이러한 분석 결과를 토대로 제4단계 스마트화가 진행되는데, 범죄발생 가능성이 높은 지역이나 시간대에 경찰력을 집중 배치하는 등 범죄예방 전략을 최적화시킴으로써 경찰 업무의 효율성을 높이고 시민들이 범죄로부터 안전하다고 느끼는 체감 치안지수를 향상시킬 수 있다. 또한 이 과정을 통해 형성된 빅데이터는 범죄가 발생했을 때 수사의 효율성을 제고시키기 위한 목적으로 지능화되어 최적의 수사가 가능하도록 한다. 범죄예방 및 수사의 디지털 트랜스폼은 이미 시작되었는데, 미국의 범죄예측 프로그램인 'PredPol(Predictive Policing)'[293]이나 'DAS(Domain Awareness System)'[294]

국법제연구원, 2018, 7면, 대통령직속 4차산업혁명위원회/관계부처합동, 도시혁신 및 미래성장동력 창출을 위한 스마트시티 추진전략, 2018.1.29., 29면. https://www.4th-ir.go.kr/article/detail/19?boardName=internalData&category= (2019년 10월 23일 최종접속).

293) PredPol(Predictive Policing)은 2010년 미국 캘리포니아 주 로스앤젤레스 경찰청과 캘리포니아 대학이 함께 개발하였으며, 인공지능 알고리즘을 이용해 종래에 발생한 범죄의 유형, 발생 위치 및 일시 등의 데이터를 분석한 후 향후 발생할 것이 예측 가능한 범죄 형태, 장소 및 시간 등을 알려주는 범죄예측 소프트웨어이다. 미국 캘리포니아 주 산타크루즈(Santa Cruz) 경찰청과 로스앤젤레스 경찰청에 의해 선도적으로 도입된 PredPol은 새로운 범죄의 발생 시마다 업데이트되고, 6개월마다 모든 기록 및 최신의 범죄 데이터를 사용하여 범죄 패턴을 재학습하며, 가로·세로의 길이가 각각 500피트 크기인 정사각형 지역 안에서 범죄의 시기와 종류 등을 알려줌으로써 예측의 구체성을 높이고 있다. 또한 PredPol은 개인 식별 가능 정보와 인구통계적 정보를 사용하지 않으므로 프라이버시 침해 문제도 피할 수 있다. 이러한 범죄예측을 토대로 경찰력의 효율적 배치 및 범죄예방의 효과도 제고되고 있는바, 로스앤젤레스의 경우에는 2013년부터 범죄율이 20%이상 감소한 것으로 나타났다. 2019년 현재 PredPol은 미국 전역의 50여 개 법집행기관에 도입되어 있다. Carla Hustedt, "A Public Value Perspective on Predictive Policing in the US", Research Paper, 2016.11., pp.7-10, https://www.researchgate.net/publication/327155597_A_Public_Value_Perspective_on_Predictive_Policing_in_the_US (2019년 10월 23일 최종접속); Jennifer Bachner, Predictive Policing: Preventing Crime with Data and Analytics, IBM Center for The Business of Government, 2013, p.25, http://www.businessofgovernment.org/sites/default/files/Predictive%20Policing.pdf (2019년 10월 23일 최종접속); "Predictive Policing Using AI Tested by Bay Area Cops", government technology 2019.3.11., https://www.govtech.com/public-safety/Predictive-Policing-Using-AI-Tested-by-Bay-Area-Cops.html (2019년 10월 23일 최종접속); PredPol 웹페이지, https://www.predpol.com/how-predictive-policing-works/ (2019년 10월 23일 최종접속) 참조.

의 활용이 대표적이다.[295]

범죄예방 및 수사의 디지털 트랜스폼 과정에서 사물인터넷(IoT)은 네트워크로 연결되어 있는 디바이스를 통해서 각종 데이터를 수집할 뿐만 아니라 정보를 공유하거나 활용할 수 있다. 종래의 CCTV나 차량번호판 판독기는 그 설치 목적에 부합하는 정보를 수집하는 것에 그쳤다면, 사물인터넷 기술 발전에 힘입어 이들은 네트워크에 연결된 개별 디바이스로서 정보를 공유하거나 활용할 수 있게 되었다. 또한 디바이스를 통해 수집된 정보의 이용 목적이나 범위도 확장될 수 있다. 일례로 기존의 방범용 CCTV는 현재 교통이나 재난 및 환경 등 여러 분야의 도시 상황을 통합해서 관리하는데 활용되고 있는데, 국토교통부가 추진하고 있는 스마트시티 통합 플랫폼 보급 사업[296]은 이러한

---

294) DAS(Domain Awareness System)는 2012년 뉴욕 경찰청이 마이크로 소프트(Microsoft)사와 공동으로 범죄를 예측하고, 실시간 감시대응 체제를 구축하고자 개발하였는데, 뉴욕 내에 설치되어 있는 방범용 CCTV, 방사능 감지장치 및 자동차 번호판 판독기를 통하여 수집된 데이터뿐만 아니라 911 신고 내역, 성범죄자 신상정보 등 범죄경력, 국세청 체납세액 정보 및 톨게이트 통행 정보 등의 빅데이터를 통합, 분석하여 의심스러운 사람 또는 물건, 차량의 위치를 추적하고, 용의자의 생활형태 등 다양한 정보를 파악한다. 또한 DAS는 데이터를 기반으로 하여 의심스러운 정황이 포착되면 즉시 경보를 발령하며, 일선 경찰관들은 모바일 기기로 사건의 발생 위치와 용의자의 동선 및 전과 기록 등의 정보를 제공받게 된다. 동 시스템의 구축 후 경찰은 수사 기간을 단축시키고 업무효율성을 증진시켰다고 평가받지만, 그로 인하여 인권 침해나 프라이버시 침해의 우려도 제기되었다. 이에 뉴욕 경찰청은 DAS 운영에 관한 가이드라인을 확립하였는데, 적법한 법집행 또는 공공 안전의 증진을 위해 이 시스템은 상시적으로 운영되지만, 사적 영역이 아닌 장소나 공공의 활동을 대상으로 해서만 이용되고, 누구라도 인종, 국적, 성별, 나이, 종교, 장애, 병역, 시민권 보유 여부나 혼인상태, 정치적 성향 및 성적 취향 등을 이유로 DAS의 목표가 되거나 감시받지 않는다. 또한, 뉴욕 경찰은 CCTV를 이용할 경우 사람들이 촬영 사실을 인식할 수 있도록 표지부착을 해야 한다. Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion", University of Pennsylvania Law Review Volume 163, University of Pennsylvania Law School, 2015, pp.378-179; E. S. Levine/Jessica Tisch/Anthony Tasso/Michael Joy, "The New York City Police Department's Domain Awareness System", Journal Interfaces, Volume 47 Issue 1, INFORMS Institute for Operations Research and the Management Sciences(INFORMS), 2017, pp.70-84; NYPD Domain Awareness System(DAS), Public Security Privacy Guidelines, 2009.4.2., http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf (2019년 10월 23일 최종접속) 참조.

295) 범죄예측 프로그램에 대해서는 그로 인하여 실제 범죄율이 감소하는지 불분명하고, 범죄 발생의 위험성을 평가하는 알고리즘 자체가 가지는 편향성으로 인해서 부당한 차별이 발생할 수 있다는 비판이 제기되고 있다. Kristian Lum/William Isaac, "To predict and serve?", Significance Volume 13, Issue 5, The Royal Statistical Society, 2016, pp.15-16; Emily Thomas, "Why Oakland Police Turned Down Predictive Policing", Motherboard 2016.12.28., https://motherboard.vice.com/en_us/article/ezp8zp/minority-retort-why-oakland-police-turned-down-predictive-policing (2019년 10월 23일 최종접속); Andrew D. Selbst, "Disparate Impact in Big Data Policing", Georgia Law Review Volume 52, Number 1, University of Georgia School of Law, 2017, pp.131-135 참조.

296) 스마트시티 통합 플랫폼은 교통환경·에너지·수자원 등 각종 도시 인프라에 인공지능(AI), 사

연계 서비스를 통해 스마트시티 구현을 위한 인프라를 구축하고자 한다.[297]

나. 범죄예방을 위한 사물인터넷 기술 적용 사례

1) 국내 사례

2016년 경찰청은 점차 흉포화·첨단화·광역화되는 전통적 범죄와 신종 범죄에 선제적으로 대응하고자 사물인터넷 등 첨단과학기술을 치안 분야에 적용하겠다는 내용이 담긴 '경찰 미래비전 2045'를 발표하였다.[298] 이에 의하면 사물인터넷(IoT)과 IT, BT, NT, RT, AT 등 이른바 5T[299] 기술이 적용된 경찰장비 등을 개발해서 치안활동의

물인터넷(IoT) 등 첨단 정보통신기술(ICT)을 연계·활용하는데 핵심 역할을 하는 기반 소프트웨어이며, 스마트시티 통합 플랫폼 기반구축 사업은 통합 플랫폼을 지방자치단체의 각종 정보시스템과 연계하여 도시 관리의 효율성을 높여 보다 편리한 스마트시티로 운영될 수 있도록 스마트시티 안전망의 구축을 목표로 한다. 국토교통부는 개별 운영 중인 지방자치단체의 방범·교통 등 각종 정보 시스템과 센터·서비스 등의 효율적인 운영을 위해 스마트시티 통합 플랫폼에 연계하고, 112·119·재난망 등을 연계하여 스마트시티 안전망을 구축하고 있으며, 동 통합 플랫폼과 5대 연계 서비스(① 112센터 긴급영상 지원, ② 112 긴급출동 지원, ③ 119 긴급출동 지원, ④ 재난안전 상황 지원, ⑤ 사회적 약자(어린이·치매노인) 지원)를 보급하고 있다. 국토교통부 보도자료, "서울·제주 등 12개 지자체 스마트시티 통합 플랫폼 사업지 선정", 2018.2.28., http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?lcmspage=1&id=95080447 (2019년 10월 23일 최종접속) 참조.

297) 2019년 9월 25일 국토교통부와 경찰청은 서울특별시, 광주광역시, 강원도 등과 함께 긴급 수배차량의 위치정보를 실시간으로 확인하여 경찰관의 신속한 현장 출동 및 피해자 구조 등을 지원하는 '스마트도시 안전망 구축 업무협약(MOU)'을 체결하였다. 동 협약은 지방자치단체의 스마트시티 센터 통합 플랫폼과 수배차량 검색시스템(Wanted Automobile Scanning System, WASS)을 연계하여 수배차량 데이터베이스와 지자체 CCTV로 인식된 차량번호의 실시간 비교·검색을 통해 긴급 수배차량 발견 시 해당 위치정보를 WASS로 전송하는 것인데, 동 사업을 통해 전국 229개 지자체 스마트시티 센터의 방범용 CCTV(차량번호 인식 솔루션 설치 시 수배차량 검색용으로 활용 가능) 51만대가 WASS와 연계되면 간선도로 외에 도심지, 골목길, 이면도로 등에서도 긴급 수배차량의 이동경로가 파악되므로 보다 촘촘한 치안 안전망이 구축될 것으로 본다. 또한 현장 출동 경찰관이 요청할 경우 스마트시티 센터에서 현장 사진, 범인 도주경로, 사건 증거자료 등을 실시간으로 제공하여 신속한 범인검거 및 사건처리 또한 적극 지원하는데, 개인정보 보호법 제18조 제2항을 적용하여 동법이 허용하는 살인, 강도, 납치 등 강력범죄의 예방·진압 및 수사 등 목적으로 긴급 수배된 차량에 한해서만 경찰청이 차량번호를 제공하면 스마트시티 센터가 해당 차량의 위치정보를 회신한다. 동 협약 체결을 통해 2019년 10월부터 서울특별시, 광주광역시, 강원도, 은평구, 서초구 등 5개 지자체를 중심으로 시범사업을 실시하고, 단계적으로 전국 지자체로 확대해 나갈 예정이다. 국토교통부 보도자료, "강력범죄 수배차량 CCTV로 실시간 추적…도시 안전망 강화", 2019.9.24., http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?id=95082822 (2019년 10월 23일 최종접속) 참조.

298) 경찰청 보도자료, "경찰청, '경찰 미래비전 2045'발표 - '선진 국민 경찰'을 지향하는 과학 경찰, 정예 경찰, 시민 경찰을 제시-", 2016.1.14., http://www.korea.kr/common/download.do?fileId=184157575&tblKey=GMN (2019년 10월 23일 최종접속) 참조.

299) 5T로 거론되는 기술들에는 ① 정보 기술(Information Technology, IT), ② 생명공학 기술(Bio

효율성과 편의성을 제고하는 한편, 빅데이터와 인공지능 기술 등을 이용하여 스마트 치안시스템을 구축한다는 전략이 제시되어 있다.[300] 그러나 여전히 경찰에서 범죄예방을 위해서 사물인터넷 기술을 활용하는 사례는 종래의 CCTV를 디바이스로 이용하는 수준에서 크게 발전하지 못했다. 경찰관의 공권력 남용이나 경찰관에 대해 가해지는 공무집행 방해 등을 막기 위해 사용되는 '웨어러블 폴리스캠(Wearable Police Cam)'이나 실종자 수색 및 도주자 추적 등에 사용되는 '드론(Dron)'은 사물인터넷 디바이스로 활용될 수 있으나, 현재 경찰은 네트워크에 연결되지 않은 형태의 장치들을 이용하고 있다.

한편 지방자치단체 차원에서 스마트 치안시스템을 구축하려는 시도가 주목된다. 2015년 10월 서울시는 길거리에 방치되어 있던 공중전화부스를 '안심부스'로 전환하는 사업을 시작하였다.[301] 범죄위협을 받는 시민이 안심부스로 대피해서 버튼을 누르면 자동으로 문이 닫히고, 사이렌과 경광등이 작동되며, 112로 연결된다. 또한 CCTV와 스마트미디어 등을 통해 범인의 인상착의가 녹화될 수 있으며, 부스 주변에서는 무료로 와이파이가 제공되어 인터넷 접속도 용이하다. 나아가 안심부스에 설치된 현금자동입출금기(ATM)를 통해서 보다 안전하게 금융서비스를 제공받을 수 있다.[302][303]

Technology, BT), ③ 나노 기술(Nano Technology, NT), ④ 로봇 기술(Robot Technology, RT), ⑤ 인공지능 기술(Artificial Intelligence Technology, AT)이 있다.

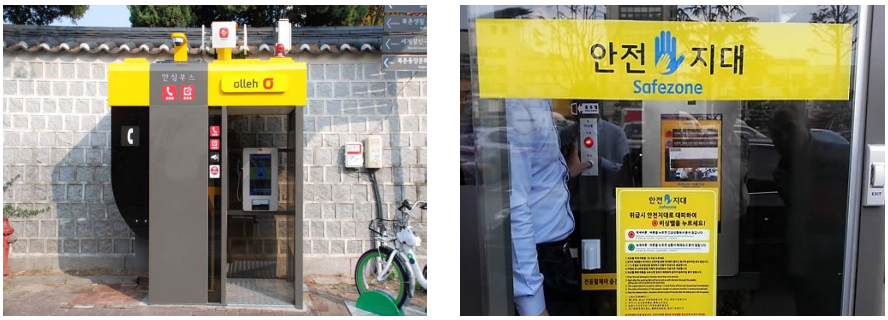
300) 조진삼, "경찰미래비전 2045", See Futures 제10호, KAIST 문술미래전략대학원 미래전략연구센터, 2016, 31-32면.

301) 서울시 보도자료, "길거리 공중전화 부스, 안심부스로 새 단장", 2015.11.9., http://spp.seoul.go.kr/main/news/news_report.jsp#view/25097?tr_code=snews (2019년 10월 23일 최종접속).

302) 서울시, 앞의 보도자료("길거리 공중전화 부스, 안심부스로 새 단장") 참조.

303) 2018년에는 서울교통공사와 KT가 함께 서울 지하철역 여자화장실에 '세이프 메이트(Safe Mate)'라는 장치를 설치하는 시범사업을 시작하였다. 이는 위기에 처한 이용자가 비명 소리를 지르거나 터치패드를 누르면 사이렌이 울리는 동시에 역무실은 물론이고 담당 근무자 휴대전화로 상황이 전달되도록 만들어졌다. "성범죄 막는 비명감지시스템, 서울 지하철 여자화장실에 설치", Newdaily 2018년 3월 23일자, http://www.newdaily.co.kr/site/data/html/2018/03/23/2018032300039.html (2019년 10월 23일 최종접속); "'여자화장실에 설치된 세이프 메이트 장치'", 중앙일보 2018년 3월 23일자, https://news.joins.com/article/22469329 (2019년 10월 23일 최종접속).

[그림 3-3] 서울시 안심부스[304]



문제는 이렇게 설치된 안심부스가 2019년 3월 기준으로 총 13개에 불과하고 그마저도 제대로 관리되지 않는다는 점이다. 비상벨을 눌러도 출입문이 닫히지 않거나, 닫혔던 문이 다시 열리는가 하면, 위급상황 시 출동해야 할 경찰과 연결이 되지 않아서 '안심부스'가 오히려 '위험부스'로 전락하고 있다는 비판이 제기되고 있다.[305]

또 다른 스마트 치안시스템으로는 서울시의 '안심이 앱'을 들 수 있다. 2016년 3월 서울시는 「여성안심특별시 2.0」 사업의 일환으로 '안심이 앱' 출시 계획을 발표한 바 있다.[306] 어플리케이션의 개발과 함께 자치구 통합관제센터와 연계 시스템이 구축되었는데, 해당 앱은 2017년 5월에 4개의 자치구(은평·서대문·성동·동작구)에서 시범운영된 것을 시작으로 하여 2018년 10월 25일부터는 전 자치구에서 서비스가 제공되었다.[307] '안심이 앱'은 25개의 자치구별로 운영 중인 통합관제센터가 컨트롤타워가 되어서 서울시 전역에 설치되어 있는 약 4만 대의 CCTV와 스마트폰 앱을 연계하여 실시간으로 위험상황을 모니터링하고 구조 지원 서비스까지 제공하는데, 2019년 3월

304) 이미지 출처: (좌) "방치된 공중전화 부스가 '안심 피난처'로 변신", 내 손안의 서울, 2015년 11월 9일자, http://mediahub.seoul.go.kr/archives/932918?tr_code=snews (2019년 10월 23일 최종접속), (우) "공중전화 부스, 범죄 위협 대피 안심부스로 大변신..어떻게?" 한국경제신문 2015년 11월 9일자, https://www.hankyung.com/news/article/2015110964005 (2019년 10월 23일 최종접속).

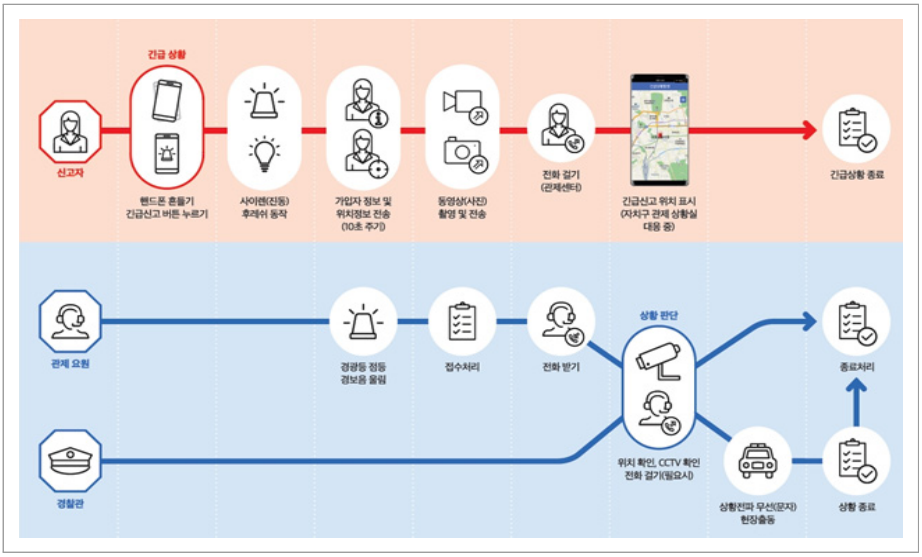
305) 서울지방경찰청 관계자는 안심부스 내에 설치된 현금자동입출금기가 고장 날 때 마다 이용자로부터 신고가 들어와서 112와의 연결을 해제했다고 말했다. "문도 안닫히는 '안심부스'…KT링커스·서울시 '뒷짐'", News1 2019년 3월 29일자, http://news1.kr/articles/?3575163 (2019년 10월 23일 최종접속).

306) 서울시 보도자료, "서울시, "밤길 두려운 여성은 '안심이 앱'을 켜세요."", 2016.3.8., http://www.seoul.go.kr/news/news_report.do#view/26191 (2019년 10월 23일 최종접속).

307) 서울시 보도자료, "서울시, '안심이 앱' 11만 명 돌파…CGV와 안전캠페인", 2019.9.23., http://www.seoul.go.kr/news/news_report.do#view/297927 (2019년 10월 23일 최종접속) 참조.

부터는 각 구별로 2명씩 안심이 관제 전담인력 50명을 확보하여 24시간 관제체제를 구축하고 있다.[308] 2019년 9월 17일 기준으로 해당 앱을 다운로드 받은 사람은 총 11만 670명이었고, 이를 통한 이용 건수는 총 3만 6,108건인 것으로 집계되었는데, 그 중 긴급신고가 9,781건, 귀가 모니터링이 2만 4,064건, 안심 귀가 스카우트가 2,263건이었다.[309] 향후 서울시는 자치구의 관제 소홀이나 자치구 간 경계지역 및 경기도 인접 지역에서 직접 관제가 어려운 상황에 대비하여 여성안전 서비스를 통합 관리할 예정이라고 한다.[310]

[그림 3-4] 서울시 안심이 긴급신고 처리 흐름도[311]



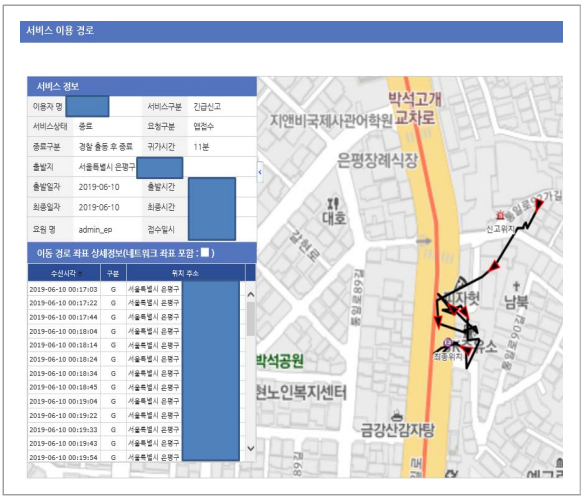
308) 서울시 보도자료, "서울시, '안심이 앱' 신고로 성범죄자 현행범 검거", 2019.6.12., https://www.seoul.go.kr/news/news_report.do#view/291016?tr_code=snews (2019년 10월 23일 최종접속).

309) 2019년 6월 10일 24시경 은평구의 한 교회 주차장 인근을 지나던 주민은 성기를 노출하여 음란 행위를 하던 사람을 목격하고 안심이 앱을 통해 긴급신고를 했다. 신고 즉시 은평구 안심이 관제요원과 상주경찰관은 피해자와 통화하며 달아난 범인의 인상착의와 위치 등을 무전전파하였고, 순찰차가 긴급 출동해서 신고 10분 만에 성추행범이 검거되었다. "'안심이 앱' 신고로 딱 걸린 성범죄자 현행범 검거", 내손안의 서울 2019년 6월 11일자, http://mediahub.seoul.go.kr/archives/1236564 (2019년 10월 23일 최종접속).

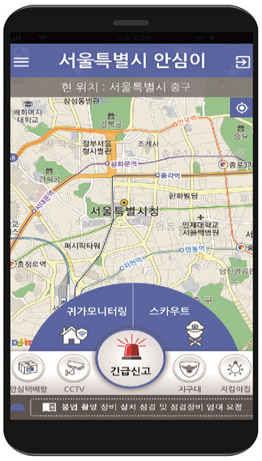
310) "서울시 '안심이 앱' 가입자 11만명 돌파", 헤럴드경제 2019년 9월 23일자, http://news.heraldcorp.com/view.php?ud=20190923000046 (2019년 10월 23일 최종접속).

311) 이미지 출처: 서울시 보도자료, "서울시, 밤길 '안심이' 전 자치구 확대…시민 대표 호신앱으로", 2018.10.26., http://www.seoul.go.kr/news/news_report.do#view/271589 (2019년 10월 23일 최종접속).

[그림 3-5] 안심이 피해자 관제화면[312]



[그림 3-6] 안심이 앱[313]



한편 범죄예방을 위해 사물인터넷을 이용하려는 움직임은 민간부문에서 보다 적극적이다. 최근 귀가하던 여성의 뒤를 따라가 닫히는 문을 강제로 열려고 시도했던 남성의 모습이 담긴 CCTV가 공개되면서 1인 가구 여성의 주거안전에 대한 경각심을 불러일으켰다.[314] 이른바 '신림동 원룸 사건'으로 불리는 이 사건이 발생한 직후 통신 3사가 출시한 사물인터넷 기반의 보안시스템이 주목을 받았다. SK 텔레콤은 HDC현대산업개발과 함께 출입자와 택배 등을 관리할 수 있는 IoT 시스템을 선보였고,[315]

---

312) 이미지 출처: 서울시, 앞의 보도자료("서울시, '안심이 앱' 신고로 성범죄자 현행범 검거") 참조.

313) 이미지 출처: 서울시, 앞의 보도자료("서울시, '안심이 앱' 11만 명 돌파…CGV와 안전캠페인") 참조.

314) 2019년 5월 28일 서울시 관악구 신림동 소재 원룸에 사는 20대 여성을 미행한 30대 남성은 여성이 현관문을 열고 집 안으로 들어갈 때 따라 들어가려고 문을 잡아당기며 침입을 시도하였으나 간발의 차이로 문이 잠기면서 실패하였다. 그러나 현관문 앞을 10여분 동안 서성이고 초인종을 누르는 모습이 CCTV를 통해 공개되며 경찰이 이 남성을 체포하였고 강간미수 혐의를 적용해 검찰에 송치하였다. 이후 2019년 10월 16일 열린 1심 재판에서 법원은 강간미수 혐의는 무죄 판단을 내렸고 주거침입 혐의만 징역 1년의 유죄로 인정하였다. "法 "신림동 사건, 강간 고의 없었다… 주거침입만 인정"", 국민일보 2019년 10월 16일자, http://news.kmib.co.kr/article/view.asp?arcid=0013825529&code=61121111&cp=nv (2019년 10월 23일 최종접속); "'신림동 원룸 사건' 남성 징역 1년…주거침입만 '인정'", JTBC 뉴스 2019년 10월 16일자, http://news.jtbc.joins.com/article/article.aspx?news_id=NB11895947 (2019년 10월 23일 최종접속) 참조.

315) "SK텔레콤, HDC현대산업개발과 인공지능 IoT 아파트'선보인다", SKT 스마트홈 보도자료 2017년 3월 27일자, https://www.sktsmarthome.com/contents/pressRelease/detail?idx=153&pageNo=3&startRow=12&view=summary (2019년 10월 23일 최종접속).

KT는 삼성물산과 공동으로 인공지능과 IoT를 이용해서 외출 시에도 출입문 통제가 가능한 기술을 구현했다.[316] 또한 LG 유플러스는 CCTV와 센서를 통해 출입문의 움직임이 감지되면 집안을 녹화하고, 이상 징후 발견 시 경보 작동과 함께 경찰 신고까지 안내하는 서비스를 공개했다.[317]

2) 국외 사례

우리나라에 비해 총기규제가 완화되어 있는 미국에서는 총기사용으로 인한 범죄가 사회적 문제가 되고 있다. 이에 피해자를 신속하게 발견하여 구조하고, 범죄수사의 효율성을 제고하고자 사물인터넷을 이용한 '샷 스포터(Shot Spotter)'라는 시스템이 이용되고 있다.[318] '샷스포터사(ShotSpotter Inc.)'가 개발한 이 시스템은 대학 캠퍼스나 특정 장소에 음향감지장치를 설치하고, 총성이 울리면 동 장치가 이를 감지해서 기록한 데이터를 경찰서 내 컴퓨터로 전송한다. 이후 총성이 개별 음향감지장치에 도달한 시간을 토대로 삼각 측량법을 이용해서 총기가 발사된 위치를 알아내는 것이다.[319] 이 시스템은 현재 캘리포니아 주의 오클랜드(Oakland), 일리노이 주 록포드(Rockford), 인디애나 주의 사우스 벤드(South Bend), 오하이오 주의 신시내티(Cincinnati), 위스콘신 주의 밀워키(Milwaukee) 등 미국 내 98개 도시에 도입되었다.[320] 2014년 3월 오클랜드 시장 진 콴(Jean Quan)은 2013년 미국의 주요 도시들 중 오클랜드에서 살인 사건 수가 가장 크게 감소했고, 그러한 결과가 발생한 데에는

316) "'래미안 IoT 플랫폼' 래미안 연지 어반파크에 첫 적용", 삼성물산 건설부분 뉴스 2019년 5월 13일자, http://www.secc.co.kr/mo/html/pr/press_view.asp?idx=MjU4MQ== (2019년 10월 23일 최종접속); "안전한 집을 위한 '사물인터넷 기술(IoT)'", 삼성물산 건설부문 공식 블로그, https://samsungblueprint.tistory.com/1046 (2019년 10월 23일 최종접속).

317) 간편버튼을 누르면 앱을 통해 지인에게 자동으로 문자메시지가 전송되는 기능도 선택할 수 있는데, 이는 신림동 사건에서와 같이 뒤따르던 사람이 혹시라도 침입하는 경우에 신속하게 도움을 청할 수 있도록 한다. "LG유플러스, 인공지능 보안 서비스 '우리집 지킴이' 출시", LG U+ 보도자료 2019년 8월 7일자, https://www.uplus.co.kr/com/cpif/lgin/lgns/RetrieveComNewsList.hpi?mid=12095 (2019년 10월 23일 최종접속).

318) "Acoustic Sensing and the Internet of Things Combat Gun Violence Outcomes", Sealevel Systems News 2018.6.18., https://www.sealevel.com/2018/06/18/acoustic-sensing-and-the-internet-of-things-combat-gun-violence-outcomes/ (2019년 10월 23일 최종접속).

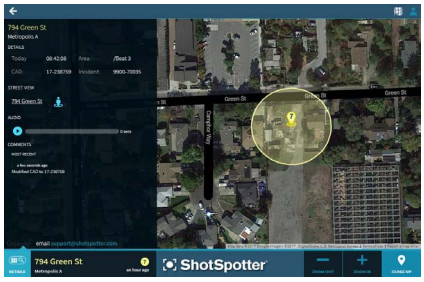
319) ShotSpotter, ShotSpotter FAQ, 2018, https://www.shotspotter.com/wp-content/uploads/2018/08/FAQ_Aug_2018.pdf (2019년 10월 23일 최종접속).

320) ShotSpotter 웹페이지, ShotSpotter Cities, https://www.shotspotter.com/cities/ (2019년 10월 23일 최종접속).

샷 스포터를 배치한 영향이 컸다고 밝히기도 했다.[321] 또한 2017년에 이 시스템을 도입한 록포드 경찰은 2018년 10월 말 기준으로 이 시스템을 이용해서 16명의 총기 사건 용의자를 체포했고, 총기 이용 범죄가 18% 가량 감소했다고 한다.[322]

[그림 3-7] 샷 스포터 시스템[323]





한편 경찰을 향한 총격은 물론이고, 업무 수행 중 경찰이 발포한 총격에 대해서도 신속하게 대응한 필요가 있는바, 캘리포니아 주의 샌디에고 경찰국(San Diego Police Department, SDPD)은 2016년 샷 스포터(Shot Spotter) 장비[324]가 장착된 경찰복을 지급하여 1년 동안 시범 프로그램을 시행한 후 계속 동 시스템을 사용하도록 하였다.[325] 또한 총 자체에 센서와 위치추적 장치를 부착해서 발사 정보를 기록하여 클라

321) "Oakland City Council Meeting Discussing ShotSpotter Benefits and Funding", KNTV 2014.3.14., https://www.youtube.com/watch?v=29OnQmQy2iE#! (2019년 10월 23일 최종접속); "Oakland City Council Meeting Discussing ShotSpotter Benefits and Funding", ShotSpotter, https://www.shotspotter.com/oakland-gunfire-reduction-program/ (2019년 10월 23일 최종접속).

322) "Rockford Police say ShotSpotter detection system has led to 16 arrests", WTVO Channel 17/WQRF Fox 39 2018.10.30., https://www.mystateline.com/news/rockford-police-say-shotspotter-detection-system-has-led-to-16-arrests/ (2019년 10월 23일 최종접속).

323) 이미지 출처: (좌) YouTube 웹페이지, ShotSpotter Respond in Action, https://www.youtube.com/watch?v=IX2tRHLRdUA&feature=youtu.be (2019년 10월 23일 최종접속), (우) ShotSpotter 웹페이지, https://www.shotspotter.com/law-enforcement-flex/ (2019년 10월 23일 최종접속)

324) 오디오 센서와 위성판독시스템(GPS)이 탑재된 이 장비는 총기나 기타 화기의 발포 위치를 정확하게 추적할 수 있도록 한다.

325) "San Diego police to continue using gunshot detection system, despite some criticism", The San Diego Union-Tribune 2017.10.7., https://www.sandiegouniontribune.com/news/public-safety/sd-me-sdpd-shotspotter-20171005-story.html (2019년 10월 23일 최종접속); "Pros And Cons Of San Diego's Gunshot Detection System", KPBS Public Media 2019.6.19., https://www.kpbs.org/news/2019/jun/19/pros-and-cons-gunshot-detection-system/ (2019년 10월 23일 최종접속).

우드로 전송하는 기능을 가진 '스마트 건(Smart Gun)'도 등장하였다.[326] 신생 벤처인 '야르담 테크놀로지스(Yardarm Technologies)사'가 개발한 이 총은 경찰의 총기 사용에 대한 투명성을 보장하고, 다른 경찰들에게 지원이 필요한 위치를 알릴 수 있다.[327] 야르담사의 스마트 건은 2015년 초 공식 출시 전에 이미 캘리포니아 주의 산타크루즈(Santa Cruz)와 텍사스 주의 캐롤튼(Carrollton) 경찰서에서 시험 사용되었다.[328] 그러나 현장에서 오랫동안 총기를 중요한 장비로 사용해 온 경찰은 제대로 검증되지 않은 새로운 기술이 적용된 스마트 건에 대해서 회의적인 입장을 취하기도 했다.[329]

사물인터넷 디바이스 중 상당수는 사람이 착용하는 웨어러블(Wearable) 기기가 될 것인데, '구글 글래스(Google Glass)'도 그 중 하나이다. 2012년 6월 27일에 공개된 구글 글래스는 안드로이드 운영체제(OS)가 탑재된 웨어러블 디바이스로서 소형 마이크와 카메라는 물론이고 헤드업 디스플레이(Head-Up Display, HUD)[330]까지 갖추어 시야를 가리지 않은 상태에서 필요한 정보를 제공받을 수 있도록 하였다. 디바이스 옆면의 터치 패널을 사용하거나 음성 명령으로 정보를 불러오거나 제어할 수 있는 구글 글래스는 두 손을 자유롭게 쓰면서 각종 정보에 접근하거나 기록할 수 있다는

---

326) 네트워크에 연결된 스마트 총 이외에도 방아쇠에 지문센서가 탑재되었거나 RFID 칩이 장착된 총도 스마트건으로 개발되었다.

327) Yardarm Technologies 웹페이지, http://www.yardarmtech.com/ (2019년 10월 23일 최종접속).

328) "Can these gun sensors keep cops safer?", CNET 2014.11.8., https://www.cnet.com/news/black-friday-sales-start-now-at-best-buy-major-price-cuts-on-ipad-macbook-air-and-more/ (2019년 10월 23일 최종접속); "This Company's System Would Allow Police Departments To Track And Monitor Their Guns By iPad", Business Insider 2015.1.13., https://www.businessinsider.com/this-companys-system-would-allow-police-departments-to-track-and-monitor-their-guns-by-ipad-2015-1 (2019년 10월 23일 최종접속).

329) "How the Internet of Things is transforming law enforcement", Network World 2014.11.3., https://www.networkworld.com/article/2842552/how-the-internet-of-things-is-transforming-law-enforcement.html (2019년 10월 23일 최종접속).

330) 헤드업 디스플레이(Head-Up Display)란 자동차나 비행기 앞면 유리를 통해 그래픽을 보여주는 장치이다. 운전자나 조종사가 고개를 든 상태에서 각종 정보를 볼 수 있도록 구현된 기술이기 때문에 헤드업(Head-Up)이라는 용어가 사용되었다. 고속주행 차량의 운전자는 계기판이나 내비게이션을 확인하고자 잠깐만 시선을 돌려도 돌발 상황에 준비 없이 노출되는 것과 같다. 이에 각종 정보를 차량 앞면 유리에 제공해서 운전자의 시선을 전방에 고정시키는 헤드업 디스플레이는 사고 발생률을 낮출 수 있다는 점에서 그 필요성이 높아지고 있다. 김경호, "헤드업 디스플레이(Head-Up Display)", KISTI market report 2015년 9월호(통권 55호), 한국과학기술정보연구원, 2015, 16-17면, http://kmaps.kisti.re.kr/rpt/findAllFile.do?rptId=2216&metaTypeCd=&metaTypeSeq=&reportGubun=1 (2019년 10월 23일 최종접속); 한동진/김현희, "마이크로 디스플레이를 이용한 소형 헤드업 디스플레이 광학계 설계", 한국산학기술학회 논문지 제16권 제9호, 2015, 6227-6228면.

점에서 주목받았다.[331]

[그림 3-8] 구글 글래스[332]



[그림 3-9] 항공기, 차량 HUD 이미지 [333]



이에 뉴욕 경찰청(NYPD)은 업무 수행을 위해 구글 글래스를 시범운영하였으나, 이후 구글 글래스에 대해서 프라이버시[334]와 안전[335]의 측면에서 문제가 제기되었고,

331) Abdul Moiz, "Control The World Through Google Glass", IEEE Ned Univ Of Eng And Tech, IEEE, https://site.ieee.org/sb-neduet/megafuel-webmagazine/mega-fuel-6th-edition/tech-fest6/control-the-world-through-google-glass/ (2019년 10월 23일 최종접속); "Google Searches for Style", The New York Times, 2013.2.20., https://www.nytimes.com/2013/02/21/technology/google-looks-to-make-its-computer-glasses-stylish.html (2019년 10월 23일 최종접속).

332) 이미지 출처: Google Glass 웹페이지, https://www.google.com/glass/start/ (2019년 10월 23일 최종접속).

333) 이미지 출처: 김경호, 앞의 글, 16면.

334) 구글 글래스에 대해서는 동의 없이 사진이나 동영상이 촬영될 수 있는 등 사생활 침해의 우려가 제기되었다. 그러나 스마트폰도 동일한 기능을 가지고 있는 상황에서 단지 의도하지 않은 촬영이 용이하다는 점에서 이를 금지하는 것은 적절하지 않다는 반론이 있었으나, 실제로 구글 글래스를 착용하고 있던 사람이 바(bar)에서 공격을 당하는가 하면, 미국 시애틀에서는 구글 글래스 착용자의 출입을 금지하는 술집도 등장하였다. "Google Glass targeted as symbol by anti-tech crowd", CNN 2014.4.15., https://edition.cnn.com/2014/04/14/tech/mobile/google-glass-attack/index.html (2019년 10월 23일 최종접속); "Seattle dive bar becomes first to ban Google Glass", CNET 2013.3.8., https://www.cnet.com/news/seattle-dive-bar-becomes-first-to-ban-google-glass/ (2019년 10월 23일 최종접속).

335) 구글 글래스를 착용하고 운전을 할 경우 시야에 영향을 미칠 수 있기 때문에 이를 금지해야

구글이 안면인식 등을 위한 어플리케이션 개발을 명시적으로 금지하면서[336] 해당 디바이스의 도입은 한계에 부딪혔다. 그러나 두바이에서는 안면인식 소프트웨어와 호환이 되는 스마트안경을 도입하여 경찰들에게 지급되었고,[337] 이미 중국에서도 용의자 확인 등을 위해서 경찰이 스마트안경을 활용하고 있다.[338]

한다는 의견이 제시되었는가 하면, 손을 사용하는 기기에 비해 위험하지 않다는 반론도 제기되었다. 2014년 10월 캘리포니아 주 샌디에이고에서는 구글 글래스를 착용한 채 운전을 한 사람에게 교통위반 벌금고지서가 발부되었고, 운전자는 그에 대한 취소 소송을 제기했다. 이후 법원은 실제로 운전자가 구글 글래스를 작동 중이었는지에 대한 증언이 없고, 과속 단속 시 사용된 경찰의 속도측정장치가 정확하게 맞춰져 있었는지에 대한 전문가 증언도 없으므로 운전자의 혐의를 합리적 의심(reasonable doubt)이 없을 정도로 입증할만한 근거가 제시되지 못했다고 보면서 교통법규 위반 혐의를 기각하고 벌금 부과를 무효화하였다. 한편 구글 글래스가 운전을 방해하는지를 묻는 온라인 투표에서는 응답자 중 약 62%가 방해가 된다고 답하였다. "Woman cleared in San Diego Google Glass driving case", Los Angeles Daily News 2014.1.16., https://www.dailynews.com/2014/01/16/woman-cleared-in-san-diego-google-glass-driving-case/ (2019년 10월 23일 최종접속); "Should Google glass be banned while driving? (Survey)", Treehugger 2014.2.28., https://www.treehugger.com/gadgets/should-google-glass-be-banned-while-driving-survey.html (2019년 10월 23일 최종접속).

336) "Google 'bans' facial recognition on Google Glass - but developers persist", The Guardian 2013.6.3., https://www.theguardian.com/technology/2013/jun/03/google-glass-facial-recognition-ban (2019년 10월 23일 최종접속).

337) "Dubai Police to use Google Glass", Gulf News 2014.5.20., https://gulfnews.com/uae/dubai-police-to-use-google-glass-1.1335784 (2019년 10월 23일 최종접속).

338) 중국 허난(河南)성 정저우(郑州)역 경찰은 안면인식기가 부착된 스마트안경을 사용하여 사람들의 얼굴을 스캔해서 취득한 정보를 태블릿으로 전송하고, 데이터베이스에 등록된 정보와의 대조를 통해 용의자로 확인되면 즉시 경보를 발령한다. 해당 디바이스는 얼굴의 70% 이상이 찍힌 사람에 대해서는 단 3초 만에 범죄 용의자인지의 여부를 확인할 수 있고, 5m 가량 떨어진 곳에 있는 범죄자도 3-4초 정도면 발견할 수 있다고 한다. 또한 최근 허페이 안후이(安徽)성 마안산(马鞍山)시 공안국 및 장수성 쑤저우(苏州)시 공안국과 안후이사이탄지능과기유한공사(安徽赛坦智能科技有限公司)가 공동으로 차세대 AR 스마트안경을 개발하였다. 동 안경은 용의자가 공공장소에서 이동하다가 어두운 곳에 숨을 경우 10M 밖에서도 범인을 식별할 수 있는 고화질 카메라와 스마트 음성인식 및 인터콤 시스템이 내장되어 있고, 네트워크 접속을 통해 법집행기록, 음성 및 이미지 인식을 하나로 통합시켜 음성과 얼굴 인식으로 기록을 조회하여 신원확인이 가능하도록 하며, 걸음걸이 인식, 번호판 인식 등 다양한 스캔서비스를 통한 3차원 측정도 가능해 실시간 인식의 정확도를 높였다고 한다. 간쑤(甘肃)성, 윈난(云南)성 등에서는 AR 스마트안경의 시범사용을 통해 신분증 도용, 절도, 마약 복용 등 10여 건의 사건 용의자가 적발 및 검거되었다. "美国网评：中国警察使用面部识别眼镜扫描游客", 每日头条 2018.2.11., https://kknews.cc/news/2e9g9jz.html (2019년 10월 23일 최종접속); "警方春运期间配"人脸识别墨镜"已抓获7名犯罪嫌疑人", EET(电子工程专辑) 2018.2.14., https://www.eet-china.com/news/201802140648.html (2019년 10월 23일 최종접속); "AR智能警用眼镜助力智能警务时代", 新华网 2019.8.19., http://www.ah.xinhuanet.com/2019-08/19/c_1124892600.htm (2010년 10월 23일 최종접속) 참조.

[그림 3-10] 두바이 경찰의 스마트안경[339]



[그림 3-11] 중국 경찰의 스마트안경[340]



2. 사물인터넷 관련 범죄 현황 및 변화 가능성

가. 사물인터넷 관련 범죄 개관

1) 사이버범죄 발생 및 보안 취약점 신고 현황

사물인터넷 디바이스나 망 자체를 공격하는 범죄는 사이버범죄의 한 분류이다. 사이버범죄의 개념에 대해서는 통일된 정의가 존재하지 않으나 수사실무를 맡고 있는 경찰청은 사이버범죄를 "사이버공간에서 행해지는 일체의 범죄"로 정의하면서, 범죄 전체가 사이버공간에서 완료되는 경우는 물론이고 그 일부가 사이버공간에서 행해지는 범죄도 포함시키고 있다.[341] 사물인터넷과 관련된 범죄는 해킹이나 악성 프로그램의 설치는 물론이고, 이를 수단으로 사생활 영역에 침범해서 불법영상을 촬영하거나 이를 유포하는 행위까지 포함된다. 나아가 사물인터넷 서비스를 제공하는 정보통신서비스제공자의 전산망에 침투해서 디도스(DDoS) 공격을 가하는 행위 등 사물인터넷 관련 범죄는 매우 다양하고 방대하다. 현재 사물인터넷과 관련된 범죄의 통계는 별도로 집계되고 있지 않기 때문에, 사이버범죄의 발생 동향과 IoT 제품의 취약성 신고

339) 이미지 출처: "Dubai Police start to use Google Glass", Gulf News 2014.10.27., https://www.emirates247.com/news/emirates/dubai-police-start-to-use-google-glass-2014-10-27-1.567748 (2019년 10월 23일 최종접속).

340) 이미지 출처: "昆明：一线民警配备高科技智能眼镜", 警务新闻 2018.2.23., http://www.ga.yn.gov.cn/jwxw/difangjingwu/kunmingjingxun/201802/t20180223_719668.html (2019년 10월 23일 최종접속).

341) 정 완, "사이버범죄의 주요 쟁점과 대응책에 관한 소고", 홍익법학 제17권 제3호, 홍익대학교 법학연구소, 2016, 369면.

건수의 추이 등을 통해서 간접적으로 파악해보는 수밖에 없다.

먼저 아래의 [표 3-2]는 최근 5년 간 사물인터넷 범죄를 포함한 전체 사이버범죄의 발생 건수 및 검거 현황을 나타낸 것이다. 2014년 110,109건이었던 사이버범죄는 2016년까지 증가하다가 2017년에 131,734건으로 감소하였으나, 2018년에는 다시 149,604건으로 증가하였다. 2018년 기준으로 전체 사이버범죄 중 정보통신망이용범죄가 123,677건(82.7%)으로 가장 많았고, 불법콘텐츠범죄가 23,039건(15.4%), 정보통신망침해범죄가 2,888건(1.93%)으로 집계되었다.

[표 3-2] 최근 5년 간 전체 사이버범죄 발생 및 검거 현황[342)]

구분	총계			정보통신망침해범죄			정보통신망이용범죄			불법콘텐츠범죄		
	발생 건수 (건)	검거		발생 건수 (건)	검거		발생 건수 (건)	검거		발생 건수 (건)	검거	
		건수 (건)	인원 (명)		건수 (건)	인원 (명)		건수 (건)	인원 (명)		건수 (건)	인원 (명)
2014	110,109	71,950	59,220	2,291	846	1,171	89,519	56,461	38,579	18,299	12,643	19,470
2015	144,679	104,888	75,250	3,154	842	1,098	118,362	86,658	50,777	23,163	17,388	23,375
2016	153,075	127,758	75,400	2,770	1,047	1,261	121,867	103,172	42,871	28,438	23,539	31,268
2017	131,734	107,489	59,369	3,156	1,398	1,141	107,271	88,779	36,103	21,307	17,312	22,125
2018	149,604	112,133	60,138	2,888	902	1,048	123,677	93,926	35,738	23,039	17,305	23,352

사물인터넷 범죄의 경우 정보통신망침해범죄가 상당수를 차지할 것으로 전망되고 있는데, 아래의 [표 3-3]은 전체 사이버범죄 중 정보통신망침해범죄 현황을 제시한 것이다. 2014년 2,291건이던 정보통신망침해범죄는 증가와 감소를 반복하고 있는데, 2018년에는 2,888건으로 그 중 902명이 검거되었다. 2018년 기준으로 정보통신망침해범죄 중 가장 많은 수를 차지하고 있는 범죄 유형은 총 584건(20.2%)으로 집계된 해킹이었고, 악성프로그램 유포는 50건(1.73%)이었으며, 이른바 디도스라고 불리는 서비스거부공격은 14건(0.48%)이 발생했던 것으로 나타났다.

342) 경찰청 사이버안전국, http://cyberbureau.police.go.kr/share/sub3.jsp?mid=030300 (2019년 10월 23일 최종접속).

[표 3-3] 최근 5년 간 정보통신망 침해범죄 현황[343]

(단위: 건)

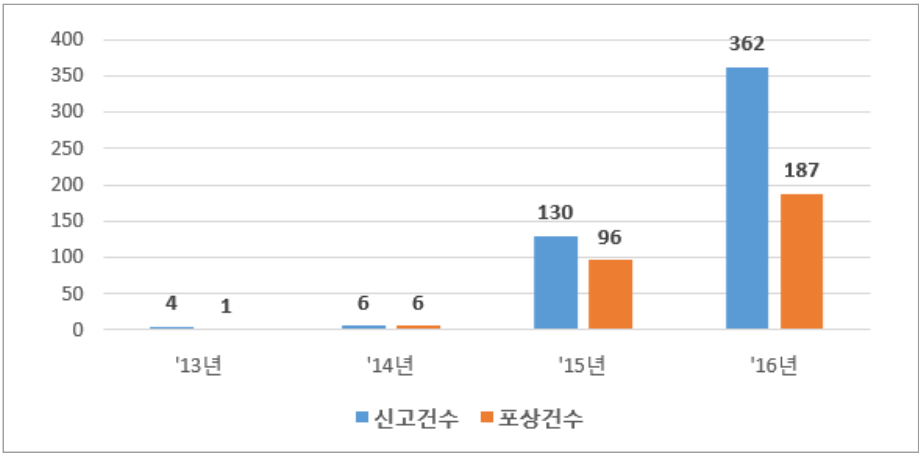
구분		총계	해킹	서비스거부공격	악성프로그램	기타
2014	검거	2,291	1,648	26	130	487
	발생	846	540	16	69	221
2015	검거	3,154	2,247	40	166	701
	발생	842	524	19	64	255
2016	검거	2,770	1,847	192	137	594
	발생	1,047	537	164	98	248
2017	검거	3,156	2,430	43	167	516
	발생	1,398	990	28	122	258
2018	검거	2,888	2,178	20	119	571
	발생	902	584	14	50	254

한편 한국인터넷진흥원(Korea Internet & Security Agency, KISA)은 스마트홈 가전 분야의 보안취약점에 대응하고자 보안취약점 신고 및 포상제도를 운영한 바 있다.[344] 아래의 [그림 3-12]는 연도별 IoT 취약점 신고 및 포상건수의 추이를 나타낸 것이다. 2013년에 4건, 2014년에 6건에 불과했던 신고건수는 2015년에 130건으로 대폭 증가하였고, 2016년에는 362건으로 전년도 대비 278% 증가하였다.

343) 경찰청 사이버안전국, http://cyberbureau.police.go.kr/share/sub3.jsp?mid=030300 (2019년 10월 23일 최종접속).

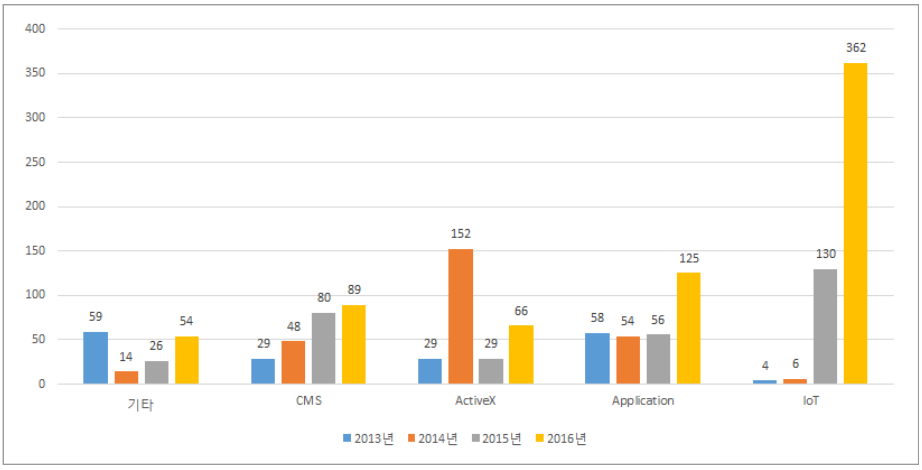
344) 한국인터넷진흥원 보도자료, "KISA, 스마트홈 가전 분야 보안취약점 대응 나선다 -침해사고 예방위해 9월까지 신규 보안취약점 집중 신고기간 운영 -건별 최고 500만원 신고 포상금 지급, 제조사에는 보안패치 요청", 2017.8.1., https://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1581 (2019년 10월 23일 최종접속).

[그림 3-12] 연도별 IoT 취약점 추이(2013-2016년)[345]



한편 아래의 [그림 3-13]은 보안 취약점의 신고 추이를 대상 유형별로 분류한 것이다. 종래에는 어플리케이션이나 액티브X(ActiveX)가 신고 대상이 된 경우가 많았으나, 2015년부터는 IoT 기기가 확대되면서 그 취약점을 신고하는 건수도 급증하였다.

[그림 3-13] 취약점 분류별 신고 추이(2013-2016년)[346]



345) 이미지 출처: 한국인터넷진흥원, 앞의 보도자료("KISA, 스마트홈 가전 분야 보안취약점 대응 나선다")에서 발췌.

346) 이미지 출처: 한국인터넷진흥원, 앞의 보도자료("KISA, 스마트홈 가전 분야 보안취약점 대응 나선다")에서 발췌.

2) 사물인터넷 범죄의 대표 사례

전술한 바와 같이 사물인터넷 범죄의 유형은 매우 다양할 수 있다. 그 중에서도 사물인터넷 디바이스를 해킹해서 프라이버시를 침해하거나 디바이스는 물론이고 웹 서버, 공유기 등의 취약점을 악용해서 DDoS 공격이나 악성 앱 감염 공격을 하는 것이 대표적이다. 우선 2014년 11월에는 세계 각국의 CCTV를 해킹해서 생중계하는 사이트인 '인세캠(Insecam)'에 의해서 우리나라에 있는 CCTV 중 약 6천여 대가 해킹당한 사건이 발생하였다.[347] 해킹 공격은 주로 공장 출고 당시에 설정된 아이디와 비밀번호를 변경하지 않은 IP 카메라를 대상으로 했고, 이를 통해서 IP 카메라가 설치되어 있던 가정집은 물론이고 사무실, 미용실, 수영장, 헬스클럽 등 다양한 장소의 영상이 공개되었다.[348] 이 사건에서 IP 카메라가 설치된 곳에 있었던 많은 사람들의 프라이버시가 침해되었으나 해당 행위는 정보통신망법상 망 침해로 처벌될 수 있을 뿐 정작 주거권자 등의 프라이버시 침해에 대해서는 형법상 처벌의 공백이 발생한다. 향후 사물인터넷의 확산에 제대로 대응하기 위해서는 사용자들의 보안의식이 한층 더 강화되어야 하는 한편, 정보통신망 침해로 인한 주거권자의 프라이버시를 보호할 수 있는 별도의 구성요건을 신설하는 방안이 모색될 필요가 있다.

2016년 10월 21일에는 대규모 분산서비스 거부(Distributed Denial of Service, DDoS) 공격으로 인하여 미국 동부에 있는 인터넷 중 절반가량이 마비되어 아마존(Amazon.com)이나 트위터(Twitter) 등 미국에 서버를 두고 있는 약 1,200개의 웹사이트에서 접속 장애 및 서비스 중단 사태가 발생하였다.[349] 이 사건은 중국의 시옹마이테크놀로지(Hangzhou Xiongmai Technology)사가 제작한 사물인터넷 제품이 '미라이(Mirai)'라는 이름의 악성코드에 감염된 것이 원인이 되었는데,[350] 이렇게 감염된

---

347) "전세계 CCTV 7만3000개 뚫렸다", 중앙일보 2014년 11월 8일자, http://news.jtbc.joins.com/article/ArticlePrint.aspx?news_id=NB10635533 http://inews24.com/view/1212865 (2019년 10월 23일 최종접속).

348) "KISA, 불법 영상유출 사이트 모니터링 자동화 한다", 아이뉴스 24 2019년 10월 4일자, http://inews24.com/view/1212865 (2019년 10월 23일 최종접속).

349) "Today the web was broken by countless hacked devices – your 60-second summary", The Register 2016.10.21., https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/ (2019년 11월 25일 최종접속).

350) 사건이 발생한 지 이틀 뒤에 시옹마이사는 자사 제품의 보안 취약성이 범죄의 수단으로 이용되었다고 시인했다. "중국 업체 "21일 DDoS 공격은 우리 IoT 제품이 원인"", CIO 뉴스 2016년 10월 24일자, http://www.ciokorea.com/news/31678 (2019년 10월 23일 최종접속).

IoT 제품들을 봇넷(Botnet)으로 이용해서 인터넷 도메인 서비스업체인 딘(DYN)의 서버에 대한 공격이 이루어졌다.[351] 이 사건에서도 해커들은 공장 출고 시 설정된 아이디와 패스워드가 변경되지 않은 취약점을 이용해서 사물인터넷 디바이스에 악성코드를 심었고, 감염된 IoT 제품들을 해킹에 악용했다.[352] 이렇듯 사물인터넷에 대한 공격은 보다 손쉽게 발생할 수 있고, 그로 인한 피해가 전 세계를 위협할 수 있음에도 불구하고 보안 개선을 위한 입법화가 제대로 이루어지지 못하는 있는 것은 문제라고 하겠다.

나. 사물인터넷 관련 범죄의 변화 가능성

1) 범죄의 고도화 및 피해의 대량화

사물인터넷 기술의 발전은 살인, 상해, 감금, 방화 등 전통적인 범죄를 한층 더 고도화시킬 수 있다. 예컨대 범죄자는 네트워크상에 연결되어 있는 차량을 해킹해서 브레이크 기능을 잠그는 방법으로 차량 안의 탑승자를 살해할 수 있고, 주행 목적지를 조작하여 원하는 곳으로 그를 납치할 수도 있다. 이를 두고 '사이버 살인'이라고 부르기도 하는데, 이는 첨단기술이 범죄수단으로 이용됨으로써 전통적인 살인죄가 고도화된 것일 뿐이지 사이버 살인이라는 새로운 유형의 범죄가 발생한 것은 아니다. 또한 스마트홈 시스템에 침입하여 거주자를 감금하거나 화재가 발생하게 만드는 것도 전통적인 범죄를 저지르는 데 첨단기술이 활용된 예다. 그러나 이 경우 범죄자는 원격지에서 현장 체포의 위험이 없는 상태로 범행을 저지를 수 있는바, 보안 강화 등의 조치가 없다면 향후 이러한 수단은 보다 빈번히 사용될 가능성이 크다. 한편 냉장고나 TV, 전기레인지, 보일러 온도조절기 등 가정에서 사용하는 수많은 사물들이 인터넷을 통해 연결될 경우 범죄로 인한 피해 규모도 막대해질 것이다.[353] '미라이(Mirai)' 악성코드에 감염된 사물인터넷 제품이 미국 동부에 있는 절반가량의 인터

---

351) Hari Mukundhan, "Anatomy of an IoT DDoS Attack and Potential Policy Responses", ISACA Journal Volume 5, ISACA, 2017, pp.48-49, https://www.isaca.org/Journal/archives/2017/Volume-5/Documents/Journal-volume-5-2017.pdf (2019년 11월 25일 최종접속).

352) 한국인터넷진흥원, 2016년 Mirai 악성코드 동향, 2016.12., 2면.

353) Marc Goodman, Future crimes: inside the digital underground and the battle for our connected world, Anchor Books, 2016, pp.301-302.

넷을 마비시킨 사건에서도 알 수 있듯이 사물인터넷 장치는 사이버공격을 유발 및 촉진하는 역할을 하고 있다. 나아가 최근에는 사물인터넷 디바이스를 대상으로 한 사이버공격이 웹사이트와 네트워크를 마비시키는 것을 넘어서 주요한 국가기반시설에 피해를 입힐 수 있다는 것을 보여주고 있는바,[354] 사물인터넷에 대한 보안 강화가 요청된다.

2) 신종 범죄 발생

2016년 4월 24일 밤 10시 40분 쯤 전남 여수시 서교동의 한 버스 정류장에서는 버스운행정보시스템(Bus Information System, BIS) 단말기의 모니터를 통해서 성관계 장면이 담긴 음란 동영상이 상영되는 일이 발생했다.[355] 사건을 수사했던 경찰은 해외 IP를 통해서 해킹 시도가 있었던 사실을 확인했는데, 해커는 버스정보시스템의 실행을 차단하면서 자동 재생되던 일반 영상의 상영을 중지시키는 한편, 다른 동영상 재생프로그램을 설치한 후 원격으로 1분 56초 분량의 음란 동영상을 다운받아서 반복 재생했다고 한다.[356] 경찰은 해커가 여수 시내에 있는 총 174개의 버스정류장에 운행정보를 제공하는 지능형교통체계(ITS)가 아닌 문제의 단말기로 직접 침투한 것으로 파악했고, 인터폴 등과 공조를 통해 해커의 행방을 추적함과 아울러 수사과정에서 발견된 보안상 취약점을 여수시와 관련 부처에 통보할 것이라고 밝혔다.[357] 이와 유사한 범죄는 필리핀[358]이나 뉴질랜드[359] 등 세계 도처에서 발생하고 있는데, 이를

---

354) ""우크라이나, 대형 인프라 사이버공격의 시험무대"", News1 뉴스 2017년 6월 28일자, http://news1.kr/articles/?3033022 (2019년 10월 23일 최종접속).

355) 순찰 중이던 경찰관이 이를 발견하여 전단지로 모니터를 가린 뒤 이 사실을 여수시에 알렸으며 밤 11시 30분 쯤 단말기 전원이 차단되었다. "여수 버스정류장 음란물 상영 "해외IP로 해킹 시도"", 중앙일보 2016년 4월 28일자, https://news.joins.com/article/19952829 (2019년 10월 23일 최종접속).

356) 당시 여수시청 교통통제센터 근무자가 뒤늦게 원격제어로 영상을 중지하려 했으나 해커는 원격제어 기능도 무력화시켰으며 우회 경로를 통해 다시 단말기에 원격으로 접속한 후, 접속기록 등을 삭제했다고 한다. "경찰, '버스정류장 야동' 해외IP 해킹 확인", 한국경제신문 2016년 4월 28일자, https://www.hankyung.com/society/article/2016042808898 (2019년 10월 23일 최종접속).

357) "경찰, '버스정류장 야동' 해외IP 해킹 확인", 한국경제신문 2016년 4월 28일자, https://www.hankyung.com/society/article/2016042808898 (2019년 10월 23일 최종접속).

358) 「필리핀의 도심 전광판에서 대낮에 음란 영상을 노출하는 황당한 사고가 발생해 당국이 조사에 착수했다. 2018년 3월 22일 현지 일간 마닐라타임스와 필리핀스타 등에 따르면 사고는 2018년 3월 20일 오후 수도 마닐라 인근 마카티시의 번화가 교차로에서 일어났다. 건물 옥상에 있는 대형 전광판에서 남녀가 성관계하는 장면이 30초가량 여과 없이 상영된 것이다. 교차

일컬어 '스마트 사이니지(Smart Signage) 범죄'라고 한다.

[그림 3-14] 여수 버스정류장 음란영상 재생 장면[360]



[그림 3-15] 필리핀 도심 한복판 음란영상 재생 장면[361]



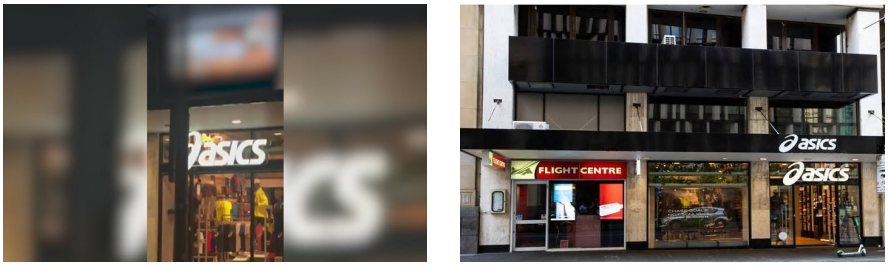
로에서 신호 대기하다가 이를 본 운전자와 행인이 휴대전화기로 사진이나 영상을 찍어 사회관계망서비스(SNS)에 올리면서 급속히 퍼졌다. 이에 따라 마카티시는 즉각 전광판 운영 중단을 명령했다. 마카티시는 "전광판 시스템이 해킹당한 것으로 보고 정확한 경로를 추적하고 있다"고 밝혔다. 전광판 운영업자도 "악의적인 공격"이라며 "시 당국의 조사에 적극 협력하겠다"고 말했다. 인구의 80% 이상이 가톨릭 신자인 필리핀에서는 음란물은 불법이고 영화와 TV 프로그램도 엄격하게 규제되고 있다.」 "필리핀 도심 전광판서 음란영상 상영…"해킹당했다"", 연합뉴스 2018년 3월 22일자, https://www.yna.co.kr/view/AKR20180322067600084 (2019년 10월 23일 최종접속).

359) 「일본의 스포츠용품 브랜드인 아식스(Asics)의 뉴질랜드 오클랜드(Auckland) 매장 홍보용 스크린에 음란물이 장시간 노출되는 일이 발생하였다. 포르노 노출은 2019년 9월 29일 새벽 뉴질랜드 오클랜드 도심에 있는 아식스의 한 주력 매장에서 벌어졌으며, 매장 출입문 위에 설치된 홍보용 스크린에 상영된 문제의 음란물은 이날 오전 10시 직원들이 출근할 때까지 재생됐다. 뉴질랜드 최대 신문인 뉴질랜드 헤럴드에 따르면 음란물은 매장 직원에 의해 꺼질 때까지 무려 9시간이나 그대로 화면에 노출된 것으로 알려졌다. 경찰 드웨인 힌안고(Dwayne Hinango)는 "몇몇 사람은 충격을 받았고 일부는 그냥 서서 바라보기만 했다"고 당시 상황을 전했다. 심지어 7살짜리 아들과 아침을 먹으러 나왔다가 음란물을 보게 된 여성 타냐 리(Tanya Lee)는 "내가 본 것을 믿을 수가 없어서 재차 확인했다면서 아이들에게 노출돼서는 안 될 매우 부적절하고 역겨운 것"이라고 비판했다. 논란 발생 후 아식스 뉴질랜드는 페이스북을 통해 낸 성명에서 "신원을 알 수 없는 누군가가 매장 스크린에 접속해 음란물을 보여준 것이라고 해명했으며, 음란물을 본 모든 분에게 사과의 뜻을 전하고 소프트웨어 및 온라인 보안 공급업체와 협력해 다시는 이런 일이 발생하지 않도록 할 것"이라고 하였다.」 "Asics apologises for porn playing for hours above Auckland store", BBC News 2019.9.30., https://www.bbc.com/news/world-asia-49874967 (2019년 10월 23일 최종접속).

360) 이미지 출처: "여수 버스정류장 '음란 동영상' 해외 IP로 해킹 확인", News1 뉴스, 2016년 4월 28일자, http://news1.kr/articles/?2647966 (2019년 10월 23일 최종접속).

361) 이미지 출처: "필리핀 도심 전광판서 음란영상 상영…"해킹당했다"", 연합뉴스 2018년 3월 22일자, https://www.yna.co.kr/view/AKR20180322067600084 (2019년 10월 23일 최종접속).

[그림 3-16] 뉴질랜드 상점 광고판 음란영상 재생 및 조치 이후 모습[362]



일반적으로 디지털 사이니지(Digital Signage)는 네트워크를 통해 원격제어가 가능한 디지털 디스플레이(LCD, LED 등)를 공공장소나 상업공간에 설치해서 정보나 엔터테인먼트, 광고 등을 제공하는 디지털 미디어를 의미한다.[363] 이는 단순히 디지털 정보를 보여주는 것에 그치지 않고 소프트웨어와 하드웨어, 네트워크 기술 및 콘텐츠 등 다양한 IT 기술이 융합되어 양방향 커뮤니케이션을 가능하게 하는 정보매체이다.[364] 종래의 디지털 사이니지가 광고 기반의 일방향 정보 서비스였다면, 사물인터넷(IoT), 인공지능(AI) 등 IT기술을 융합해 인터넷 및 네트워크 기반의 양방향 서비스 및 맞춤형 서비스가 가능한 공간 미디어를 두고 '스마트 사이니지(Smart Signage)'라고 부른다.[365] 상기의 사건들은 사물인터넷 기술이 적용된 스마트 사이니지를 해킹해서 범죄가 발행한 것으로서 이 경우 음란물을 공연히 상영한 것으로 현행 형법상 음란물죄로 처벌이 가능하다.[366] 다만 이는 원격지에서 국경을 초월하여 음란물 상영

362) 이미지 출처: "Porn on the big screen in central Auckland: Asics video monitor hacked", New Zealand Herald 2019. 9. 29., https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12271975 (2019년 10월 23일 최종접속).

363) POPAI: Digital Signage Standard Terminology. Rev. 1.0, 2010.10.

364) 채송화, "디지털 사이니지(Digital Signage) 기반 콘텐츠산업의 현황과 전망", 코카포커스 2012-06호(통권 54호), 한국콘텐츠진흥원, 2012, 4면.

365) 곽진교, "스마트사이니지포럼", TTA 저널 제170호, 한국정보통신기술협회, 2017, 12면; 송민정, "IoT 기반 스마트 사이니지 현황 및 발전 방향", TTA 저널 제170호, 한국정보통신기술협회, 2017, 56면,

366) 형법 제243조(음화반포등) 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.
아동·청소년의 성보호에 관한 법률 제11조(아동·청소년이용음란물의 제작·배포 등) ① 아동·청소년이용음란물을 제작·수입 또는 수출한 자는 무기징역 또는 5년 이상의 유기징역에 처한다.
② 영리를 목적으로 아동·청소년이용음란물을 판매·대여·배포·제공하거나 이를 목적으로 소지·운반하거나 공연히 전시 또는 상영한 자는 10년 이하의 징역에 처한다.
③ 아동·청소년이용음란물을 배포·제공하거나 공연히 전시 또는 상영한 자는 7년 이하의 징

죄를 저질렀다는 점, 사물인터넷 기술이 적용된 디지털 디스플레이를 대상으로 공격했다는 점에서 종래의 범죄 발생 양상과 다른 특징을 보인다.

제3절 | 사물인터넷 관련 법제 정비 현황 및 그 한계

1. 법제 정비 현황

가. 국외 동향

1) 미국

(1) 미국 연방

연방 차원에서 제정된 사물인터넷 관련 법률로는 「사물인터넷 혁신과 성장을 위한 법(Developing Innovation and Growing the Internet of Things Act, DIGIT Act)」[367]을 들 수 있다. 2016년 3월 1일 미국 상원에 「사물인터넷 관련 작업반 및 운영위원회 설치 등의 사물인터넷 혁신과 성장을 위한 법안(Developing Innovation and Growing the Internet of Things Act(DIGIT Act), S.2607)」이 발의되었고,[368] 이는 2016년 4월 27일에 상무위원회(Senate Commerce Committee)를 통과하였다.[369] 상무위원회는 사물인터넷 혁신과 성장을 위한 법을 승인함으로써 국가적 차원의 사물인터넷 산업 발전을 도모하였다. 동 위원회에서는 사물인터넷 산업 발전에 대한 정부의 역할에

역 또는 5천만원 이하의 벌금에 처한다.
④ 아동·청소년이용음란물을 제작할 것이라는 정황을 알면서 아동·청소년을 아동·청소년이용음란물의 제작자에게 알선한 자는 3년 이상의 징역에 처한다.
⑤ 아동·청소년이용음란물임을 알면서 이를 소지한 자는 1년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
⑥ 제1항의 미수범은 처벌한다.

367) Congress.gov 웹페이지, https://www.congress.gov/bill/114th-congress/senate-bill/2607, https://www.congress.gov/bill/115th-congress/senate-bill/88 (2019년 10월 23일 최종접속).

368) 공화당 상원의원 뎁 피셔(Deb Fischer), 켈리 아요트(Kelly Ayotte) 등과 코리 부커(Cory Booker), 브라이언 샤츠(Brian Schatz) 등 민주당 상원의원이 공동으로 발의하였다.

369) "Senate Panel Passes "Internet of Things" Bill", National Law 2016.4.28., https://www.natlawreview.com/article/senate-panel-passes-internet-things-bill (2019년 10월 23일 최종접속).

대한 공개의견을 수렴하였으며, 사물인터넷 관련 다양한 이슈 검토를 통해 의회에 유관산업의 발전을 위한 정책·제도적 제안을 권고할 수 있는 실무반(working group)[370]을 운영하도록 하였다.[371] 동 법안은 사물인터넷(IoT)에 관한 정책이 기업, 정부 및 소비자에게 이익이 되도록 사물인터넷이 네트워크에 연결되거나 상호 연결된 기기의 수가 증가함에 따라 잠재력과 개발을 극대화하는 것을 목적으로 한다(사물인터넷 관련 작업반 및 운영위원회 설치 등의 사물인터넷 혁신과 성장을 위한 법안 제2조). 동 법안에 의할 때 상무부(Department of Commerce)는 IoT에 관한 권고사항과 보고서를 의회에 제공하기 위해 실무반을 소집해야 하고, 실무반[372]에 조언하기 위해 연방정부 외부의 이해당사자로 구성된 운영위원회[373]를 설치해야 한다(동 법안 제4조). 또한 연방통신위원회는 (1) IoT용 주파수 요청, 규제 장벽, 면허 및 비면허 주파수의 증가에 대한 공개 의견을 구하고, (2) 해당 의견을 요약한 보고서를 의회에 제출해야 한다(동 법안 제5조).[374] 2016년 9월 27일에 상공·과학·교통위원회(Committee on Commerce, Science, and Transportation)는 법안 제목과 위원회 관련 내용 등을 수정하기 위한 논의를 진행했고,[375] 2017년 1월 10일 미국 상원에 수정안이 발의된 후 같은 해 8월 3일에 만장일치로 「사물인터넷의 혁신과 성장을 위한 법(DIGIT ACT, S.88)」[376]이 통과되었다. 동법은 사물인터넷을 지원하기 위한 적절한 범위의 계획을

370) 실무반은 교통부(Transportation Department), 상무부(Commerce Department), 연방통상위원회(Federal Trade Commission), 연방통신위원회(Federal communications Commission), 과학기술정책실(Office of Science and Technology Policy) 및 미국국립과학재단(National Science Foundation) 등의 대표를 포함하여 구성되었다.

371) 운영위원회는 IoT 활용 현황을 평가하여 산업저해 규제 도출, 소비자권익, 개인정보보호, 사이버보안 관련 개선방안을 마련할 수 있다. Congress.gov 웹페이지, https://www.congress.gov/bill/114th-congress/senate-bill/2607/text (2019년 10월 23일 최종접속).

372) 실무반은 (1) IoT 개발을 억제하는 연방법 및 규정, 보조금 관행, 예산 또는 관할권 과제 및 기타 부문별 정책을 파악하고, (2) IoT 관할 연방기관 간의 조정을 장려하고 개선하는 정책 또는 프로그램을 고려하며, (3) 운영위원회의 권고사항을 이행해야 한다. (4) 연방기관이 어떻게 IoT의 혜택을 얻거나 사용 또는 대비하거나 및 보안을 유지할 수 있는지 검토하며, (5) 비정부 이해당사자와 협의한다.

373) 운영위원회는 법률, 예산, 주파수의 필요성, 개인정보 보호, 보안, 중소기업 문제, IoT에 영향을 미치는 국제소송 또는 협상에 대해 실무반에 조언해야 한다.

374) 동 법안의 제정 후 18개월 이내에 실무그룹은 그 조사 결과와 권고사항, 운영위원회 권고안에 대한 조치의 이유 및 권고사항을 이행하기 위한 연방기관의 진행 상황을 보고해야 한다.

375) Congress.gov 웹페이지, https://www.congress.gov/bill/114th-congress/senate-bill/2607/text (2019년 10월 23일 최종접속).

376) Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/senate-bill/88 (2019년 10월 23일 최종접속).

세우고, 관할 기관 간 권한 조정을 보장하는 것을 포함하고 있다. 또한 실무반의 경우 운영위원회를 통해 사물인터넷의 다섯 가지 측면을 조사할 책임이 있는데, ① 사물인터넷 발전에 방해되는 연방규정, 예산, 관할권 문제 및 기타 정책의 파악(SEC. 4.(e)(2)(A)), ② 적절한 주파수 및 향후 주파수 제공을 위한 규제 장벽(SEC. 4.(e)(2)(B)), ③ 개인정보 보호, 인프라 보안, 소비자 보호, 연방정부 기관의 조정 등 정책 또는 프로그램(SEC. 4.(e)(2)(C)), ④ 중소기업의 사물인터넷 기술 사용과 관련된 과제(SEC. 4.(e)(2)(D)), ⑤ 미국이 당사자인 사물인터넷 관련 국제적 소송, 협상 등의 문제(SEC. 4.(e)(2)(E))가 그것이다. 이후 2019년 5월 22일에는 사물인터넷(IoT)의 확산을 위한 연방정부의 역할을 논하기 위해서 정부 실무반의 창설(Federal working group)을 요구하는 내용의 동법 개정안(DIGIT ACT, S.1611)이 상원에 발의되었다.[377]

한편 2017년 8월 1일에는 연방 정부에서 구매하는 IoT(Internet of Things) 디바이스에 대한 사이버보안(Cybersecurity)을 강화하기 위한 법안인 「사물인터넷 사이버보안 증진법(IoT Cybersecurity Improvement Act of 2017, S.1691)」[378]이 상원에 발의되기도 했다.[379] 아쉽게 채택되지는 못하였지만 그 내용을 살펴볼 필요가 있다. 우선 동 법안은 네트워크 기술과 사물인터넷 기술의 발전에 따라 무선통신기술이 탑재된 제품의 이용이 보편화되고 있으나, 현재의 데이터보안 수준은 소비자 이익이나 데이터 보호 및 사생활 보호에 충분하지 못하기 때문에 IoT 기기의 보안시스템 수준이 보다 향상되어야 한다고 언급하고 있다.[380] 이에 동 법안은 IoT 기기에 도입되어야 하는 최소한의 표준보안 수준을 연방정부가 제시함으로써 시장의 실패를 방지하는 것을 목적으로 한다고 밝히고 있다.[381] 다음으로 동 법안은 IoT 제조사들이 기기 제조 시 준수해야 하는 보안수준을 규정하면서,[382] 해당 의무가 부가되지 않는 예외

377) Congress.gov 웹페이지, https://www.congress.gov/bill/116th-congress/senate-bill/1611/text (2019년 10월 23일 최종접속).

378) Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act%22%5D%7D&r=1&s=10 (2019년 10월 23일 최종접속).

379) Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/senate-bill/1691/text (2019년 10월 23일 최종접속).

380) "Proposed Internet of Things Cybersecurity Bill May Create Hurdles for Government Contractors", Lexology 2017.8.11., https://www.lexology.com/library/detail.aspx?g=c0da944b-4c46-4812-8bbf-dbf2540db87f (2019년 10월 23일 최종접속).

381) Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/senate-bill/1691/titles (2019년 10월 23일 최종접속).

사유를 제시하고 있다.[383] 또한 산업계가 미국 국토안전부(Department of Homeland Security) 산하의 국가보호프로그램국(National Protection and Programs Directorate)과 협업해서 IoT 기기를 미국 정부에게 판매하는 제조사들이 준수해야 하는 가이드라인을 수립하도록 했으며, 제조사들로 하여금 동 가이드라인을 따르도록 함으로써 연구자들은 IoT 기기 보안의 취약점을 발견할 수 있고 이를 공유하도록 하였다. 나아가 동 법안은 「디지털밀레니엄법(Digital Millennium Copyright Act, DMCA)」 및 「컴퓨터 사기와 남용에 대한 법률(Computer Fraud and Abuse Act, CFAA)」을 개정하여 보안 연구자들과 기기 제조사들이 저작권법 침해나 컴퓨터 사기와 남용에 대한 법규 침해로부터 면책 받을 수 있도록 했으며, 취약점이 발견된 부분은 패치파일이나 하드웨어 교체 등의 방법으로 즉시 조치가 취해지도록 했다.

2019년 3월 11일에 상기의 법안과 그 취지를 같이하는 「사물인터넷 사이버보안 개선법 2019(Internet of Things Cybersecurity Improvement Act of 2019, S. 734, H.R.1668)」[384]이 상원과 하원에 발의되었다. 2017년 최초로 제안된 법안이 입법화에 실패한 상태에서 이를 수정한 동 법안이 발의된 것이다. 동 법안은 IoT 기기의 보안을 강화하기 위해 국립표준기술연구소(National Institute of Standards and Technology, NIST)가 보안 권고 사항 및 표준을 마련하고, 해당 보안 요건을 준수하는 기기의 공공구매를 촉진하는 것을 그 내용으로 하는바, 그 대상은 인터넷에 접속되어 데이터를 수집하거나 송·수신할 수 있는 IoT 기기이며, 스마트폰 및 범용 컴퓨터 장치는 포함되지 않는다. 동 법안은 국립표준기술연구소의 IoT 사이버보안 위험관리에 대한 권고 사항,[385] IoT 기기의 사용 및 관리에 대한 연방기관[386]의 정책,[387] IoT 기기

---

382) IoT 제조사는 자신들이 판매하는 IoT 기기에 패치파일이 설치될 수 있도록 해야 하며 IoT 기기의 보안에 결함이 있는 것으로 밝혀진 경우 이를 즉시 당국에 알려야 한다. IoT 기기는 표준 프로토콜(standard protocol) 수준을 준수해야 한다. IoT 기기는 보안수준이 낮은 비밀번호(hard-codded password: 비밀번호의 보안수준이 매우 낮음을 뜻하며 악의적인 이용자의 경우 쉽게 그 접근권한을 얻을 수 있는 비밀번호)를 사용해서는 안 된다.

383) 문제가 되는 IoT 기기의 특성상 위의 조치가 취해지기 어렵지만 네트워크 기술로 그 한계를 극복할 수 있는 경우에는 미국 예산관리국(Office of Management and Budget)에 해당 IoT 기기는 예외적으로 상기 조치의 적용범위에서 제외할 것을 요청할 수 있다. 또한 당국이 자체적으로 IoT 기기에 대한 적절한 수준의 보안을 유지하는 경우에는 예외적 사유에 해당된다.

384) Congress.gov 웹페이지, https://www.congress.gov/bill/116th-congress/senate-bill/734/text?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act+of+2019%22%5D%7D&r=1&s=1 (2019년 10월 23일 최종접속).

385) 국립표준기술연구소장은 법 제정 후 180일 이내에 IoT 기기의 보안 위험관리 고려사항에 대

보안 취약점 공개 지침[388] 및 보고 지침[389]에 관한 내용을 담고 있다. 2017년 상원에 제안된 '사물인터넷 사이버보안 개선법 2017(Internet of Things(IoT) Cybersecurity Improvement Act of 2017(S.1691))'은 IoT 기기의 암호와 소프트웨어 업데이트(보안 패치)에 초점을 맞춘데 반해, 동 법안은 IoT 기기의 보안 요건을 강화하는데 목표를 두고 국립표준기술연구소가 보안 요건과 표준을 마련하도록 규정하였다. 요컨대 동 법안이 통과되면 연방기관뿐만 아니라 민간 부문에서도 해당 권고 사항 및 표준을 따를 것으로 예상되므로 전반적인 IoT 보안 수준이 향상될 것으로 기대되고 있다고 한다.[390] 이후 동 법안은 2019년 6월 19일 상원 소관 위원회(Committee on Homeland Security and Governmental Affairs) 회의에서 논의되었고,[391] 2019년 9월

한 보고서 초안을 마련하고, 연방기관이 소유하거나 통제하는 사물인터넷 기기의 적절한 사용과 관리를 위해 최소한의 보안요건이 규정된 표준 및 권고 사항을 2020년 3월 31일까지 개발해야 한다.

386) 44 USC 3502: Definitions의 기관으로 행정부, 군부, 정부 관리 법인 또는 정부 집행부의 다른 기관(대통령 집행부 포함) 또는 독립적인 규제기관이 해당한다. Office of the Law Revision Counsel of the United States House of Representatives 웹페이지, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title44-section3502(8)&num=0&edition=prelim (2019년 10월 23일 최종접속).

387) 국립표준기술연구소장이 권고 사항의 개발을 완료한 날로부터 180일 이내에 관리예산국장은 해당 권고 사항에 따른 지침을 각 연방기관에 배포해야 한다. 관리예산국장은 해당 지침이 미국 법전에 명시된 정보보안 관련 규정(44 U.S. Code Chapter 35, Subchapter II)에 잘 부합되는지 확인해야 한다. 관리예산국장과 국립표준기술연구소장은 서로 협의하여 지침을 검토 및 수정해야 한다.

388) 국립표준기술연구소장은 법 제정 후 180일 이내에 민간 부문 전문가와 협의하여 IoT 기기의 보안 취약점 공개 절차 및 방법에 대한 지침을 개발하고, 누구나 열람할 수 있도록 연구소 홈페이지 등에 게시해야 한다. 제품과 서비스 등의 취약점 공개 국제표준(ISO/IEC 29147)과 처리절차(ISO/IEC 30111)를 고려하여 작성한다. 동 지침에는 연방정부에 IoT 기기를 제공하는 계약자 또는 공급업체의 보안 취약점 공개를 위해 생성해야 하는 정보 항목과 해결 방안이 포함되어야 한다.

389) 관리예산국장은 사이버보안 위험관리 권고 사항에 따른 지침이 발표된 후 180일 이내에 조달청장과 협의하여 각 연방기관에게 보안취약점 보고 지침을 제공해야 한다. 공공조달에 참여하는 계약자 또는 공급업체는 보안 취약점 공개 지침을 준수해야 한다. 연방기관은 보안 취약점 공개 지침을 준수하지 않은 계약자와 공급업체로부터 IoT 기기를 취득 또는 사용하는 것이 금지된다.

390) "New Federal IoT Security Bill Has Narrower Scope, But Big Impact", LAW.COM, Legaltech News 2019.3.13., https://www.law.com/legaltechnews/2019/03/13/new-federal-iot-security-bill-has-narrower-scope-but-big-impact/?slreturn=20190919010336 (2019년 10월 23일 최종접속).

391) 위원회의 의장인 론 존슨(Ron Johnson)의원은 IoT 정의 규정 삭제, IoT 기기에 대한 관리예산실(Office of Management and Budget, OMB)의 지침 개발 및 보안 취약점 공개 프로그램(Vulnerability Disclosure Program, VDP)에서 국토안보부(Department of Homeland Se curity, DHS)의 역할을 명확히 한 수정안을 제안하였으며, 론 존슨의 수정안은 호의적으로 보고되었다. Congress.gov 웹페이지, https://www.congress.gov/congressional-report/116th-congress/senate-report/112 (2019년 10월 23일 최종접속).

23일 일반 명령(General Orders)에 의해 상원 입법 일정표에 상정되었다.[392]

미국 하원에서는 2018년 6월 7일 발의된 「IoT의 현대적 적용, 연구 및 현황에 관한 법안(State of Modern Application, Research, and Trends of IoT Act(SMART IoT Act), HR 6032)」이 2018년 11월 28일에 통과되었다.[393] 동 법안은 IoT 기술과 관련된 다양한 제도(정책적 고려사항)를 마련하기 위한 중요한 첫 걸음이라고 그 의미가 부여되었다. 이후 동법은 11월 29일에 상원의 상공·과학·교통위원회에 회부되었는데,[394] 향후 검토 후 표결을 거치게 될 예정이라고 한다. 동 법안에 의하면 상무부 장관은 통상 사물인터넷(IoT)으로 알려진 미국의 인터넷 커넥티드 디바이스 산업 현황을 조사해야 하는데,[395] ① 사물인터넷 기기를 개발하는 산업 분야의 목록과 ② 사물인터넷 기기에 대한 의무적·자발적 표준을 개발하였거나 개발 중인 국제기구나 산업단체, 그리고 사물인터넷 기기의 도입이나 사용을 촉진하고자 하는 민관협력에 대한 목록, ③ 산업계의 의무적·자발적 표준 현황, ④ 사물인터넷 기기의 개발이나 사용 또는 그 사용을 촉진하는 방법 등에 대한 설명이 포함되어야 한다((SEC. 2. Study and report on Internet of Things (a)(1)). 또한 상무부 장관은 동 조사를 통해 확인된 기업과 산업 부문에 대해서 관할권을 가지는 연방기관에 대한 포괄적인 목록을 작성해야 하고((SEC. 2. Study and report on Internet of Things (a)(2)), 기업이나 산업 부문과 상호 작용을 하는 연방기관을 확인해야 하며(SEC. 2. Study and report on Internet of Things (a)(3)), 관할권을 가지는 연방기관들 간에 이루어지는 (실무그룹이나 여타의 공동 활동과 같은) 활동 사항을 파악해야 한다(SEC. 2. Study and report on Internet of Things (a)(4)).[396] 아울러 상무부 장관은 기업 및 산업 부문과 관련된

392) Congress.gov 웹페이지, https://www.congress.gov/bill/116th-congress/senate-bill/734/all-actions?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act+of+2019%22%5D%7D&r=1&overview=closed#tabs (2019년 10월 23일 최종접속).

393) Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/house-bill/6032 (2019년 10월 23일 최종접속).

394) Congress.gov 웹페이지, https://www.congress.gov/bill/116th-congress/senate-bill/734/all-actions?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act+of+2019%22%5D%7D&r=1&overview=closed#tabs (2019년 10월 23일 최종접속).

395) State of Modern Application, Research, and Trends of IoT Act(SMART IoT Act), H.R.6032, SEC. 2. Study and report on Internet of Things (a), Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/house-bill/6032/text (2019년 12월 9일 최종접속).

연방기관의 관할권과 전문성에 대한 간략한 설명을 해야 하며(SEC. 2. Study and report on Internet of Things (a)(5)), 산업단체에 의해서 시행되는 모든 지침이나 의무적·자발적 표준 및 기타 정책은 물론이고, 관할권이 있는 것으로 확인된 개별 연방기관이 시행하는 모든 규정과 지침, 의무적·자발적 표준 및 여타의 정책들을 모두 확인해야 하며(SEC. 2. Study and report on Internet of Things (a)(6)), 소비자와 소규모 기업이 사물인터넷 기기를 평가하는 데 쓰일 수 있는 연방정부의 재원도 파악해야 한다(SEC. 2. Study and report on Internet of Things (a)(7)),[397] 한편 상무부 장관은 동법이 제정된 날로부터 1년 이내에 위의 조사 결과와 함께 인터넷 커넥티드 디바이스의 안전한 발전을 통하여 미국의 경제 성장을 도모할 수 있는 권고가 포함된 보고서를 하원의 에너지·상업위원회 및 상원의 상공·과학·교통위원회에 제출해야 한다(SEC. 2. Study and report on Internet of Things (b)).[398]

(2) 캘리포니아 주

캘리포니아 주는 IoT 장치에 사이버보안 기능 탑재를 법적으로 규정한 미국 최초의 주이다. 2018년 8월 28일 캘리포니아 주에서는 일명 'IoT 보안법'으로 알려진 「SB-327 Information Privacy: Connected Devices」 법안이 발의되었고, 상·하원 의회의 투표를 거쳐서 2018년 8월 29일에 최종 통과되었다.[399] 같은 해 9월 28일에 주지사가 최종 서명을 하면서 2020년 1월 1일부로 발효될 예정이다.[400] 동법은 보안 기능이

---

396) State of Modern Application, Research, and Trends of IoT Act(SMART IoT Act), H.R.6032, SEC. 2. Study and report on Internet of Things (a), Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/house-bill/6032/text (2019년 12월 9일 최종접속).

397) State of Modern Application, Research, and Trends of IoT Act(SMART IoT Act), H.R.6032, SEC. 2. Study and report on Internet of Things (a), Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/house-bill/6032/text (2019년 12월 9일 최종접속).

398) State of Modern Application, Research, and Trends of IoT Act(SMART IoT Act), H.R.6032, SEC. 2. Study and report on Internet of Things (a),SEC. 2. Study and report on Internet of Things (b), Congress.gov 웹페이지, https://www.congress.gov/bill/115th-congress/house-bill/6032/text (2019년 12월 9일 최종접속).

399) California Legislative Information 웹페이지, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (2019년 10월 23일 최종접속).

400) 이는 Title 1.81.26 SECURITY OF CONNECTED DEVICES 부분으로서, 정보프라이버시와 관련하여 민법 제3장 제4부에 추가되는 내용이다. Douglas G. Bonner/Richard J. Caira, Jr., "California Bill Mandates Privacy By Design For IoT Devices", The NATIONAL LAW REVIEW 2017.4.27., National Law Forum, https://www.natlawreview.com/article/california-bill-mandates-privacy-design-iot-devices (2019년 7월 15일 최종접속).

거의 전무한 채로 생산되는 IoT 장비들을 막기 위한 것으로서 정보 연결장치[401]를 판매하는 자 등은 합리적 보안기능을 갖추어야 하고, 관련 정보를 소비자에게 통지해야 하며,[402] 개인정보의 수집 또는 전달 전에 소비자의 동의를 받도록 규정하고 있다.

캘리포니아 주 SB 327(Information Privacy: Connected Devices)
제886장 (CHAPTER 886)

법제실의 요약

현행법은 사업체가 고객 정보를 더 이상 보관할 수 없는 경우, 개인정보를 포함한 고객정보를 파쇄, 삭제, 또는 해당 정보를 읽을 수 없거나 판독할 수 없도록 수정하는 등의 방법으로 고객 기록을 처리하기 위한 모든 합리적 조치를 취할 것을 요구하고 있다. 또한 현행법은 사업체를 소유하거나, 면허를 받거나 또는 캘리포니아 주민에 관한 개인정보를 보유하는 사업자가 개인정보에 대한 무단 접근, 이용, 수정 또는 누설하는 것을 막기 위해서 해당 정보의 속성에 적합한 보안 절차와 실행방안을 강구할 것을 요구한다. 현행법은 이러한 규정 위반에 의해 손해를 당한 소비자에게 민사상 손해배상소송을 제기할 수 있는 권리를 부여하고 있다.

2020년 1월 1일부터 시행되는 이 법안은, 용어에서 정의된 바와 같이, 연결장치의 제조업체에게 연결장치의 특성과 기능에 적합하고, 해당 장치가 수집, 포함 또는 전송하는 정보에 적합한 보안기능을 탑재할 것과 무단 접근, 파괴, 사용, 수정 또는 누설로부터 해당 장치에 내재된 정보를 보호하도록 설계할 것을 요구하는 것이다.

이 법안은 2017-18년 회기의 AB 1906 법안이 제정되어 발효하여야 시행된다.

제1조 제1.81.26편(Title 1.81.26)[제1798.91.04조(Section 1798.91.04)로 시작하는]은 민법전(Civil Code)의 제3장(Division 3)의 제4부(Part 4)에 추가된다.

제1.81.26편. 연결된 장치의 보안

제1798.91.04조 (a) 연결장치의 제조사는 연결장치에 합당한 보안 기능 또는 다음의 조건을 모두 만족시킬 수 있는 보안 기능을 탑재하여야 한다:
(1) 장치의 본질과 기능에 적합할 것
(2) 연결장치가 수집, 포함 또는 전송할 수 있는 정보에 적합할 것
(3) 연결장치 및 해당 장치에 포함된 모든 정보에 무단으로 접근하거나, 파괴, 사용, 수정 또는 공개로부터 보호하도록 디자인되어 있을 것
(b) (a)항의 모든 요건을 충족한 경우에, 만약 연결장치가 근거리통신망(LAN) 외부의 인증을 위한 장치가 탑재되어 있다면, 다음의 요구조건 중 하나라도 충족하는 경우에는 (a)항에 따른 합리적인 보안기능을 탑재하고 있는 것으로 간주된다.
(1) 제조된 장치마다 고유한 사전 프로그래밍된 암호가 존재하는 경우
(2) 해당 장치에 대한 최초의 접근 권한이 부여되기 전에, 사용자가 새로운 인증 수단을 생성해야 하는 보안 기능이 포함된 경우

401) Section 1798.91.04의 '연결장치'는 직·간접적으로 인터넷에 연결될 수 있거나 다른 연결장치에 연결될 수 있는 모든 기기, 센서 또는 여타의 물리적 사물을 의미한다.
402) 장치가 수집하는 다양한 개인정보의 종류, 기기의 개인정보 수집 절차 및 수집 빈도, 장치와 상호작용 하는 다른 기기의 종류, 연결장치에 대한 보안 패치와 기능 업데이트 방법 등에 대한 모든 정보를 제공해야 한다.

캘리포니아 주 SB 327(Information Privacy: Connected Devices)
제886장 (CHAPTER 886)

제1798.91.05조 이 장에서 사용하는 용어의 뜻은 다음과 같다.
(a) "인증"이란 정보 시스템의 리소스에 접근하기 위하여 사용자, 프로세스 또는 장치의 권한을 확인하는 방법을 말한다.
(b) "연결된 장치"란 인터넷에 직접 또는 간접적으로 연결할 수 있고 인터넷 프로토콜(IP) 주소 또는 블루투스(Bluetooth) 주소가 할당된 장치 또는 기타 물리적 장치를 말한다.
(c) "제조업체"란 캘리포니아 내에서 판매되거나 판매를 위하여 공급된 연결장치를 제조한 자 또는 위탁 생산 계약을 한 자를 말한다. 본 항의 해석상 위탁 생산 계약에는 연결장치를 단지 구매하는 계약 또는 연결장치를 구매 및 상표화하는 계약은 포함되지 않는다.
(d) "보안 기능"은 해당 장치에 보안을 제공하도록 설계된 기능을 말한다.
(e) "무단 접근, 파기, 사용, 수정 또는 공개"란 소비자에 의해 승인되지 않은 접근, 파기, 사용, 수정 또는 공개를 말한다.

제1798.91.06조 (a) 사용자가 연결장치에 추가한 독립적 타사 소프트웨어 또는 응용프로그램과 관련된 연결기기의 제조자에게도 의무를 부과하고 있는 것으로 해석되어서는 아니 된다.
(b) 전자 상점, 게이트웨이, 마켓플레이스 또는 소프트웨어나 응용 프로그램의 구매·다운로드를 제공하는 자에게도 이 편의 규정을 준수하거나 검토하여야 할 의무를 부과하고 있는 것으로 해석되어서는 아니 된다.
(c) 연결장치의 제조사에게 해당 장치의 사용자가 재량으로 그 장치에서 실행되는 소프트웨어나 펌웨어를 수정하는 행위를 포함해 연결장치를 완전히 제어하는 것을 방지할 의무를 부여한 것으로 해석되어서는 아니 된다.
(d) 연방법이나 규칙 또는 법집행기관에 의해 연방기관에서 공표한 지침에 따른 보안요건을 준수하여야 하는 연결장치 기능에는 적용되지 않는다.
(e) 사적 권리의 근거로 해석되어서는 아니 된다. 법무부장관, 시변호사, 자치구 변호사 또는 지방검사가 이 편의 집행에 대한 독점적 권한을 가진다.
(f) 이 편에 따라서 부과된 의무와 책임은 타법에 의해 부과된 의무나 책임에 병과되며, 일방 당사자에게 타법에 의해 부과된 의무와 책임을 경감시켜 주는 것으로 해석되어서는 아니 된다.
(g) 법률 또는 관할 법원의 명령에 따라 제조업체로부터 연결장치의 정보를 획득할 수 있는 법집행기관의 권한을 제한하기 위하여 원용되어서는 아니 된다.
(h) 피보험자, 의료서비스제공자, 사업자, 의료서비스 계획, 계약자, 고용주, 기타 「1996년 연방의료보험 이동성 및 책임에 관한 법률」[the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191)] 또는 「의료정보비밀에 관한 법률」[the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1)]의 대상이 되는 자는 그러한 법률에 규정된 행위와 관련하여 이 편의 적용을 받지 않는다.
(i) 이 편은 2020년 1월 1일부터 시행한다.

제2조 이 편은 2017-18년도 정기 의회의 제1906호 법률안(Assembly Bill 1906)이 제정되고 발효된 경우에만 시행된다.

2) 유럽연합

유럽 전기통신표준협회(European Telecommunication Standards Institute, ETSI)는 인터넷에 연결된 가전제품의 보안 기준을 수립하고, 향후 IoT 인증체계의 기반을 제공하기 위해 2019년 2월 19일 「소비자 IoT 보안 표준(Cyber Security for Consumer

Internet of Things(ETSI TS 103 645, 2019)」을 발표하였다.[403] 이 표준은 지난 2018년 12월에 유럽의회와 유럽이사회 및 유럽연합집행위원회가 최종 합의한 「EU 사이버보안법(EU Cybersecurity Act)」[404]에서 도입된 유럽 사이버보안 인증 프레임워크[405]의 구현을 지원하기 위한 것으로, 소비자 IoT와 관련하여 공급업계에 최초로 적용되는 산업표준이다. 동 보안표준은 인터넷에 연결된 카메라, TV 및 스피커, 홈 자동화 및 경보 시스템, 연기 감지기 및 도어 잠금장치, 냉장고와 세탁기 등 일반 가정에서 사용되는 IoT 기기를 개발 및 제조하는 공급자를 대상으로 하며, 공급자에게 권고하는 주요 보안 규정은 범용 기본 암호의 사용 금지, 보안 취약점의 관리 및 보고, 지속적인 소프트웨어의 업데이트, 보안에 민감한 데이터의 안전한 저장 등 13개의 세부조항으로 구성되어 있다.[406]

유럽연합 소비자 사물인터넷(IoT) 보안 표준[407]

4. 소비자 사물인터넷(IoT)에 대한 사이버보안 규정

(4.1) 범용 기본 암호 사용 금지
모든 사물인터넷 장치의 암호는 고유해야 하고, 암호 변경 시 사용자는 제조업체에서 출하할 당시의 기본값(예상 가능한 값)으로 재설정할 수 없어야 한다.

403) "ETSI releases first globally applicable standard for consumer IoT security", ETSI 2019.2.10., https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security (2019년 10월 23일 최종접속); ETSI, CYBER; Cyber Security for Consumer Internet of Things, ETSI TS 103 645 V1.1.1 (2019-02), https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (2019년 10월 23일 최종접속).

404) EU 사이버보안법은 개정작업을 통해 2019년 3월 12일 승인되었으며, 같은 해 6월 27일부터 발효되었는데, 유럽 사이버보안 인증 프레임워크를 제정하고 EU의 사이버보안 기관인 ENISA의 새로운 권한을 설정하고 있다. "The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification", European Commission News 2019.6.26., https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity (2019년 10월 23일 최종접속); EUR-Lex 웹페이지, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC (2019년 10월 23일 최종접속).

405) IoT 제품 및 서비스 공급자들이 설계 단계에서부터 보안 기능을 반영토록 하는 '보안 내재화(security by design)'를 포함하며, 유럽 전체에 보편적으로 적용할 수 있는 사이버보안 인증을 법제화한 것이다.

406) IoT ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things, pp.8-13, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (2019년 10월 23일 최종접속).

유럽연합 소비자 사물인터넷(IoT) 보안 표준[407]

(4.2) 취약성 보고 관리를 위한 수단의 구현
인터넷에 연결할 수 있는 장치와 서비스를 제공하는 모든 회사는 다른 사용자가 보안 취약성 등 문제를 정부에 보고할 수 있도록 취약성 공개 정책의 일환으로 공개 연락처를 제공해야 하며, 공개된 취약점은 적시에 조치를 취해야 한다.

(4.3) 소프트웨어 업데이트 유지관리
인터넷에 연결된 장치의 모든 소프트웨어 구성요소는 안전하게 업데이트할 수 있어야 하고, 업데이트는 적절한 시기에 이루어져야 하며 업데이트 중에도 장치의 기본기능에 영향을 주지 않아야 한다. 또한 제품의 수명주기 정책(end-of-life policy)은 네트워크의 말단에 접속된 장치에 대해 게시되어 장치가 소프트웨어 업데이트를 수신하는 최소 시간과 지원 기간에 대한 이유를 명시적으로 표시해야 하고, 각 업데이트의 필요성을 소비자에게 명확히 설명해야 하며, 업데이트의 실행이 용이해야 한다.

(4.4) 인증서 및 보안에 민감한 데이터의 안전한 저장
모든 인증서와 보안에 민감한 데이터[408]는 서비스 및 장치 내 저장소 등을 통해 안전하게 저장되어야 하고, 장치의 소프트웨어에서 하드 코딩된 인증서는 사용해서는 아니 된다.

(4.5) 안전한 의사소통
원격관리 및 제어를 비롯하여 보안에 민감한 데이터는 전송 중에도 암호화되어야 하며 사용 속성에 적합하여야 하고, 모든 키는 안전하게 관리되어야 한다.

(4.6) 공격 취약 부분의 최소화
장치와 서비스는 최소 권한의 원칙(principle of least privilege)[409]이 적용되어야 하는데, 사용되지 않은 소프트웨어 및 네트워크 포트는 닫혀 있어야 하고, 하드웨어는 불필요한 접근에 노출되어서는 안 되며, 사용되지 않는 소프트웨어 서비스는 제공하지 않고, 서비스/장치가 작동하는데 필요한 기능으로 코드를 최소화해야 한다. 또한 소프트웨어는 보안과 기능 모두를 고려하여 적절한 권한으로 실행하여야 한다.

(4.7) 소프트웨어 무결성 보장
보안부팅 메커니즘(secure boot mechanisms)을 사용하여 사물인터넷 장치의 소프트웨어를 검증해야 하고, 무단 변경이 감지되면 장치는 소비자, 관리자에게 문제를 경고해야 하며, 경고 기능을 수행하는 데 필요한 것보다 확장된 네트워크에 연결해서는 아니 된다.

(4.8) 개인정보 보호 보장
장치 및 서비스가 개인정보를 처리하는 경우 일반데이터보호규정(General Data Protection Regulation, GDPR)[410]과 국가별 개인정보보호 관련 법령을 준수하여 개인정보를 보호해야 하고, 장치 제조업체 및 서비스 제공업체는 각 장치와 서비스에 대해 개인정보를 누구에 의해 어떠한 목적으로 어떻게 사용되고 있는지 소비자에게 명확하고 투명한 정보를 제공해야 하고, 이는 광고주를 포함하여 제3자에게도 적용된다. 또한 개인정보가 소비자의 동의를 바탕으로 처리되는 경우 이 동의는 유효한 방법으로 확보되어야 하고 소비자는 언제나 동의를 철회할 수 있어야 한다.

(4.9) 전원 중단 시 시스템 복원
데이터 네트워크 및 전원 중단의 가능성을 고려하여 복원기능은 사용시 필요하거나 다른 사용 시스템에서 필요한 사물인터넷 장치 및 서비스에 구축되어야 하고, 사물인터넷 서비스는 합리적으로 가능한 한 서비스 네트워크의 연결이 끊길 경우 정상적으로 로컬기능이 작동할 수 있도록 해야 하며, 전원 중단상태에서 복구할 경우에도 작동되어야 한다. 장치는 대규모 재연결이 아닌 예상가능하고 작동될 수 있는 안정적 상태에서 정상적 방식으로 네트워크에 복귀할 수 있어야 한다.

(4.10) 시스템 원격 측정 데이터 검사
사물인터넷 장치 및 서비스에서 사용·측정되는 데이터와 같이 원격으로 측정되는 데이터를 수집하는 경

유럽연합 소비자 사물인터넷(IoT) 보안 표준[407]
우에는 보안 위험에 대해 모니터링이 이루어져야 하고, 원격 측정 데이터를 수집할 경우 소비자에게 수집되는 데이터 및 수집의 이유에 대한 정보를 제공해야 한다. (4.11) 소비자를 위한 용이한 개인데이터 삭제 개인데이터의 소유권 이전이 있을 때, 소비자가 데이터를 삭제하고자 할 때, 소비자가 장치를 폐기하고자 할 때 등 소비자가 개인정보를 쉽게 삭제할 수 있도록 IoT 장치 및 서비스를 구성해야 하고, 소비자에게 개인정보 삭제 방법에 대한 명확한 지침을 제공해야 한다. (4.12) 손쉬운 장치 설치 및 유지관리 IoT 장치의 설치 및 유지관리는 최소한의 단계를 거쳐야 하고, 보안 모범 사례에 따라야 한다. 또한 소비자에게 안전하게 장치를 설치하는 방법에 대한 지침을 제공해야 한다. (4.13) 입력 데이터 유효성 검증 사용자 인터페이스를 통해 데이터가 입력되고 어플리케이션 프로그래밍 인터페이스(Application Programming Interfaces, API)를 통해 서비스와 장치의 네트워크 사이에서 전송된 데이터는 유효성 검사를 해야 한다.

3) 일본

2016년 일본은 인터넷 등 정보통신 네트워크를 통해서 유통되고 있는 다양한 정보를 효과적으로 활용할 수 있는 환경을 조성하고자 「관민데이터 활용 추진 기본법(官民データ活用推進基本法)」을 제정하였다.[411] 동법은 일본 법률상 최초로 인공지능(AI)

407) IoT ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things, pp.8-13, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (2019년 10월 23일 최종접속).

408) 암호화 키, 장치 식별자, 초기화 벡터 등 장치 또는 서비스의 보안과 관련된 데이터를 말한다.

409) 최소 권한의 원칙(principle of least privilege)이란 모든 사용자에게는 허락된 작업들을 수행하는데 필요한 최소한의 권한만을 주어지도록 하는 것이 보안에 유용하다는 원칙이다.

410) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation).

411) 「유럽의 경우 데이터는 개인의 것이라는 기본적 사고방식 하에 데이터 이동권(Date Portability)을 개인의 권리로서 인정하고 있으나, 일본의 경우에는 데이터에 대한 개인의 소유권 개념이 명확하게 정립되지 않고 있다. 따라서 개인의 금융데이터나 의료데이터 및 운전데이터 등 다양한 데이터를 활용하는 것이 현실적으로 어렵다. 유럽처럼 데이터에 대한 개인의 소유권이 명확하게 인정된다면, 개인의 의사에 따라 그 데이터를 쉽게 다른 회사에 이전하는 것이 가능하다. 그런데 일본의 경우 데이터에 대한 개인소유권을 인정하지 않고 있으며, 따라서 정부나 특정 회사가 이미 보유하고 있는 특정 개인의 데이터를 그 개인의 의사로 다른 회사가 사용할 수 있도록 할 수 없기 때문이다. 이에 일본은 인터넷 등에 유통되고 있는 다양한 개인 데이터를 활용하기 쉬운 환경을 정비하기 위하여 2016년 「관민데이터 활용 추진 기본법(官民データ活用推進基本法)」을 제정하였다.」라고 그 입법 취지가 언급되고 있다. 內閣官房 情報通信技術(IT)

이나 사물인터넷(IoT) 등에 대한 정의 규정을 두고 있다는 점에서 주목되는데,[412] 이에 의할 때 '사물인터넷 활용 관련 기술'이란 '인터넷 상에 다양한 다수의 사물 연결되어, 그 사물로부터 송신되거나 또는 그 사물에 수신되는 대량 정보의 활용과 관련된 기술'로 정의된다.[413]

2014년에는 개인 등의 데이터 활용을 원활하게 하기 위한 전제조건으로서 「사이버시큐리티기본법(サイバーセキュリティ基本法)」을 제정하여 데이터 유통을 위한 사이버보안을 강화하였다.[414] 동법은 국가 사이버보안 정책의 기본 원칙 수립, 국가 그리고 지방 정부 및 기타 관련 당사자의 책임 소재 확정, 필수적인 사이버보안 관련 정책 규정, 그리고 사이버보안 전략본부의 설립을 목적으로 한다.[415] 2018년 12월 일본 의회는 2020년 도쿄 올림픽 및 패럴림픽 개최 기간 중 우려되는 사이버 공격에 대한 보안을 보장하기 위해서 동법을 개정하였다.[416] 개정법에 따라 일본 정부는 사이버보안 조치의 촉진을 논의하는 '사이버보안 협의회'를 설립했는데,[417] 위원회는 국가 정부 기관, 지방 정부, 중요 정보 인프라 운영자, 사이버 공간과 관련된 사업 단체, 교육 및 연구 기관 등으로 구성된다(サイバーセキュリティ基本法 第17条). 또한 사이버 시큐리티 전략본부는 앞으로 내각의 명령에 의해 그 기능의 일부를 정보통신진흥청과 같은 기관에게 위임할 수 있게 된다. 이 위임 기능에는 국가 행정 기관에 대한 사이버보안 조치 관련 표준의 제정, 감사를 포함한 평가 조치의 이행 촉진, 사이버보안 위반 및 위협 발생 시 일본 및 해외의 관련 개인 및 단체와의 조정 등이 포함된

總合戰略室, 「官民データ活用推進基本法について」, http://www.pref.okayama.jp/uploaded/life/501302_3729515_misc.pdf (2019년 12월 9일 최종접속).

412) 井出一仁, "「官民データ活用推進基本法」が成立、AIやIoTも法律で初めて定義", 新・公民連携最前線 ュース, 日経BP 2016.12.9., https://project.nikkeibp.co.jp/atclppp/PPP/news/120800115/ (2019년 12월 9일 최종접속).

413) 官民データ活用推進基本法 第二条 (定義) 3, e-Gov法令検索, https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=428AC1000000103 (2019년 12월 9일 최종접속).

414) "「サイバーセキュリティ基本法」が全面施行、NISCは省庁横断の司令塔に", 日経 xTECH 2015.1.13., https://tech.nikkeibp.co.jp/it/atcl/news/15/011300129/ (2019년 10월 23일 최종접속).

415) e-Gov法令検索, https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=428AC1000000103 (2019년 10월 23일 최종접속).

416) 参議院 議案情報, https://www.sangiin.go.jp/japanese/joho1/kousei/gian/197/meisai/m197080196045.htm; https://www.sangiin.go.jp/japanese/joho1/kousei/gian/197/pdf/k0801960451970.pdf (2019년 10월 23일 최종접속).

417) "NISC「サイバーセキュリティ協議会」が新たに発足、世界的にも先進的な組織へ", Trend Micro News 2019.4.2., https://www.is702.jp/news/3472/ (2019년 10월 23일 최종접속).

다(同法 第26条, 第31条).

한편 IoT 기기의 보급률이 높아짐에 따라서 IoT 기기를 겨냥한 사이버 공격은 최근 증가 추세에 있고, 국외에서도 IoT 기기를 악용한 대규모 사이버 공격(DDoS 공격)을 통한 인터넷 장애 등 심각한 피해가 발생하고 있는바, 2020년 도쿄 올림픽·패럴림픽을 앞두고 일본에서는 그 대책 마련의 필요성이 커졌다. 이에 도쿄 올림픽을 지원하는 인프라를 겨냥한 사이버 공격에 IoT 기기가 이용되는 것을 막기 위해[418] 사이버 공격 대책의 일환을 마련하였는바, 가정이나 기업에 있는 인터넷 가전 등 IoT 기기에 침입해서 보안이 충분한지에 대한 조사를 실시하는 것이다.

「IoT 기기조사 및 이용자의 주의 환기 NOTICE(IoT機器調査及び利用者への注意喚起「NOTICE(National Operation Towards IoT Clean Environment)」라 명명된 동 조사는 2019년 2월 20일부터 총무성의 감독 하에 정보통신연구기구(NICT)가 시행하는데,[419] 정보통신연구기구의 담당자에게는 기본 암호(Default Password)와 암호사전을 이용해서 IoT 디바이스의 해킹을 시도할 수 있는 권한이 부여된다.[420] 대부분의 경우 제품 출고 시에 설정된 패스워드가 그대로 사용됨으로써 디바이스가 침해되고 있는바, 당해 조사를 통해서 취약한 디바이스가 발견되면 소유자에게 보안조치를 촉구하는 한편, 당국과 ISP 양쪽 모두에 리포트가 송신된다고 한다.[421] 그러나 이에 대해서는 실질적으로 해킹과 다르지 않은 행위를 국가가 실시한다는 점에서 전 세계적으로 유례를 찾아볼 수 없는 조사라는 비판이 제기되고 있다.[422]

---

418) 실제로 재작년 1년간 정보통신연구기구가 관측한 사이버공격의 대략 54%가 IoT 기기를 타겟으로 삼고 있었으므로 정부는 도쿄 올림픽을 위한 대책을 강화할 필요가 있다고 하고 있다. "「通信の秘密に抵触のおそれ」無差別侵入し調査へ", NHK 2019.1.25., https://www.nhk.or.jp/politics/articles/statement/13452.html (2019년 10월 23일 최종접속).

419) 総務省, 国立研究開発法人情報通信研究機構, "IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施", 2019.2.1., https://www.nict.go.jp/press/2019/02/01-1.html (2019년 10월 23일 최종접속).

420) 総務省 国立研究開発法人情報通信研究機構, IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施, 2019.2.1., https://www.nict.go.jp/press/2019/02/01-1.html (2019년 10월 23일 최종접속).

421) "日本におけるIoTデバイスのハッキング許可をする法律", iedge 2019.2.4., https://iedge.tech/news/7221/ (2019년 10월 23일 최종접속); "Japan's law now allows it to hack people's IoT devices", IoT News 2019.1.29., https://www.iottechnews.com/news/2019/jan/29/japan-law-hack-iot-devices/ (2019년 10월 23일 최종접속).

422) "「通信の秘密に抵触のおそれ」無差別侵入し調査へ", NHK 2019.1.25., https://www.nhk.or.jp/politics/articles/statement/13452.html (2019년 10월 23일 최종접속).

동 조사의 실시를 위해 「전기통신사업법 및 국립연구개발법인 정보통신연구기구법의 일부를 개정하는 법률(電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律)」을 2018년 5월 개정하여 2018년 11월 1일부터 시행하였는데,[423] 동 개정법률 중 정보통신연구기구법의 일부를 개정하는 법률(国立研究開発法人情報通信研究機構法の一部改正) 제2조에서 타인의 IoT 기기에 ID와 패스워드를 입력하는 부정 액세스를 금지하나 정보통신연구기구(NICT)는 5년 동안 한시적으로 그 적용을 받지 않도록 규정하였다.[424] 또한 동 조사는 총무성의 감독 하에 정보통신연구기구가 실시하는데, 조사 업무를 실시함에 있어 필요한 입력 식별부호의 기준 및 인가 수속 등 관련 내용을 규정하기 위해서 국립연구개발법인 정보통신연구기구법 부칙(国立研究開発法人情報通信研究機構法附則) 제8조 제4항 제1호 및 제9조에서 규정하는 총무성령(総務省令)을 제정하기로 하였다.[425]

나. 국내 현황

1) 가이드라인 수립

2014년 5월 8일 정부는 '초연결 디지털 혁명의 선도국가 실현'이라는 비전으로 '사물인터넷 기본계획'을 발표하였다.[426] 전 세계 인터넷에 연결된 사물의 수가 비약적으로 증가하는 것에 주목한 정부는 사물인터넷 관련 국가전략을 수립하였는바,

---

423) 参議院 議案情報, https://www.sangiin.go.jp/japanese/joho1/kousei/gian/196/meisai/m196080196033.htm (2019년 10월 23일 최종접속).

424) 参議院 議案情報, https://www.sangiin.go.jp/japanese/joho1/kousei/gian/196/pdf/s0801960331960.pdf (2019년 10월 23일 최종접속).

425) 総務省, 報道資料, http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00002.html, http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00003.html (2019년 10월 23일 최종접속).

426) 우리 정부는 2013년부터 미래를 바꿀 4대 정보통신 기술로 ① 사물인터넷, ② 클라우드 컴퓨팅, ③ 빅데이터, ④ 모바일 인터넷을 선정하고, 이들 산업의 육성 정책을 추진해 왔는데, 2014년에는 사물인터넷 기본계획이 수립되었고, 2015년에는 사물인터넷 확산 전략이 마련되었다. 미래창조과학부, 제5차 국가정보화 기본계획(2013-2017), 2013, http://www.korea.kr/archive/expDocView.do?docId=34778 (2019년 10월 23일 최종접속); 관계부처 합동, 초연결 디지털 혁명의 선도국가 실현을 위한 사물인터넷 기본계획, 2014.5.8., http://www.korea.kr/news/pressReleaseView.do?newsId=155963726 (2019년 10월 23일 최종접속); 관계부처 합동, K-ICT 사물인터넷 확산 전략, 2015.12.7., https://www.msit.go.kr/SYNAP/skin/doc.html?fn=57891 6b87924e90a3eb2ec49568670c2&rs=/SYNAP/sn3hcv/result/201911/ (2019년 10월 23일 최종접속).

① 소프트웨어와 센서, 부품 및 디바이스의 경쟁력을 강화하고,[427] ② 사물인터넷 서비스와 제품의 창출 및 혁신을 주도할 전문기업을 육성하며,[428] ③ 사물인터넷 제품이나 서비스의 기획 단계부터 보안을 내재화 한다[429]는 주요과제를 설정하였다.[430] 사물인터넷 발전을 위한 인프라 조성에 초점을 두었던 '사물인터넷 기본계획'을 발표한 이후 정부는 2015년 12월에 본격적인 비즈니스 모델을 발굴하고 사물인터넷 산업의 경쟁력 강화를 추진하고자 'K-ICT 사물인터넷 확산 전략'을 발표하였다.[431] 기본계획이 백과사전식으로 사물인터넷 전 분야를 망라하고 있었던 것에 비해 확산 전략은 '공급 강화'와 '수요 확대'라는 틀을 크게 구분한 후 각 분야 별로 집중해야 할 단기 과제들을 기술하고 있다.[432] 아울러 2015년부터 3년 동안 K-ICT 사물인터넷 실증사업을 추진하겠다는 계획이 포함되었다.[433] 2018년 3월 '대통령직속 4차산업혁명위원회'는 '스마트 공장 확산 및 고도화 전략'[434]을 발표했고, 그 후

---

427) ① 유망 IoT 플랫폼 개발 및 서비스 확산, ② ICBM(사물인터넷(IoT), 클라우드(Cloud), 빅데이터(BigData), 모바일(Mobile)) 융합 신서비스 개발, ③ 이용자 중심의 창의적 서비스 개발이 세부과제로 추진되었다. 관계부처 합동, 초연결 디지털 혁명의 선도국가 실현을 위한 사물인터넷 기본계획 참조.

428) ① 개방형 글로벌 파트너십 추진, ② 스마트 디바이스 산업 육성, ③ 스마트 센서 산업 육성, ④ 전통산업과 소프트웨어 신산업 동반성장 지원, ⑤ 생애 전 주기 종합지원이 세부과제로 추진되었다. 관계부처 합동, 초연결 디지털 혁명의 선도국가 실현을 위한 사물인터넷 기본계획 참조.

429) ① 정보보호 인프라 강화, ② 유무선 인프라 확충, ③ 기술개발, 표준화 및 인력양성, ④ 규제 없는 산업환경 조성 등이 세부과제로 추진되었다. 관계부처 합동, 초연결 디지털 혁명의 선도국가 실현을 위한 사물인터넷 기본계획 참조.

430) 미래창조과학부 보도자료, "초연결 디지털 혁명의 선도국가 실현을 비전으로 사물인터넷 국가전략 수립", 2014.5.8., https://www.bioin.or.kr/board.do?num=244882&cmd=view&bid=division (2019년 10월 23일 최종접속) 참조.

431) 관계부처 합동, K-ICT 사물인터넷 확산 전략 참조

432) 추진과제로 (1) 6대 분야 비즈니스 모델 발굴 및 사업화 집중 지원에서는 (전략분야) 6대 분야에 대한 집중투자로 초기 시장 수요 창출, (시범활용분야) IoT 본격 활용을 위한 사업화 추진, (기반조성분야) 각 분야별 시장성 검토 및 활용 기술 개발, (2) IoT 산업 경쟁력 강화에서는 센서 및 스마트 디바이스 경쟁력 확보, IoT 전용네트워크 구축, 플랫폼 개방·공유 활성화, 표준화 적극 대응, (3) IoT 활용 확산 공통기반 강화에서는 보안 강화 및 내재화 추진, 개인정보 보호 및 데이터 이용 촉진, IoT 신제품·서비스 개발·실증 인프라 강화 등이 있다.

433) 미래창조과학부 보도자료, "미래부, 사물인터넷(IoT) 실증사업 본격 추진", 2015.6.24., http://www.korea.kr/news/pressReleaseView.do;JSESSIONID_KOREA=uxVm_bMg1GnRn6wJGl74ko0Qye5bBb8OQmsDKzzTnQm22lZpf3FI!-1097879007!331664680?newsId=156060879&pageIndex=4381&repCodeType=&repCode=&startDate=2008-02-29&endDate=2019-08-06&srchWord= (2019년 10월 23일 최종접속).

434) 4차산업혁명위원회/관계부처 합동, 스마트공장 확산 및 고도화 전략, 2018.3.8., https://4th-ir.go.kr/article/download/247 (2019년 10월 23일 최종접속).

속 조치로서 스마트공장 및 스마트시티 등에 사용되는 사물인터넷과 같은 초연결 네트워크 기술을 육성하기 위한 관련 규제를 개선하여 2018년 12월 5일부로 시행되도록 하였다.[435]

한편 2019년 7월 16일 행정안전부는 각 행정기관이 사물인터넷을 보다 쉽게 기획·구축·활용할 수 있도록 '정부사물인터넷 도입 가이드라인'을 마련하였다.[436] 정부사물인터넷(G-IoT)이란 정부가 공공부문은 물론이고 산업부문이나 개인부문 등을 포함한 국가사회의 현안을 해결하기 위한 수단으로 사물인터넷 기술을 활용하기 위해 도입 또는 운영하는 서비스나 플랫폼, 네트워크, 디바이스 등을 일컫는다.[437] 해당 가이드라인에는 일선기관의 담당자가 실무상 참조해야 할 구체적 내용들이 담겨있는데, 표준기술 동향을 비롯하여 네트워크나 디바이스 등의 도입 기준과 품질 관리 및 보안 준수사항 등이 포함되어 있다.[438] 또한 지침은 상용망[439]의 활용이나 자체망[440]의 구축 등 사물인터넷 네트워크의 다양한 모델을 제시하면서 사물인터넷 서비스의 특성에 따라 중점적으로 고려해야 할 사항들을 안내하고 있다.[441] 특히 기관별로

---

435) 와이파이 속도 향상을 위해 와이파이 채널을 추가 확보하고, IoT 통신 효율을 높이기 위해 IoT 수신확인신호 기술규제의 완화 및 IoT 센싱 기술을 활용하는 스마트공장 활성화를 위해 현재 개발 중인 제조 현장용 IoT 센서의 기술개발에 발맞추어 기술규제를 완화하였다. 과학기술정보통신부 보도자료, "와이파이·사물인터넷 등 신산업 육성을 위한 규제 개선 시행", 2018. 12.5., https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1438471 (2019년 10월 23일 최종접속).

436) 행정안전부 보도자료, "공공 사물인터넷, 품질은 높이고 도입은 더 쉽게 – 행안부, "정부사물인터넷 도입 가이드라인" 마련", 2019.7.17., https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do;jsessionid=tya06eNYqGy3FpvJUr9ulYj+.node40?bbsId=BBSMSTR_000000000008&nttId=71879&bbsTyCode=BBST03&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1&searchCnd=&searchWrd=&searchCode1=&searchCode2=&searchCode3=&searchBgnDe=&searchEndDe=&searchSttusCode= (2019년 10월 23일 최종접속).

437) 행정안전부/한국정보화진흥원, 정부사물인터넷 도입 가이드라인, 2019.7., 5면, https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000045&nttId=71876 (2019년 10월 23일 최종접속).

438) 행정안전부, 앞의 보도자료("공공 사물인터넷, 품질은 높이고 도입은 더 쉽게 – 행안부, "정부사물인터넷 도입 가이드라인" 마련") 참조.

439) 상용망은 통신사업자가 제공하는 IoT 무선망에 가입할 경우 커버리지, 디바이스 적합성, 보안성, 이용 요금 등을 고려하여 도입되며, 통신사의 IoT망을 활용함으로써 IoT 단말 간 로밍으로 전국적인 서비스가 가능하다. 행정안전부, 앞의 보도자료("공공 사물인터넷, 품질은 높이고 도입은 더 쉽게 – 행안부, "정부사물인터넷 도입 가이드라인" 마련") 참조.

440) 자체망은 상용망 이용에 비해 경제성·타당성을 확보할 수 있을 경우에 구축한다. 행정안전부, 앞의 보도자료("공공 사물인터넷, 품질은 높이고 도입은 더 쉽게 – 행안부, "정부사물인터넷 도입 가이드라인" 마련") 참조.

441) 행정안전부/한국정보화진흥원, 앞의 가이드라인, 16면.

구축한 사물인터넷망을 연계할 수 있도록 '정부사물인터넷 공통기반'의 활용 방법에 대해서도 상세히 안내하고 있다.[442] 무엇보다 동 가이드라인은 무선망을 기반으로 하여 다양한 디바이스들이 연결되어 있어서 각종 보안위협에 노출되는 사물인터넷망에 대한 단계별 보안 대책의 적용방안을 마련하고 있다는 점에서 주목된다. 요컨대 사물인터넷망의 설계·개발,[443] 배포·설치·구성,[444] 운영·관리·폐기[445] 등 일련의 단계에서 고려되어야 할 보안 원칙들이 제시되고 있는 것이다.

2) 법률 정비

사물인터넷 관련 법제[446] 정비 현황은 해당 산업을 활성화시키기 위한 측면과 그로부터 야기될 수 있는 법익침해나 위태화를 막기 위한 측면에서 검토될 수 있다.

우선 전자와 관련하여 정비가 이루어진 법률로는 「위치정보의 보호 및 이용 등에 관한 법률」(이하 '위치정보법'이라고 함)을 들 수 있다. 스마트폰이나 스마트카와 같이 사물인터넷 디바이스 중 상당수는 이동성이 있는 기기이며, 이러한 디바이스들이 사물인터넷 환경을 구축하기 위해서는 위치정보를 필요로 하게 된다. 동법은 「위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화」하는 것을 목적으로 하는데(위치정보법 제1조), 이때 위치정보란 "이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것"을 말한다(동법 제2조). 여기서 "이동성이 있는 물건"은 그것이 수송수단이건 아니면 수송수단에 의해서 수송되는 것이건 상관없다. 위치정보는 개인정보와 마

---

442) 행정안전부/한국정보화진흥원, 앞의 가이드라인, 23-25면.

443) 정보보호와 프라이버시 강화를 고려한 IoT 인프라 설계, 보안취약점 사전예방을 위한 안전한 소프트웨어 및 하드웨어의 검증과 적용이 중요하다.

444) IoT 제품 및 서비스 설치 및 제공시 보안 설정, 안전성을 보장하기 위한 보안 프로토콜 준수 및 파라미터 설정이 중요하다.

445) IoT 제품·서비스의 취약점 보안패치 및 업데이트 지속 이행, 안전한 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련이 중요하다.

446) 사물인터넷의 특성상 정보통신, 환경, 건축, 교통, 의학, 안전 등 다양한 분야와 관련이 있으며, 사물인터넷이 특정 분야, 특정 서비스에 한정된 문제가 아닌 우리 생활 전반에 걸쳐 활용되는 측면이 강하기 때문에 다양한 분야의 많은 법령이 사물인터넷과 관련이 있다. 김성준/박주석/박지웅/전은정/김나라/강혜정/정혜인/신세미/김정은/민경은/최홍선/안호정/김우리, IoT 제품·서비스 책임강화 방안연구, 한국인터넷진흥원, 2015.11., 80면.

찬가지로 정보자기결정권의 보호가 필요한 영역인바, 위치정보법도 개인정보 보호법과 마찬가지로 정보주체의 동의가 없으면 해당 정보를 수집·이용·제공할 수 없도록 금지되어 있다.[447] 특히 현행 위치정보법은 순수한 사물의 위치정보도 규율하고 있기 때문에 위치정보를 요하는 이동형 사물인터넷 디바이스의 경우에는 개인과 연관되었는지 여부를 불문하고[448] 모두 동법의 적용을 받게 되므로 사물인터넷 환경에서 동법의 중요성은 더 부각되고 있다.[449]

종래 위치정보법은 "누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니된다."고 규정하고 있었다. 이에 동법에 대해서는 단순한 사물의 위치정보도 소유자의 동의를 받아야만 수집할 수 있도록 함으로써 사실상 사물인터넷의 활성화는 거의 불가능하다는 비판이 제기되었다. 예컨대 도로에 설치된 교통정보수집용 카메라를 통해서 그 지점을 통과하는 차량을 촬영해서 해당 도로를 이용하는 차량의 유형이나 속도 및 빈도 등을 파악한다고 가정해보자. 차량의 유형은 번호판을 식별해서 자동차 등록정보를 조회함으로써 파악될 수 있는데, 이 짧은 시간에 해당 정보가 보관된다고 하더라도 이것은 위치정보의 수집과 이용에 해당한다. 이에 특정 개인의 위치정보가 아닌 단순 사물의 위치정보는 프라이버시를 침해할 가능성이 없으므로 현행 위치정보법상 동의 없는 수집이나 이용 등이 금지되는 대상에 사물위치정보는 포섭되지 않아야 한다는 비판이 제기되었다.[450]

사물인터넷 관련 산업의 진흥을 위해서는 해당 조문의 정비가 요청되었는바, 2018년 4월 17일 동법 개정을 통해 사물위치정보의 경우에는 소유자의 사전 동의를 받지 않더라도 그 정보가 처리될 수 있도록 하였다. 또한 동 개정을 통해 시장진입 규제를

---

447) 위치정보법은 개인정보 중에서도 위치정보를 특별히 보호하는데, 일반법적 성격을 가지는 개인정보 보호법과의 관계에서 위치정보법은 특별법으로서 우선 적용된다.

448) 대부분 개인과 연관되기 때문에 상당수의 위치정보는 개인정보가 될 것이고, 드론에 의해서 무인으로 물건이 배송되는 경우에는 개인정보를 포함하지 않는 위치정보가 될 것이다.

449) 오병철, "IoT환경에서의 프라이버시 보호에 관한 연구", NAVER Privacy White Paper, 네이버, 2016, 84-85면, https://privacy.naver.com/download/2016_NaverPrivacyWhitePaper_2.pdf (2019년 10월 23일 최종접속).

450) 오병철, 앞의 글, 85면; 정상조, "위치기반서비스 규제에 관한 연구", 2015 NAVER privacy White Paper, 네이버, 2016, 28-29면, https://privacy.naver.com/download/2015_NaverPrivacyWhitePaper_fin.pdf (2019년 10월 23일 최종접속).

완화하고자 사물위치정보사업자가 방송통신위원회의 '허가'를 받도록 하던 종래의 규정은 '신고'를 하는 것으로 완화되었다. 또한 1인 창조기업이나 소상공인의 경우에는 신고 절차를 간소화시켜서 위치기반서비스사업을 할 수 있도록 하였다.[451] 2018년 12월 24일에는 위치정보사업자 등이 14세 미만 아동으로부터 개인위치정보의 수집·이용 등에 대한 동의를 받을 경우 법정대리인이 실제로 동의했는지 여부를 확인하도록 했다. 아울러 동 개정법은 위치정보사업자 등이 개인위치정보주체에게 정보 처리와 관련된 사항에 대한 고지 등을 할 때에는 이해하기 쉬운 양식을 이용하며, 명확하고 알기 쉬운 언어를 사용하도록 하였다.[452]

[표 3-4] 위치정보법 제15조 제1항 신구조문 대비표[453]

위치정보법 [시행 2017. 7. 26] [법률 제14840호, 2017. 7. 26, 타법개정]	위치정보법 [시행 2018. 10. 18] [법률 제15608호, 2018. 4. 17, 일부개정]
제15조(위치정보의 수집 등의 금지) ① 누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.	제15조(위치정보의 수집 등의 금지) ① 누구든지 개인위치정보주체의 동의를 받지 아니하고 해당 개인위치정보를 수집·이용 또는 제공하여서는 아니 된다.----------.

사물인터넷 환경이 본격적으로 조성되면 상대적으로 개인정보자기결정권이 약화될 수 있다는 우려가 제기되고 있다. 반면 제4차 산업혁명 시대의 데이터 경제 활성화를 위해서는 지나치게 엄격하다고 평가되는 개인정보 보호 규정을 완화시켜야 한다는 목소리도 커지고 있다. 실제로 2019년 10월 현재 국회에는 가명정보 활용 등을 주요 내용으로 한 이른바 '데이터 3법(개인정보보호법·신용정보보호법·정보통신망법 개정

451) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=203231&ancYd=20180417&ancNo=15608&efYd=20181018&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

452) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=206086&ancYd=20181224&ancNo=16087&efYd=20190625&nwJoYnInfo=Y&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

453) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=203231&ancYd=20180417&ancNo=15608&efYd=20181018&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

안)'[454]이 상정되어 있다. 한편 규제 완화의 필요성이 강력히 제기되고 있는 흐름 속에서도 글로벌 사업자로부터 개인정보를 보호하기 위한 「정보통신망법」 개정이 단행되기도 했다. 즉 대한민국 국민은 글로벌 사업자에 대하여도 개인정보자기결정권을 실질적으로 행사할 수 있도록 하고, 해외로 이전된 국민의 개인정보가 제3국으로 재이전될 경우에도 해당 정보가 안전하게 유통될 수 있도록 2018년 9월 18일에 정보통신망법이 개정되어 2019년 3월 19일부터 시행되고 있는 것이다.[455]

[표 3-5] 정보통신망법 제32조의5, 제63조 신구조문 대비표[456]

정보통신망법 [시행 2018. 12. 13] [법률 제15628호, 2018. 6. 12, 일부개정]	정보통신망법 [시행 2019. 3. 19] [법률 제15751호, 2018. 9. 18, 일부개정]
〈신 설〉	제32조의5(국내대리인의 지정) ① 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 다음 각 호의 사항을 대리하는 자(이하 "국내대리인"이라 한다)를 서면으로 지정하여야 한다. 1. 제27조에 따른 개인정보 보호책임자의 업무 2. 제27조의3 제1항에 따른 통지·신고 및 같은 조 제3항에 따른 소명 3. 제64조 제1항에 따른 관계 물품·서류 등의 제출

454) 개인정보보호법 개정안(인재근의원 대표발의), 정보통신망법 개정안(노웅래의원 대표발의), 신용정보법 개정안(김병욱의원 대표발의) 등 데이터 3법은 개인정보, 가명정보, 익명정보에 대해 정의하고, 전문기관의 승인 하에 결합 정보의 활용을 허용하며, 개인정보 관련 감독 기관을 개인정보보호위원회로 일체화시키는 한편, 금융분야 빅데이터의 분석 및 이용에 대한 법적 근거를 명확화하는 것 등을 그 내용으로 한다.

455) 개정 법률은 「대한민국 국민이 글로벌 사업자에게도 국내 사업자에 대해 행사하는 것과 마찬가지로 본인의 개인정보에 대해 수집·이용·제공 등의 동의 철회, 열람청구, 정정요구 등 자기결정권을 실질적으로 행사할 수 있도록 하고, 방송통신위원회가 글로벌 사업자의 개인정보 침해 여부를 판단하기 위해 자료를 요청할 경우 필요한 자료를 신속하게 제출할 수 있도록 하는 한편, 글로벌 사업자가 대한민국 국민의 개인정보를 해외로 이전한 후 제3국으로 재이전 하는 등 해외 시장에서 유통되고 있음에도 법적 근거가 마련되어 있지 않고, 특히 우리나라보다 개인정보 보호 수준이 낮은 나라로의 이전에 대해서는 국제규범상 동등하게 보호하는 등 우리 국민의 개인정보가 해외에서도 안전하게 유통될 수 있는 방안을 마련하려는 것」이다. 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=204481&ancYd=20180918&ancNo=15751&efYd=20190319&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

456) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/lsInfoP.do?lsiSeq=204481&ancYd=20180918&ancNo=15751&efYd=20190319&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

정보통신망법 [시행 2018. 12. 13] [법률 제15628호, 2018. 6. 12, 일부개정]	정보통신망법 [시행 2019. 3. 19] [법률 제15751호, 2018. 9. 18, 일부개정]
	② 국내대리인은 국내에 주소 또는 영업소가 있는 자로 한다. ③ 제1항에 따라 국내대리인을 지정한 때에는 다음 각 호의 사항 모두를 제27조의2에 따른 개인정보 처리방침에 포함하여야 한다. 1. 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명을 말한다) 2. 국내대리인의 주소(법인의 경우에는 영업소 소재지를 말한다), 전화번호 및 전자우편 주소 ④ 국내대리인이 제1항 각 호와 관련하여 이 법을 위반한 경우에는 정보통신서비스 제공자등이 그 행위를 한 것으로 본다.[본조신설 2018.9.18]
제63조(국외 이전 개인정보의 보호) ① ~ ④ (생 략)	제63조(국외 이전 개인정보의 보호) ① ~ ④ (현행과 같음)
〈신 설〉	⑤ 이용자의 개인정보를 이전받는 자가 해당 개인정보를 제3국으로 이전하는 경우에 관하여는 제1항부터 제4항까지의 규정을 준용한다. 이 경우 "정보통신서비스 제공자등"은 "개인정보를 이전받는 자"로, "개인정보를 이전받는 자"는 "제3국에서 개인정보를 이전받는 자"로 본다.
〈신 설〉	제63조의2(상호주의) 제63조에도 불구하고 개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 그러하지 아니하다.

이보다 앞서 2016년 3월 29일에는 「개인정보 보호법」이 개정되었는데, 일정한 범위의 개인정보처리자가 정보주체 이외로부터 개인정보를 수집해서 처리할 때에는 해당 정보주체에게 그 수집의 출처 및 처리 목적 등을 고지하도록 함으로써 개인정보 자기결정권을 보다 두텁게 보호하고자 하였다. 그리고 종래 대통령령에 근거하여 이루어지던 영상정보처리기기의 설치 및 운영이 동법에 근거 규정을 두는 것으로 개정되면서 일부 미비사항이 보완되었다.

[표 3-6] 개인정보 보호법 제20조, 제25조 신구조문 대비표[457]

개인정보 보호법 [시행 2015.7.24] [법률 제13423호, 2015.7.24, 일부개정]	개인정보 보호법 [시행 2016.9.30] [법률 제14107호, 2016.3.29, 일부개정]
제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ①·② (생 략)	제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ①·② (현행과 같음)
〈신 설〉	③ 제2항 본문에 따라 알리는 경우 정보주체에게 알리는 시기·방법 및 절차 등 필요한 사항은 대통령령으로 정한다.
〈신 설〉	④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다. 1. 고지를 요구하는 대상이 되는 개인정보가 제32조 제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우 2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
제25조(영상정보처리기기의 설치·운영 제한) ① ~ ③ (생 략)	제25조(영상정보처리기기의 설치·운영 제한) ① ~ ③ (현행과 같음)
④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.	④ ---------- 다음 각 호의 사항이 포함된 안내판을 설치하는 ----------. 다만, 「군사기지 및 군사시설 보호법」 제2조 제2호에 따른 군사시설, 「통합방위법」 제2조 제13호에 따른 국가중요시설, 그 밖에----------.
〈신 설〉	1. 설치 목적 및 장소
〈신 설〉	2. 촬영 범위 및 시간
〈신 설〉	3. 관리책임자 성명 및 연락처
〈신 설〉	4. 그 밖에 대통령령으로 정하는 사항
⑤ ~ ⑧ (생 략)	⑤ ~ ⑧ (현행과 같음)

457) 법제처 국가법령정보센터 웹페이지, http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=182015&ancYd=20160329&ancNo=14107&efYd=20160930&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2019년 10월 23일 최종접속).

2. 현행 법제도의 한계

가. 형사실체법적 한계

사물인터넷 기술이 발전하면서 살인, 상해, 감금 등 전통적인 범죄의 발생 양상이 변모할 수 있다. 그러나 이것은 범죄의 수단이 첨단화된 것일 뿐 현행 형법 규정을 적용하여 처벌하는 데에는 별다른 문제가 없을 것이다. 그러나 사물인터넷에 연결되어 있는 전기레인지나 보일러 온도조절장치 등을 조작해서 화재를 일으킨 경우에 현행 형법상 방화죄가 적용될 수 있을지에 대해서는 의문이 제기된다. 형법상 방화죄의 구성요건적 행위는 '불을 놓아' 목적물을 소훼하는 것이라고만 규정되어 있는데, 종래에는 법해석을 통해 방화의 방법에는 제한이 없다고 이해되었다. 그러나 원격지에서 사물인터넷 디바이스를 조작해서 화재를 일으킨 경우의 행위까지도 '불을 놓아'라는 문언의 범주 내에 있다고 해석하는 것은 명확성의 원칙에 반할 수 있다는 문제가 제기되고 있다.[458]

네트워크와 정보통신 기술의 비약적 발전은 사물인터넷을 이용해서 자신의 주거에 있는 가전기기들이나 설비를 관리함으로써 생활의 편익을 향상시키고 있다. 그러나 확대된 네트워크는 해킹 등으로 인해 사생활의 자유가 침해될 가능성도 높이고 있다. 현행 정보통신망법상 망을 침해한 행위는 처벌의 대상이 되고 있으나, 이때 보호법익은 정보통신망의 안정성이며, 피해자는 정보통신서비스 제공자가 된다. 해킹이나 망 침해를 통해 프라이버시가 침해되는 집주인은 정작 법적으로 피해자가 되지 않는다. 그렇다고 해서 이 경우 형법상 주거침입죄를 적용하기도 어렵다. 주거침입죄는 사생활의 평온과 안전을 그 보호법익으로 하는바, 어디까지나 주거권자의 의사에 반해 주거 안으로 진입하면서 사실상의 평온을 침해하는 것이다. 이에 정보통신망에 '침입'

458) 국회 법제실, 4차 산업혁명 입법과제, 2017. 12, http://likms.assembly.go.kr/law/lawsLawyInqyList1011.do?mappingId=%2FlawsLawyInqyList1011.do&genActiontypeCd=2ACT1010&genDoctreattypeCd=DOCT2041&procWorkId=&workstepId=&repFlowId=&flowId=&workId=&workSno=&winWd=&winHg=&winTypeAttr=M&nextWinWd=&nextWinHg=&nextWinTypeAttr=&nextMappingId=&nextGenActiontypeCd=&dispNum=233&pageSize=10&genMenuId=menu_serv_nlaw_lawt_5010&srchNm=&pageNum=2&boardNo=4&articleNo=382471&srchType=title&back_dispNum=233&back_pageSize=10&back_genMenuId=menu_serv_nlaw_lawt_5010&back_srchNm=&back_pageNum=2&back_boardNo=4&back_articleNo=382471&back_srchType=&dumy=&orderType=&orderObj= (2019년 10월 23일 최종접속).

해서 IoT 디바이스를 조작하는 등의 행위를 신체의 물리적 진입 여부를 판단하는 주거침입죄의 '침입'에 포섭할 수는 없다. 또한 형법상 개인의 프라이버시와 관련된 보호수단은 비밀침해죄와 업무상 비밀누설죄 밖에 존재하지 않는데, 정보통신망 침해를 통해 봉함 기타 비밀장치한 타인의 편지 등을 개봉하거나 의사나 변호사 등이 업무처리 중 지득한 타인의 비밀을 누설한 것이 아닐 때에는 해당 구성요건이 적용될 수 없다. 요컨대 정보통신망 침해로 인한 주거권자의 프라이버시는 보호되고 있지 않으며, 처벌의 공백상태가 발생하고 있다.

나. 형사절차법적 한계

사물인터넷 시스템을 침해하는 범죄의 주된 무대는 인터넷 사이버 공간이고, 범죄실행의 단서나 범죄행위의 증거가 모두 네트워크에 연결된 사이버 공간과 전자통신기기에 있는 상황에서 그 공간을 대상으로 한 수사가 이루어질 수 있어야 한다. 특히 원격지에서 서버에 접속하여 범죄혐의와 관련된 데이터를 선별·압수할 수 있는 강제처분이 필요하다. 원격지 온라인 압수·수색이 필요한 이유로는, 첫째 대부분의 경우 피압수자 등의 협조를 구하기가 어렵고, 둘째 집행이 지체될 경우 중요 증거가 삭제되거나 훼손될 우려가 있다는 것이다. 사물인터넷 환경의 고도화는 원격지 압수·수색에 대한 필요성을 한층 더 제고시킬 것으로 예상되지만, 현재 우리 형사소송법에는 이에 대한 근거 규정이 없는 상황이다.

한편 다크웹을 통해 사물인터넷에 대한 해킹 프로그램이 거래되는 경우에 범죄수사를 위해 해당 사이트에 접근하는 것은 기술적으로 쉽지 않다. 이에 독일이나 미국은 온라인수색 혹은 네트워크 수사기법(Network Investigative Technique, NIT)이라고 불리는 수사방법을 활용하고 있다. 다크웹이 범죄의 온상으로 빠르게 변화되고 있는 오늘날, 폐쇄형 가상공간상에서 일어나는 범죄를 수사하기 위한 적절한 수사방법이 법제화되어 있지 않다는 것도 형사절차법적 한계로 지적될 수 있다.

나아가 현행 형사소송법이 종이 형태의 물리적 영장제도를 전제하고 있고, 그 발부와 제시에 대한 규정이 엄격히 해석되고 있다는 점도 문제이다. 사이버 공간에서 이루어지는 네트워크 침해범죄의 경우에는 그 특성상 해당 수색 대상자에게 물리적인 영장을 제시하는 것이 곤란하거나 현저한 시간과 비용이 드는 경우가 많다. 그럼에도

불구하고 사이버 공간을 기반으로 하여 이루어진 사건에서 물리적 방식으로 영장을 제시하도록 하는 것은 비효율적일 뿐만 아니라 그 집행을 지체시켜서 수사에 지장을 초래할 우려가 있다.

다. 형사정책적 한계

사물인터넷과 관련해서는 기술 혁신 및 산업 발전에 초점을 둔 정책이 수립되고 법률 정비가 이루어지는 경향이 있다. 정작 사물인터넷 디바이스의 폭발적인 증가로 인한 보안의 위기가 심각한 문제로 지적되어야 함에도 불구하고, 초창기 기술 혁신 및 시장 성장에 걸림돌이 될 것을 우려해서 이와 관련해서는 적극적인 논의가 이루어지지 못하고 있다. 그러나 보안에 취약한 디바이스를 공격하여 네트워크 전체를 마비시킬 경우 그 피해는 막대할 것이다. 2018년 11월 24일 발생한 'KT 아현지사 통신구 화재 사건'[459]을 계기로 초연결 시대에 통신망의 장애가 사람들의 일상에 얼마나 큰 영향을 미치는지가 알려졌는데, 불과 2시간 정도의 통신장애로 인해 응급실이 폐쇄되는가 하면, 일부 경찰서의 112 신고 시스템도 작동하지 않는 등 그 피해 규모는 막대했다.[460] 이러한 장애는 오프라인상의 화재가 아닌 사물인터넷에 대한 공격으로도 충분히 발생할 수 있는바, 사물인터넷 보안 기준을 설정하는 법제가 마련되어야 할 것이다. 앞서 검토했던 미국의 경우 사물인터넷 혁신과 성장을 위한 법제 정비가 먼저 이루어졌지만, 사물인터넷 사이버보안 개선을 위한 입법화 노력도 지속되고 있다. 특히 첨단기술 혁신의 모태인 실리콘 밸리가 있는 캘리포니아 주에서 미국 최초로 IoT 보안법이 제정되었다는 것은 우리에게 시사하는 바가 크다.

---

459) 2018년 11월 24일 오전 11시경 서울 서대문구 충정로에 위치한 KT 아현지사 건물 지하의 통신구 연결통로에서 화재가 발생하여 통신구 약 79m가 소실되었고 서울시 5개구(서대문구, 마포구, 용산구, 중구와 은평구 일대) 및 경기도 고양시 일대에 통신장애가 발생하였다. 이로 인하여 KT망을 사용하는 인터넷, 휴대전화 무선통신 등을 사용하지 못하게 되었는바, 카드결제가 불가능하고 112신고 시스템 및 종합병원 의료진의 콜폰도 불통이 되어 불편을 겪었다. 이후 경찰은 5개월 간의 수사 결과 발표했는데 장시간 화재로 인한 현장 훼손으로 발화 지점 및 원인 등의 규명이 불가능한 것으로 종결하였다. "KT 아현화재 통신대란 1년…"5G시대 재난 대응책, 더 고민해야"", 연합뉴스 2010년 11월 17일자, https://www.yna.co.kr/view/AKR20191115153000017 (2019년 12월 13일 최종접속).

460) "KT 화재로 인근 경찰서 통신망 일부도 연결 끊겼다", 한겨레 2018년 11월 25일자, http://www.hani.co.kr/arti/society/society_general/871678.html (2019년 12월 13일 최종접속).

블록체인

전현욱·김진묵·류부곤·이병욱

제4장

블록체인

제1절 | 블록체인의 기술적 이해와 특징

1. 블록체인의 등장

2008년 어느날 암호학 커뮤니티의 메일링 리스트에 '사토시 나카모토(Satoshi Nakamoto)'[461]라는 이름으로 작성된 "Bitcoin: A peer-to-peer Electronic Cash System"이라는 제목의 9장짜리 논문[462]이 첨부된 메일이 발송되었다. 논문 내용은 신뢰받는 제3자가 개입 없이 사용할 수 있는 화폐와 그 결제 시스템에 대한 구상이었다. 논문에서는 신뢰받는 제3자를 배제하려는 주목적을 '프라이버시의 보호'로 설명하고 있으며, 부가적으로 중재(mediation)의 역할을 제거하여 어떤 경우도 한번 발생한 거래는 되돌릴 수 없게 한다고 부연하고 있다.[463] 이와 함께 중재자들이 사라지면, 그들에게 지급되던 비용도 절감될 것이라는 기대도 언급하고 있다.[464]

초기에는 주목을 받지 못했던 이 논문은 10년의 세월이 흐르면서 '블록체인'이라는 신조어를 파생시켰고, 이후 '암호화폐'라는 용어와 결합하면서 여러 측면에서 주목받게 된다. 블록체인을 4차 산업혁명의 기반기술이라 설명하는 사람[465]이 있는가 하면,

461) 사토시 나카모토는 가명이며, 대략 3~5인의 단체를 지칭하는 것으로 보인다. 이 중 호주의 전산학자 스티븐 크레이그 라이트(Steven Craig Wright)는 자신이 사토시 나카모토라고 주장하였고, 그가 소유한 개인 암호화키로 유추해 보건대 그 일원임이 확실해 보인다. 이와 함께, 현재 bitcoin.org 도메인을 소유하며, 운영하고 있는 사람들도 그 일원으로 알려지고 있다.

462) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009.3. 이 논문은 정식으로 peer review를 거쳐 학술지에 게재된 것이 아니라, 논문 형식을 빌려 개념을 정리한 후 이메일의 첨부 파일로 배부되었다.

463) Satoshi Nakamoto, Ibid., p.1.

464) Satoshi Nakamoto, Ibid., p.1.

2008년 경제위기를 정확히 예측하여 유명해진 뉴욕대학의 경제학자 누리엘 루니비(Nouriel Roubini) 교수는 블록체인은 무용지물이며, 모든 ICO는 사기라고 주장한다.[466] 한편 노벨 경제학상을 받은 대표적 학자인 조셉 스티글리츠(Joseph E. Stiglitz)와 로버트 쉴러(Robert Shiller)교수는 암호화폐의 용도는 투기와 검은 돈을 위한 은닉처 이외는 없다[467]고 하지만 크리스틴 라가르드(Christine Lagarde) IMF 총재는 '잠재력이 있으나 지켜봐야 한다'는 다소 중립적인 입장이며,[468] JP모건의 제이미 다이먼(Jamie Dimon)은 암호화폐는 사기라고 역설했다가 자신의 발언을 수정하고 스스로 JPM이라는 이름의 코인을 발행한다.[469] 한편, 자신의 견해를 변경한 경우 중 뉴욕시립대의 폴 크루그먼(Paul Krugman)은 대단히 주목받은 사례인데, 노벨 경제학상 수상자이기도 한 그는 평소 암호화폐에 대한 대표적인 회의론자로 유명했지만, 태도를 바꾸고 "비트코인은 금보다 우수하다"고 주장하기도 했다.[470]

블록체인에 이토록 상반된 주장이 오가는 이유는 무엇일까? 여기서 주목해야 할 중요한 사실이 하나 있다. '기술'이라 지칭된 블록체인이 정작 뜨겁게 주목받는 부분은 대부분 '돈'과 관련된 측면이라는 점이다. 그렇다면 블록체인은 과연 '무엇'을 하는 기술이며 그 실체는 무엇인가?

---

465) 예컨대 방태웅, "4차산업혁명의 기반기술, 블록체인", Weekly TIP Vol. 108, 융합연구정책센터, 2018.2, https://crpc.kist.re.kr/user/nd88987.do?View&pageST=TOTAL&pageSV=&pageLS=10&page=1&pageSC=REGDATE&pageSO=DESC&dmlType=&boardNo=00006326&dmlType=# (2019년 11월 4일 최종접속) 참조.

466) "Economist Nouriel Roubini Says 'Blockchain Is Useless, All ICOs Are Scams'", Forbes 2018.8.31., https://www.forbes.com/sites/naeemaslam/2018/08/31/nouriel-roubini-says-blockchain-is-useless-all-icos-are-scam/#445167723f3a (2019년 11월 4일 최종접속) 참조.

467) "Joseph Stiglitz: Bitcoin ought to be outlawed", World Economic Forum 2017.11.30., https://www.weforum.org/agenda/2017/11/joseph-stiglitz-bitcoin-ought-to-be-outlawed/ (2019년 11월 4일 최종접속) 참조.

468) "Winds of Change: The Case for New Digital Currency", IMF 2019.11.14., https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency (2019년 11월 4일 최종접속) 참조.

469) "Jamie Dimon hated bitcoin. Now JPMorgan is getting ahead of the crypto revolution", CNN Businiess 2019.2.15., https://edition.cnn.com/2019/02/15/investing/jpmorgan-bitcoin-crypto-jamie-dimon/index.html (2019년 11월 4일 최종접속) 참조.

470) "Paul Krugman: Bitcoin Has More Utility Than Gold", NullTX 2018.8.16., https://nulltx.com/paul-krugman-bitcoin-has-more-utility-than-gold/ (2019년 11월 4일 최종접속) 참조.

2. 블록체인의 정의

네이버에서 '블록체인'을 검색하면, 가장 먼저 '가상화폐로 거래할 때 해킹을 막기 위한 기술'이라고 나온다. 이 정의는 시사상식 사전 내용으로 출처가 소개돼 있다.[471] 그러나 이 정의는 잘못 되었음은 물론 블록체인과는 별 관련 없는 단어들로만 조합돼 있다. 특히 블록체인은 해킹을 '막는' 기술이 아니라, 기록 변경을 '사후에 탐지'하는 해시라는 기술을 '사용'만 하고 있을 뿐이다.

한편, 과학기술정보통신부가 작성한 '신뢰할 수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전전략'이라는 보고서를 보면 "블록체인은 절차 간소화, 비용 절감은 물론 우리의 일하는 방식까지 혁신하여 사회편익을 높이는 성장 잠재력이 높은 기술"이라고 설명하고 있다.[472] 또한 "블록체인은 데이터의 신뢰성을 확보하는 기반기술"이며, "기존 중앙집중식 방식에서 탈중앙화 분산식으로 바꾸면서 업무효율화 및 사회혁신을 지향"하고 있다고 쓰고 있다.[473] 그러나 이는 블록체인을 정반대로 설명하고 있다. 블록체인을 사용하면 오히려 절차가 복잡해지고 비용도 크게 증가한다. 또한 블록체인은 업무의 효율화가 아니라 그와는 반대로 업무효율을 크게 떨어뜨린다. 흔히들 블록체인을 분산원장 혹은 분산 시스템으로 표현[474]하지만 이는 부정확한 설명이다. 블록체인은 일을 '분산'하는 것이 아니라 '중복'하기 때문이다. 즉, 블록체인은 가장 비효율적인 방식으로 일을 중복하도록 설계된 시스템이다. 이런 중복은 익명의 노드로만 구성된 네트워크에서 신뢰를 생성하기 위해 치러야 할 비용이자 대가이다. 신뢰는 곧 돈이다. 익명이 아닌 네트워크에서는 굳이 중복이라는 막대한 비효율을 무릅쓰고 블록체인을 사용할 이유를 찾기는 쉽지 않다.[475]

---

471) 네이버 '블록체인' 검색화면, https://search.naver.com/search.naver?sm=top_hty&fbm=0&ie=utf8&query=%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8 (2019년 11월 4일 최종접속) 참조.

472) 과학기술정보통신부, 신뢰할 수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전전략, 2018.6, 1면.

473) 과학기술정보통신부, 앞의 보고서, 5면.

474) 네이버 시사상식 사전 '블록체인' 설명, https://terms.naver.com/entry.nhn?docId=2838482&cid=43667&categoryId=43667 (2019년 11월 4일 최종접속) 참조.

475) 이병욱, 블록체인 해설서, 에이콘 출판사, 2019, 24면.

가. 블록과 체인

와이파이(Wi-Fi)를 설명할 때는 '무선 통신기술'이라는 짧은 한마디로 표현하면 충분하다. 그렇다면, 같은 맥락에서 블록체인을 설명해 줄 수 있는 짧은 한마디는 무엇일까? 놀랍게도 블록체인의 정확한 정의는 어디에도 없다. 따라서 이를 간단히 설명해 줄 짧은 한마디란 존재하지 않는다. 학문적 정의가 없다면 업계의 표준적 합의라도 있을 법한데, 그 조차 없다. 심지어 사토시 나카모토의 원 논문에는 블록체인이라는 고유명사가 단 한 차례도 언급조차 되지 않는다. 논문에는 전산학에서 한꺼번에 처리하는 데이터의 모음을 지칭할 때, 보편적으로 사용하는 용어인 '블록(block)'과 데이터들이 순서대로 나열된 모습을 묘사한 '체인(chain)'이라는 일반 명사만 별도로 언급된 것이 전부이다.[476] 그 뒤 저마다의 해석으로 '블록체인'의 정의를 내리기 시작했고, 급기야 중앙화 시스템조차 블록체인 명칭을 사용하는 일이 흔해졌다. 대표적인 예가 에스토니아이다. 많은 사람들이 에스토니아를 블록체인 선진국이며, 블록체인 정부의 미래라고 주장[477]하며, 경쟁적으로 견학도 다녀오지만 에스토니아의 소위 KSI (Keyless Signature Infra Structure) 블록체인은 중앙화 시스템이므로 블록체인으로 볼 수 없다.[478] 이 시스템을 블록체인이라 주장한 배경은 블록체인에서 사용된 머클트리(Merkle Tree)를 적용했기 때문인데, 머클트리는 아키텍처와 상관없이 보편적으로 사용되는 범용 해시기술로서, 1979년에 랄프 머클(Ralph Merkle)이 특허를 받은 일반적 기법일 뿐이다. 따라서 기술적 관점에서 에스토니아의 행보를 '디지털화(digitalization)'를 위한 노력으로 평할 수는 있겠지만, 블록체인과는 무관한 셈이다. 이렇듯 블록체인의 명확한 정의가 없다는 점은 수많은 혼란을 야기하고 있으며, 심지어는 '디지털화'와 '블록체인'조차 여러 곳에서 혼용하여 사용되는 지경에까지 이르렀다.

시중에서 블록체인이라 언급되는 시스템의 종류는 대단히 광범위해서 사실상 거의

---

476) Satoshi Nakamoto, Ibid., p.1-2.

477) 예컨대, "초대형 블록체인 서밋 개막…8개국 전문가 한자리에", 머니투데이 2019년 1월 24일자, http://news.mtn.co.kr/newscenter/news_viewer.mtn?gidx=2019012317140145083 (2019년 11월 4일 최종접속) 참조.

478) 에스토니아의 정부 CIO인 심 시쿳(Siim Sikkut)은 인터뷰에서 에스토니아의 KSI는 블록체인이 아니라고 명백히 밝히기도 했다. "The mystery of the non-existent Estonian digital identity blockchain: solved!", disruptiv.asia 2017.3.29., https://disruptive.asia/estonian-digital-identity-blockchain/?fbclid=IwAR1zswS6ctVfraPK1HsiHmcJeV6xD6QOpbIJpG1dp75J-N1Tevm0wagRK_8 (2019년 11월 4일 최종접속) 참조.

모든 시스템이 해당되며, 분류의 실익을 찾기 힘들 지경이다. 이는 저마다 '블록체인'이라는 키워드를 마케팅으로 활용하기 위해 그 명확한 정의가 없는 점을 악용하여 무분별하게 명칭을 남용한 결과이기도 하다. 이 때문에 동일한 '블록체인'이라는 단어를 사용하지만 서로 정반대의 사물을 지칭할 경우마저 생긴다. 그 대표적인 예가 IBM이 주도적으로 만들고, 삼성을 비롯한 여러 기업에서 변형해서 사용하고 있는 하이퍼 레저 패브릭이다. 이 시스템은 블록체인이라는 명칭을 사용하고 있지만 비트코인 블록체인과는 거의 정반대의 속성을 가지고 있으며, 무엇보다 블록체인의 가장 기본적인 가정인 '익명의 네트워크'도 아니며 '탈중앙화 시스템'도 아니다.

본 보고서에는 연구 논리의 전개에 있어 그 모호성을 없애기 위해, 먼저 블록체인에 대한 명확한 정의를 내린다. 용어에 대한 정의 없이 '블록체인'을 언급한다면 사물을 특정할 수 없으므로 논지만 흐려 이해를 방해할 것이고, 불필요한 오해만 야기할 것이기 때문이다. 또한 본 보고서의 목적은 기존의 제도나 법률 틀에서 고려하지 못한 새로운 기술적 측면을 살피고자 함인데, 이미 잘 분류된 기존 시스템 체계로까지 블록체인의 정의를 확장하여 고려할 실익이 없기 때문이다.

나. 블록체인의 명확한 정의

블록체인의 명확한 정의를 내리기 위해서는 그 원형인 비트코인의 기본 속성은 물론 탄생 배경과 목적까지도 종합적으로 고려해야 할 것이다. 물론, 그 원형을 개선하여 효율화한 아류 시스템도 기본 속성만 충실히 유지했다면 블록체인으로 분류해야 함은 자명하다. 그러나 비트코인이 구현하려던 핵심 개념을 벗어난 변형, 예컨대 '신뢰할 수 없는 익명의 네트워크'라는 기본가정과 정반대되는 속성인 '신원확인을 통해 신뢰를 확보한 중앙 통제형 네트워크' 등의 변형 사례까지로 범위를 확장한다면, 블록체인은 사실상 '모든' 소프트웨어를 포함하게 되므로, 분석자체가 무의미해 진다. 따라서 본 보고서에서는 명백한 정의를 통해 핵심개념을 변형한 아류를 명백히 구분할 수 있는 기준을 제공한다. 이들 아류에 대해 다른 판단을 한다면 이는 각자의 몫으로 남겨둔다. 그 판단에 대한 추가적인 논의는 본 보고서의 범위를 벗어나기 때문이다.

본 보고서에서 블록체인이라 함은 '익명의 노드가 인터넷을 통해 자발적으로 연결된 네트워크 시스템'을 의미하며 그 중 다음의 네 가지 성질을 모두 만족하도록 설계된

것만을 의미한다. 그러나 기술적 한계로 인해 이를 온전히 만족하지는 못하더라도, 속성상 이 네 가지 성질을 모두 만족시키기 위해 설계되었고 동시에 이 속성 모두를 강화하는 방향으로 지속적인 개선을 해 나가는 경우까지 포함한다. 이제 각 네 가지의 성질이 무엇인지, 각 성질이 무엇을 의미하기 때문에 블록체인의 정의에 포함시켰는지 살펴보자. 전술한대로 이 정의는 비트코인 블록체인의 속성을 바탕으로 분석한 전문가적 견해이며, 학문적 관점 혹은 업계의 합의에 의한 정의란 존재하지 않는다.

1) 각 노드는 자의에 의해 네트워크의 구성원으로 참여하거나 탈퇴할 수 있어야 한다. 따라서 그 규모 역시 동적이어야 하며 어떠한 제약도 없어야 한다.
2) 모든 노드는 동일한 권리와 의무, 정보를 가져야 하며, 어느 한 노드도 더 많은 권한이나 의무, 정보를 가져서는 안 된다.
3) 각 노드는 원할 경우, 언제든지 기록 및 검증에 참여할 수 있어야 한다.
4) 기록의 불변성은 작업증명에 의한 '엄두도 못 낼 비용'이 들거나, 작업증명이 아닐 경우, 두 가지 성질 즉 첫째, 작업증명이 가진 기록자 선정의 무작위성과 둘째, '기록 변경 자체의 어려움'이라는 속성을 모두 갖춰야만 한다.[479]

이제, 이 네 가지 속성이 각각 어떤 의미를 가지는지 살펴보자.

1)번 속성은 네트워크 환경이 인위적으로 구성된 것이 아니라 자발적으로 형성돼야 한다는 점을 강조한다. 1)의 속성이 깨어진다면, '누군가' 참여와 탈퇴에 관여한다는 의미가 되고 그 누군가는 참여와 탈퇴를 통제할 수 있는 정보를 가지게 되므로 '익명의 자발적 노드'라는 기본가정 자체가 무너진다.

2)번 조건은 '내부자에 의한 시스템 남용'을 방지하는 역할을 한다. 현재의 강력한 보안 시스템은, 외부로부터의 해킹은 효과적으로 방어하지만, 내부자의 침입에는 여전히 취약하다. 권한을 가진 누군가의 강압이나, 운영자 권한을 가진 자가 자신의 이익을 위해 시스템을 남용할 가능성은 여전히 남아 있다. '신뢰받는 제3자'를 배제하려는 이유는 어느 특정 노드가 더 많은 권한이나 정보를 가질 수 없게 하기 위함이다. 이를 통해 어떠한 내부자 위협도 발생하지 않게 할 수 있다. 블록체인은 내외부인의 구분 자체가 무의미하기 때문이다. 모두가 내부자이자 외부자이다. 따라서 이 조건이 깨어지면 내부인에 의한 위협이 되살아난다.

479) 아직까지 작업증명 이외에 이 두 가지 속성을 만족하는 방법은 찾아진 것이 없다.

3)은 기록자체에 대한 신뢰를 위한 요소이다. 모든 노드는 원할 경우 기록할 권리를 얻기 위한 과정에 참여할 수 있어야 하고, 타인이 기록한 내용의 진위를 검증하는 과정에 참여할 수 있어야 한다. 기록할 권리나 기록의 진위를 검증할 권리를 소수의 노드가 독점하면 2)의 가정이 무너진다. 작업증명을 사용하지 않는 거의 모든 변형 블록체인은 기록과 검증을 소수의 노드가 배타적으로 독점하고 수행하고 있다. 나머지 노드는 권한을 가진 내부자가 기록한 내용이 '변경되었는지'의 여부만 탐지할 수 있을 뿐 정작 그 기록이 진실인지에 대한 어떠한 정보도 얻을 수 없다. 애초에 내부자가 거짓을 기록한다면, 그 거짓기록의 변경 유무는 무의미 하다.

4)의 성질은 3)에 더해 기록의 '비가역성'을 추구한다. 기록의 관점에서 블록체인과 그 변형은 크게 세 부류로 나눌 수 있다. 첫째는, 비트코인 부류로서, '진실만 기록'하고 '기록변경도 힘들게' 구현한 것이다. 이를 위해 기록의 진위는 전체 노드가 검증하고, 기록의 범위도 사전에 정의된 극도로 단순한 몇 가지로 제한되며 이에 따라 '제한된 진실'만 기록하는 효과를 볼 수 있다. 이 때문에 그 용도 또한 지극히 제한되는 단점이 따른다. 둘째는, 소위 스마트-컨트랙트를 흉내 낸 이더리움 부류로서, 비트코인처럼 사전에 정의된 제한적 기록에 '무엇이든 기록'할 수 있는 기능을 추가한 것이다. 이 기능의 추가로 인해 블록체인은 이제 더 이상 제한된 진실만 기록하는 장치가 아니라, 무엇이든 기록하는 장치가 된 셈이지만, 여전히 그 기록의 변경이 힘든 성질은 유지된다. 그러나 더 이상 기록 자체의 진위 검증은 불가능하다. 비트코인과 달리, '무엇이든 기록'할 수 있으므로 이를 검증할 수 있는 규칙 자체가 존재할리 없다. 마지막 세 번째 부류는, 무엇이든 기록할 수도 있고, 언제든지 변경도 쉽게 되는 것이다. 소위 지분증명을 사용한 EOS나 이와 유사한 페이스북의 리브라, 또 중앙화 시스템으로 구성된 리플과 이와 유사한 하이퍼 레저 패브릭 등이 이 부류에 속한다. 따라서 이 세 번째 부류는 필자의 정의에 따르면 블록체인이 아니다. 사실상 비트코인과 이더리움 정도를 제외하고는 블록체인의 정의에 부합하는 것이 없는 셈이다.

이 네 가지 조건 중 어느 하나만 위배돼도, '신뢰받는 제3자가 없어도 작동할 수 있는 익명의 시스템'은 구성할 수 없다. 아이러니한 것은, 이 네 가지 조건을 모두 완전히 만족하는 시스템은 단 한 번도 존재한 적이 없다는 사실이다.[480] 이 네 조건은

480) 미래에도 존재할 가능성은 거의 없다고 보인다.

초창기 비트코인이 구현하고자 희망했으며, 초기에 일정 시간 매우 유사한 형태로 운영도 됐지만, 곧 채굴(=기록)이 극소수 노드에 독점되면서 2)번 조건이 무너졌다. 결론적으로 지속적이고 항구적으로 이 네 조건을 만족할 수 있는 방법은 단 한 번도 찾은 적이 없는 셈이다. 2번 조건을 일부 완화하면 겨우 비트코인과 이더리움 정도가 부합된다. 한편, 하이퍼 레저 패브릭, 리플, EOS 등은 이 네 조건 중 단 한 가지도 만족하지 않는다. 이들 시스템은 형태상으로는 중앙집중 방식이며, 익명이 아니고, 절대 신뢰하는 제3자가 개입돼야 한다. 또, 기록의 비가역성이 존재하지 않고,[481] 특정 노드가 대부분의 정보와 권한을 배타적으로 소지하여 내부자의 위협이 그대로 살아 있다. 또한 블록체인의 기본 가정마저도 위배된다.

3. 블록체인의 속성과 논란

가. 탈중앙화의 비용

'기술'은 해결하려는 명백한 지향점을 가져야 한다. 새로운 기술이란, 주로 어떤 문제를 기존 기술로 해결할 수 없을 때 등장한다. 따라서 기술에는 해결하고자 하는 문제점이 반드시 존재해야 하며, 그렇지 않다면 '기술'이라는 말을 사용하는 것이 적절하지 않다.[482] 그렇다면, 블록체인은 도대체 무엇을 해결하기 위한 '기술'일까?

사토시 나카모토의 논문에 설명된, 비트코인 블록체인 기술이 해결하고자 한 명백한 지향점은 "프라이버시의 보호"였다.[483] 이러한 프라이버시 보호 운동은 그보다 20여년 전부터 시작된 사이퍼펑크(cypherpunk)의 정신을 이어받은 것인데, 사이퍼펑크란 암호를 뜻하는 cipher와 인터넷 악동을 뜻하는 cyberpunk를 조합한 신조어로서 '암호화 기술을 통해 (특히 정부로부터) 프라이버시 보호를 극대화하려는 행동주의자'를 일컫던 말이다.[484]

---

481) 이들 시스템이 주장하는 '기록의 비가역성'은 운영주체인 자신들을 '믿어야' 하는 비가역성이다. 운영주체는 언제든 기록을 쉽게 변경할 수 있다. 일정이상 채굴업자를 규합해 막대한 에너지를 투입해야 겨우 기록을 변경할 수 있는 비트코인과 이더리움의 작업증명 시스템과는 거리가 멀다.

482) 이점이 과학, 공학, 기술이라는 세 가지 용어가 뚜렷이 구분되는 출발점이다.

483) Satoshi Nakamoto, Ibid., p.1, p.6.

484) 이병욱, 앞의 책, 42면.

사이퍼펑크의 기술적 효시는 데이비드 차움(David Chaum)으로 볼 수 있는데, 그는 거래 내역을 암호화 기술로 보호하기 위해 현재 비트코인의 기술적 효시가 된 디지캐시(DigiCash)라는 개념을 제안했다.[485] 그는 정부의 사생활 침해는 물론, 일반적인 개인 정보 유출로 인한 무차별적인 스팸 등을 방지하기 위해 소위 추적정보(tracing information) 노출을 방지하는 것에 중점을 두었다.[486] 그러나 데이비드 차움의 프라이버시 보호는 슈도니머스(Pseudonymous)에 기반한 것이지만, 비트코인의 익명성은 어노니머스(Anonymous)에 기반한다는 점에서 큰 차이가 있다. 이 두 개념의 차이는 유사시에 신원을 파악할 수 있는지 여부에 있다. 둘 다 가명을 사용하지만 슈도니머스는 필요시 언제든 신원을 특정할 수 있지만, 어노니머스는 어떤 경우든 신원을 특정할 수 없는 절대 익명을 의미한다.[487] 이런 관점에서, 데이비드 차움은 금융에서의 익명성이 거래의 건전성을 파괴한다는 폐해를 잘 알고 있었던 셈이다. 슈도니머스를 위해서는 암호화 기술로 충분할 수 있으나, 어노니머스라는 절대 익명을 위해서는 암호화 기술만으로는 역부족이었고, 이 때문에 블록체인이라는 가장 비효율적인 중복의 대가를 치루고 '절대 익명의 환경'을 구축하게 된 것이다.

사실 블록체인이 탈중앙화 시스템이라는 설명에는 어폐가 있다. 현재 비트코인을 비롯한 모든 블록체인은 중앙집중 시스템보다 오히려 더 중앙화 되었다. 그나마 가장 탈중앙화에 더 가깝다는 비트코인조차 수천만 이용자가 단 10여개의 채굴업자에게 종속돼 있다. 비유하자면 전세계에 단 10개의 은행만 존재하는 셈이다.[488] 또한, 여러 관계 법령에 의해 투명성을 견제 받으며 운영되는 시중 은행에 비해, 블록체인은 그 개발자와 운영자들의 자의에 의해 얼마든지 프로그램과 규칙이 변경되고 수정되지만, 이를 견제할 수 있는 어떠한 장치도 존재하지 않는다. 이더리움의 속성을 어떻게 변경할지는 사실상 그 창립자인 비탈릭 부테린(Vitalik Buterin)이 결정하면 그것으로 끝이다. 그 누구도 견제하기 힘들며, 실제로 여러 번 전횡에 가까운 변형도 가해졌다. 이더리움 클래식이 하드포크[489]로 분리된 것도 비슷한 사례 중 하나이다.

---

485) David Chaum, "Blind signature for untraceable payments", Advances in Cryptology, springer, 1983, pp.199-203.

486) David Chaum, "Security without identification: Transaction systems to make big brother obsolete", Communications of the ACM, Vol. 28 No. 10, Association for Computing Machinery, 1985.10., pp.1030-1032.

487) Data & Marketing Association(DMA) 웹페이지, https://dma.org.uk/article/anonymous-and-pseudonymous-data-are-they-actually-important (2019년 11월 4일 최종접속) 참조.

488) 이병욱, 앞의 책, 163면.

489) 동일한 블록체인 시스템 상에 서로 다른 두 개의 블록체인 데이터가 영원히 합의되지 않고 갈라져 존재하는 상황을 일컫는 용어이다.

나. 작업증명 - 비효율의 정점 그리고 비가역성의 시작

기록의 비가역성이란 한번 기록하면, 변경하기가 지극히 힘들도록 구현한 방식을 의미한다. 이를 위해 비트코인에서는 작업증명(Proof-Of-Work)이라는 방식을 사용했다. 작업증명이란 1993년 신시아 드워크(Cynthia Dwork)와 모니 나오르(Moni Naor)에 의해 제안된 개념으로, 네트워크 자원 등의 남용을 막기 위해, 의도적으로 많은 에너지가 소모되도록 강제하는 기법이다.[490] 이는 악의적 행동에 드는 에너지가 그로 인해 얻게 되는 이익보다 더 크게 만들어, 악의적 행동을 근본적으로 억제하려는 철학을 가지고 있다. 이 작업증명에 소요되는 에너지를 흔히 난이도라고 하며, 난이도가 올라갈수록 더 많은 에너지를 소모하게 된다.

그렇다면 "한번 기록되면 다시는 변경할 수 없는 장치"가 블록체인의 구현에 있어 어떤 기능적 역할을 하는지 살펴보자. 비트코인은 생성되는 모든 기록을 전체 노드가 검증하는 방식으로 구현돼 있다. 만약 비트코인 블록체인에서 기록의 비가역성이 없다면, 한번 검증한 기록도 끊임없이 되풀이하며 다시 검증해야 한다. 과거에 검증한 기록도 언제든지 변경될 수 있기 때문이다. 그러나 기록이 변경되지 않는다는 가정이 있다면, 데이터가 생성되는 시점에 단 한번만 검증하면 된다. 따라서 전체가 검증을 되풀이하는 무한 고리를 끊기 위해서는 비가역적 저장장치가 절대적으로 필요하다.

한편, 비트코인의 "한번 기록되면 다시는 변경할 수 없는 장치"의 보다 정확한 기술적 표현은 "기록하기가 무척 힘든 장치"이다. 전자는 최초 기록은 쉽지만 그 다음 변경이 어려운 장치인 것으로 오해될 소지가 있지만, 후자는 기록 자체가 무척 힘들어 최초 기록은 물론 그 변경을 위한 기록도 동일하게 힘든 장치라는 점을 분명히 알려준다. 또 '변경할 수 없는' 장치란 이상일 뿐 현실세계에서는 존재하지 않는다. 따라서 작업증명을 통해 '변경하기 힘든(resistant)' 장치를 구현한 것이다.

작업증명의 난이도에 비례해서 비가역적 성질은 증가한다. 이는 반대로 난이도가 내려간다면 비가역성이 사라진다는 의미이기도 하다. 2017년 비트코인 채굴에 사용된 전력을 약 32.56TWh로 추정한 사람도 있는데, 이는 덴마크(30.7TWh)나 아일랜드(25.07TWh)의 2015년 전력 사용량보다도 많은 양이다.[491] 또한 30TWh는 대한민국

490) 이병욱, 앞의 책, 120면.

491) "Bitcoin: Does it really use more electricity than Ireland?", BBC News 2017.12.12., https://www.bbc.com/news/technology-42265728 (2019년 11월 4일 최종접속) 참조.

6대 도시의 가정에서 소요하는 1년치 전력량을 모두 합친 것과 맞먹는데, 우리나라가 세계 7~8위권의 전력 소비 및 생산 국가인 점을 감안하면, 채굴에 얼마나 막대한 에너지가 소비되는지 짐작이 갈 것이다.[492]

2018년 말 기준의 채굴 난이도[493]를 고급사양의 가정용 컴퓨터로 해결하려면, 대략 31조분 즉, 6천만년의 시간이 소요되며, 동시에 한 달 24시간 사용되는 컴퓨터의 전기료를 3만원으로 어림해도 6천만년 동안의 전기세는 무려 21.6조원이나 된다.[494] 결국, 비트코인 블록체인은 프라이버시 보호를 위해 익명의 세계에서도 거래가 가능케 하려는 목적은 일부 달성했으나, 그 시스템 유지를 위해 드는 천문학적인 비용은 전혀 고려하지 못했다. 사토시 나카모토는 중재를 없앰으로써, 수수료를 낮출 여지가 있다고 기대했지만, 실상은 중앙서버에 비해 수천 배 이상 더 많은 에너지가 소모되며 결론적으로 비트코인 블록체인으로 거래하면 기존보다 수천 배 더 많은 비용이 소모된다.[495]

블록체인 거래로 수수료를 낮출 수 있다는 잘못된 주장은 중재(仲裁, mediation)와 중계(中繼, relay)를 구분하지 못한 것에서 비롯된다. 제3자의 적극적 개입을 의미하는 중재 혹은 중개(仲介)와 제3자가 수동적 가교 역할을 하는 중계는 완전히 다르다. 은행을 통해 계좌이체를 할 때 은행의 역할은 중재가 아니라 중계이며, 대부분의 금융 수수료는 중계에서 발생한다. 사토시 나카모토는 블록체인으로 중재[496]를 없앴지만, 어떤 경우도 중계를 없앨 수는 없다. 블록체인은 P2P 아키텍처의 노드로 구성되며, 각 노드가 항상 중계 역할을 해야만 작동되기 때문이다. 또한 중재는 중앙화 시스템에서도 쉽게 없앨 수 있다.

블록체인은 기존보다 최소 수천 배 이상 에너지를 더 소모하고 있다. 그러나 실제 막대한 수입은 오로지 채굴업자와 암호화폐 중개소만 취하고 있고, 나머지 모든 노드는 많은 에너지를 소비하지만 단 한푼도 얻지 못한다.[497] 채굴업자와 중개소는 모두

---

492) 이병욱, 앞의 책, 242면 참조.

493) 2009년 최초의 제네시스 블록의 난이도에 비해 무려 7조배나 상승했다. 이병욱, 앞의 책, 272-274면 참조.

494) 이병욱, 앞의 책, 62면 참조.

495) 비트코인을 거래하려면 채굴업자에게 수수료를 지불해야 한다. 2017년 기준 비트코인 수수료는 30달러에 육박하기도 했다(""비트코인 수수료", 2017년 12월 대비 88% 낮아… "사용 수요 감소 탓"", coinreaders 2019년 8월 30일자, http://coinreaders.com/5313 (2019년 11월 4일 최종접속) 참조). 일례로 수수료를 30,000원이라고 가정할 때, 단돈 1원 어치의 비트코인을 송금하기 위해서 30,001원을 지급해야 하는 것이다.

496) 논문에는 'mediation'이라는 단어를 사용하였다. Satoshi Nakamoto, Ibid., p.1.

예전에는 불필요하던 존재였다. 그 중 블록체인의 기록을 담당하는 채굴업자는 그나마 비트코인 블록체인 운영을 위한 필요악으로 볼 수 있으나, 중개소는 블록체인 구성과 전혀 무관한 요소일 뿐 아니라 오히려 전체 운영비용만 크게 부풀린 측면도 있다.

블록체인은 항상 같은 일을 수만 번 이상 중복하므로 늘 동일한 작업을 하는 중앙화 시스템보다 더 많은 에너지를 소모하고 더 비효율적일 수밖에 없다. 이 때문에, 블록체인으로 거래 비용을 낮춘다는 주장은 수학적으로 수긍될 수 없는 측면이 있다. 중복에 기반하므로 항상 비용이 더 올라갈 수밖에 없는데, 거래 비용이 낮아진다고 주장하는 것은 흡사 '1+1〈= 1'이라는 얘기가 된다.

> 일부에서는 블록체인의 핵심 기능이 기록의 비가역성이며, 그 자체가 투명성이라 주장하는 사람이 있지만, 이는 블록체인을 잘못 이해한 설명이다.[498] 블록체인의 핵심기능은 '프라이버시의 보호'이다. 앞서 설명한 것처럼 기록의 비가역성은 반복적인 검증을 막기 위한 수단이자 고육지책일 뿐이며, 그 자체가 블록체인을 의미하는 것이 아니다. 비트코인에서 기록의 불변성을 위해 구현한 작업증명은 오히려 블록체인의 가장 치명적인 결함이기도 하다. 이는 채굴의 독점을 통한 중립성의 훼손과 함께 시스템을 유지하기 위한 천문학적인 비용으로 인해 블록체인 무용설이 확대된 근본 원인이기도 하다. 한편, '비가역적 저장장치'라는 것이 도대체 왜 필요한 지 한번 생각해 보자. 블록체인은 진실을 기록하는 장치가 아니라 해시함수를 통해 일관성을 유지하는 장치일 뿐이다. 따라서 비가역적 저장장치란 진실이 영원히 기록된 장치를 의미하는 것이 아니라 그저 규칙에 부합하는 일관된 기록이 변경되기 힘들게 한 것뿐이다. 어떤 기록이든 진실을 가릴 수 있는 소프트웨어라는 것은 애초에 존재할 수도 없다. 블록체인 세계의 진실(consistency)이란 그저 규칙에 부합한다는 의미일 뿐 현실세계의 진실(truth)과는 거리가 멀다.

다. 블록체인의 용도

블록체인은 절대 익명이라는 속성을 가지고 있다. 그러나 익명은 금융의 건전성에는 직접적으로 반한다. 실제로 비트코인이 세상에 가장 활발히 알려진 몇 가지 사건은 모두 돈 세탁이나 검은 거래와 연계돼 있다. 마약과 무기를 밀거래하던 블랙마켓인 실크로드(SilkRoad)는 매매 당사자의 신원을 철저히 숨기기 위해 비트코인을 활용했다. 그 운영자인 로스 윌리엄 울브리히트(Ross William Ulbricht)는 현재 FBI에 체포되어 가석방 없는 종신형을 선고받고 복역 중이다.[499] 2017년 12월 전세계 150개국의

497) 이 점은 [4-사]에서 좀 더 자세히 설명한다.
498) 이 주장은 비트코인 원논문에서 "비가역성을 통해 중재자가 기록변경을 못하도록 한다"는 문구에서 기인한 것으로 추측된다.

20만대 이상의 컴퓨터를 감염시킨 랜섬웨어(Ransom Ware)인 워너 크라이(Wanna Cry) 역시 감염자에게 예외 없이 비트코인을 요구했다.[500] 이는 모두 자신의 정체를 가리기 위한 익명의 거래가 필요했기 때문이다.

이렇듯, 블록체인은 건전한 금융과 상극인 속성을 가지며 이는 금융 건전성의 측면에서 허용할 수 없는 성질이기도 하다. 이 때문에 블록체인과 암호화폐는 많은 공격을 받았고, 다양한 집단에서 이를 극복하기 위한 새로운 주장들을 제기하기 시작했다. 블록체인을 안전한 데이터베이스라고 주장하는 사람[501]부터, 보안 도구 혹은 핀테크 도구라는 주장[502]들도 있다. 새롭게 등장한 주장들의 허구성에 대한 기술적 설명은 이 보고서의 범위를 벗어나므로 생략하지만, 거의 예외 없이 과장되고 정확하지 않은 그야말로 주장일 뿐이라는 점은 언급할 필요가 있다. 아직 그 누구도 익명 거래 이외의 블록체인의 효용을 찾은 사람은 없다. 이점이 바로 와이파이와 달리 그 누구도 단 한마디로 블록체인을 설명할 수 없는 결정적 이유이자 동시에 블록체인을 기술이라 부르는 것이 부적절한 이유이기도 하다.

라. 이더리움과 스마트 컨트랙트

이더리움(Ethereum)은 비탈릭 부테린(Vitalik Buterin)이라는 러시아 청년이 솔리더티 프로그램 언어를 개발한 개빈 우드(Gavin Wood) 등과 함께 비트코인의 기능 일부를 수정한 뒤 2015년 7월 30일에 런칭한 새로운 블록체인이다.[503] 이더리움의 등장과 함께, 소위 스마트 컨트랙트(Smart Contract)가 주목받게 된다. 스마트 컨트랙트란 1990년 말 닉 사보(Nick Szabo)가 제시한 개념이다.[504] 닉 사보는 디지털 환경을 잘 구성하면, 제3자의 개입 없이도 법률적 행위를 자동으로 실행할 수 있으며, 이

499) "미국 마약밀거래 사이트 '실크로드' 운영자에 종신형 선고", 연합뉴스 2015년 5월 30일자, https://www.yna.co.kr/view/AKR20150530012800072 (2019년 11월 4일 최종접속) 참조.
500) "워너크라이가 노린 진짜 목표는 비트코인이었다", 보안뉴스 2017년 5월 31일자, https://www.boannews.com/media/view.asp?idx=55031&kind=0 (2019년 11월 4일 최종접속) 참조.
501) "안토노풀로스 "블록체인은 안전한 데이터베이스일 뿐..." '비트코인 vs 블록체인' 논쟁에 대한 입장 밝혀", ZDNet Korea 2019년 4월 22일자, http://www.zdnet.co.kr/view/?no=20190422111031 (2019년 11월 4일 최종접속) 참조.
502) "블록체인, 어느 분야에 사용될까?", 인터스트리 뉴스 2017년 12월 27일자, https://www.industrynews.co.kr/news/articleView.html?idxno=20720 (2019년 11월 4일 최종접속) 참조.
503) 이병욱, 앞의 책, 173면.
504) 이병욱, 앞의 책, 91-93면 참조.

경우 법률 집행을 위해 변호사나 법무사 같은 제3자가 개입하여 수수료를 낭비하는 것을 막을 수 있을 것이라 생각했고, 이 '가상의 거래 프로토콜' 이름을 '스마트 컨트랙트'라고 명명했다. 물론 그의 구상은 단 한 번도 구현된 적도 없고, 그 구상 자체에도 여러 허점이 있다.[505] 이더리움은 블록에 오직 정적 데이터만 저장할 수 있던 비트코인을 조금 수정하여 블록에 컴퓨터 프로그램까지 저장하고 이를 호출을 통해 실행할 수 있도록 보강한 뒤 그 기능에 '스마트 컨트랙트'라는 이름을 붙였다.

블록체인이 제3자의 개입을 배제하려 노력한다는 점과 블록에 프로그램을 저장하고 실행할 수 있다는 두 가지 사실이 결합되면서, 이더리움은 마치 닉 사보가 구상했던 스마트 컨트랙트가 완전히 구현된 것처럼 비춰졌고 이로 인해 코인 가격이 들썩이기도 했으나, 이더리움에 구현했다고 주장하는 스마트 컨트랙트는 그 명칭만 같을 뿐 닉 사보의 구상과는 거리가 멀다.[506] 이더리움 스마트 컨트랙트의 허점은 상당히 많지만 그 중 핵심적인 것 네 가지만 정리하면 다음과 같다. 첫째, 법률관계를 프로그램 언어인 스크립트로 제작한다는 것과, 그 스크립트를 보고 거래 상대방이 완벽한 법률 구문으로 이해한다는 발상 자체가 일반인은 물론 전산을 전공한 사람에게도 사실상 불가능하다.[507] 둘째, 블록체인의 모든 정보는 보편적 검증을 위해 암호화되지 않고, 모든 노드에 브로드캐스팅[508]을 통해 그대로 노출된다. 따라서 개인정보는 물론, 어떤 민감한 정보도 기록하면 안 된다. 기록하는 즉시 바로 노출되기 때문이다. 결국 어떠한 민감한 정보도 계약에 담을 수 없으므로 의미 있는 계약을 작성하는 것이 사실상 힘들다. 셋째, 운영의 안정성을 담보할 수 없다. 이더리움 블록체인은 채굴이 멈추면 그 즉시 멈춘다. 채굴은 투입한 막대한 에너지가 적절한 보상을 받을 때만 지속 가능한 것으로서, 채굴 난이도 급증에 따라 이미 한계 상황에 와 있다.[509]

---

505) 이 구상도 중재와 중계를 구분하지 못하고 있고, 구체적인 방법론 없이 모호한 개념으로 기술돼 있다. 이병욱, 앞의 책, 93면 참조.

506) 스마트 컨트랙트와 이더리움의 한계에 대해서는 이병욱, 앞의 책, 91-94면 및 206-208면 참조.

507) 이런 관점에서는 역시 1990년대 말에 등장한 리카르도 계약(Ricardo contract)이 오히려 훨씬 더 효용이 크다. 리카르도 계약은 닉 사보의 모호한 구상이 아닌 실제 구현된 시스템으로서, 법률 문구를 효율적으로 디지털화 하여 보관하고 검색하는 마크업(Mark-Up) 언어에 대한 연구이다. 이는 스마트 컨트랙트와 달리 법률의 '집행'이 아닌, 효율적 '기록'과 '열람'이 목표이다. 이병욱, 앞의 책, 94면 참조.

508) 브로드 캐스팅(Broadcasting)은 공중파 방송을 연상하면 된다. 공중파 송신자는 수신자를 특정할 수 없다. 범위 내에 있으면 모두 수신자가 된다. 마찬가지로, 송신의 도착지를 별도로 지정하지 않고, 연결된 모든 곳에 송신하는 방식을 브로드 캐스팅이라고 한다. 이병욱, 앞의 책, 59면.

결국 중요한 계약의 저장과 집행이 안정성이 담보되지 않은 시스템에 의존한 셈이 돼버린다. 마지막으로, 닉 사보는 제3자를 제거해 수수료를 절감할 수 있는 프로토콜이라고 구상했지만, 앞서 언급한 것처럼 블록체인으로 구현하면 수수료를 절감할 수가 없다. 중재는 없애도 중계를 없앨 수는 없으며, 이더리움은 수만 번의 중복을 통해 유지되는 시스템이기 때문이다.

마. 하이퍼 레저 등 기타 변종 블록체인

본 보고서에서는 하이퍼 레저나, 리플, EoS 등의 변종 블록체인에 대해서는 별도로 설명하지 않는다. 이들 시스템은 앞서 설명한 대로 블록체인이라는 명칭을 사용하고는 있지만, 블록체인의 정의에 부합하지도 않으며 기존의 중앙화 시스템과 거의 동일한 구조를 가지므로, 기존과는 다른 새로운 문제를 부가적으로 발생시키지 않고, 기존의 제도 틀에서 살펴도 되기 때문에, 별도로 살펴야 할 실익이 없다고 할 수 있다. 다만 리플이 주장하는 외화 송금 수수료의 절감 등의 금융적 측면은 후반부에서 다시 간략히 살펴본다.

하이퍼 레저(Hyper ledger)는 리눅스 재단이 여러 업체의 지원을 받아 진행하는 블록체인 프로젝트의 명칭이며, 그 중 IBM이 주도가 된 하이퍼 레저 패브릭(Fabric)이 가장 주목받고 있다. 하이퍼 레저 패브릭은 삼성, SDS에서는 넥스 레저, LG CNS에서는 모나 체인, 아마존에서는 AMB(Amazon Managed Blockcchain)라는 다양한 이름으로 일부 변형하여 사용되고 있다. 그러나 인증된 실명에 기반한 중앙화 시스템으로 구성되는 이들 시스템을 블록체인이라 부르는 것에 대해 많은 사람들이 의문을 제기한다. 이들 업체 중 일부는, 블록체인이 미래의 신기술이라고 여전히 강하게 주장하고 있는데, 결국 장밋빛 전망에만 그칠 것인지 아니면 정말로 진정한 가치를 보여 줄 것인지 가까운 미래에 알 수 있게 되길 바란다.

---

509) 이 때문에 이더리움은 곧 지분증명으로 바꾸려 끊임없이 노력하고 하지만 여러번 실패했다. 본 보고서에서는 자세히 설명하지는 않겠지만, 지분증명으로 바꾸는 순간 앞서 정의한 네가지 속성에 모두 위배된다. 더 이상 블록체인이 아닌 셈이다. 이병욱, 앞의 책, 204-206면, 216면 참조.

4. 블록체인과 암호화폐

지금까지 블록체인의 정의를 명확히 규정하고 그 기술적 배경과 용도라는 측면에서 살펴보았다. 여기에서는 블록체인이 촉발한 암호화폐라는 측면을 별도로 살펴보자. 암호화폐와 함께 가상화폐, 가상통화 등의 여러 다양한 용어도 혼용되고 있지만, 대체로 암호화폐는 블록체인 기반의 익명성을 전제로 한 경우에 일관되게 사용되고 있다. 그러나 명칭에 포함되어 있는 '화폐'라는 단어는 수많은 혼란을 야기한다. 특히 가상통화라는 명칭의 경우 '통화'는 '유통화폐'의 줄임말이므로, 오로지 디지털화 되어 거래되는 법화에만 국한해서 사용해야 할 것이다. 최근에는 전 세계적으로, 암호화폐가 화폐처럼 오인되는 것을 방지하기 위해 각국 정부가 '암호자산(Crypto-Asset)'이라는 용어를 더 선호하고 있지만,[510] 사실 그 성질을 가장 잘 표현하는 단어는 법무부가 사용한 '가상증표'이다[511]. 명칭은 사고를 지배한다. 따라서 암호화폐라는 단어는 처음부터 일반인에게 '화폐'라는 잠재적 암시를 강요한 의도된 단어인 셈이다. 그 정체성을 명확히 규정하기 전까지 모든 용어를 '가상증표'로 통일하는 것이 가장 중립적으로 보인다.

가. 암호화폐 vs. 토큰

블록체인을 사용해 암호화폐를 발행하려면 먼저 네트워크 구성을 위한 클라이언트 프로그램을 개발해야 한다. 2009년 비트코인이 최초로 개발된 이래, 모든 소스는 공개되어 있으므로, 이를 살짝 수정하여 클라이언트를 만드는 것은 사실 그리 어렵지 않다. 실제로 비트코인 소스코드에서 채굴 시간만 조금 조정하는 등의 수정 후 만들어진 아류 코인도 부지기수다.

암호화폐 발행에 있어 사실상의 걸림돌은 프로그램이 아니라, 안정적으로 채굴할 노드와 검증할 노드를 모집해서 네트워크 생태계를 조성하는 것이다. 이는 마치 웹사이트를 제작하는 것은 쉽지만, 일정 이상의 사용자를 모으는 것은 지극히 어려운 것에 비유할 수 있다. 이처럼 하나의 생태계로 꾸린 독립적 블록체인 네트워크를 보통 메인넷(main-net)이라 부른다.

---

510) "암호화폐 바라보는 정부 부처 '동상이몽'", 팍스넷뉴스 2019년 7월 24일자, https://paxnetnews.com/articles/50721 (2019년 10월 23일 최종접속) 참조.

511) FATF는 가상자산(Virtual Asset)이라는 용어를 사용하고 있다. 자세한 내용은 후술한다.

이더리움은 메인넷 구성의 어려움을 간파하고, 자신들의 메인넷 생태계를 활성화시키기 위해 스마트 컨트랙트를 활용한 새로운 형태의 암호화폐 발행 방법을 제공했다. 즉, 별도의 메인넷을 구성하는 번잡함 없이, 스마트 컨트랙트를 이용하여, 이더리움 생태계 내에서 간편히 암호화폐를 발행할 수 있는 방법을 제공한 것이다.[512] 모든 생태계는 이더리움을 그대로 활용하되, 자신만의 암호화폐를 손쉽게 제작하고 매매할 수 있는 길이 열린 것이다. 이더리움은 이러한 암호화폐를 메인넷을 갖춘 암호화폐와 구분하기 위해서 토큰(Token)이라는 용어를 사용하기 시작했고, 현재 암호화폐 커뮤니티에서는 암호화폐란 자체적 메인넷을 갖춘 것을, 토큰은 그렇지 않고 메인넷에 기생(寄生)하는 것을 가리키는 용어로 널리 사용되고 있다.[513] 이더리움은 크게 ERC-20과 ERC-721이라는 두 가지 표준을 정하고, 각각의 샘플 코드를 배부하며 적극 홍보[514]하였고, 그 결과 2019년 11월 3일 기준으로, 이더리움에는 222,795개의 ERC-20 토큰과 2,712개의 ERC-721 토큰이 기생하고 있으며, 이 중 980여개는 중개소를 통해 직접 판매되고 있다.[515] 판매되는 토큰 상당수는 중개소들이 직·간접적으로 제작에 개입한 것으로서, 토큰은 숙련된 프로그래머의 경우 겨우 며칠이면 제작할 수 있을 정도로 간단하다. 이러한 토큰들은 임의로 발행된 뒤 중개소 등을 통해 그럴싸한 내용으로 포장된 다음 대대적인 마케팅과 함께 일반인에게 판매된다. 이러한 토큰들은 제작 및 매매만을 용이하게 만든 가상의 디지털 숫자일 뿐 다른 그 어떠한 기능이나 효용도 찾아보기 힘들다.[516]

ERC-20 토큰은 많은 업체들이 자신들을 블록체인 기업이라고 포장할 때 악용되기도 한다. 제대로 된 사업모델이나 기술을 갖지 못한 업체가 스마트 컨트랙트 몇 줄로 ERC-20 토큰을 발행한 다음, 블록체인 기술 기업으로 주장하는 사례가 그것이다. 이들의 주된 목표는 자극적인 아이디어를 나열하며 일반인들을 호도하고, 중개소에

---

512) "What is Ethereum, and What Are Smart Contracts?", How-To Geek 2018.5.9., https://www.howtogeek.com/350322/what-is-ethereum-and-what-are-smart-contracts/ (2019년 10월 23일 최종접속) 참조.

513) 토큰(Token)이란 원래 보상을 위한 모든 행위나 체계를 의미하는 포괄적 용어로서, 이더리움이 사용하는 토큰의 의미와는 완전히 다르다.

514) "What Is ERC-20 and What Does It Mean for Ethereum?", Investopedia 2019.6.25., https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/ (2019년 11월 4일 최종접속) 참조.

515) 이더스캔(Etherscan) 웹사이트, www.etherscan.io (2019년 11월 4일 최종접속) 참조.

516) 이병욱, 앞의 책, 34면.

토큰을 등록한 다음 비싼 값에 파는 것이다.[517] 이러한 일련의 과정에 아이디어의 구체성과 실현 가능성은 중요하지 않다. 이익추구의 관점에서만 보면, 판매자나 구매자 모두 아이디어를 구체적으로 실현해 수익을 얻는 것이 아니라, 오로지 중개소에 토큰을 등록하여 이익을 취하는 것이 더 손쉽고 빠르기 때문이다. 오히려 아이디어가 보다 허황되고 자극적일수록 코인 값 폭등에는 도움이 되기도 한다. 이러한 사례의 경우에는 조잡한 프로그램 몇 줄 이외에는 그 어떠한 효용이나 기술이 개입되지 않아도 된다.

블록체인으로 상거래 비용을 대폭 낮췄다고 주장하는 상당수 업체들도 ERC-20 코인을 동원한다.[518] 이들은 중앙화 서버를 구축해 상거래 모형을 만든 뒤, 수수료가 무료거나, 반값이라고 선전하며 손해를 감수한다. 이러한 손해는 별 문제가 되지 않는다. 동시에 발행한 ERC-20 토큰을 통해 자신들을 블록체인 기업이라 홍보할 수 있기 때문이다. 이들은 ERC-20을 내세워 표면적으로는 블록체인이라는 신기술을 통해 비용을 절감한 것처럼 내세우면서, 중개소에 등록한 토큰을 일반인에게 판매해 실질적인 이익을 취한다. 이렇게 조달된 자금은 수수료 감소로 입은 손해를 모두 복구하고도 남을 만큼 넉넉하다. 전 세계 여러 업체들이 이 방법을 사용하며, 우리나라도 예외가 아니다. 토큰이나 지역화폐를 생각하고 있다면, 중앙화 서버로 발행된 안정된 방식을 택해야 한다. 단지 ERC-20을 발행했다고 스스로 블록체인 기업이라 주장하는 것은 기술을 호도하는 행위로 평가될 우려가 있다.

나. 블록체인과 금융

블록체인을 이용해 금융비용을 대폭 낮춘다는 주장들도 많다. 대표적인 것이 리플이다.[519] 리플은 블록체인을 활용해 국제송금에서 SWIFT의 고비용을 없앨 수 있는

---

517) 이 과정은 ICO의 기망행위와 직결되며, ICO는 뒷부분에서 다시 살펴본다.

518) 예컨대, COINJINJA 웹사이트를 보면 "Cryptocurrency를 받아들일 수 있는 오랫동안 기다려온 POS 네트워크. 암호 보유자는 날마다 물건을 쇼핑할 수 있습니다. 판매자는 매우 독특하면서도 전통적인 결제 단말기를 이용할 수 있습니다. Coinnup POS 단말기는 최대 200%의 비용 절감으로 올인원 지불 솔루션을 제공합니다."와 같은 말로 금융 거래 비용을 절감할 수 있다고 홍보하고 있다(COINJINJA 웹페이지 https://ko.coinjinja.com/ico/coinnup (2019년 11월 4일 최종접속) 참조).

519) 리플은 앞서 설명한 것처럼, 블록체인의 정의에 부합하지 않는다. 대표이사인 브래드 갈링하우스(Brad Garlinghouse) 스스로가 리플은 블록체인이 아니라고 여러 번 언급했지만, 정작 자사 홈페이지에는 "가장 진보한 블록체인"이라고 선전하는 모순적 태도를 보이고 있다.

획기적 방식을 개발한다고 홍보한다.[520] 그러나 리플 등이 주장하는 금융혁신은, 기술 관점의 개선보다 기존의 거버넌스를 우회하는 측면이 있다.

국제 송금의 과도한 비용은 기술부족 때문이 아니라, 대부분 제도나 배타적 지배력에서 기인한 측면이 강하다. 금융거래의 지급-결제-청산 비용이나, 자금세탁 방지를 위한 KYC(Know Your Customers)가 그 대표적 예이며, SWIFT는 특히 미국의 자금세탁 방지를 위한 수많은 거버넌스 요구를 지키기 위해 고군분투하고 있다. 물론 독점적 지위를 가진 SWIFT의 전횡도 일정 부분 존재하지만, 금융에 있어 거버넌스는 고비용을 무릅쓰더라도 반드시 지켜야 할 중대한 사안이다. BNP Paribas는 2014년 이란, 쿠바 등에 달러 결제를 한 혐의로 미국으로부터 역대 최고 금액인 무려 한화 10조원에 해당하는 89억달러의 과징금으로 부과받았으며,[521] 스탠다드 차타드도 2019년에 비슷한 혐의로 11억 달러의 벌금을 부과받았다.[522] 이처럼, 대테러 자금 방지와 관련되어 자금세탁 방지에 관한 까다로운 규정은 전 세계적으로 막대한 비용을 야기하고 있다.

그런데 리플이 XRapid라 이름 붙인 새로운 송금 방식을 들여다보면, 외화 송금 당사자가 자국의 코인 중개소에서 송금하려는 금액만큼의 리플코인을 구매 후 이를 수취인에게 전송하고, 수취인은 자국의 중개소에서 이를 매매해 송금액을 다시 되찾는 방식으로 구성된다. 이 방식은 기술 혁신 보다는 오히려 중개소를 통한 환치기로도 해석될 수 있는 형태이다. 한편, 이 과정에서 KYC는 모두 해당국 각자의 서로 다른 법령을 따르는 중개소에 맡겨지므로 급격히 약해진다. 이 방식을 허용할 것이라면, 오히려 아마존 등의 중앙화 서버를 이용해 구현하는 것이 비용이나 추적 관점에서 오히려 훨씬 효율적일 수 있다.

XRapid의 실효성에 대한 의문이 제기되자, 리플은 XCurrent라 이름의 새로운 방식

---

520) Mike Faden, "The Future of Cross-border Payments: Ripple versus SWIFT", American Express, https://www.americanexpress.com/us/foreign-exchange/articles/ripple-vs-swift-gpi-cross-border-payments/ (2019년 11월 4일 최종접속) 참조.

521) "BNP Paribas sentenced in $8.9 billion accord over sanctions violations", Reuters 2015.5.2., https://www.reuters.com/article/us-bnp-paribas-settlement-sentencing/bnp-paribas-sentenced-in-8-9-billion-accord-over-sanctions-violations-idUSKBN0NM41K20150501 (2019년 11월 4일 최종접속) 참조. 이 사건은 필자가 BNP Paribas 그룹 재직 시 발생한 것으로, 벌금 부과 후 그룹 내 거버넌스와 KYC의 대폭 강화는 물론 모든 의사결정 과정의 모니터링 강화를 위해 천문학적인 부가 비용이 투입되었다.

522) "Standard Chartered Fined $1.1 Billion for Violating Sanctions and Anti-Money Laundering Laws", The New York Times 2019.4.9., https://www.nytimes.com/2019/04/09/business/standard-chartered-sanctions-violations.html (2019년 11월 4일 최종접속) 참조.

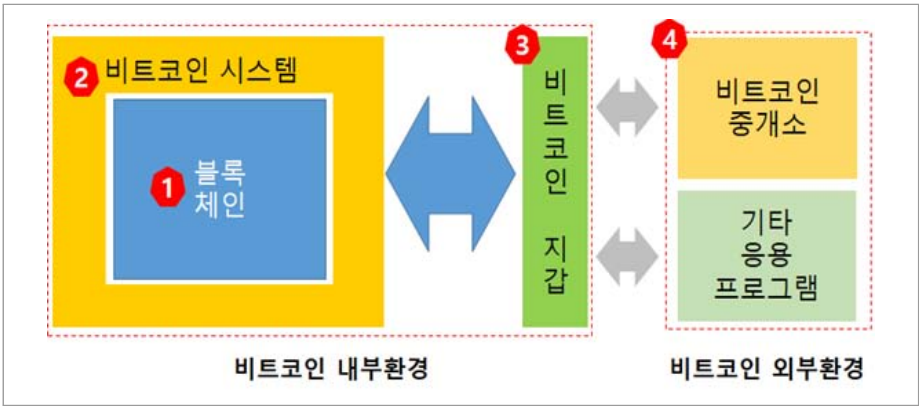
을 제안한다. 그러나 XCurrent는 사실상 모든 금융기간 간 청산 및 결제를 위한 계좌를 서로 직접 개설하여 운영하는 방식과 유사하므로 더 많은 비용이 소모될 수 있고, 통합적 KYC 관리가 약화되며, 각 금융기관이 쌍을 이뤄 각각의 계좌를 직접 개설한다는 것도 사실상 불가능하다.

이렇듯 저마다 블록체인을 내세워 핀테크 금융혁신을 주장하는 업체가 많지만, 많은 경우 금융의 거버넌스, 특히 KYC를 약화 또는 우회하여 비용을 낮추려는 시도에 해당될 뿐 기술혁신은 찾아보기 힘들며 경우에 따라 금융의 기본 질서를 무너뜨릴 수 있는 위험도 있다. 한편, 전술한 대로 리플은 탈중앙화 시스템도 아니므로 블록체인도 아니지만, 여전히 블록체인이라는 주장을 고집한다. 한편 블록체인은 금융의 건전성에 정면으로 반하는 익명성을 가지므로, 블록체인으로 금융을 혁신한다는 시도는 근본적인 모순을 안고 있는 측면이 있다.

다. 암호화폐 지갑과 암호화폐 중개소

[그림 4-1]은 비트코인 블록체인과 이를 둘러싼 환경 사이의 상호관계를 보여준다. 블록체인은 여러 방식과 응용으로 구현할 수 있고, 블록체인을 지급결제 수단에 응용한 사례가 바로 비트코인이다. 비트코인은 그림에서 블록체인(①) 자체와 그 응용(②)을 같이 칭하는 것으로서 시스템의 핵심 요소이다.

[그림 4-1] 블록체인과 외부환경의 관계[523]



523) 이미지 출처: 이병욱, 앞의 책, 157면.

이 중 그림의 ③은 블록체인과는 직접 관련이 없지만, 블록체인에 보관된 비트코인을 사용하기 위해 반드시 필요한 요소인 지갑이다. 지갑은 응용프로그램으로서 이를 통해 비트코인 블록체인과 통신한다. 비록 블록체인과는 직접적인 관련은 없지만, 지갑이 없이는 비트코인을 사용할 수 없으므로 ①, ②, ③을 모두 묶어 통상 비트코인의 내부환경이라 말할 수 있다.[524]

한편 그림의 우측에 있는 ④는 블록체인과는 무관한 요소로서, 사용의 편의성만을 위해 존재하는 외부환경이다. ④는 지갑 소프트웨어와 통신한다. 따라서 ④가 없더라도, 블록체인 사용에는 아무런 지장이 없다. 많은 경우, 중개소들이 자신들의 중개매매 시스템을 통합해 제작한 지갑 소프트웨어를 직접 배부하여 코인 매매를 적극 유도한다. 중개소는 외부 요소로서, 증권사의 HTS 거래 시스템을 흉내 낸 중앙화 시스템으로 운영된다. 대부분의 암호화폐 거래자는 자신이 구매한 암호화폐가 자신의 명의로 블록체인에 안전하게 보관돼 있을 것이라 착각하지만 실상은 그렇지 않다. 통상 자신이 구매한 암호화폐는 자신의 명의로 블록체인에 존재하지 않으며 오직 중개소의 중앙화 서버에 거래 수량만 기록돼 있다. 그리고 각 중개소는 해킹의 위협에 그대로 노출돼 있다. 이 부분은 아래 3)에서 자세히 좀 더 살펴보자.

1) 암호화폐 지갑

[그림 4-1]에서 ③번 영역이 암호화폐 지갑이다. 지갑이라는 명칭 때문에 암호화폐가 이곳에 직접 보관되는 것으로 오해할 수 있지만, 사실 지갑에는 어떠한 암호화폐도 보관되지 않는다. 암호화폐는 오직 블록체인 내에서만 존재한다. 비트코인 지갑은 크게 세 가지 역할을 수행하는데, 첫째는 거래에 사용되는 암호화 키를 생성하고, 보관하는 일이며, 둘째는 거래에 사용될 계좌번호에 해당되는 비트코인 주소를 생성하는 일이다. 이 비트코인 주소는 지갑이 생성한 암호화 키 중 공개키로부터 일정 규칙에 의해 고쳐 생성된다. 마지막으로, 지갑은 암호화 키와 비트코인 주소를 사용하여, 거래 내역을 작성한 후 블록체인 네트워크에 제출하는 일을 수행한다.

블록체인은 비대칭 암호화 기법을 사용하는데, 이는 쌍이 되는 두 개의 키를 이용한

524) 암호화폐가 없는 블록체인 시스템에서는 지갑이 아예 없거나, 트랜잭션만 구성하는 용도 등으로 사용될 수 있다.

다. 쌍이 되는 키 중 자신만이 비밀리에 보관하는 키를 개인키(Private Key) 또는 비밀키(Secret Key)라 부르고, 타인에게 공개하는 키는 공개키(Public Key)라고 부른다. 공개키는 개인키를 사용해 생성하지만, 공개키로는 개인키를 생성할 수 없다. 암호화에는 개인키나 공개키 모두 사용할 수 있는데, 개인키로 암호화 한 것은 해당 공개키로만 복호화 되고, 공개키로 암호화 한 것은 오직 해당 개인키로만 복호화 된다. 비대칭 암호화 기법은 전자서명의 용도에 활용할 수 있는데, 문서 내용의 해시를 생성한 후 이를 개인키로 암호화하면 전자 서명이 된다. 지갑에는 이 개인키가 보관되어 있다.

블록체인의 개인키는 통상 256비트(=32바이트)이상의 길이를 가진 임의의 정수로 생각하면 된다.[525] 이 개인키는 블록체인에 보관되어 있는 암호화폐의 소유권을 증명할 때 필요하다. 블록체인의 모든 거래 데이터는 각 수령인의 공개키 해시[526]를 사용해 잠금 장치를 하고 이 데이터는 송신인의 개인키로 서명한다. 이 잠금장치는 해당 키를 소유한 사람만이 해제하고 사용할 수 있다.

32바이트 이상의 길이를 가진 임의의 정수를 무차별 대입법으로 찾아내는 것은 불가능하다.[527] 그러나 이 개인키를 보관하고 있는 지갑 소프트웨어의 비밀번호는 얘기가 다르다. 사용자가 비밀번호를 어떻게 설정했느냐에 따라 통상적 방법으로도 해킹이 가능할 수 있다. 지갑의 비밀번호를 알아내면, 지갑에 보관된 개인키를 소유한 셈이지만, 이 소유권은 배타적인 것이 아니다. 다른 사람이 동시에 비밀번호를 알고 있는 경우나 개인키 자체를 복제한 경우라면 복수의 사람이 동일한 권한을 가질 수 있기 때문이다.

2) 암호화폐의 몰수

2018년, 대법원은 범죄에 연루된 피고인의 비트코인의 몰수를 인정한 판결[528]을

525) 따라서 이렇게 긴 숫자를 외우는 것은 불가능하다. 대부분의 블록체인은 256비트의 길이를 사용하지만, 더 긴 키를 사용할 수도 있다.
526) 이 값은 상대방의 비트코인 주소에 포함돼 있다.
527) 전산에서의 불가능은 impossible 대신 resistance라고 부른다. 앞서 6천만년이 걸리면 채굴이 가능하다고 했다. 6천만년은 수학적으로는 가능한 것이지만, 실질적으로는 불가능하다고 말할 수 있다. 모든 비밀번호는 언젠가는 알 수 있다. 시간이 문제이다. 따라서 전산에서는 통상 지수(exponential) 시간에 해결되는 문제들은 불가능(resistance)이라는 말을 많이 사용한다.
528) 대법원 2018. 5. 30. 선고 2018도3619 판결.

내린 바 있다. 비트코인은 블록체인에 보관돼 있으므로, 이에 임의로 접근하여 몰수할 수 있는 방법은 없다. 따라서 이를 몰수하려면, 우선 해당 개인키를 사용해 잠금 장치를 풀어야 한다. 그러므로 피고인의 개인키가 보관된 지갑 소프트웨어의 비밀번호를 알아내거나 개인키 자체를 알아내야 한다. 이를 알아내는 방법은 피고인이 자백하거나 해킹으로 피고인 지갑의 비밀번호를 알아내는 수밖에 없다. 개인키 자체를 해킹으로 알아내는 것은 불가능하기 때문이다.

한편, 지갑의 비밀번호를 알아낸다고 해서 바로 해당 비트코인에 대한 압류가 이루어진 것은 아니다. 개인키는 얼마든지 복제할 수 있으므로, 앞서 설명한 대로 지갑의 비밀번호를 알아냈다는 것은, 단지 해당 비트코인에 접근할 수 있는 사람들 중 한 명이 되었다는 것에 불과하다. 이를 확실히 몰수하려면 해당 비트코인을 피고인이 접근하지 못하는 다른 곳으로 옮겨야 한다. 예컨대, 새로운 개인키를 사용해 비트코인 주소를 생성한 후, 피고인의 개인키를 사용해 몰수대상 비트코인을 새로 생성한 주소로 전송하면 된다. 일단 이렇게 전송된 비트코인은 이제, 피고인이 가진 개인키로는 다시는 접근할 수 없다.

3) 중개소와 해킹

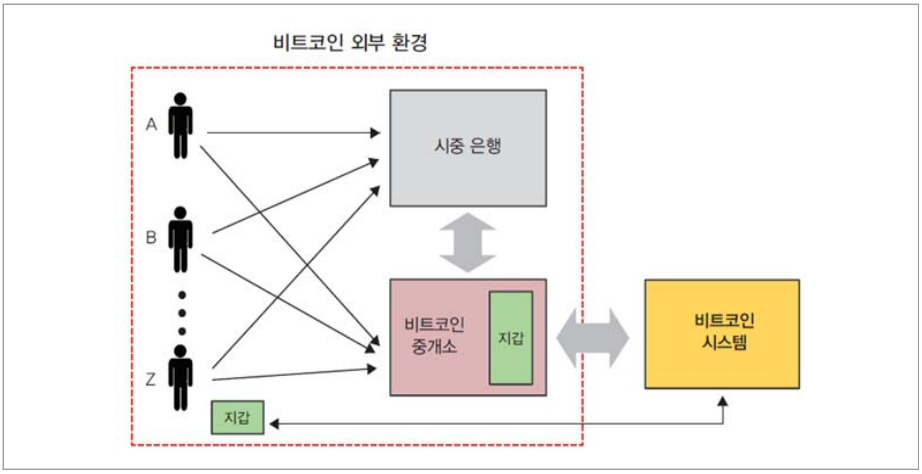
암호화폐 중개소는 암호화폐의 구매자와 판매자를 이어주는 브로커들이다. 스스로는 거래소라 칭하며 마치 잘 제도화된 거래환경이 갖춰진 것으로 포장하지만, 관계법령에 따라 운영되며 모든 매매 주문을 단일가로 통일해 관리하는 증권거래소와는 거리가 멀다.[529] 모든 거래 주문은 개별 브로커들에 의해 매치되므로 형성 가격도 브로커들마다 제각각이며, 어떤 암호화폐를 중개할지도 오롯이 브로커들이 자의적으로 정한다. 그러므로 중개소라는 명칭이 보다 적절하나, 거래소라는 용어도 혼재되어 사용되고 있는 것이 현실이다. 암호화폐 시세 및 거래량 등 암호화폐 현황 분석·제공 사이트 코인마켓캡(CoinMarketCap)에 따르면, 2019년 11월 3일 현재 전 세계에 알려진 브로커만 21,051개나 되며, 하루 20~30개나 새로 생겨난다.[530] 이처럼 전 세계적으로 중개소가 넘쳐나는 이유는 쉽게 돈벌이가 되는 반면 별다른 기술이 필요 없기

529) 이병욱, 앞의 책, 35면.
530) CoinMarketCap 웹사이트, http://www.CoinMarketCap.com (2019년 11월 4일 최종접속) 참조.

때문이며, 특히 국내의 경우에는 업종도 금융이 아닌 통신판매업으로 분류돼 설립도 쉽기 때문이다.

이제 다음 그림을 보면서 중개소에서 암호화폐를 구매하면 어떤 일이 벌어지는지 살펴보자.

[그림 4-2] 중개소를 통한 비트코인 거래[531]



[그림 4-2]는 사용자들과 중개소의 관계를 보여준다. A와 B가 암호화폐를 구매하면, 중개소들은 실제 거래가 일어난 것처럼 중앙화 서버에 있는 숫자를 조작해 표시해 주므로, A, B는 구매한 암호화폐가 그들의 명의로 블록체인에 보관된 것으로 착각하지만, 블록체인상의 거래는 일어나지도 않는다. 실제 블록체인 거래는 시간도 오래 걸리고 채굴업자에게 별도의 수수료를 지불해야 하는 등 번거롭기 때문이다. 사용자들의 매매에 비례하여 중개소의 수수료 수입[532]이 증가하므로, 매매 회전률을 극대화하기 위해 중개소들은 마치 실제 거래가 일어난 것처럼 꾸밀 뿐이다. 결국 A, B는 자신들의 가상계좌를 통해 법화를 중개소에 건넸지만 자신들의 거래는 유보된 셈이고 실제로 비트코인을 소유한 적은 단 한 번도 없다. 모든 비트코인은 중개소 명의의 주소에 위탁 보관된 셈이다.

---

531) 이미지 출처: 이병욱, 앞의 책, 169면.
532) 대체로 거래액의 0.1~0.2%이며, 이는 HTS 증권거래 수수료의 10배에서 100배나 된다.

이 때, 그림의 Z처럼 지갑을 설치하고 자신의 비트코인 주소로 암호화폐를 송금할 것을 요청하면, 중개소는 비로소 위탁 분량 중 요청한 수량만큼 실제 블록체인 거래를 일으켜 이전해 준다. 이때도 고객에게는 통상 고액의 인출 수수료를 부과한다.

중개소들의 보안 수준은 천차만별이지만, 적절한 관리감독은 이루어지지 않고 있다. 통신판매업으로 신고하고 영업하기 때문이다. 해커들은 경우에 따라 비교적 손쉬운 방법으로 중개소를 해킹한 다음, 암호화폐를 절취할 수 있다. 다시 [그림 4-2]를 보자. 그림 중 Z가 해커라고 가정하자. Z는 다음의 절차를 통해 A의 암호화폐를 절취할 수 있다.

① Z는 중개소를 해킹한 다음, 자신의 신원이 A인 것처럼 속인다.
② Z는 해킹한 중개소에 자신이 지정한 비트코인 주소로 A가 위탁한 모든 암호화폐를 송금할 것을 요청한다.
③ 해킹을 당해 Z를 A로 오인하고 있는 중개소는 A가 위탁한 모든 비트코인을 중개소 명의의 비트코인 주소에서 Z의 비트코인 주소로 송금한다.

만약 중개소는 오로지 중개역할만 하고, A, B 각자 명의의 비트코인 주소로 매번 실제거래가 일어났다면 해커들은 중개소를 통해 이들의 암호화폐를 해킹할 방법이 없다. 이 경우 모든 책임은 A, B 각자에 귀속되며 중개소는 책임이 없다고 보는 것이 옳다. 그러나 전술한 것처럼 실제는 이와 많이 다르다. Z에게 해킹 당해 송금한 중개소는 A명의로 블록체인에 있던 비트코인이 아닌, 중개소 소유의 비트코인을 Z에게 송금한 것이다. 결국 기술적 측면에서는 A는 자신의 암호화폐를 도난당한 적이 없다고 해석할 수 있는 여지가 생긴다.

2018년 12월 국내 중개소가 해킹 당해 4억 7,000만원을 도난당한 박모씨가 중개소를 상대로 낸 손해 배상 청구소송에서 국내 법원은 중개소의 배상 책임이 없다는 판결을 내렸다. 재판부는 가상화폐는 「전자금융거래법」을 적용할 수 없다고 판시하였다.[533] 그러나 이 판결은 기술적 관점에서 보면 부정확하다고 판단할 소지가 있다. 사용자들은 구매를 위해 법화를 중개소에 건넸지만, 실제 구매는 일어나지 않고 유보된 상태였으므로, 고객들은 암호화폐가 아닌 법화를 보관해 둔 것으로 해석할 수도

533) 서울중앙지법 2018. 12. 20. 선고 2017가합585293 판결.

있다. 또한 해킹을 통해 사라진 것도 고객 명의의 암호화폐가 아니라 중개소 명의의 암호화폐이기 때문이다. 경찰청 자료에 따르면 2016년 7월부터 2019년까지 3월까지 알려진 것만해도 국내 중개소가 8번의 해킹을 당해 총 1,635억원을 도난당했으며, 이 중 국내 최대 규모 중개소인 빗썸은 3건의 해킹을 통해 무려 793억원의 손실을 입은 것으로 파악됐다.[534]

라. 디지털 자산

디지털 자산은 가치가 형성된 유무형의 자산들, 예컨대 저작권이나 권리 등을 그 거래나 보관의 편의성을 위해 디지털화한 것을 의미한다. 디지털화한 음악, 소설 등이 무형자산을 디지털화한 대표적인 예이며 KRX의 금거래는 매매의 편의성을 위해 실물 금을 디지털화한 대표적인 예이다. 즉 디지털 자산이란 유형이든 무형이든 '이미 가치를 가진 그 무엇'을 디지털화한 표식이다. 암호화폐를 디지털 자산이라 주장하는 사람도 있지만 이는 잘못된 것이다. 암호화폐는 '이미 가치를 가진 그 무엇'이 아니다. 암호화폐의 가치는 0이며, 디지털 숫자에 불과하다. 물론 암호화폐도 미래에 어떤 가치를 가질 가능성이 있지만, 미래의 가능성까지 포함한다면 전 세계의 모든 디지털 데이터는 디지털 자산으로 분류해야 할 것이므로, '디지털 자산'이라는 별도의 용어를 사용할 실익이 없다.[535] 가치를 지니고 있는 자산을 디지털화하여 보관하려는 추세는 자연스러운 것이며, 향후에도 가속화 될 것이지만, 이미 가치를 가진 그 무엇을 디지털화한 것을 지칭하는 '디지털 자산'과, 가치를 갖고 있지 않은 디지털 숫자에 가치를 주입하려는 시도는 완전히 구분해야 되며, 이러한 시도에까지 '디지털 자산'이라는 용어를 사용하는 것은 적절치 않다.

마. 자산유동화 토큰

디지털 자산에서 파생된 개념인 '자산유동화 토큰'도 사정은 비슷하다. '자산유동화

534) "가상화폐 거래소 해킹 피해 금액 3년간 1천635억 원", SBS 뉴스 2019년 10월 14일자, https://news.sbs.co.kr/news/endPage.do?news_id=N1005465666&plink=ORI&cooper=NAVER (2019년 11월 4일 최종접속) 참조.

535) 분류의 실익을 떠나 용어만 따지면, '자산의 디지털화'와 '디지털 자산'도 구분할 수 있다.

토큰'은 '이미 가치를 가지고 있는 그 무엇'을 여러 조각으로 개념적으로 분할한 다음 토큰과 매치시킨다는 개념이다. 예컨대 고가의 자산을 개념적으로 n조각으로 분할 후 이를 n개의 토큰과 매칭하면, 적은 자금으로도 고가의 자산 중 일부를 손쉽게 소유할 수 있다는 주장이다. 일각에서는 자산유동화 토큰이라는 이름으로 부동산, 미술품 등을 ERC-20 이더리움 토큰 등과 매칭하여 금융혁신을 이룬다는 주장도 등장했다. 미국 부동산 네트워크 플랫폼이라 주장하는 RealT가 RealToken을 코인 중개소에 등록한 것이 좋은 예이다. 이 회사는 미시간 주 디트로이트에 있는 부동산을 기반 자산으로 매칭한다고 홍보하고 있다.[536]

자산유동화 개념 자체는 자산의 디지털화 과정에서 등장할 수 있는 자연스러운 발상이며, 향후에도 여러 자산에 적용을 시도할 것으로 보인다. KRX 금거래는 이미 잘 정착된 자산유동화 토큰의 사례로 볼 수 있다. 물론, KRX 금거래에는 명시적인 토큰이 발행되지 않지만, 거래에 따른 잔고가 기록된 한국예탁결제원 서버의 '디지털 숫자'가 토큰과 동일한 역할을 한다고 볼 수 있다.[537]

자산유동화 토큰 성공의 핵심은 토큰의 소유권과 자산의 소유권 사이의 등가성을 보장해 주는 것에 있다. 많은 사람들이 '블록체인'을 활용한 토큰으로 자산유동화를 하면 토큰 소유권과 자산에 대한 소유권이 일치한다고 착각하고 있다. 이러한 오해는 상당부분 토큰 발행회사가 의도적으로 기술을 호도해 사실관계를 왜곡한 측면도 강하다. 토큰을 소유하더라도 그 자체로는 자산에 대한 그 어떠한 권리도 발생하지 않는다.

부동산을 예로 들어보자. 주지하듯, 부동산에 대한 권리의 등록과 관리는 오직 등기소에서만 이루어진다. 토큰을 소유한다고 해서 등기소에 1/n 조각이 자신의 명의로 자동으로 등록되는 일 따위는 결코 일어나지 않는다. 따라서 토큰으로 부동산에 대한 1/n의 권리를 행사할 수 있는 유일한 방법은 토큰 발행사가 그 권리를 보장해 줄 때 뿐이다. 모든 부동산은 그 업체가 자신의 명의(혹은 신탁회사)로 등기소에 등록해 두었을 것이기 때문이다. 이때, 토큰 발행사가 계약과 관련한 신의칙을 위배하면, 권리행사는 심각한 위협을 받는다. 결국, 자산유동화의 핵심은 소프트웨어가 아니라,

---

536) "백트, 커스터디 서비스 정식 출시...라이선스 취득". 매일경제 2019년 11월 12일자, https://www.mk.co.kr/news/economy/view/2019/11/933319/ (2019년 11월 30일 최종접속) 참조.

537) 예탁원 서버에 기록된 토큰을 암호화폐처럼 개인 간에 직접 매매할 수 있게 중개하는 주는 곳은 없지만, 이는 기술의 문제가 아니라 정책의 문제이다.

토큰 발행 기관이 디지털 형태로 대위(代位)된 권리를 보장해 줄 수 있을 만큼의 절대 '신뢰'를 가진 곳이냐에 달려 있다.

KRX 금거래를 다시 예로 들어보자. KRX 금거래는 자산유동화를 통해 증권거래소에서 1 그램 단위로 금을 쉽게 매매할 수 있는 편리한 방식이다. 구매한 금은 모두 디지털화(=토큰화) 돼서 보관되며, 원할 경우 1kg 단위로 현물로 인출할 수도 있다. 고객들이 이 방식을 안심하고 이용할 수 있는 근본적인 이유는 이 거래에는 절대 신뢰를 가진 기관이 무려 세 군데나 개입되기 때문이다. 첫째, 한국예탁결제원은 고객이 매입한 금에 해당하는 실물을 책임지고 보관한다. 둘째, 한국조폐공사는 금의 순도가 99.99%라는 것을 보장한다. 셋째, 증권거래소는 거래의 투명성을 보장한다.

한편, 자산유동화를 위해 토큰을 발행할 때 중앙서버가 아닌 ERC-20 등을 활용하면, 관리와 운용 측면 모두에서 매우 비효율적일 수 있다. 또한 ERC-20 토큰은 발행 후 소유자가 임의로 매매할 경우, 실소유자를 추적할 수도 없고, 일부가 개인키 분실 등으로 ERC-20 토큰을 잃어버리면 되찾을 수 있는 방법도 없다. 이런 경우, 미래에 대상 부동산을 매각하기 위해 발행된 토큰을 모두 회수해야 할 경우, 이를 처리할 수 있는 방법도 없다. 따라서 이런 관점에서는 부동산을 ERC-20으로 매치하는 시도는 해서는 안 되는 선택으로 볼 수도 있다.

수많은 단점에도 불구하고 ERC-20을 선호하는 이유는 '블록체인'이라는 키워드를 통해 인위적 가치가 주입될 수 있다는 기대 때문으로 보인다. 블록체인으로 자산을 유동화 한다는 말은 새로운 기술로 효용을 창출하는 것처럼 들릴 수 있지만 이는 사실이 아니다. 정리하자면, 자산유동화의 핵심은 전산 인프라가 아니라 토큰의 권리를 보장해 줄 수 있는 '신뢰할 수 있는 기관'의 책임 있는 개입이다. 토큰의 소유는 그 자체로 절대 자산의 소유권을 보장해 주지 않는다.

바. ICO

ICO는 'Initial Coin Offering'의 약자로 투자를 대가로 주식을 지불하는 IPO(Initial Public Offering)에 빗댄 신조어다. ICO를 간편한 자금 조달 창구라 주장하며, 그 필요성을 역설하는 사람이 있지만,[538] ICO는 구조적으로 여러 결함을 갖고 있다. ICO의 핵심적 문제점은 '투자자 보호' 장치의 결여다. ICO가 '간편한' 자금 조달 창구

역할이라는 주장에서의 '간편'은 모금자의 입장에서의 평가일 뿐, 이를 위해 투자자의 권리와 그 보호는 크게 희생된다. ICO에서는 법화가 아닌 암호화폐로 투자되므로 IPO처럼 법령에 의한 투자자 보호 장치는 작동하지 않는다. 공시 의무도, 정보 청구권도, 준법 감시 의무도 없다. 오직 당사자들의 민사적 협약에 따른 규칙만 존재할 뿐이다.

한편, ICO의 성공은 제품이나 서비스의 출시를 통한 매출이 아니라, 발행한 토큰이 대형 중개소에 등록 되느냐의 여부에 달려있다. 때문에 사업의 실현 가능성보다는 자극적인 아이디어를 포함시켜서 코인 값을 부양하는 것이 더 우선이다. 이 때문에, 이익 창출에 성공한 ICO는 상당수 직·간접적으로 중개소와 연계된다. 이 시장은 제품이나 서비스 매출을 통해 가격을 반영하는 것이 아니라 대형 중개소로의 등록 유무가 가격에 결정적 역할을 하는 시장이다. 이 때문에 ICO는 모집자의 의도와 상관없이 그들을 기망행위를 하도록 구조적으로 내몬다. 악화가 양화를 구축하듯, 기술개발보다 개념 부풀리기가 더 큰 이익이 되는데, 굳이 힘든 기술개발에 매달릴 이유가 없다. 2017년에 이루어진 ICO의 80%이상이 사기라는 분석[539]도 있지만, 간접적인 기망행위까지 포함하면 그 수치는 더 크게 치솟을 것이다. 이제 ICO는 거의 사라져 가고, 리버스 ICO, IEO를 등을 거쳐 STO라는 새로운 이름으로 변형되고 있다. 그 명칭을 떠나 핵심은 투자자 보호장치의 유무이다. 자금유치를 간편화 한다는 명목으로 투자자 보호 장치를 걷어내는 어떠한 방법도 용납돼서는 안 된다. 모든 정책은 보편타당해야 한다.

사. 해 묵은 논란 - 블록체인과 암호화폐는 분리 가능한가?

암호화폐와 블록체인이 분리가능한 것인가라는 무의미한 논란이 여전히 지속되고 있다.[540] 암호화폐 가격과 직·간접적인 이해관계를 가진 사람들 중 상당수는 분리가

538) "IPO 아니죠, ICO 맞습니다…가상화폐, IT 기업의 새 자금조달 창구", 중앙일보 2017년 6월 29일자, https://news.joins.com/article/21712510 (2019년 11월 4일 최종접속) 참조.

539) "New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams", Cointelegraph 2018. 7.13., https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams (2019년 11월 4일 최종접속) 참조.

540) "'블록체인과 암호화폐, 분리할 수 있을까'…한자리 모인 각국 의원들의 답은", 블록인프레스 2018년 10월 11일자, https://blockinpress.com/archives/9617 (2019년 11월 4일 최종접속) 참조.

불가능하다고 주장할지 모른다. 이들은 암호화폐의 익명성과 거래의 도박성에서 파생된 모든 문제를 블록체인이라는 정의되지 않은 미지의 기술과 연계해 사안의 초점을 최대한 흐리려 하고, 이를 통해 문제를 우회하는 시도를 하는 것으로 보인다. 그러나 이 질문은 인센티브 공학의 측면에서 볼 때 무의미하다. 암호화폐는 비트코인 블록체인에서 구현한 인센티브 방식일 뿐이며, 무수히 많은 보상 방식 중 하나에 불과하다. 보상 방식은 정하기 나름이며, 법화를 사용할 수도 있고 심지어 보상이 없을 수도 있다. 블록체인과 암호화폐가 불가분이라는 주장은 그 근거와 논리적인 측면에서 설득력을 가지기 어렵다.

한편, 비트코인 블록체인에서 인센티브가 절실했던 이유는, 작업증명에 막대한 에너지가 소모되기 때문이며, 작업증명이 없다면 블록체인에서 인센티브가 있어야 할 당위성도 크게 사라진다. 재미있는 점은 CoinMarketCap.com 기준으로 2019년 11월 현재 전 세계 중개소에서 거래되는 3,000여개 코인들 중 작업증명을 사용하고 있는 것은 고작 비트코인과 이더리움 정도뿐이며, 나머지는 아예 작업증명을 사용하지 않는다. 이더리움 마저도 지분증명으로 변경하기 위해 계속 시도하고 있으나 번번히 실패하고 있다. 따라서 이제 비트코인을 제외한 거의 모든 알트코인들의 경우 암호화폐 분리 가능성 논쟁은 고사하고 사실상 인센티브의 필요성 자체에 대한 논리가 거의 사라진 셈이다.[541]

사실 비트코인 블록체인의 인센티브 구조는 심각한 결함을 여럿 가지고 있다. 이 중 세 가지만 간단히 살펴보자. 첫째, 블록체인의 건전성은 보편적으로 검증에 참여하는 노드의 수에 비례한다. 그러나 블록체인의 모든 인센티브는 오로지 채굴업자에게만 지급되며, 검증에 참여한 노드에게는 단 한 푼도 지급되지 않는다. 비트코인의 경우 검증에 참여하려면 최소 250여 기가바이트에 이르는 하드디스크를 사용하여, 지속적으로 컴퓨터 자원을 소비해야 하지만 단 한 푼의 인센티브도 주어지지 않는 것이다. 이 때문에 비트코인과 이더리움의 검증 노드 수는 지속적으로 급격히 줄어들고 있는 추세이고, 나중에는 오직 채굴업자만 남아 자기가 기록한 것을 스스로 검증하여 검증 자체가 무의미한 최악의 상황도 충분히 벌어질 수 있다.[542] 둘째, 내재

541) 이들도 기록 노드를 형성하는데 사용된 에너지를 주장할 수 있으나, 그 에너지는 작업증명에 비하면 극히 미미하고, 그 논리대로라면 전기를 사용하는 모든 노드가 보상을 받아야 하는데, 그런 비현실적 구조는 필요가 없을 뿐만 아니라 그 구현도 불가능하다.

가치가 0인 암호화폐를 인센티브로 사용하므로 운영의 안정성을 담보할 수 없다. 등락하는 암호화폐 가격에 따라 채굴업자의 채산성은 크게 달라지고, 일정 가격 이하가 되면 채굴을 멈출 수밖에 없다. 셋째, 난이도는 지속적으로 증가하고 이에 따라 채굴단가가 기하급수적으로 증가하도록 설계된 반면, 정작 인센티브는 약 4년을 주기로 반감하도록 설계돼 있다. 따라서 채굴에 드는 비용은 기하급수로 증가하고 이에 대한 보상은 기하급수로 감소하는 구조가 된다. 이는 필연적으로 채굴 중단을 초래할 수밖에 없는 구조이다. 블록체인 네트워크에 참여한 모든 노드는 오직 경제적 이익만을 추구할 뿐 타인을 위한 봉사를 위해 모인 것이 아니기 때문이다. 비트코인의 생산량이 한정되어 있으므로 미래에는 금이 될 것이라 주장하는 사람은 채굴단가가 손익을 넘어야만 블록체인이 지속될 수 있다는 기본적인 사실을 이해 못하고 있는 셈이다.

5. 요약

블록체인은 기술의 호도를 통해 다양한 기망행위가 발생하는 위협을 잘 보여주는 사례였다. 블록체인에는 '기술'이라는 수식어가 붙지만 프라이버시 보호를 위한 익명성 이외에는 중복에 의한 비효율적 구조 상 그 어떤 다른 뚜렷한 효용도 아직 찾지 못했다. 비트코인은, 금융위기와 명목화폐 시스템, 부패한 정부 등 다양한 요소를 해결해 줄 수 있는 마법의 소프트웨어처럼 부풀려졌지만 모든 소프트웨어는 사람이 만들고 운영하며 지배한다. 소프트웨어 하나로 인류가 평등하게 될 것이라는 주장은 여러 사건을 통해 그 민낯과 함께 허구가 드러났다. 이더리움 재단의 전횡이나, 비트코인 채굴의 독점 등을 통해 블록체인은 이제 오히려 더 중앙화되고 사유화 되었으며 이를 견제하거나 통제할 수단도 없다. 한편, 블록체인은 암호화폐라는 광풍과 맞물리면서 자금세탁, 탈세, 검은 돈 등 여러 탈법의 온상으로 변질되었다. 이는 블록체인이 가진 익명성에 기인한 것으로서 필연적인 귀결이기도 했다.

이후 디지털 자산과 자산유동화 토큰 등의 새로운 개념도 제시되었지만 이는 디지털화와 관련 있을 뿐 블록체인과는 무관하며 단지 '블록체인'이란 단어가 상술로 활용된 측면도 있다. 특히 ERC-20을 이용한 자산유동화 토큰은 비용과 관리 등의 여러

542) 이병욱, 앞의 책 267면.

측면에서 매우 불합리한 선택이 될 수 있다. 한편, 암호화폐 등의 기망행위와 완전히 단절하고 기술로서 블록체인을 부각하기 위한 하이퍼 레저 프로젝트 등도 등장했지만, 하이퍼 레저 패브릭 등은 블록체인의 정의에 부합되지 않는 것은 물론 비트코인과는 정반대의 속성을 가지고 있다. 이러한 시도가 그저 얄팍한 상술로 귀결될 것인지 진정한 효용을 보여줄 수 있을지는 여전히 미지수이다.

제2절 | 블록체인 기술로 인한 범죄 발생 양상의 변화 가능성

제1절에서는 기술적 관점에서, 블록체인 기술이 그 핵심가치라고도 할 수 있는 '탈중앙화'를 실현하면서도 중앙관리주체가 없는 상황에서 비가역성을 충분히 담보해 내기 위하여 필연적으로 초래할 수밖에 없는 비효율과, 바로 탈중앙화의 결과로 등장하게 되는 익명성, 그리고 이로 인하여 커지는 범죄적 활용 가능성과 아직까지 극복되지 않은 스마트 컨트랙트의 기술적 한계 등을 살펴보았고, 이러한 문제를 해결하기 위한 시도라고 할 수 있는 하이퍼 레저와 같은 일종의 프라이빗 블록체인 기술의 개념 모순성 등을 검토해 보았다. 이러한 분석을 바탕으로, 지난 몇 년간 지속된 장밋빛 전망에도 불구하고 블록체인 기술이 아직까지 사회혁신의 기술적 원동력이 되지 못한 채, 단지 사기의 기망수단이 되거나 외환관리 및 자금세탁 방지 등 각종 금융규제를 탈법적으로 벗어나기 위한 도구에 머물고 있는 현실적 한계를 조금 더 깊이 이해할 수 있을 것으로 생각한다.

그러나 블록체인 기술의 활용방안과 관련된 깊이 있는 논의가 본격적으로 전개되기 시작한지 불과 얼마 되지 않은 현실을 고려하면, 이러한 기술적 관점의 분석에 대하여 여전히 '중앙화'의 위험이나 비용 또는 비효율이 탈중앙화의 비효율에 비하여 오히려 훨씬 더 클 수도 있다는 주장이 아직 틀린 것으로 확정된 것도 아니며, 아울러 제1절에서 비효율의 주요 원인으로 지목되는 작업증명(PoW) 방식이 개선될 기술적·제도적 발전의 가능성, 예컨대 지분증명(PoS) 방식의 정밀화를 통한 대체, 또는 이른바 스마트 컨트랙트의 활성화를 통한 기술 효과성 제고, 아니면 제한된 영역에서 프라이빗 블록

체인의 적극적 활용 가능성 등이 기술적·사회경제적 관점에서 활용 불가능할 정도의 실패로 확정된 것이 아직 아니라는 반대되는 주장도 여전히 가능하다. 오히려 블록체인 기술 및 그 활용방안은 여전히 연구개발 중이며, 특히 산업적 관점에서 블록체인 기술을 어떠한 방식으로건 보다 적극적으로 활용하고자 하는 노력은 지금도 계속되고 있다.

더욱이 제1절의 기술적 검토를 형사정책적 관점에서 다시 검토해보면, 상술한 기술적 한계들로 인하여 블록체인과 관련된 범죄적 현상들이 주로 암호화폐의 활용의 형태로 우리사회에 필연적으로 발생하고 그 심각성이 점점 더 커질 수밖에 없다는 구조적 문제 상황을 더욱 잘 이해할 수 있다. 결국, 암호화폐로 대표되는 블록체인 기술과 관련된 문제의 심각성이 점점 더 커져가고 있는 현실 속에서 블록체인 기술의 부정적 활용 가능성을 사전에 완벽하게 예방하기 위하여 블록체인 기술의 개발 및 활용을 금지하거나 암호화폐의 활용을 국가정책적으로 엄격하게 금지하고 강력하게 처벌하는 것이 불가능할 뿐만 아니라 결코 바람직하지 않다는 점에 대하여 동의하는 것을 전제한다면, 상술한 기술적 이해를 토대로 블록체인 기술이 초래하고 있는 사회적 변화, 특히 범죄적 양상의 실태 및 변화 가능성을 형사정책적 관점에서 분석하여 검토하고, 이를 적절한 정책적 대응방안을 제시하기 위한 논의의 출발점으로 삼아야 할 것이다.

1. 블록체인 기술의 활용에 관한 형사정책적 이해

가. 개관

기술의 발전은 삶의 방식을 변화시킨다. 삶의 방식이 변하면 사회의 구조가 변하게 되고, 결국 이에 대응하여 법과 정책이 달라져야 한다.[543] 그러나 블록체인 기술에 대한 폭발적인 관심이 쏟아진 이후로 현재 약 2년 이상의 시간이 지났지만, 여전히 블록체인 기술의 발전이 우리나라의 법과 정책에 미친 영향은 그리 크지 않은 것으로

543) "암호화폐(Cryptocurrency)와 관련하여 이러한 법제도적 변화현상에 대한 분석에 관하여 상세한 내용, 연성진/전현욱/김기범/신지호/최선희, 암호화폐(Cryptocurrency)관련 범죄 및 형사정책 연구, 한국형사정책연구원, 2017, 7면 이하 참조.

보인다. 이른바 'AI', 'IoT' 등과 함께 4차 산업혁명의 가장 중요한 핵심기술의 하나로 부각되었던 블록체인 기술에 대한 높은 관심과 이에 상응하는 사회경제적 자본의 투자 등에 비하여, 블록체인 기술의 활용은 여전히 오직 암호화폐와 관련된 영역에 집중되어 있으며, 그 외의 영역으로는 거의 확산되지 못하고 있다. 그래서 암호화폐에 관하여 자금세탁 방지와 거래소 규제 등에 관한 수많은 법률안이 제안되는 등 여러 가지 정책적 논의가 전개되고 있는 와중에도, 블록체인 기술 그 자체를 위한 국가(형사)정책적 논의는 거의 이루어지지 않고 있으며, 여전히 소규모의 예산을 동원한 기술 발전 촉진 수준에 머물러 있다.

1) 암호화폐가 선도하는 블록체인 기술 활용

주지하는 바와 같이 2008년 블록체인 기술이 처음 등장한 직후에는 그리 주목을 받지 못했던 것이 사실이다. 그러나 2010년대 이후 비트코인 등 암호화폐 시스템이 실제 작동한다는 사실이 경험적으로 입증되고 이에 대한 관심이 세계적으로 확산되면서, 탈중앙적 전자 거래시스템을 표방하는 블록체인 기술에 대한 관심도 이와 함께 점차 높아지기 시작하였다. 블록체인 기술에 대한 관심이 고조되는 흐름은 암호화폐의 가격이 정점을 찍었던 2017년 말에 최고조에 이르게 된다. 즉 블록체인 기술의 활용형태 중 하나인 암호화폐가 블록체인에 대한 관심을 선도하는 형태로 이끌어온 것이다. 현재까지 활용단계에 이른 거의 대부분의 블록체인 기술은 사실상 암호화폐를 참여자에 대한 일종의 보상체계로 이용하는 것을 전제로 개발되어 왔다고 해도 과언이 아니라고 할 수 있다. 때문에 제1절에서 살펴본 바와 같이 블록체인과 암호화폐가 정보기술적 관점에서는 본질적으로 분리 불가능한 것은 아니라 하더라도, 사회적 인식과 관심은 오히려 암호화폐를 중심으로 확산되었다. 그러나 2017년 말 비트코인 등 암호화폐의 가격이 폭락하면서 블록체인 기술에 대한 일반인의 관심은 급격히 식었으며, 이후 최근에 이르기까지 관심의 정도는 지속적으로 낮아지고 있다. [그림 4-3]은 이러한 추세의 변화를 잘 나타내고 있다.

[그림 4-3] 최근 5년간 "블록체인" 키워드에 대한 관심도 변화[544]



다만 2019년 10월 24일, 중국의 시진핑 국가주석이 블록체인 산업을 육성하겠다는 국가정책기조를 발표하고, 블록체인과 암호화폐 관련 산업을 육성하기 위한 제도를 정비할 목적으로 "암호법"을 제정하는 등의 정책적 변화를 실제로 추진한 이후부터 블록체인 기술에 대한 관심이 다시 높아지고 있는 추세로 변화하고 있는 것으로 보인다.[545] 정부와 기업을 중심으로 암호화폐와 분리된 블록체인 기술 그 자체의 사회적 활용 가능성을 구체화하기 위한 본격적인 관심과 논의가 다시 시작되고 있는 것이다.

2) 블록체인 기술 전망

암호화폐 이외의 분야에서 블록체인 기술은 아직 주목할 만한 성과를 거두지 못하고 있다. 블록체인 기술의 발전 동향과 관련하여, 미국의 정보기술자문회사인 가트너(Gartner)는 '2019년 블록체인 비즈니스 예측 보고서'[546]에서, 기업적 관점에서 블록체인 기술은 부풀려진 최고의 관심 단계(Peak of Inflated Expectation)를 넘어 환상이 깨지는 침체기(Trough of Disillusionment)에 접어들고 있는 것으로 진단한 바 있으

544) 이미지 출처: Google 트렌드 웹페이지, https://trends.google.co.kr/trends/explore?date=today%205-y&q=blockchain (2019년 11월 8일 최종접속).
545) 이에 관하여 상세한 내용은 ""블록체인 육성" 시진핑 한마디에 비트코인 40% 급등", 조선비즈 2019년 10월 28일자, https://biz.chosun.com/site/data/html_dir/2019/10/27/2019102701318.html (2019년 11월 8일 최종접속) 참조.
546) Gartner, Predicts: Blockchain Business, 2018.12.13., https://www.gartner.com/en/doc/374378-predicts-2019-blockchain-business (2019년 11월 8일 최종접속) 참조.

며, 앞으로 수년 내에 침체기를 벗어난 후 지속적으로 발전할 것으로 예측하였다. 같은 보고서에서 가트너는 2022년경부터 블록체인 기술의 본격적인 투자성공모델이 등장하기 시작하고, 2027년경부터 전지구적으로 영향을 미칠만한 대규모의 경제적 성장을 기록하는 원동력이 될 것으로 예상하였다.[547]

우리나라 과학기술정보통신부 역시 향후 5년간 블록체인 관련 시장이 10배 이상 성장할 것으로 전망하면서 "4차 산업혁명의 핵심기술인 블록체인의 초기시장 형성과 글로벌 기술경쟁력 확보를 통한 민간주도 성장 지원"을 위하여 2018년 "블록체인 기술 발전전략"을 수립[548]하였다. 과학기술정보통신부는 이 전략에 따라 우리나라 블록체인 산업의 진흥을 촉진하기 위하여 "블록체인 공공 시범사업"을 추진하고 있다. 2019년에는 투입 예산을 지난해의 약 두 배에 해당하는 85억원으로 확대하였으며, 아래 [표 4-1]과 같은 총 12개 과제를 공공선도 시범사업으로 선정하여 지원하고 있다.[549]

[표 4-1] 2019년도 12대 공공선도 시범사업 선정 과제[550]

분야	제안기관	과제명
관광	전라북도	블록체인 기반 전라북도 인공지능 맞춤형 관광 설계시스템
계약	방위사업청	블록체인 기반 제안서 접수 및 평가 시스템 구축
식품안전	식품의약품안전처	국민향(向) 해썹(HACCP) 서비스 플랫폼 구축 시범사업
의료	서울의료원	블록체인 기반 맞춤형 의료 서비스 시스템 구축
인증	병무청	인증서 없는 민원서비스 제공을 위한 블록체인 플랫폼 구축 사업
재난재해	부산광역시	블록체인 기반 재난재해 대응 서비스 구축 시범사업

547) 가트너의 블록체인 기술에 관한 하이프 사이클 분석에 관하여 자세한 내용은 국경완, "블록체인 기술 및 산업 분야별 적용 사례", 주간기술동향 1900호, 정보통신기획평가원, 2019.6.12., 13면 이하 참조.

548) 과학기술정보통신부의 '블록체인 기술 발전전략'에 관하여 상세한 내용은, 과학기술정보통신부 보도자료, "블록체인 글로벌 기술경쟁력 확보, 선도사업 본격 추진", 2018.6.21., http://eiec.kdi.re.kr/policy/callDownload.do?num=177925&filenum=1 (2019년 11월 4일 최종접속) 참조. " "안은 해당 보도자료에서 인용.

549) 과학기술정보통신부의 '블록체인 공공 시범사업'에 관하여 상세한 내용은, 과학기술정보통신부 보도자료, "블록체인 공공 시범사업 2배로 확대하고 민간 프로젝트도 함께 추진한다", 2018.12.21., http://www.korea.kr/goNews/resources/attaches/2018.12/21/30a914e8c9e4f958b8e098340907b06e.pdf (2019년 11월 4일 최종접속) 참조.

550) 과학기술정보통신부, 앞의 보도자료("블록체인 공공 시범사업 2배로 확대하고 민간 프로젝트도 함께 추진한다") 참조.

분야	제안기관	과제명
전자 문서	우정사업본부	블록체인 기반 전자우편사서함 시범사업
	국가기록원	블록체인을 적용한 신뢰기반 기록관리 플랫폼 구축 시범사업
	서울특별시	시간제 노동자 권익보호(근로계약서)
친환경	환경부	블록체인 기반 탄소배출권(외부감축사업) 이력관리 시스템 구축
	제주도	블록체인 기반 폐배터리 유통이력 관리시스템 구축 시범사업
	한국남부발전	블록체인 기반 신재생에너지 공급의무화제도(RPS) 통합관리 서비스 시범사업

과학기술정보통신부는 이 외에도 "민간의 창의적인 아이디어를 바탕으로 실생활에서 이용 가능한 블록체인 서비스 개발과 조기 상용화를 지원"하기 위하여, "탈중앙 기부 플랫폼", "중고차 서비스 플랫폼", "블록체인 ID/인증 네트워크"를 자유공모형식으로 선정하여 각 과제에 15억씩 총 45억의 예산을 지원하는 민간주도 국민프로젝트를 진행 중이다.[551] 이 외에도 국내외 다수의 민간기업들은 주로 금융분야, 물류·유통·제조분야, 사회·문화(저작권)분야 등을 중심으로 블록체인 기술의 시장 적용 가능성을 연구하고 있다.

[참고] 블록체인 기술과 선거

블록체인 기술의 보안성과 투명성으로 인하여, 특히 선거분야에서의 블록체인 기술 활용에 관한 연구는 이미 상당부분 진행되었으며, 어느 정도는 실제 적극적으로 활용되고 있다.

중앙선거관리위원회는 한국인터넷정보학회에 용역을 발주하여 2017년 "블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구"라는 보고서를 발표하였다. 이 연구는, 블록체인 기술의 장점을 활용할 경우 투표 결과의 위·변조가 불가능할 뿐만 아니라 결과를 투표 완료 즉시 확인할 수 있다는 장점이 있으나, 아직까지 전자적 방식의 투표가 진행된 바 없으며, 대중의 신뢰를 획득할 필요가 있으므로 K-voting[552] 시스템과 같은 중·소규모의 민간선거에서부터 블록체인 기술을 활용하는 것이 바람직하다고 결론내리고 있다.[553]

뿐만 아니라 중앙선거관리위원회는 이러한 연구성과를 토대로 과학기술정보통신부와 함께 2018년 블록체인 시범사업으로 이미 "블록체인 기반 온라인 투표시스템"의 개발을 완료하고 2019년 현재 시범운영중이다. 중앙선거관리위원회는 학교, 공동주택 등에서 대표자를 선출하는 등의 투표를 하는 것을 지원할 때 이 시스템을 바탕으로 서비스를 제공한다. 중앙선거관리위원회에 따르면 블록체인 기반 온라인투표시스템은 기존의 K-voting 시스템에 비하여 다음과 같은 장점이 있다고 한다.

▸ 분산컴퓨팅에 기반을 둔 데이터의 위·변조를 방지하는 기술인 블록체인은 해킹 등 공격시도에 안전

551) 이에 관하여는 과학기술정보통신부 보도자료, "민간의 혁신 아이디어, 블록체인 기술로 실현한다", 2019.2.28., http://www.korea.kr/common/download.do?fileId=186414532&tblKey=GMN (2019년 11월 4일 최종접속) 참조. " "안은 해당 보도자료에서 인용.

하기 때문에 정보의 보안과 투명성을 높일 수 있고, 이를 통해 온라인투표 과정과 결과에 대한 신뢰성을 확보할 수 있음.[554]

- K-Voting과는 다르게 유권자 정보 등이 블록에 기록됨. 저장된 블록체인은 분산형 시스템이기 때문에 투표결과를 조작하는 것은 거의 불가능에 가까움.
- 이해관계자가 투·개표과정을 참관할 수 없었던 K-Voting과는 다르게 「블록체인 기반 온라인투표시스템」은 이해관계자에게 권한을 부여해서, 분산 저장되어 있는 투·개표결과 관련 정보를 직접 비교·검증할 수 있게 함으로써 선거의 신뢰성을 제고할 수 있음.[555]

3) 관련 정책 연구 동향

이처럼 블록체인 기술은 정부와 기업을 중심으로 여전히 유망한 차세대 성장동력의 하나로 인식되고 있으나, 그 기술의 활용의 정도는 여전히 "공공선도 시범"사업의 형식으로 가능성을 검토하고 있는 단계에 머물러 있다. 그러므로 블록체인 기술의 활용은 세계적으로도 그리고 우리나라에서도 본격적인 궤도에 올랐다고 하기에는 아직 이른 것으로 보인다. 기술의 활용 현황을 개관하는 것을 통하여 기술에 뒤따르기 마련인 형사정책적 대응방안을 블록체인 기술 일반에 관하여 분석하고 전망하는 연구를 수행하는 것은 사실상 불가능한 상황이라는 사실을 확인할 수 있다. 더욱이 이러한 점은 현재까지 실제 수행된 블록체인 기술 관련 연구 동향, 또는 문헌들의 목록을 살펴보는 것을 통해서도 확인된다.

2017년 말, 암호화폐 가격의 폭락 이후에도 탈중앙이라는 블록체인 기술의 특징은 많은 연구자들의 연구적 호기심을 또한 불러일으켰고, 우리나라의 연구자들도 관련 연구를 다수 수행해오고 있다. 2019년 11월 4일 현재, 한국학술정보의 학술문헌검색서비스(kiss.kstudy.com)에 본문을 포함하여 "블록체인"을 언급하고 있는 문헌을 검색하면 총 934개의 결과가 검색된다. 그 중 219건의 연구가 2017년에 발표되었으며,

---

552) 선거관리위원회가 제공하는 온라인투표시스템으로 주로 정당이나 학교, 공동주택의 대표를 선출하거나 안건에 대하여 표결할 때 이용된다.

553) 홍승필/민경식/김혜리, 블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구, 선거연수원, 2017, 67-68면.

554) 블록체인 기반 온라인투표시스템의 장점에 관한 서술은 중앙선거관리위원회 보도자료, "중앙선관위, "블록체인을 적용한 온라인투표 서비스 첫 개시"", 2018.11.28., https://www.nec.go.kr/portal/bbs/view/B0000342/39054.do?searchYear=2018&menuNo=200602 (2019년 11월 4일 최종접속) 참조.

555) 중앙선거관리위원회, 앞의 보도자료("중앙선관위, "블록체인을 적용한 온라인투표 서비스 첫 개시"")에서 인용.

2018년에는 415건이, 2019년에는 현재까지 총 286건이 발표되었다. 검색의 범위를 KCI등재지 또는 등재 후보지로 좁히고, 분야를 사회과학분야로 한정하면 총 261건의 문헌이 검색된다. 그 중 대부분인 220건이 2018년부터 2019년 현재까지 발표되었다. 사회과학분야, 특히 블록체인 기술과 관련한 정책적 관점의 논의가 본격적으로 이루어지기 시작한지는 아직 약 2년 정도의 시간밖에 지나지 않았다는 사실을 다시 한 번 확인할 수 있다.

분야를 다시 법학으로 좁히면 총 90건의 문헌이 검색되고, 그 중 2018년부터 2019년 현재까지 총 76건이 발표되었다.[556] 하지만 법학분야의 블록체인 연구는 대부분 "스마트계약"이나 "전자금융거래법", "규제", "조세", "ICO", "해외 법제" 등에 관한 연구이며, 대체로 암호화폐와 관련된 (전자)금융법적 논점이나 자금세탁 방지 등 기술발전과 법적 규제에 관한 논점을 다루고 있음을 알 수 있다. 그런데 검색된 문헌 중 형사정책적 관점으로 분류될 수 있는 제목을 가지고 있는 연구는 단지 4편에 불과하다. 그 4편중에서도 2편은 암호화폐에 관련된 형사정책적 논점을 광범위하게 전망하는 글이며, 나머지 2편은 대법원의 암호화폐에 대한 몰수 판결(2018도3619)을 법리적으로 분석하는 글이다.[557]

한국학술정보 문헌검색서비스에서 검색된 문헌들을 통하여 확인할 수 있는 바와 같이 현재 블록체인 기술의 발전 및 이에 관한 법정책적 논의는 대체로 암호화폐, 즉 탈중앙적 디지털 가치교환수단이라는 특성에 집중되고 있다. 특히 자본시장법이나 금융법적 관점에서 ICO 또는 거래소 규제 등, 암호화폐가 자금세탁 및 범죄자의 수익창출 수단으로 활용되는 것을 억제하기 위해 각종 제도를 도입하는 것에 관하여는 이미 상당한 논의가 전개되어 초국가적 관점에서 규범화가 진행되고 있으나, 그 외의

---

556) 한국학술정보 문헌검색서비스시스템 홈페이지, http://kiss.kstudy.com (2019년 11월 4일 최종접속) 참조.

557) 이정훈, "블록체인과 가상화폐의 형사법적 문제와 전망 -대법원 2018. 5. 30. 선고 2018도3619 판결을 중심으로-", 홍익법학 제20권 제1호, 홍익대학교 법학연구소, 2019, 57-88면; 한성훈, "가상화폐 관련 형사법적 문제에 관한 소고", 경상대학교 법학연구 제27권 제2호, 경상대학교 법학연구소, 2019, 125-148면; 이규호, "4차 산업혁명의 효과와 형사정책적 과제", 법학연구 제75권, 한국법학회, 2019, 445-476면; 최호진, "비트코인에 대한 몰수 가능성 - 대상판결 : 대법원 2018. 5. 30. 선고 2018도3619 판결 -", 비교형사법연구 제20권 제3호, 한국비교형사법학회, 2018, 57-81면. 검색방법을 달리하면 더 많은 연구 성과가 검색될 수 있으나, 다만 형사정책 관련 연구의 추세나 연구된 주제의 범위에 대한 이해를 위해서는 검색방법을 제한하는 것이 오히려 도움이 될 수 있을 것으로 생각한다.

블록체인의 형사사법적 문제 또는 긍정적 활용방안에 관한 논의는 일부 정보보안 수단으로서의 활용가능성 정도의 관심을 제외하고는 대부분 아직 관련분야 전문가의 주관적 '전망'단계에 머물러 있는 것으로 보인다.

4) 소결 – 탈중앙적 디지털 가치교환수단이라는 특성을 중심으로

상술한 바와 같이 기술적 관점으로는 블록체인 기술이 암호화폐와 필수적으로 연결되어야 하는 것이 아니라 할지라도, 현재까지 블록체인 기술의 발전은 암호화폐가 주도하는 가운데 진행되었으며 현실적으로 암호화폐 이외의 영역에서 블록체인 기술은 아직까지 거의 활용되고 있지 않다. 그래서 이와 관련한 법정책적 연구들 역시 거의 모두 암호화폐와 관련된 논점들을 다루고 있다.

제1절의 기술적 분석을 통해서도 비판적으로 검토했던 것처럼, "블록체인은 절대 익명의 금융거래에 적합한 속성"을 가지고 있으며 "익명은 금융의 건전성에는 직접적으로 반하는 것이다." 그러므로 이러한 관점에서 블록체인 기술을 통해 구현해낸 탈중앙적 디지털 가치교환수단은 현대 사회에서 "건전한 금융과는 상극"으로 작용할 가능성이 높으며, 따라서 암호화폐의 탈중앙적 디지털 가치교환수단이라는 특성이 바로 현재 우리 사회에서 문제로 지적되고 있는 익명성 내지 사기친화성 등과 같은 블록체인 기술과 관련된 대부분의 형사정책적 논점들을 만들어내는 출발점이 되고 있다고 해도 과언이 아니다.

이러한 상황에서 이 보고서에서 검토하고자 하는 블록체인 기술에 관한 형사정책적 논의들은 블록체인 기술 전반으로 확대하는 것은 사실상 무의미할 뿐만 아니라 가능하지도 않을 것으로 생각한다. 결국 블록체인 기술 관련 형사정책적 논의들은 대체로 탈중앙적 디지털 가치교환수단의 측면, 즉 암호화폐의 범죄적 활용 억제라는 측면에 초점이 맞추어질 수밖에 없을 것이다.

게다가 연구의 범위를 암호화폐라는 비교적 제한된 범위의 소재에 관한 기술적·규범적 논의로 국한한다 하더라도, 당연히 블록체인 기술의 본질로부터 도출되는 새로운 논점들에 관한 것이므로, 블록체인 기술 전반에 관한 형사정책적 논의를 위해 필요한 주제의 상당부분에 연결되는 다양한 내용들을 대부분 무리 없이 포섭하거나, 추후 관련 논의로 확장하기 위한 논거가 될 수 있을 것으로 생각한다. 그래서 우선

이 보고서는 블록체인 기술에 관한 형사정책적 검토에 들어가기에 앞서, 논의의 효율성을 높이기 위하여, 우선 암호화폐에 관련하여 현재까지 다루어진 논점들을 중심으로 연구의 범위를 보다 명확히 하고자 한다.[558]

나. 암호화폐부터 가상자산까지

블록체인 기술은 현재까지 대부분 탈중앙적 디지털 가치교환수단의 구현원리로 활용되고 있다. 그래서 아직 활용도가 낮은 블록체인 기술의 다른 측면에 비하여 암호화폐에 관하여는 연구보다 실무 차원에서 보다 많은 형사정책적 쟁점들이 등장하고 있으며, 또 실무의 필요에 따라 개념의 내용과 정책의 방향이 정리되어가고 있는 것으로 보인다. 형사정책적 관점의 연구들은, 대법원의 암호화폐에 대한 넓은 범위의 형사법적 쟁점 연구나 몰수판결에 대한 평석에서 확인할 수 있듯이, 실무에서 드러나는 쟁점들을 포괄적으로 또는 개별적으로 리뷰하는 형식으로 진행되고 있다. 빠르게 발전하는 정보기술분야에서 언제나 기술발전에 뒤따르기 마련인 법정책의 발전이 일정부분 실무에 의해서 선도되고 있는 것이다.

이러한 관점에서 블록체인 기술과 관련된 형사정책의 논의를 보다 효율적으로 전개하기 위하여 이하에서는 우선 주로 이미 현실적 문제로 등장한 블록체인 기술을 이용한 탈중앙적 디지털 가치교환수단에 관하여 실무상 정리되고 있는 개념과 특성을 형사정책의 관점에서 살펴본다. 이를 위하여 관련 실무에서 가장 최근에 등장한 이후 점차 그 사용 범위가 확산되고 있는 가상자산(Virtual Assets)의 개념을 우선 살펴보고, 왜 이러한 용어를 사용하게 되었는지를 확인해 보는 것을 통하여 (형사)정책의 기본 방향에 관하여 서술한다.

1) 가상자산(Virtual Assets) 개념의 등장

2019년 6월 16일부터 21까지 개최된 제30기 제3차 국제자금세탁방지기구(Financial Action Task Force, 이하 'FATF'라 한다)[559]총회는 가상자산(Virtual Assets)에 관한

558) 다만 각주 508에서 언급한 보고서 '연성진/전현욱/김기범/신지호/최선희, 암호화폐(Cryptocurrency) 관련 범죄 및 형사정책 연구(2017)'에서 이미 관련된 많은 소재들이 개괄적으로 다루어진 바 있으므로 이 절의 작성을 위하여 필요한 범위 내에서 관련 내용을 간략히 요약하고 이후의 논의들을 추가하는 방식으로 서술한다.

주석서(Interpretive Note to R.15)를 확정하고, 성명서(Public Statement) 채택하였으며, 지침서(Guidance)를 발간하였다. 그리고 구속력이 있는 주석서를 통하여 가상자산 서비스 제공자(Virtual Assets Service Provider)에 적용될 규제 권고안을 발표하였다.[560] FATF는 이미 지난해 10월 제30기 제1차 총회[561]에서 가상자산 관련 권고(Recommendation. 15)를 채택하여 가상자산의 정의규정을 마련하고 관련자에게 자금세탁 및 테러자금 조달을 방지할 의무를 부과한 바 있다. 이번 규제 권고안 채택은 이를 구체화기 위한 것이다.

[참고] 가상자산 자금세탁방지 관련 FATF 주석서의 주요 내용[562]

① **인·허가(license) 또는 신고·등록(register)**

- 가상자산 취급업소는 **감독당국에게 허가를 받거나 신고, 등록**을 하여야 함(자율규제기관에 의한 허가 등은 불인정)
- 범죄(경력)자의 가상자산 업(業) 진입을 차단하고, **미신고영업은 제재**(sanction)

② **자금세탁방지 관련 규제·감독(Regulation and supervision)**

- **감독당국에 의해 감독**되어야 하고, 감독당국은 **효과적인 감독수단***을 보유해야 함

* 감독당국은 가상자산 취급업소의 **의무위반시 허가·신고를 취소·제한·중지**시킬 수 있는 권한, **효과적·비례적·억제적 제재**(effective, proportionate and dissuasive sanctions) 부과권한 보유

③ **예방조치(preventive measures) 이행의무**

- 가상자산 취급업소에게 금융회사에 준하는 **자금세탁방지의무***를 부과

* 고객확인의무(Customer Due Diligence), 의심거래보고(Suspicious Transaction Report) 등

- 기존 금융회사와 동일하게, **가상자산 송금**도 송금·수취기관 모두 송금인·수취인 **관련 정보를 수집·보유**하고 **필요시 당국에 정보를 제공**

559) FATF는 자금세탁방지 및 테러자금조달금지를 위하여 1989년 설립된 국제기구로 우리나라는 2009년 10월 이에 정회원으로 가입하였다.

560) FATF 제30기 제3차 총회에 관하여 보다 상세한 내용은 금융위원회 보도자료, "제30기 제3차 국제자금세탁방지기구(FATF) 총회 참석", 2019.6.24., http://www.korea.kr/common/download.do?fileId=187071114&tblKey=GMN (2019년 11월 4일 최종접속) 참조.

561) FATF 제30기 제1차 총회에 관하여 보다 상세한 내용은 금융위원회 보도자료, "국제자금세탁방지기구(FATF) 총회 참석 결과", 2018.10.22., http://www.korea.kr/common/download.do?fileId=186144482&tblKey=GMN (2019년 11월 4일 최종접속) 참조.

562) 주석서의 번역 및 요약 내용은 금융위원회, 앞의 보도자료("제30기 제3차 국제자금세탁방지기구(FATF) 총회 참석")에서 인용.

FATF는 블록체인 기술을 이용한 탈중앙적 디지털 가치교환수단에 대하여 수차례의 총회를 통하여 개념과 규제방안을 정리하는 과정을 거쳤으며, 현재는 가상자산과 가상자산 서비스 제공자라는 개념을 사용하고 있다. FATF는 2018년 6월 개최된 제29기 제3차 총회에서 이후 적절한 용어가 정리되기 전까지 블록체인 등 기술적 수단을 이용한 탈중앙적 가치교환수단을 가상통화/암호자산(Virtual Currency/Crypto- Assets)으로 병기하여 표현하기로 결정하였다.[563] 그러나 2018년 10월 프랑스 파리에서 개최된 제30기 제1차 총회에서 가상자산에 대한 권고를 채택하면서, 용어를 "Virtual Asset"으로 다시 정리한 것이다. FATF 권고의 개념정의에 따르면 가상자산은 다음과 같이 정의된다. "가상자산이란 가치의 디지털 표상으로, 디지털적인 방법으로 거래, 전송될 수 있고, 지불이나 투자목적으로 이용될 수 있는 것이다. 가상자산은 현실화폐나 증권 또는 FATF 권고에서 이미 규정한 금융자산을 디지털화한 것(digital representations)을 포함하지 않는다."[564]

블록체인 등 기술적 수단을 이용한 탈중앙적 가치교환수단을 지칭하는 용어에서 "Currency"라는 단어를 삭제하였다는 점으로 미루어보면, 2019년 FATF의 개념정의는 일차적으로는 블록체인을 이용한 가치교환수단이 통화(Currency)의 범주에 포함되기 어려운 경우가 있다는 점을 보다 명백히 하려는 의도를 담고 있는 것으로 보인다. 블록체인, 암호기술을 이용한 가치교환수단이 현실화폐와 구별되는 가장 중대한 표지는 바로 탈중앙화이며 따라서 전통적인 경제학적, 법정책적 관점에서 이를 기존의 통화 개념을 통하여 그대로 담아내기가 어려운 경우가 분명 있을 것으로 생각한다. 그러나 거듭 생각해보면, 자산(assets)이건 통화(currency)건 상관없이 어떠한 방식으로든 디지털화 되어 가상(Virtual)이라는 수식어가 붙는 순간 가치의 매개라는 현상 이외의 모든 특성이 사실상 무의미해진다고 할 수 있으며, 따라서 전통적인 경제학적 관점에서 자산과 통화의 구분이 무색해질 수밖에 없음을 알 수 있다. 특히 인터넷

563) FATF 제29기 제3차 총회에 관하여 보다 상세한 내용은 금융위원회 보도자료, "제29기 제3차 자금세탁방지기구(FATF) 총회 결과", 2018.7.3., http://www.korea.kr/common/download.do?fileId=186006992&tblKey=GMN (2019년 11월 4일 최종접속) 참조.

564) "A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations." Financial Action Task Force, The FATF Recommendations, 2019.6., p.126.

공간에서 자산과 통화의 구분이, 경제적 관점이 아니라 규범적 관점에서 어떠한 유의미한 차이점을 가져올 수 있을지는 아직 더욱 알기 어렵다. 실제 FATF는 가상자산을 지칭하는 용어에서 Currency를 삭제하였음에도, 개념정의에서 가상자산의 개념을 "지불(payment)"수단에 해당한다고 정의하고 있다. 즉 FATF가 Currency를 삭제한 것은 FATF의 자금세탁방지규정이 적용되는 범위를 확정함에 있어 불필요한 형식논리적 개념 논쟁에서 벗어나, 규정의 적용이 필요한 범위를 빠짐없이 포괄하기 위한 것으로 볼 수 있다. 디지털 가치매개수단을 이용한 자금세탁을 방지하기 위해서는 결국 용어의 표지와는 관계없이 관련 서비스 제공자에게 자금세탁 방지의무를 부과해야 하기 때문이다. 그래서 FATF의 개념정의는 FATF 권고가 규정하고 있는 자금세탁 방지의무의 적용범위를 최대한으로 넓혀 보다 실효적으로 자금세탁을 방지하기 위한 목적으로 이해된다.

2) 개념 비교

가상자산의 개념을 보다 명확히 하고 이후의 논의의 편의를 위하여 가상자산의 개념을 유사한 다른 개념들과 비교해본다.[565]

우선 현행법에서 사용하고 있는 용어 중 가장 관련이 있을 것으로 보이는 것으로 "전자화폐(Electronic Currency)"가 있다. 전자금융거래법 제2조 등에서 전자화폐(Electronic Currency)라는 개념을 사용하고 있으나, 현행 법률이 정하는 바에 따라 엄격한 중앙집중적 관리를 전제로 한다는 점에서 디지털화된 현실화폐에 불과할 뿐이며, 이 보고서에서 논의하고자 하는 블록체인 기술에 기반하여 비교적 최근 등장한 가치교환수단의 개념을 담기에는 적절하지 않은 것으로 판단된다.

최근까지 영어를 사용하는 국가들을 중심으로 블록체인 기술영역에서 가장 폭넓게 사용되어온 개념으로 "암호화폐(Crypto-currency)"가 있다. 암호화폐라는 개념은 해시함수 등 암호학적 기술이 사용되는 전자서명의 체인이 바로 블록체인이라는 기술적 특성과 블록체인의 탈중앙적 작동구조를 적절하게 드러내는 개념이라고 생각한다. 비트코인 등 대부분의 블록체인 기반 가치교환수단에서 암호기술이 실제로 탈중앙적

565) 관련개념에 대한 논의는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 15-21면의 내용을 요약정리하고 서술을 보완하는 방식으로 작성하였다.

신뢰체계를 구축하는데 가장 핵심적인 역할을 하는 기술적 요소로 작동하고 있기 때문이다. 이러한 이유로 암호화폐라는 용어는 최근까지 블록체인 기술 전문가 그룹이나 영어권에서는 "Virtual Currency"보다 더 높은 빈도로 사용되었다.[566] 다만 기술적 분석에 익숙하지 않은 사람들에게 "암호(Crypto)"라는 기술적 용어의 사용이 오히려 직관적 이해를 저해하는 면이 있다. 더 나아가 암호기술을 명시하는 용어이므로 기술중립적 용어라고 하기도 어려워, 규범적 관점에서 각종 법령이나 규제의 적용범위를 다소 축소할 우려가 없지 않으며, 또한 미래에 혹시 있을 수 있는 또 다른 기술변화 및 발전을 넉넉하게 포섭하기 어려운 측면이 있다.

우리나라의 언론 등에서는 가상화폐(Virtual Currency)라는 용어를 가장 폭넓게 쓰고 있는 것으로 보인다. 우리 정부는 "화폐"라는 용어가 주는 불필요한 오해를 피하기 위하여 공식 문건에서 Currency를 통화로 번역하여 가상통화라는 용어를 사용하고 있다. 다만 주지하는 바와 같이, 규범적 관점에서 통화는 통용 또는 유통하는 화폐를 말하는 것[567]으로 이러한 맥락에서 이미 유통되고 있는 경우에는 통화와 화폐의 개념은 사실상 구분되지 않는다고 할 수 있다.

가상통화 또는 가상화폐는 오로지 '가상'이라는 표지만을 용어에 담음으로써 디지털화된 가치교환수단을 모두 포함하는 개념으로 사용될 수 있다.[568] 그래서 가상자산이라는 용어가 등장하여 사용되기 전까지 가장 폭넓은 범위를 포괄하는 개념으로 사용되었다. 이러한 이유로 자금세탁방지 관련 규제에 관한 국제조약 등 규범적 관점에서는 규제의 적용범위를 보다 확대하기 위한 목적으로 가상통화 또는 가상화폐라는 용어를 사용하는 경향이 있다. EU 자금세탁방지지침(EU Directive 2018/843)도 2018년 5월 30일 제5차 개정을 통해 "Virtual Currency"라는 용어를 도입하면서 개념정의규정을 신설하였다. EU 자금세탁방지지침은 Virtual Currency를 "중앙은행이나 공적 권위에 의해 발행되거나 보증되지 않는 가치의 디지털 표상으로, 합법적으로 발행된 통화와 연결될 필요가 없으나, 자연인 또는 법인에 의하여 가치교환수단으로 받아들여져야 하며, 이전, 보관, 거래가 전자적으로 이루어질 수 있는 것"[569]으로 정의하였다.

---

566) 암호화폐의 개념에 관하여는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 19-21면 참조. 해당 연구보고서에서는 기술적 관점에서 '암호화폐'를 가장 적절한 용어로 판단하고 있다.

567) 형법 제207조(통화의 위조 등) 참조.

568) 가상통화라는 표현 그 용어 자체가 포섭 가능한 의미의 넓은 범위에도 불구하고 현재는 암호기술을 이용한 탈중앙적 시스템을 전제로 하는 용어로 주로 사용되고 있다.

EU 자금세탁방지지침의 Virtual Currency에 대한 개념정의는, 자금세탁방지라는 규범적 관점에서 가능한 한 규범의 적용범위를 넓히는 것일 뿐만 아니라, 동시에 탈중앙적 특성을 적절히 포섭하면서도 기술중립적인 것으로 보인다. 그러나 암호화폐라는 개념에 비하여 블록체인의 "탈중앙성"이라는 기술적 특성 표지가 명확하지 않으며, 추가적인 개념정의 규정에 의한 보완이 필수적인 용어라고 생각된다. 게다가 자산은 통화 또는 화폐라는 개념을 포함하므로 가상통화 또는 가상화폐는 가상자산이라는 개념에 포함된다. 따라서 규범의 적용범위를 넓혀 예상치 못한 흠결이 발생하는 것을 막아야 한다는 자금세탁방지의 정책적 목적을 고려하면 개념정의 규정의 보완을 전제로 FATF의 가상자산 개념을 사용하는 것이 합리적일 것이다.

3) 소결 - 형사정책적 착안점

지금까지 블록체인 기술을 이용한 탈중앙적 디지털 가치교환수단에 관한 개념들을 검토해 보았다. 기술적 관점에서는 암호화폐라는 용어가, 정책적 관점에서는 가상자산 또는 가상통화(화폐)라는 용어가 사용되고 있음을 확인하였다.

정책적 관점에서는 용어를 구성하는 단어 자체가 드러내는 명확성은 다소 떨어지지만 가상자산이라는 용어가 가장 적합한 것으로 보인다. 상술한 바와 같이 "자금세탁방지"가 실무상 정책적으로 가장 중요한 이슈가 되고 있으며, EU도 블록체인 기술을 이용한 탈중앙적 디지털 가치교환수단을 이용한 자금세탁을 막기 위하여 자금세탁방지지침을 개정하면서 정의규정을 통하여 개념을 보충하면서까지 다소 명확성이 떨어지는 것으로 볼 수밖에 없는 가상통화(화폐)라는 용어를 사용하고 있다. FATF는 여기서 한 걸음 더 나아가 훨씬 광범위한 개념인 가상자산이라는 용어를 쓰고 있다.

그러나 FATF의 개념정의에서 확인할 수 있는 것처럼 가상자산이라는 개념은 "탈중앙성" 표지마저 담고 있지 않으며, 단지 디지털로 표상된 가치이면서 현실의 금융자산과 구분되는 것이기만 하면 모두 여기에 포함된다. 자금세탁 방지의 관점에서는 일부러 범위를 좁힐 필요가 없으므로 가치의 디지털 표상 전반에 걸친 의미로 이해할

569) EU Directive 2018/843 Article 3. (d) (18) "'virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."

필요가 있기 때문이다. 그래서 블록체인에 관한 형사정책을 논의하기 위한 관점에서 정책의 대상이 되는 개념을 명확하게 정리하기에는 적합하지 않은 개념이다. 특히 탈중앙성이라는 블록체인 기술의 특성을 적절히 드러내기 위해서는 암호화폐라는 개념이 보다 유용할 것으로 생각된다. 블록체인의 작동원리로 이용되는 암호기술은 탈중앙성과 익명성으로 이어지게 되며, 따라서 블록체인 기술에 관한 형사정책을 검토함에 있어서 자금세탁과 관련된 논의가 매우 중요하게 되는 근본적인 이유가 된다. 이러한 관점에서 이 보고서에서도 암호화폐, 가상자산, 가상통화, 가상화폐 등의 용어를 논의의 맥락과 필요에 따라 사용할 수밖에 없을 것으로 생각된다.[570]

실무상 관련 용어의 사용례로부터 다음의 몇 가지 형사정책적 착안점을 다시 한 번 정리할 수 있다.

1. 자금세탁방지가 가장 중요한 형사정책적 이슈 중 하나다.
1.1. 자금세탁 방지를 위하여는 FATF의 가상자산처럼 가장 넓은 개념을 채택할 필요가 있다.
1.2. 다만 정책적 논의를 위한 소재의 특성을 명확히 하기 위하여 현실화폐의 디지털 표상은 제외되어야 한다.
2. 블록체인 및 암호기술을 바탕으로 하는 탈중앙성이 현실화폐와 구분되는 핵심 키워드가 된다.
2.1. 탈중앙성이 익명성을 강화하고 범죄적 목적의 자금세탁을 방지해야할 주요한 원인이 된다.
2.2. 기술적 특성이 범죄에 이용될 뿐만 아니라 그 자체가 범죄의 목적이 될 수도 있다.

2. 암호화폐 관련 범죄의 고도화 및 신종범죄

가. 암호화폐의 형사정책적 특성[571]

지금까지 탈중앙적 디지털 가치교환수단을 지칭하는 용어에 담긴 함의를 바탕으로 형사정책적 착안점들을 정리해 보았다. 이하에서는 이러한 분석을 토대로 암호화폐의 특성을 형사정책적 관점에서 보다 세분하고 유형화하여 정리한다.

---

570) 그러나 특별한 사정이 없는 한 이 장에서는 서술의 편의를 위하여 암호화폐라는 용어를 주로 사용한다. 이는 이 장에서 검토하는 내용이 이 보고서의 주제인 블록체인 기술을 이용한 경우로 한정된다는 것을 나타내기 위함이며, 가상자산, 가상통화 등과 개념적으로 엄밀히 구별되는 것은 아니다.

571) 가상자산의 형사정책적 특성에 관하여는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 26-28면의 내용을 요약정리하고 서술을 보완하는 방식으로 작성하였다.

1) 탈중앙성

상술한 바와 같이 블록체인 기술은 본질적으로 탈중앙화를 추구하기 위한 것이라고 할 수 있다.[572] 이러한 기술이 실현된 암호화폐는 따라서 발행 및 거래를 보증하기 위한 중앙기관이 없는 것이 원칙이다. 암호화폐의 이러한 특성 및 작동원리, 특히 그 비효율성에 대한 비판적 검토 등에 대한 기술적 분석은 제1절에서 이미 검토한 바 있으므로 반복하여 상술하지는 않는다. 다만 형사정책적 관점에서 탈중앙성의 의미를 검토해 본다.

중앙관리기관이 없다는 특성은 예컨대 중앙은행이나 거래매개자 등으로 인한 위험 자체가 존재하지 않아서 기존의 화폐 및 거래체계에 비하여 더 안전한 것으로 받아들여지기도 한다. 이론적 관점에서 보면 중앙관리기관의 내부적 부패나 해킹 등 관리시스템에 대한 외부적 공격 등의 문제가 없기 때문이다. 그러므로 "이론적"으로는 암호화폐에 대한 형사정책은 부패범죄나 결제 시스템 해킹범죄 등과 같은 중앙관리기관과 관련된 문제로부터 기존 현실 화폐 기반 시스템의 경우보다 상대적으로 자유로울 수 있다.

그러나 최근 거래소 등 암호화폐 서비스 제공자, FATF의 개념정의에 따르면 가상자산 서비스 제공자(Virtual Assets Service Provider, VASP)가 암호화폐 거래의 매개자 또는 현실경제와의 접점이 되면서 그 역할이 커지고 있으며, 이로 인하여 사실상 새로운 중앙관리기관의 역할을 수행하고 있다는 점이 문제로 제기된다.[573] 거래소 등은 우리나라에서 아직까지 입법적 불비로 인하여 기존의 각종 금융기관 관련 기준이나 규제의 적용을 받지 않는 경우가 많으므로 안전보장을 위한 규제의 사각지대에 있는 것으로 평가되기도 한다.[574] 따라서 "현실적"으로는 새로운 중앙관리기관에 대한 안전성확보가 암호화폐에 관한 형사정책에서 매우 중요한 쟁점으로 등장하게 된다. 따라서 거래소를 금융기관에 준하여 관리하는 방안을 마련하여, 거래소 내부의

572) 암호화폐의 본질이 탈중앙화라는 점에 대한 분석은 이원삼, "가상화폐의 의미와 법적 지위 – 비트코인을 중심으로 -", 상사판례연구 제31집 제2권, 한국상사판례학회, 2018, 300면, 302면 참조. 이 논문은 탈중앙화라는 최초의 의도가 범죄적 목적으로 이용되는 문제를 지적하고 있다.

573) 이른바 암호화폐의 중앙화 현상에 관해서는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 27면 참조. 이러한 문제에 대하여 분산거래소(Decentralized Exchange) 등 기술적 해결방안들이 제시되고 있다.

574) 거래소 규제정책의 필요성에 관한 분석은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 153-157면 참조.

부패와 거래소 외부로부터의 공격을 막아내도록 하는 것이 형사정책적 대안의 주요한 부분을 차지해야 한다. FATF의 자금세탁방지를 위한 노력도 결국 가상자산 서비스 제공자를 금융기관과 같은 수준으로 관리하고 금융기관과 같은 자금세탁방지 관련 의무를 부과하는 것을 그 본질적인 내용으로 하고 있다. 이 외에도 현실화폐로의 환전 시세조종 등도 거래소의 새로운 중앙화가 초래하는 위험요소이다. 자금세탁방지 뿐만 아니라 자본시장법적 규제 및 제재수단이 마련되어야 한다.

다른 한 편으로 분산자율조직(Decentralized Autonomous Organization)[575] 등 탈중앙적으로 구성된 암호화폐의 작동체계는 본질적으로 초국가성을 갖게 되므로, 특정 국가의 정책적 수단이 사이버 공간을 이용하여 손쉽게 우회될 수 있다는 어려움을 극복해야 한다는 상반된 또 다른 형사정책적 문제가 동시에 해결되어야 한다. 특정된 중앙관리기관이 없다는 것은 어떠한 국가도 중앙관리기관의 감독 관할 권한을 가질 수 없다는 것을 의미하기 때문이다. 특히 암호화폐의 거래는 인터넷 공간에서 이루어지므로, 특정국가의 법적 강제수단은 근본적인 한계를 가질 수밖에 없으며, 특히 법관이 영장을 발부하더라도 이를 집행하는 강제수사의 성공 가능성 자체가 극도로 낮아지게 된다. 그러므로 탈중앙적 암호화폐와 관련된 범죄에 신속하고 효율적으로 대응하기 위하여 초국가적 형사사법공조체계의 구축이 절실하게 요청된다.

2) 익명성

관리할 중앙조직이 없다는 것은 또한 이용자의 신원을 확인할 방법이나 주체가 없다는 것을 의미한다. 즉 익명성은 탈중앙성의 목적이 되면서 동시에 탈중앙성을 추구한 결과라고 할 수 있다. 블록체인 기술의 이러한 특성은 프라이버시를 중시하는 사람들에게 매우 매력적으로 다가왔으며, 암호화폐의 설계나 기술의 응용단계에서 익명성을 강화하는 방향으로 기술이 개발되기도 하였다. 비트코인을 처음 개발한 것으로 알려진 사토시 나카모토의 신원은 아직도 명확하게 확인되지 않았다. 이러한 이유로 현재 거의 대부분의 암호화폐의 거래에 참여하고자하는 자는, 특별히 거래소를 이용하지 않고 직접 거래하는 경우, 누구나 원칙적으로 개인정보를 제공하지 않고

575) 분산자율조직(DAO)에 관하여 상세한 설명은 이지언/이보미, "ICO 현황과 규제방안 – 자본시장법 중심으로 -", KIF VIP 리포트 2018-07, 한국금융연구원, 2018, 30면 이하 참조.

도 손쉽게 거래를 위한 주소를 만들 수 있다. 암호화폐의 거래는 원칙적으로 익명을 전제로 이루어지게 된다.

암호화폐의 이러한 특징은 자신의 자산 또는 거래내역을 숨기고자 하는 자, 대체로 불법거래 또는 범죄를 목적으로 하는 자들에게 매우 매력적인 것이 될 수밖에 없다.[576] 결국 암호화폐는 '금융실명제', '의심거래 신고의무'등 각종 규제로 법집행 당국에 의하여 사실상 주요 거래내역이 모두 파악될 수밖에 없게 된 기존의 금융시스템에 비하여 훨씬 매력적인 자금세탁 수단이 되는 것이다. 특히 암호화폐의 익명성은 범죄수익을 현실화할 수 있는 기회를 범죄자에게 제공함으로써 기존의 금융시스템에서라면 수익창출이 어려운 범죄나 사실상 쉽게 성공하기 어려운 범죄, 예컨대 음란물 유포나 도박 등 불법적 사이트 운영, 또는 랜섬웨어[577]와 같은 범죄의 수단이 되는 문제가 있다.

물론 현실화폐를 이용한 거래도 익명성이 유지되는 것이 원칙이다. 일상의 거래에서 현금을 사용한 경우라면 특별히 다른 정보들의 조합을 통하여 거래 당사자가 확인되지 않는 한, 해당 거래의 익명성은 보장되며 거래당사자를 추적해 밝혀내는 것도 원칙적으로는 불가능하다. 다만 현대사회의 거래방식이 금융서비스와 결합하면서 신용카드를 사용하거나 온라인으로 지불하는 경우가 훨씬 많아지면서, 거래기록에 실명이 함께 남게 되었고, 계좌추적이나 신용카드 거래내역 확인 등과 같은 범죄수사 방법들도 이러한 기록에 크게 의존하는 것에 익숙해졌다. 특히 거액의 거래인 경우 현금 운반의 물리적 한계 등으로 인하여 현실세계에서는 어쩔 수 없이 추적이 가능한 방법을 이용할 수밖에 없으나, 암호화폐를 이용할 경우 금액에 크기에 상관없이 익명거래가 가능하다. 암호화폐의 이러한 특징은 따라서 FATF는 ICO 단계에서부터 암호화폐의 익명성을 완화할 것을 요구하거나 가상자산 서비스 제공자에게 실명확인의무 등을 부여하는 등의 방법을 통하여 익명성을 완화하는 가이드를 준수할 것을 요구하고 있다.

---

576) 익명성으로 인하여 범죄적 활용이 이루어질 가능성이 발생한다는 분석으로 유주선/강현구, "가상통화에 대한 입법적 방안과 법적 쟁점 연구", 금융법연구 제15권 제1호, 한국금융법학회, 2018, 216면.

577) 랜섬웨어에 관한 형사정책에 대하여는 양종모, "랜섬웨어 공격에 대한 형사법적 고찰", 홍익법학 제20권 제1호, 홍익대학교 법학연구소, 2019, 31-55면 참조.

반면 이러한 법적 제도적 규제에 대한 반발로 익명성이 강화된 암호화폐, 이른바 다크 코인[578] 또는 프라이버시 코인에 대한 개발도 지속적으로 이루어지고 있다. 익명성이 강화된 지캐시(Zcash)나 대시(Dash), 또는 모네로(Monero)와 같은 가상화폐들은, FATF의 자금세탁방지의무 강화 이후에 거래소를 통한 거래는 점차 어려워지고 있는 것이 사실이나, 여전히 개인간 직접 거래는 가능하다. 게다가 비트코인 등 거래내역을 일정부분 추적할 수 있는 암호화폐의 경우에도 각종 믹싱(Mixing) 서비스를 이용하여 거래내역을 뒤섞는 방법으로 어렵지 않게 익명성을 강화할 수 있다. 그러므로 암호화폐에 대한 형사정책은 자금세탁 등 범죄적 목적으로 암호화폐의 익명성을 이용하는 경우에 대한 적절한 대응 방안을 모색해야 한다.

3) 기술종속성

블록체인 및 암호기술은 탈중앙성을 실현하기 위한 수단이며, 따라서 암호화폐의 기술종속성은 탈중앙성으로부터 기인하는 것이다. 암호화폐는 공개키-비밀키 기반의 전자서명 방식으로 거래된다.[579] 암호화폐의 거래를 위한 지갑에 대한 처분 권한은 오로지 비밀키를 아는지 여부만으로 결정되며, 다른 방법으로 확인하거나 정정할 중앙관리기구가 없다. 따라서 어떠한 이유로건 특정 지갑의 비밀키를 손에 넣게 되면 해당 지갑에 대한 완전한 처분권한을 행사할 수 있게 되므로, 비밀키의 유출은 암호화폐의 손실로 직결된다. 이용자의 지갑관리를 보다 편리하게 하기 위하여 비밀키에 관한 정보를 정보처리장치 안에 함께 보관하는 경우, 또는 역시 이용자의 편리를 도모하기 위하여 이용자의 비밀키 정보를 거래소 서버에 보관하는 경우가 많아, 암호화폐에 대한 해킹범죄가 지속적으로 발생하는 원인이 되고 있다. 이러한 이유로 보안성이 매우 높다고 알려진 블록체인 기술을 기반으로 하는 암호화폐에 대한 해킹이라는 모순적 상황이 계속 나타나고 있는 것이다.

게다가 암호화폐의 기술종속성은 범집행기관에 대해서도 예외 없이 적용된다. 수사기관이 암호화폐를 압수 또는 몰수하는 경우에도, 암호화폐가 설계된 코드가 사전에 정해놓은 방법으로만 가능하다.[580] 따라서 대부분의 암호화폐의 코드에 법집행을 위

578) 다크 코인과 법적 규제에 관한 설명은, 성희활, "가상화폐의 공모(ICO)와 상장에 대한 적정 규제방안", 상사법연구 제37권 제1호, 한국상사법학회, 2018, 91면, 특히 각주 75번 참조.
579) 암호화폐 거래에 관한 상세한 기술적 설명은 본장 제1절 참조.

한 별도의 방법이 미리 마련되어 있을 리 없고, 법집행을 위한 예외를 인정할 중앙관리기관도 없으므로, 대부분의 경우 수사기관은 암호화폐의 거래를 정지시킬 방법이 없다. 이 경우 수사기관은 별도의 지갑을 마련하여 암호화폐를 옮기는 방법을 택할 수밖에 없게 된다. 이 때 범죄이용 암호화폐 지갑의 비밀키를 확보하지 못하면 암호화폐를 옮길 방법이 없으며, 신속하게 조치하지 않으면 공범 등 제3의 협조자가 범죄에 이용된 암호화폐를 은닉하는 것을 막을 수 없다. 따라서 비밀키의 신속한 확보를 위한 수사협조자 책임감면 규정을 도입하는 것을 고려하는 등, 암호화폐에 적합한 강제수사 방식에 관하여 새로운 법적 근거를 마련해야 한다.

중앙관리기관으로서의 기능을 수행하고 있는 거래소를 이용한 경우라면, 예외적으로 거래소의 적극적인 협조를 전제로 지급정지 등의 방법을 이용할 수 있다. 그러나 국외의 거래소에 대하여 국내 수사기관이 강제적 법집행을 할 실효적 방법이 사실상 존재하지 않는다는 한계가 있다. 또한 국내 거래소에 대하여도 법집행기관에 대한 협조를 강화하기 위하여 면책 및 강제집행을 위한 법제도가 마련되어야 할 것이다.

아울러 암호화폐의 기술종속성은 정보기술을 활용한 사이버범죄의 수단이 되기도 한다. 예컨대 피해자의 정보처리장치의 연산력을 암호화폐의 채굴에 몰래 이용하는 악성코드가 새로운 문제로 등장하였다.[581] 또한 기술적 복잡성으로 인하여 일반인의 경우 작동원리에 대한 이해가 쉽지 않은 탓으로 사기나 유사수신범죄의 수단이 되는 경우도 많다.

4) 불가역성

암호화폐의 불가역성은 탈중앙성의 부수작용 또는 부작용이라고 할 수 있다. 암호화폐는 중앙관리주체가 없으므로 비밀키를 이용한 거래가 한번 승인되어 블록체인에 기록되면 이를 돌이킬 방법이 없는 것이 원칙이다. 설령 해킹범죄의 피해로 암호화폐가 유출되었음이 명백히 확인된 경우라 하더라도 해당 거래를 취소하고 암호화폐를

580) 이러한 현상을 '아키텍처 규제(Architectural Regulation)'의 관점에서 이해할 수 있다. 정보기술영역에서 아키텍처 규제에 관하여 상세한 내용은 심우민, "정보통신법제의 최근 입법동향: 정부의 규제 개선 방안과 제19대 국회 전반기 법률안 중심으로", 언론과 법 제13권 제1호, 한국언론법학회, 2014, 88면 이하 참조.

581) 이른바 채굴악성코드에 관하여는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 53-54면 참조.

되돌릴 방법이 없다. 해커의 비밀키를 알아내어 해커의 지갑으로부터 암호화폐를 다시 송금하는 것이 유일한 방법이다. 따라서 거래에 관하여 당사자간 분쟁이 발생할 경우 사후적으로 이를 해결할 방법이 없다.

5) 투명성

블록체인 기술은 분산원장[582]에 거래내역을 기록하는 방법으로 탈중앙적인 불가역성을 확보한다. 블록체인은 프라이버시를 보호하면서도 거래의 투명성을 확보하는 기술인 것이다. 하지만 어떠한 방법으로건 거래에 이용된 지갑의 주소를 확인할 수 있으면 분산원장에 기록된 정보를 분석하여 해당 지갑과 관련된 거래내역을 확인할 수 있다. 일종의 계좌추적이 가능한 것이다. 물론 상술한 것처럼 믹싱서비스를 이용하는 경우, 또는 일반적인 블록체인 기술과는 다른 방법으로 익명성을 강화한 암호화폐의 경우에는 추적이 불가능할 수도 있다. 이에 대응하기 위한 수사절차를 법제화하기 위한 노력이 필요하다. 절차법적으로는 분산원장의 정보를 분석하여 거래내역을 추적하는 경우 금융거래내역에 대한 강제수사로 볼 것인지 아니면 공개된 정보에 대한 수사(OSINT)로 볼 수 있을 것인지에 대하여 어떠한 입장을 지지할 것인지에 따라 증거능력에 대한 판단이 달라질 수 있다는 문제가 발생한다. 입법적 결단이 필요한 상황이다.

나. 암호화폐 관련범죄

1) 유형 분류

지금까지 블록체인의 기술적 특성과 그와 관련된 문제현상들로 인하여 실무상 정리되고 있는 형사정책적 고려사항들을 살펴보았다. 탈중앙성, 익명성 등의 특성들로 인하여 암호화폐는 실제 범죄자에게 상당히 매력적인 범죄수익 실현 수단이 되고 있으며, 그 결과로 다양한 형태의 범죄현상으로 구체화되고 있다. 암호화폐는 기존 범죄를 고도화하는 수단이 되기도 하며, 암호화폐와 관련된 새로운 범죄현상이 발생하는 원인이 되기도 한다. 2017년에 수행된 연구는 암호화폐와 관련된 다양한 범죄들

582) 분산원장에 관하여는 정승화, "블록체인 기술기반의 분산원장 도입을 위한 법적과제", 금융법연구 제13권 제2호, 한국금융법학회, 2016, 108면 참조.

을 아래 [표 4-2]와 같은 유형으로 분류하였다.

[표 4-2] 암호화폐 범죄 분류체계[583]

구 분	유 형	개 념
암호화폐 침해범죄	해킹범죄	거래소, 개인지갑 등을 해킹하여 암호화폐를 탈취하는 행위
	악성코드 유포범죄	악성코드를 유포하여 암호화폐를 탈취하거나 타인의 컴퓨터를 이용하여 불법 채굴하는 행위
암호화폐 이용범죄	마약·총기거래 범죄	마약·총기 등 금제품 거래에 암호화폐를 사용하는 행위
	랜섬웨어 범죄	악성코드를 유포하여 감염자 컴퓨터에 저장된 정보를 암호화한 후 공갈하여 암호화폐를 요구하는 행위
	불법콘텐츠 범죄	암호화폐를 대가로 도박·음란물 등 불법콘텐츠 서비스를 운용하거나 불법콘텐츠를 이용하는 행위
	유사수신 및 사기범죄	암호화폐 투자를 빙자하여 유사수신을 하거나 투자사기를 하는 행위
	자금세탁 범죄	범죄수익 등 자금세탁이나 불법환전을 위해 암호화폐를 이용하는 행위
	시세조종 범죄	암호화폐의 시세 차익을 얻을 목적으로 허위사실 등 기타 수단을 이용하여 암호화폐의 시세를 임의적으로 조종하는 행위
	기타	기타 암호화폐를 이용하는 범죄행위

위 표는 언론보도 및 경찰 수사자료 등을 토대로 분석한 것으로 큰 틀에서 이 분류를 따르면서 그 이후의 논의들을 추가하는 방식으로 서술하고자 한다. 위 표에 따르면 암호화폐 관련 범죄는 크게 암호화폐 침해범죄와 암호화폐 이용범죄로 구분된다. 이러한 분류에 따르면, 암호화폐 침해범죄는 암호화폐 그 자체 및 채굴 등 암호화폐 작동 체계를 직접적인 범행의 목적으로 하는 범죄를 말하며, 암호화폐 이용범죄는 암호화폐를 다른 범죄의 수익을 실현하기 위한 수단으로 이용하는 범죄를 말한다. 암호화폐 이용범죄는 다시 크게 암호화폐를 범죄수익을 실현하기 위한 수단으로 이용하는 경우와, 암호화폐 유통체계를 이용하여 범죄수익을 얻는 경우, 그리고 암호화폐 관련 기술에 대한 대중의 관심을 이용한 사기범죄로 나누어 볼 수 있다. 암호화폐 침해범죄에는, 거래소나 지갑 등을 해킹하여 비밀키를 취득하고 이를 이용하여 암호화폐를 탈취하는 해킹범죄와 타인의 정보처리장치에 악성코드를 감염시키는 등의

583) 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 48면에서 인용.

방법으로 정보처리장치의 연산력을 도용하여 채굴 등에 이용하고 전기 사용료를 피해자에게 부담시키는 악성코드 유포범죄 또는 크립토재킹(Cryptojacking) 등이 포함된다. 이 외에도 암호화폐를 목표로 하는 보이스피싱 범죄 등이 여기에 포함될 수 있다. 암호화폐를 범죄수익 실현수단으로 이용하는 범죄는 랜섬웨어를 유포하거나 마약·총기·불법컨텐츠 등을 판매하고 그 대가를 암호화폐로 받는 경우를 말한다. 암호화폐의 유통체계를 이용하는 범죄는 암호화폐를 이용하여 불법적인 자금을 세탁하는 경우, 암호화폐 거래시장의 영세성을 이용하여 시세를 조종하고 차액을 얻는 경우 등이 있다. 관련하여 최근에는 대포통장 대신 거래소의 계좌를 이용하여 범죄자금을 세탁하는 경우도 발생하고 있다. 마지막으로 암호화폐를 이용한 사기범죄는 대체로 암호화폐 관련 블록체인 기술이 일반인에게 쉽게 이해되지 않는다는 점을 이용하여 유사수신 또는 사기의 수단으로 암호화폐를 이용하는 방법으로 이루어진다. 암호화폐에 대한 관심이 한창이던 2017년 경 채굴기 분양사기 등이 사회문제가 된 바 있는데, 이 또한 넓은 의미에서 암호화폐를 이용한 사기범죄에 포함되는 것으로 볼 수 있다.

상술한 암호화폐 관련 범죄들은 또 다른 관점에서, 기존 구성요건이 적용될 수 있는 범죄와 새로운 구성요건의 제정이 필요한 범죄로 나눌 수 있다. 암호화폐 침해범죄의 경우는 대부분 기존의 사이버범죄에 해당하므로, 정보통신망법 등의 구성요건을 적용하여 처벌할 수 있을 것이다. 암호화폐 이용범죄 중 범죄수익 실현수단으로 암호화폐를 이용하는 범죄의 경우에도 대부분 수익을 실현하고자 하는 범죄행위에 적용되는 구성요건을 확인할 수 있다. 반면 암호화폐 유통체계를 이용하여 범죄수익을 얻는 범죄에 대하여는 「유사수신행위의 규제에 관한 법률」이나 「자본시장과 금융투자업에 관한 법률」 등 기존의 금융서비스를 전제로 하는 구성요건의 적용이 가능한 경우도 있지만 적용 가능 여부가 명확하지 않거나, 불가능한 경우도 있다. 암호화폐를 이용한 사기범죄는 대체로 무리 없이 사기죄 규정이 적용될 수 있을 것으로 생각한다. 이하에서는 각각의 범죄 유형에 대하여 보다 상세하게 서술한다.

2) 암호화폐 탈취

(1) 거래소 해킹

암호화폐의 기술종속성과 불가역성으로 인하여, 비밀키만 확보하면 바로 암호화폐

를 탈취하여 직접 재산상 이익을 얻을 수 있으므로 국내외를 막론하고 비밀키 관리가 허술한 거래소들은 해커들의 주된 공격 대상이 되고 있다. 2014년 당시 세계 최고 규모의 암호화폐 거래소였던 일본 마운트 곡스(MT.GOX)[584]의 해킹사실이 알려진 이후 암호화폐 거래소는 해커들의 목표가 되어왔다. 마운트 곡스 해킹사건 이후 2015년 슬로베니아의 비트스탬프(Bitstamp), 2016년 홍콩의 비트피넥스(Bitfinex)와 미국의 크립트시(Cryptsy) 등 거래소 해킹사건이 지속적으로 발생한 바 있으며[585], 2018년 1월에는 일본에서 코인체크(Coincheck)라는 거래소가 해킹당하여 무려 약 5,700억 원 상당의 피해를 입기도 하였다.[586]

2019년 국정감사에서 과학기술정보통신부가 국회에 제출한 자료에 따르면 우리나라에서 거래소 해킹이 정부당국에 처음 보고된 것은 2017년 4월로, 이후 3년간 국내 거래소 해킹 피해 누적 금액은 무려 약 1,266억 원에 달하는 것으로 추정된다. 특히 우리나라에서 가장 규모가 크고 거래가 활발한 거래소 중 하나인 빗썸은, 2018년 한국인터넷진흥원(KISA)의 정보보호관리체계 인증(Information Security management System, ISMS)을 받았음에도 불구하고 올해 3월 해킹을 당해 수백억 원의 손실을 입은 것으로 드러나 암호화폐 거래소의 보안 강화를 위한 대책이 필요하다는 지적을 받은 바 있다. 최근 3년간 보고된 암호화폐 거래소 해킹 사례는 아래 [표 4-3]과 같다.[587]

---

584) Mt.Gox는 일반적으로 "마운트 곡스"로 읽는다. 2007년 카드게임의 일종인 매직 더 게더링(Magic: the Gathering)의 온라인 카드거래소로 설립되었으며, 그래서 Magic The Gathering Online eXchange의 약자를 거래소의 명칭으로 하고 있다. 2010년부터 본격적인 암호화폐 거래업무를 시작하였고 세계 비트코인 거래량의 약 80%를 차지할 정도로 거대한 거래소로 성장하였다. 2014년 해킹피해를 당한 사실이 알려진 이후 파산하였다.

585) 거래소 해킹사건에 관하여 보다 상세한 내용은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 49-50면 참조.

586) 코인체크 해킹사건에 관하여 상세한 내용은 "코인체크: 일본 역대 최대 가상화폐 해킹에 관해 궁금한 3가지", BBC 코리아 2018년 1월 28일자, https://www.bbc.com/korean/news-42850184 (2019년 11월 8일 최종접속) 참조.

587) "국내 암호화폐 거래소, 최근 3년간 해킹으로 1200억원 손실", 코인데스크 2019년 10월 2일자, https://www.coindeskkorea.com/57799/ (2019년 11월 8일 최종접속).

[표 4-3] 최근 3년간 거래소 해킹 사례[588][589]

사건 발생월	피해 업소	피해 내용	경제적 피해규모 (언론보도 추정)
2017.4	코인빈(야피존)	가상통화 유출	약 55억
2017.6	비티씨코리아(빗썸)	개인정보 약 3.6만건 유출	약 70억
2017.9	코인이즈	가상통화 유출	약 21억
2017.12	유빗(구 야피존)	가상통화 유출	약 170억
2018.6	코인레일	가상통화 유출	약 500억
2018.6	빗썸	가상통화 유출	약 350억
2018.10	올스타빗	가상통화 유출	확인불가
2019.3	빗썸	가상통화 유출	약 100억~200억
합계			약 1,266억

이처럼 새롭게 중앙관리기관으로 자리매김하고 있는 거래소의 경우 현행법상 정보통신서비스 제공자에 해당하여 정보통신망법의 적용을 받으며, 이 법이 정하고 있는 일반적인 수준의 보안에 관한 규제와 감독을 받는다. 그래서 암호화폐 거래소인 빗썸이 KISA의 ISMS 인증을 받았던 것이다. 금융기관이 「전자금융거래법」에서 요구하는 강화된 보안기준을 준수해야 하는 것에 비하여, 상대적으로 낮은 기준이 적용된다고 할 수 있다. 그러나 거래소를 해킹하여 암호화폐 지갑의 비밀키를 확보할 경우 암호화폐를 탈취할 수 있으므로, 이용자의 편리를 위하여 지갑의 비밀키 정보를 거래소 서버에 보관하는 경우가 많은 거래소는 일반적인 정보통신서비스 제공자에 비하여 훨씬 매력적인 해킹범죄의 타겟이 된다. 거래소에 대한 해킹은 금융기관에 대한 해킹과 전혀 다르지 않은 것이다. 그러므로 거래소에 대하여 금융기관에 준하는 보안의무를 부과하고 특히 비밀키 관리 등과 관련하여서는 거래소의 특성에 맞는 의무가 설정

588) "국내 암호화폐 거래소, 최근 3년간 해킹으로 1200억원 손실", 코인데스크 2019년 10월 2일자, https://www.coindeskkorea.com/57799/ (2019년 11월 8일 최종접속).

589) 위의 기사("국내 암호화폐 거래소, 최근 3년간 해킹으로 1200억원 손실")에 따르면, ISMS는 기업의 정보자산 관리체계가 적절한지를 심사하여 인증을 부여하는 제도로 「정보통신망이용촉진 및 정보보호 등에 관한 법률」 제47조 제2항이 정한 요건을 충족하는 정보통신서비스 제공자는 의무적으로 인증을 받아야 한다. 정보통신서비스 부문의 전년도 매출액이 100억 이상이거나 3개월간 일일평균 이용자수가 100만명 이상인 경우 인증의무대상이 된다. 2019년 현재 빗썸 등 인증의무 기관인 4개 거래소와 그 외의 3개 거래소가 인증을 받았다고 한다. 거래소 해킹에 관한 국정감사에 관한 자세한 내용은 위의 기사 참조.

되어야 한다. 아울러 침해사고 발생 시 이용자의 보호를 위하여 일종의 예금자보호 등과 같은 정책적 고려가 필요한지 여부에 대한 검토가 요청된다.

(2) 개인 계정 해킹

개인의 정보가 해킹당하여 지갑의 비밀키나 거래소 접속정보가 유출되고 암호화폐를 탈취당하는 경우도 있다. 실제 2014년 11월 비트코어(bitcore) 거래소의 개인 계정이 해킹당하여 15비트코인이 유출된 사건이 우리나라의 첫 번째 암호화폐 해킹사건으로 기록되어 있다.[590] 2016년에는 이더리움 재단이 소유한 지갑에 대하여 환불 시스템 오류를 이용한 해킹사건이 발생하여 당시 시가 기준으로 약 750억원 규모의 이더리움이 유출되는 사고가 발생하기도 하였다.[591] 개인 계정에 대한 해킹은 정보기술을 이용한 전형적인 해킹 방법을 통하여 이루어질 수도 있고, 사회공학적 방법을 동원하여 비밀키나 계정의 비밀번호를 알아내는 경우도 있다.

이러한 해킹 범죄를 예방하기 위해서는 무엇보다도 이용자 스스로 비밀키 또는 거래소 접속정보가 유출되지 않도록 주의해야 하는 것이 우선일 것이다 하지만 암호화폐 및 거래소 서비스의 개발단계에서부터 취약점을 사전에 면밀히 검토하고 이용자 검증 방법을 다원화하는 등의 노력을 기울일 필요가 있으며, 정책적으로는 암호화폐 서비스 제공자(VASP)들이 이러한 기준을 준수하도록 적절한 규제체계가 제도화 되어야 할 것이다.

(3) 크립토재킹(악성코드 유포범죄)

크립토재킹(Cryptojacking)이란 암호화폐(CryptoCurrency)와 (비행기) 납치를 의미하는 하이재킹(Hijacking)을 합성한 말로, 피해자의 정보처리장치의 연산력을 불법적으로 도용하여 암호화폐의 채굴에 이용하는 범죄를 말한다. 크립토재킹은 크게 악성코드를 피해자 정보처리장치에 설치하는 다운로드형과, 악성코드의 설치 없이 특정 자바스크립트 코드가 내재된 웹사이트에 방문하기만 해도 연산력을 도용하는 드라이브 바이 크립토재킹(Drive By Cryptojacking)[592]으로 나눌 수 있다.[593] 보안업체인

590) "국내 첫 비트코인 해킹 사례 발생", 코리아헤럴드 2014년 12월 8일자, http://www.koreaherald.com/view.php?ud=20141208001040 (2019년 11월 4일 최종접속) 참조.

591) 이 사건은 이더리움 클래식이 '하드포크'되는 원인이 되었다. 상세한 내용은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 52면 참조.

맥아피(McAfee)에 따르면 2017년 4분기에만 약 40만 건의 암호화폐 채굴 악성코드가 발견되었고, 2018년 1분기에는 무려 약 290만 건이 감지되었다고 한다.[594]

가상화폐의 가치가 급상승하였던 2017년경부터 악성코드를 유포[595]하여 감염된 PC나 스마트폰과 같은 정보처리장치의 백그라운드에서 지속적으로 채굴을 위한 연산을 수행하도록 하는 형태의 범죄가 급속히 확산되었다. 이후 특정 웹사이트에 접속하기만 해도 별도의 악성코드가 다운로드 되거나 설치되지 않은 상태에서 웹사이트에 설치된 자바스크립트(Java Script)가 동작하여 웹사이트에 접속한 컴퓨터의 연산능력을 사용하여 암호화폐를 채굴하는 방식의 드라이브 바이 크립토재킹 방식이 등장하였다. 본래 웹사이트를 통한 암호화폐 채굴은 웹사이트의 광고를 대체하여 웹사이트 운영자에게 수익모델을 제공하기 위한 공개적으로 운영되는 사업모델로 개발된 것이었다. 그러나 이러한 서비스를 제공하였던 코인하이브(Coinhive)와 같은 서비스들이 당초의 취지에도 불구하고 범죄자들에 의하여 악용되기 시작하였고, 웹사이트 관리자도 모르게 암호화폐를 채굴하는 자바스크립트를 웹사이트에 설치하거나 피해자의 컴퓨터에 설치하여 수익을 가로채는 경우가 늘어났다.[596] 코인하이브에서 이용한 자바스크립트는 아래 [그림 4-4]와 같다.

---

592) "드라이브 바이"라는 말은 별도의 다운로드 없이 웹브라우저의 취약점을 이용하여 악성코드를 실행하는 방식을 말한다. 드라이브 바이 크립토재킹에 관하여는 "드라이브 바이 크립토재킹? 암호화폐 채굴 얼마나 많나", 보안뉴스 2018년 4월 18일자, https://www.boannews.com/media/view.asp?idx=68562 (2019년 11월 8일 최종접속) 참조.

593) 자바스크립트도 "코드"라는 점에서 양자 모두 악성코드를 이용한 범죄라는 사실은 차이가 없다.

594) "증가하는 위협: 크립토재커와 랜섬웨어의 결합", IT 데일리 2018년 12월 14일자, http://www.itdaily.kr/news/articleView.html?idxno=92268 (2019년 11월 8일 최종접속) 참조.

595) 악성코드를 타인이나 거래소가 보유하고 있는 암호화폐를 탈취하기 위한 해킹범죄의 수단으로 이용하는 경우도 있으나 이는 상술한 악성코드 탈취범죄에 포함되는 것으로 보아야 할 것이다.

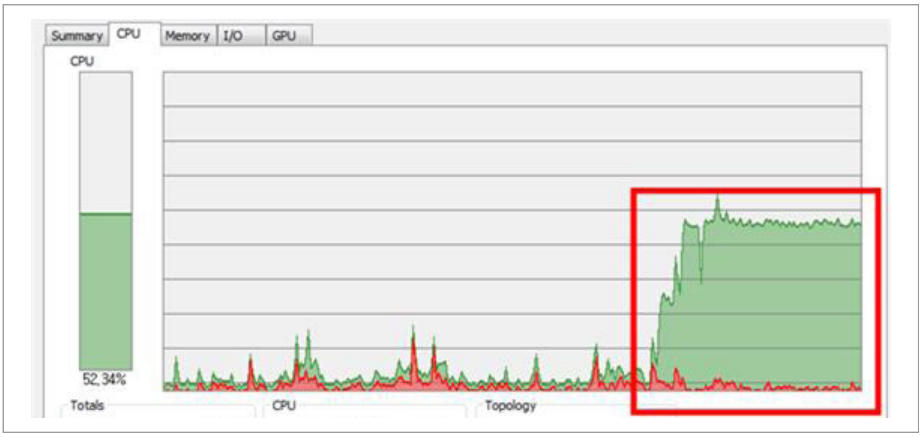
596) 2017년 10월 한 조사에 따르면 전세계 주요 웹사이트 10만 곳 중 2.2%인 220개 웹사이트에 5억명 가량의 방문자의 컴퓨터가 암호화폐 채굴에 도용되었다고 한다. "PC 5억대, 암호화폐 채굴에 몰래 동원돼", ZDNet Korea 2017년 10월 15일자, http://www.zdnet.co.kr/view/?no=20171015121657 (2019년 11월 8일 최종접속) 참조.

[그림 4-4] Coinhive의 자바스크립트 코드[597]

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.User('<site-key>', 'john-doe');
    miner.start();
</script>
```

악성코드를 다운로드하여 설치하는 방식이건, 웹사이트상에서 작동하는 드라이브바이 크립토재킹 방식이건 모두 피해자의 인지나 동의 없이 정보처리장치의 연산력을 도용하는 것이기 때문에 피해자는 자신의 컴퓨터나 스마트폰의 응답속도가 느려지는 것을 경험하게 되며 추가로 발생한 전기소모에 대한 비용을 지불해야 하는 손해를 부담하게 된다. 크립토재킹을 위한 악성코드에 감염된 PC는 아래 [그림 4-5]처럼 CPU 사용률이 증가하게되며, 증가된 부분만큼 전기소모량이 늘어날 뿐만 아니라 업무처리가 느려지게 된다.

[그림 4-5] 크립토재킹을 위한 악성코드 감염 후 CPU 사용률 증가[598]

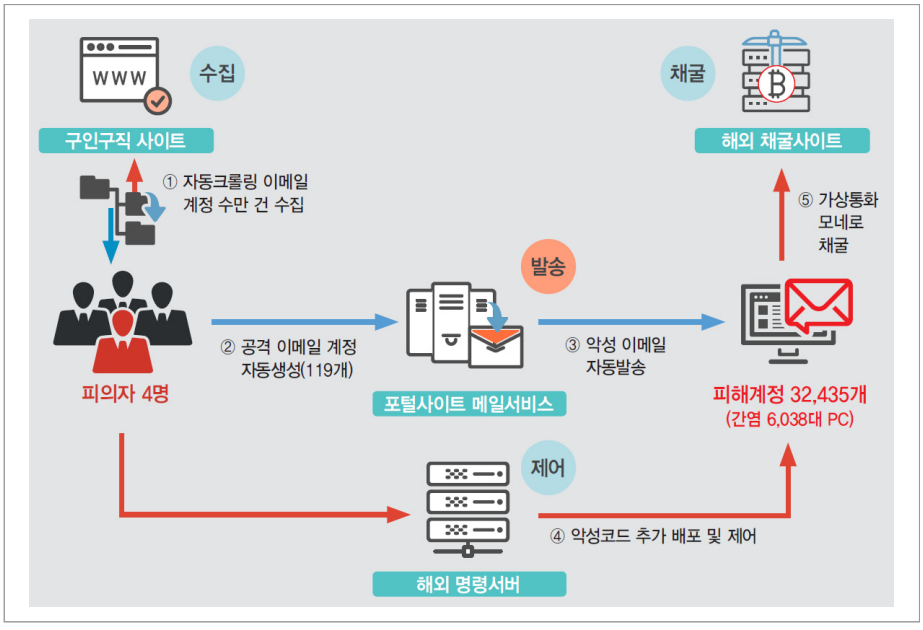


597) 이미지 출처: 한국인터넷진흥원 인터넷보호나라 웹사이트, https://www.krcert.or.kr/search/boardView.do?bulletin_writing_sequence=26843 (2019년 11월 4일 최종접속).
598) 이미지 출처: 경찰청, 2018 사이버위협 분석 보고서, 2019, 9면.

따라서 보안프로그램들은 업데이트를 통하여 이러한 악성코드에 대응하기 시작하였고, 보안프로그램 등에 의하여 다운로드형 악성코드 및 웹사이트 자바스크립트 코드들은 지속적으로 차단되고 있다. 공개적으로 운영하였던 코인하이브는 결국 수익성이 악화되고 법적 분쟁의 소지가 커지자 수익모델을 포기하고 2019년 3월 서비스를 중단하였다.[599]

우리나라에서는 2017년 말경 구인구직 사이트에서 수집한 채용지원 접수용 이메일 계정으로 입사지원서로 위장한 악성코드를 발송하고 문서가 실행되면 모네로를 채굴하는 악성코드가 설치되게 하여 6,038대의 PC를 감염시키고 CPU 연산능력의 50%를 도용하여 가상통화를 채굴한 범죄자 4명이 경찰에 검거된 바 있다. 피의자들은 이러한 방법으로 실제 약 100만원 상당의 암호화폐를 채굴하였다고 한다. 이러한 범행 수법을 도식화하면 아래 [그림 4-6]과 같다.

[그림 4-6] 2017년 검거된 크립토재킹 사건[600]



599) "코인하이브 "암호화폐 채굴 서비스 3월 초 중단"", ZDNet Korea 2019년 2월 28일자, http://www.zdnet.co.kr/view/?no=20190228094221 (2019년 11월 8일 최종접속) 참조.

600) 이미지 출처: 경찰청, 2018 사이버위협 분석 보고서, 2019, 8면.

2019년 국정감사에서 한국인터넷진흥원(KISA)이 국회에 제출한 자료에 따르면 우리나라에서 2016년부터 2019년 8월까지 탐지된 크립토재킹은 총 1,473건이며, 2018년에 1,355건을 기록한 이후 2019년에는 8월까지 90건만 탐지되는 등 그 수가 다시 감소하였다. 탐지된 크립토재킹의 대부분은 2018년에 총 1,355건이 탐지된 드라이브 바이 크립토재킹이다. 다운로드형 악성코드와 드라이브 바이 크립토재킹 모두 2019년 이후 그 수가 크게 줄어들었다. 크립토재킹이 CPU 사용량 증가라는 명백한 특성이 있는 탓으로 다른 악성코드에 비하여 비교적 탐지 및 차단이 쉽기 때문인 것으로 보인다. 최근 4년간 한국인터넷진흥원에 탐지된 크립토재킹 현황은 아래 [표 4-4]와 같다.[601]

[표 4-4] 최근 4년간 크립토재킹 탐지현황[602]

구분	2016	2017	2018	2019.8월	합계
악성코드형 크립토재킹 탐지현황	2	23	49	7	81
스크립트형 크립토재킹 탐지현황	0	3	1,306	83	1,392
총합	2	26	1,355	90	1,473

4) 랜섬웨어

랜섬웨어(Ransomware)는 납치 또는 유괴된 사람에 대한 석방대가(Ransom)와 소프트웨어(software)를 합성한 말로, 파일들을 모두 암호화시킨 후 복호화의 대가로 돈을 요구하는 악성코드를 말한다.[603] 랜섬웨어는 PC는 물론 스마트폰이나 스마트워치, 스마트TV, 각종 IOT 기기 등 다양한 정보처리장치에 폭넓게 설치될 수 있다. 2017년 워너크라이(WannaCry)라는 랜섬웨어의 피해가 전세계적으로 확산되면서 주

601) 크립토재킹 관련 국정감사에 관하여는 "타인 컴퓨터 암호화폐 채굴에 사용 '크립토재킹' 최근 4년간 677배 늘어", IT조선 2019년 10월 1일자, http://it.chosun.com/site/data/html_dir/2019/10/01/2019100101028.html (2019년 11월 8일 최종접속) 참조.

602) "타인 컴퓨터 암호화폐 채굴에 사용 '크립토재킹' 최근 4년간 677배 늘어", IT조선 2019년 10월 1일자, http://it.chosun.com/site/data/html_dir/2019/10/01/2019100101028.html (2019년 11월 8일 최종접속)에서 인용.

603) 랜섬웨어에 관해서는 김대근/임석순/강상욱/김기범, 신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구 – 기술적 수단을 사용한 사이버 금융사기를 중심으로, 한국형사정책연구원, 2016, 121-128면; 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 61-63면 참조.

목받기 시작했다.

우리나라에서는 2017년 6월, 인터넷 호스팅 업체인 '인터넷나야나'의 서버 153대가 에레버스(Erebus)라는 랜섬웨어에 감염되어 암호화되면서 호스팅업체를 이용하여 인터넷 웹사이트를 운영하던 다수의 운영자에게 피해가 발생하였다. '인터넷나야나'는 2017년 기준으로 약 16년가량 웹호스팅 서비스를 제공해 온 기업으로, 당시 약 1만여 개 이상의 웹사이트를 호스팅하고 있었다. 공격자는 당시 시가 기준 약 26억 원의 '몸값'을 요구했고, 처음에는 백업데이터 등을 이용하여 자체적으로 복구하려 했으나 백업 서버까지 랜섬웨어에 감염된 탓으로 복구 및 복호화에 실패하였다. 결국 호스팅 업체의 특성상 약 5천여 이용자들의 요청으로 인하여 피해업체는 랜섬웨어 유포자에게 당시 시가 기준 약 13억원의 비트코인을 지불하고 복호화코드를 받았다.[604]

암호화폐가 존재하기 이전에도 감염된 정보처리장치의 파일들을 암호화해서 사용할 수 없게 하는 악성코드가 존재했다. 최초의 랜섬웨어는 1989년 플로피 디스크형태로 유포된 AIDS Trojan으로 알려져 있다. 당시에 랜섬웨어의 유포자는 파나마에 있는 우편사서함을 통하여 189달러를 받고 파일을 복구할 수 있는 디스크를 보내주었다고 한다.[605] 그러나 대가를 받기 위해서는 AIDS Trojan의 경우처럼 우편사서함이나 대포통장 등을 이용해야만 했기 때문에, 범죄자의 추적 및 검거가 상대적으로 용이했고, 따라서 유사한 범죄가 확산되지 않아 랜섬웨어라는 개념 자체가 정립되지 않았다.

그러나 대표적인 암호화폐인 비트코인이 등장하고, 동시에 토르(Tor)[606] 기반의 다크웹 생태계가 만들어지면서 랜섬웨어 제작자들이 본인의 신원을 노출하지 않고도 수익을 현실화할 수 있는 방법이 생겼으며, 이후 크립토락커(CryproLocker)[607]와 이와 유사한 변종 랜섬웨어들이 다수 등장하였다. 그래서 최근에는 대부분의 랜섬웨어가 파일암호화와 비트코인 그리고 다크웹의 조합 형태로 작동하고 있다. 랜섬웨어에

---

604) "'인터넷나야나' 13억 몸값 지불에 다른 기업들 한숨쉬는 이유", 한겨레 2017년 6월 18일자, http://www.hani.co.kr/arti/economy/it/799226.html (2019년 11월 8일 최종접속) 참조.

605) AIDS에 관하여 상세한 내용은 Knowbe4 홈페이지, https://www.knowbe4.com/aids-trojan (2019년 11월 8일 최종접속) 참조.

606) 토르는 The Onion Router의 약자로 인터넷상에서 익명화를 가능하게 해주는 다크웹 소프트웨어이다. 상세한 내용은 토르 공식 웹사이트, https://torproject.org/ (2019년 11월 8일 최종접속) 참조.

607) 크립토락커에 관하여는 "Cryptolocker ransomware has 'infected about 250,000 PCs'", BBC News 2013.12.24., https://www.bbc.com/news/technology-25506020 (2019년 11월 8일 최종접속) 참조.

감염된 컴퓨터는 아래 [그림 4-7]과 같은 창을 띄워 감염사실을 알리고 파일복구를 원하는 경우 암호화폐로 금전을 지불할 것을 요구한다.

[그림 4-7] 워너크라이 감염 화면[608]

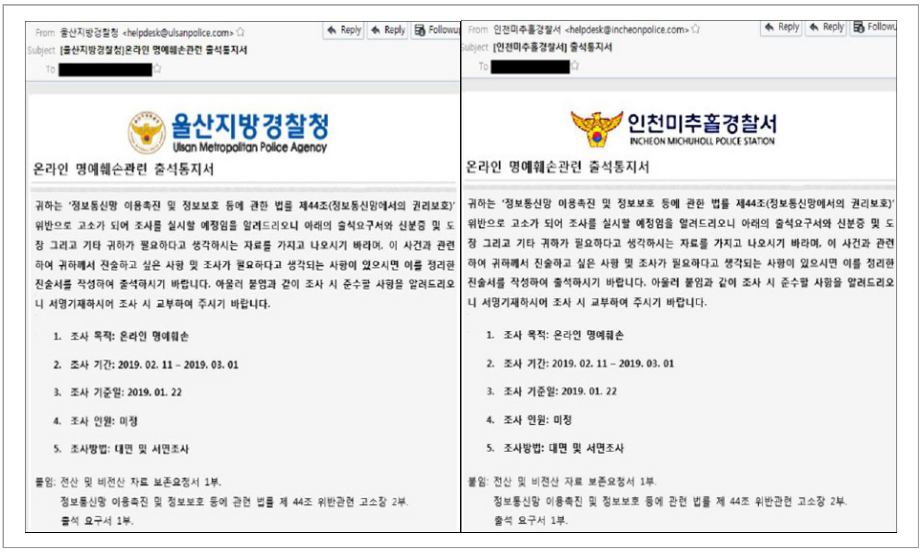


2019년 상반기에는 갠드크랩(GandCrab)이라는 랜섬웨어가 확산되고 있다. 갠드크랩은 서비스형 랜섬웨어(Ransomeware as a Service: RaaS)의 하나로, 서비스형 랜섬웨어란 랜섬웨어를 제작할 역량이 없는 공격자를 위하여 랜섬웨어 제작을 서비스해주고 공격자와 제작자가 수익을 나누는 형태의 랜섬웨어로, 다크웹 등을 통하여 다수의 공격자가 암호화폐로 대가를 지불하고 악성코드를 구매하여 공격에 활용할 수 있는 특성이 있다. 따라서 공격자가 유포 및 공격 대상에 적합도록 변경하기가 쉬우며, 우리나라에서는 주로 아래 [그림 4-8]과 같은 "경찰서 출석요구서"나 "입사지원서"를

608) 이미지 출처: 한국인터넷진흥원 블로그, https://m.post.naver.com/viewer/postView.nhn?volumeNo=10236582&memberNo=3326308 (2019년 11월 8일 최종접속).

위장한 이메일을 발송하는 방식으로 첨부파일을 열어보도록 유도하여 랜섬웨어가 설치되도록 하는 방식으로 그 피해가 확산되고 있다.[609]

[그림 4-8] 랜섬웨어 유포 이메일[610]



네덜란드 경찰청의 National High Tech Crime Unit, 유로폴의 European Cybercrime Centre, 카스퍼 스키 랩, 인텔시큐리티는 범죄자에게 돈을 지불하지 않고도 파일을 복구할 수 있도록 "노모어랜섬(No More Ransom)"이라는 프로젝트를 운영하고 있다.[611] 노모어랜섬 웹사이트에 접속하면 이미 해독된 랜섬웨어의 경우 무료로 파일복구를 지원한다.

5) 불법거래

랜섬웨어의 경우에서 볼 수 있는 것처럼, 암호화폐의 익명성은 다크웹과 결합하면서 훨씬 증폭되며, 따라서 불법적인 영업을 수행하는 자들이 자신의 신원을 노출시키

609) 2019년 6월, 갠드크랩 제작자가 총 '20억 달러를 벌었으며 앞으로 판매를 중단하겠다'고 선언했다. 갠드크랩 랜섬웨어와 서비스형 랜섬웨어에 관하여 상세한 내용은 경찰청, 2019년 상반기 사이버위협 분석 보고서, 2019, 6-8면 참조.

610) 이미지 출처: 경찰청, 2019년 상반기 사이버위협 분석 보고서, 7면.

611) 노모어랜섬 한국어 홈페이지, https://www.nomoreransom.org/ko/index.html (2019년 11월 8일 최종접속) 참조.

지 않고도 거래 대가를 현실화할 수 있는 매력적인 수단이 되고 있다. 상술한 것처럼 2010년 마운트 곡스가 본격적으로 암호화폐 거래소 영업을 시작하면서 암호화폐의 현실화폐로의 환금성이 비교적 안정적으로 보장된다는 사실이 알려지기 시작하자, 마약, 총기, 아동음란물 등 금제품이나 신용카드 복제, 신분증 위조, 각종 범죄청부 등 금지된 용역을 불법적으로 거래하던 범죄자들은 암호화폐를 더욱 적극적으로 이용하여 수익을 창출하기 시작하였다. 2011년 1월부터 운영되기 시작하여 2013년 10월 폐쇄된 실크로드(Silk Road)는 전세계의 이용자에게 암호화폐를 매개로 마약을 판매하였다. FBI의 수사에 따르면 실크로드에는 오직 비트코인만이 사용되었으며, 실크로드가 운영되는 기간 동안 약 1억 8천 3백만 달러에 달하는 마약 등의 금제품이 거래된 것으로 밝혀졌다.[612] 실크로드 운영자가 검거되자 금제품 거래는 알파베이(Alphabay), 한자마켓(Hansa Market), 드림마켓(Dream Market), 월 스트리트 마켓(Wall Street Market) 등으로 차례로 옮겨갔다. 다크웹상의 주요 마켓들은 차례로 법집행기관에 의하여 폐쇄되거나 사라졌지만, 금제품이나 금지된 용역을 불법적으로 거래하고자 하는 자들은 계속 이를 대체하는 수단을 만들고 있다.[613]

우리나라에서도 2017년 하이코리아(High Korea)라는 다크웹상의 마켓에서 마약을 거래한 일당이 검거된 바 있다. 국제우편 등으로 대마, 필로폰 등을 국내로 반입한 이후 비트코인을 대금으로 받고 임의의 장소에 마약을 투척하는 방식으로 거래하였다. 경찰은 범죄에 이용된 비트코인 주소를 확보하여 거래내역을 분석한 후 국내 거래소 정보를 이용하여 신원을 확인, 검거하였다.[614]

2019년 10월에는 우리나라 경찰청, 미국 국토안보수사국(HSI), 영국 국가범죄청(NCA) 등 세계 32개국 수사기관이 공조하여 한국인이 운영하던 아동음란물 거래 다크웹인 웰컴투비디오(Welcome to Video, W2V)를 수사한 결과가 발표되었다. 우리나라 경찰은 이미 2018년 아동음란물 다크웹 사이트 W2V 운영자를 검거, 구속하였으며,

---

612) 실크로드에 관하여 상세한 내용은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 58-60면 참조.

613) 다크웹상의 불법거래 '마켓'에 관하여 상세한 내용은 "접속 10분 만에 총·마약·불법영상…'다크웹' 클릭 한 번에 범죄자 될 수도", 경향신문 2019년 10월 24일자, http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201910240600075 (2019년 11월 8일 최종접속) 참조.

614) 하이코리아에 관하여 상세한 내용은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 57-58면 참조.

이때 압수한 W2V 서버를 분석하여 이용자 계정정보를 확보하였다. 우리나라 경찰은 이 정보를 이용하여 한국인 이용자 223명을 검거하였으며, 국외에서 접속한 유료회원 계정 3340개의 정보를 31개국 수사기관에 전달하여 각국의 수사기관이 총 87명을 추가로 검거하였다. 경찰은 수사가 일단락 된 후 다크웹 이용자에게 경각심을 고취하기 위하여 W2V 홈페이지에 아래 [그림 4-9]와 같은 화면을 게시하였다.[615]

[그림 4-9] 공조수사 결과 발표 후 W2V 사이트 화면[616]



이처럼 암호화폐와 다크웹의 결합은 마약, 총기, 아동음란물 등 금제품과 범죄청부 등 불법적 용역을 초국가적으로 거래할 수 있게 해주는 통로가 되고 있다. 우리 경찰은 이에 대응하기 위하여 올해 안에 다크웹상의 정보를 자동수집한 후 경찰이 보유하고 있는 정보와 연동하여 분석하는 '다크넷 내 불법정보 수집·추적 시스템(가칭)'을 개발

615) 상세한 내용은 "아동음란물 제공 'W2V' 한국인 이용자 9월까지 223명 검거", 경향신문 2019년 10월 16일자, https://news.khan.co.kr/kh_news/khan_art_view.html?artid=201910162300005&code=940100 (2019년 11월 8일 최종접속); 경찰청 보도자료, "미국 법무부, 아동음란물 다크웹사이트 국제공조사건 수사결과 발표", 2019.10.16., https://www.police.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000105274&fileSn=1&bbsId=B0000011&type=0 (2019년 11월 4일 최종접속) 참조.

616) 이미지 출처: 경찰청, 앞의 보도자료("미국 법무부, 아동음란물 다크웹사이트 국제공조사건 수사결과 발표"), 붙임 2 참조.

하는 등 다크웹과 암호화폐를 이용하는 범죄에 대한 수사역량을 강화하고 있다. 그러나 기존 가입자의 추천을 받아야 가입할 수 있는 경우처럼 가입 자체가 어렵게 되어있는 회원제 마켓 내부의 정보를 확보하려면, 그리고 신원이 철저하게 감춰진 다크웹 이용자들을 추적해서 검거하기 위해서는 경찰에게 보다 강력한 수사권한이 주어질 필요가 있다. 실제 실크로드 등 다크웹을 수사하기 위하여 미국 FBI는 범죄자로 신분을 위장한 잠입수사관을 활용하였으며, 독일 등 대부분의 선진국 수사기관은 법원의 허가를 받는 등의 절차를 거쳐 전자적 감시 수사기법을 수사에 활용하고 있다. 잠입수사[617]나 정보통신기술을 이용한 전자적 감시 등의 수사기법은 분명 다크웹상의 범죄를 수사하기 위하여 효율적인 수사기법임에는 틀림없다. 그러나 수집된 증거가 위법수집증거로 배제되지 않기 위해서는 범의유발형 불법함정수사에 해당하는 것은 아닌지 또는 피의자 진술거부권이 부당하게 침해되는 것은 아닌지 등의 쟁점들을 충분히 검토하여야 하며, 비례성 원칙을 준수하는 범위 내에서 합리적인 수사방안이 도출되어야 한다. 궁극적으로는 그 결과가 입법적 결단으로 이어져 적법절차로 법제화 되어야 할 것이다.[618]

6) 유사수신 및 사기

2017년 우리 사회 내에서 암호화폐에 대한 대중의 관심이 빠른 속도로 높아지고 있을 당시, 암호화폐 투자 열풍에 편승한 각종 사기 및 유사수신행위가 폭증하였고 그 피해가 심각한 규모로 확산되었다. 블록체인 기술은 제4차 산업혁명의 핵심기술로 당장이라도 핀테크 등에 활용가능한 기술인 것처럼 홍보되었고, 블록체인 기술의 총아인 암호화폐의 가격이 수년간 몇 십 배, 몇 백 배 가격이 상승했다는 언론보도는 조금이라도 빨리 선점하지 않으면 큰 손해일 것 같은 불안한 마음을 들게 하였다. 이처럼 정보기술에 대한 낙관론은 저금리·저성장 기조에 투자처가 마땅치 않은 상황에서 암호화폐가 매력적인 투자처로 보이게 하였다.[619] 특히 일반인은 물론 상당한 관심과 배경지식이 있는 사람이라 할지라도 블록체인 기술과 그 기술이 활용되는

617) 잠입수사기법의 법적 쟁점에 관하여는 도중진, "범죄수사에 있어서 잠입수사관제도의 도입여부", 중앙법학 제13집 제3호, 중앙법학회, 2013, 169면 이하 참조.
618) 박웅신/이경렬, "다크넷의 범죄현상과 형사법적 대응방안", 형사법의 신동향 제58호, 대검찰청, 2018, 245면 이하 참조.
619) 금융위원회, 관계기관 합동 가상통화(Virtual currency) 현황 및 대응방안, 2017.9., 1면.

구조를 직관적으로 이해하기 어려워, 기술적 관점에서 건전성 여부를 판단하기가 사실상 불가능하다는 점을 이용하여 신규 암호화폐 발행(ICO)이나 채굴사업을 내세운 암호화폐 투자사기가 다수 발생하였다.

주로 헷지비트코인, K코인, 코알코인 등 실제 유통이 불가능한 암호화폐를 만들어 다단계방식으로 판매하거나 '마이닝맥스'처럼 채굴기 투자를 빙자한 사기범죄가 발생하였다.[620] 특히 신규 암호화폐의 안전성에 의심을 갖는 투자자들도 상장 후 '거래소의 영업이익'을 보유하고 있는 암호화폐의 양에 따라 배당한다는 말로 기망하여 이른바 '거래소 코인' 또는 '배당형 코인'에 대한 대규모 투자를 유치한 후 투자받은 암호화폐를 세탁하고 도주하는 경우도 발생하였다.

우리 경찰은 2017.7.12.부터 무기한으로 「가상화폐 투자사기 등 불법행위 특별단속」에 돌입하였고 "다단계 조직을 이용한 가상화폐 판매 사기, 가상화폐사업·채굴사업 등을 빙자하여 고수익 배당을 미끼로 투자금을 모집하는 유사수신 투자사기"와 "가상화폐 거래업체나 구매대행자 등에 의한 횡령·사기"에 수사력을 집중하였다.[621] 이러한 노력에 힘입어 경찰은 실제 같은 해 9.1.부터 9.15.까지 2주간 실시된 암호화폐 투자사기 집중수사에서 피해금액이 1천억원이 넘는 사례를 포함하여 10건의 투자사기를 적발하였다.[622]

경찰 및 금융감독원 등 정부부처의 강력한 대응에도 불구하고 암호화폐 관련 유사수신 또는 사기범죄는 여전히 줄어들지 않고 있다. 2019년 3월에도 암호화폐 거래소 코인업 대표가 다단계수법을 이용한 투자사기로 수천 명에게 수천억 원의 피해를 입힌 혐의로 구속되었으며[623], 암호화폐 거래소 히트코리아의 뮤토코인도 상장폐지되면서 투자자들에게 피해를 야기하였다.

2019.4.25. 금융감독원이 발표한 보도자료에 따르면 ICO나 채굴을 빙자한 암호화폐 유사수신범죄는 2016년 27건, 2017년 39건을 수사 의뢰 하였으나, 2018년에는

620) 각 사례의 구체적인 내용에 대하여는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 65-66면 참조.

621) 경찰청 보도자료, "경찰청, 가상화폐 다단계·유사수신 사기 뿌리 뽑는다", 2017.7.12., https://www.police.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000097751&fileSn=1&bbsId=B0000011&type=0 (2019년 11월 4일 최종접속)에서 인용.

622) 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 65면 참조.

623) "수천억대 가상화폐 투자사기 '코인업' 고위 간부 5명 구속", 연합뉴스 2019년 4월 30일자, https://www.yna.co.kr/view/AKR20190430062900004 (2019년 11월 8일 최종접속) 참조.

44건을 수사 의뢰 하는 등 최근 3년간 점차 그 수가 증가하고 있다.[624] 2017.7.부터 2019.6.까지 2년간 암호화폐 투자사기, 다단계, 유사수신 범죄, 거래소 관련 범죄 총 165건을 검거하였으며 그 중 132명을 구속기소하고 288명을 불구속기소하였다. 이 범죄들로 인한 총 피해액은 무려 2조 6,985억 원에 달한다고 한다.[625]

7) 자금세탁

암호화폐의 익명성은 그 자체로 자금 이동 경로의 추적을 어렵게 한다. 익명성이 강화된 암호화폐들 간에 수많은 허위거래를 만들어 그 추적을 더욱 어렵게 하는 방법으로 손쉽게 자금세탁을 할 수 있다. 특히 기존의 금융기관들이 실명 확인의무 또는 의심거래 보고의무 등 자금세탁방지를 위한 각종 법적 규제의 적용을 받기 때문에 자금의 이동경로를 숨기고 싶은 자들에게 현실화폐로의 환금성이 보장되는 암호화폐는 역시 매력적인 수단이 될 수밖에 없다. 자금세탁은 일반적으로 암호화폐를 이용한 모든 범죄에 수반하여 발생한다. 범죄로 얻은 수익을 환수당하지 않으려면 추적을 회피해야 하기 때문이다. 따라서 암호화폐 탈취, 크립토재킹, 랜섬웨어, 불법거래, 유사수신 및 사기는 물론 후술할 각종 암호화폐 범죄의 경우에도 대부분 자금세탁이 수반되게 된다. 특히 암호화폐를 이용한 불법거래나 랜섬웨어 등은 암호화폐의 자금세탁 기능에 의지하여 범죄수익 현실화를 하는 범죄이므로 자금세탁과 분리해서 생각하기 어려운 범죄 유형이라고 할 수 있다. 과거 비트인스턴트(BitInstant)나 리버티리저브(Liberty Reserve) 등은 비교적 현재에 비하면 단순한 암호화폐의 익명성을 이용한 대규모 무허가 송금행위가 자금세탁에 해당하는 것으로 기소되어 처벌된 바 있다.

---

624) 금융감독원 보도자료, "2018년 유사수신 혐의업체 특징 및 소비자 유의사항", 2019.4.25., http://www.fss.or.kr/fss.hpdownload?file=190425_%C1%B6%B0%A3_2018%B3%E2+%C0%AF%BB%E7%BC%F6%BD%C5+%C7%F8%C0%C7%BE%F7%C3%BC+%C6%AF%C2%A1+%B9%D7+%BC%D2%BA%F1%C0%DA+%C0%AF%C0%C7%BB%E7%C7%D7.pdf&path=/nws/nbd/ (2019년 11월 4일 최종접속) 참조.

625) 법무부 보도자료, "법무부, 가상통화 관련 범죄에 대해 지속적 엄정 대응 방침", 2019.7.19., http://www.korea.kr/common/download.do?fileId=187437238&tblKey=GMN (2019년 11월 4일 최종접속) 참조.

(1) 믹싱

단순히 허위거래를 반복하는 수준을 넘어서 기술적 방법을 이용하여 다종의 암호화폐간 다수의 거래를 서로 다른 시간차를 두고 반복적으로 섞는 방법으로 암호화폐의 거래내역을 추적하지 못하게 하는 것을 믹싱(Mixing)이라고 한다.[626] 각국의 수사기관 및 일부 암호화폐 관련 기업들은 믹싱기법을 연구하여 추적을 위한 솔루션을 만들기도 한다. 그러나 믹싱기법의 다양한 변화가능성과 무작위성으로 인하여 추적이 어려운 것이 사실이다.

믹싱 서비스를 제공하는 자를 믹서(Mixer)[627]라고 하는데, 믹서는 믹싱서비스를 제공해주고 수수료를 받아 이익을 취한다. 암호화폐가 생긴 이후 지금까지 다양한 믹서들이 다크웹에서 영업하였다. 그러나 상술한 FATF 권고 또는 유럽연합 자금세탁 방지지침 제5차 개정 등에서 볼 수 있듯이, 각국의 자금세탁 방지 규정이 엄격해지면서 다수의 믹서가 단속되어 폐쇄되고 있으나, 다른 한편으로는 범죄적 수요가 상존하므로 수수료 수익을 목적으로 하는 새로운 믹서들이 계속 생겨나고 있다. 2019.5.22. 유로폴은 네델란드 금융범죄수사국을 비롯한 유럽 여러 국가의 수사공조 끝에 베스트믹서(Bestmixer.io)를 적발하여 폐쇄했다고 발표했다. 유로폴에 따르면 베스트믹서는 3대 믹싱 서비스 중 하나로 지난해 5월 생긴 이후로 1년 만에 최소 2억 달러의 매출을 거두었다고 한다. 네델란드 세무조사국은 베스트믹서의 서버로부터 거래내역 등을 확보하여 주변국가와 공유하고 자금세탁 내역을 확인할 계획이라고 한다.[628]

(2) 환치기

탈중앙성으로부터 나오는 초국가성으로 인하여 암호화폐는 각종 외환거래 관련 규제를 우회하는 수단이 된다. 적법한 환전절차 없이 타국으로 금전을 보내는 행위를 '환치기'[629]라고 한다. 일반적으로 환치기는 중간에 이른바 양 국가에 모두 일당이

626) 믹싱에 관하여 상세한 내용은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 67-69면 참조.
627) 텀블러(tumbler)라고 불리기도 한다.
628) "유로폴, 비트코인 돈세탁 사이트 '베스트믹서' 폐쇄", 코인데스크 2019년 5월 23일자, https://www.coindeskkorea.com/47365/ (2019년 11월 8일 최종접속); "유로폴, '비트코인 믹서' 첫 차단…자금세탁방지 속도 붙이나", 블록인프레스 2019년 5월 23일자, https://blockinpress.com/archives/17470 (2019년 11월 8일 최종접속) 참조.
629) 외환을 바꿔친다는 의미라고 한다. 이와 관련해서는 김종호, "비공식 자금이체 방식인 이른바 환치기 거래의 정산방법 분석과 그 거래규모의 측정을 통한 정책적 함의의 탐색", 한양법학 제34호, 한양법학회, 2011, 179-211면 참조.

있는 환치기상이 개입하여 A국에서 A국 통화로 대금을 지급받으면 B국에 있는 일당이 보유하고 있는 B국 통화를 지정된 사람에게 지급하는 방식으로 이루어진다. 비공식적으로 환전함으로써 외환거래 관련 규제를 회피하는 것이다. 그런데 A국에서 B국으로 암호화폐를 송금하면 훨씬 빠르고 안전하게 국가 간 자금을 송금할 수 있다. 특정국가에서 암호화폐를 구입하여 다른 국가로 보내기만 하면 되는 것이다. 이 경우에도 중간에 환치기상이 개입하는 경우가 대부분이지만, 암호화폐의 특성을 고려하면 돈을 받을 사람과 적절히 협의만 되면 보내는 사람이 손쉽게 직접 외국으로 돈을 보내는 것도 어렵지 않다. 그러나 본래 외국환 업무는 원칙적으로 금융회사에게만 허용되며 요건을 갖추어 등록하지 않고 외국환거래업무를 한 자는 외국환거래법 제27조의2 제1항에 의하여 3년 이하의 징역으로 또는 3억원 이하의 벌금으로 처벌된다.

금융감독위원회 보도자료에 따르면 단기간 수십억 원에 해당하는 암호화폐가 특정 계좌로 보내진 뒤 바로 현금으로 인출되는 사례가 발생하고 있는데, 바로 수출대금 과소신고 후 가상통화로 차액을 지불하는 방법으로 외국환 거래비용을 절감하고 관세와 세금을 적게 내는 경우로 의심된다고 한다.[630]

(3) 암호화폐 대리구매

최근에는 보이스피싱 등으로 송금된 범죄수익의 자금세탁을 위하여 사용되던 대포통장 등에 대한 규제가 강화되면서, 이른바 암호화폐 대리구매를 통한 자금세탁이 발생하고 있다. 인터넷을 통해 암호화폐를 대리구매해주면 약 3%가량을 수수료를 지급한다는 광고를 올리고, 인증이 완료된 거래소 계정을 갖고 있는 사람 중에서 일종의 '아르바이트'를 할 사람을 모집한 후, 보이스피싱 등의 피해자에게 대리구매자의 통장으로 돈을 송금하게 한 다음, 사정을 모르는 대리구매자에게 입금된 돈이 유학자금 송금 등의 목적이라고 속인 후 입금된 금액 중 수수료 부분을 자신이 갖고 나머지로 암호화폐를 구입하여 특정인에게 보내도록 하는 방식으로 보이스피싱 등으로 얻은 범죄수익을 세탁하는 것이다.[631]

---

630) 금융위원회 보도자료, "가상통화 투기근절을 위한 특별대책('17.12.28) 중 금융부문 대책 시행", 2018.1.23., http://www.fsc.go.kr/downManager?bbsid=BBS0030&no=123186 (2019년 11월 4일 최종접속) 참조.

631) 이 사례는 한서희, "가상자산 관련 범죄에 대한 연구 – 실제 사례를 중심으로", 한국형사정책연구원/블록체인법학회 공동학술대회 발표자료집, 2019.10.7.의 발표문에서 언급된 사례의 내용을 재구성한 것이다.

(4) 가상통화 관련 자금세탁방지 가이드라인

FATF의 권고 취지에 맞게 거래소(VASP)에게도 금융기관과 같은 수준의 자금세탁 방지의무를 부과하여야 한다. 금융기관에 적용되는 자금세탁 방지 관련 규제는 다음과 같다. 우선 「특정금융거래정보의 보고 및 이용 등에 관한 법률」 제4조는 금융회사에게 불법재산 등으로 의심되는 거래에 대한 보고의무를, 제4조의2는 고액거래에 대한 보고의무를 규정하고 있다. 이 외에도 금융기관은 고객의 신원을 확인해야 하며(제5조의2) 필요시 법적 책임을 질 우려 없이 수사기관에 정보를 제공한다(제7조). 이 외에도 「범죄수익은닉의 규제 및 처벌 등에 관한 법률」은 금융회사에 범죄수익에 대한 신고의무(제5조)를 부여한다.

금융위원회는 암호화폐를 이용한 자금세탁을 방지하기 위하여 2018.1.30. 「가상통화 관련 자금세탁방지 가이드라인」을 제정·시행하였다.[632] 가이드라인은 고객확인의무와 의심거래 보고의무를 주요 내용으로 한다.

우선 가이드라인은 "가상통화"를 "거래상대방으로 하여금 교환의 매개 또는 가치의 저장 수단으로 인식되도록 하는 것으로서 전자적 방법으로 이전 가능한 증표 또는 그 증표에 관한 정보"라고 정의하고, 이를 "보관·관리·교환·매매·알선 또는 중개하는 것을 업으로 하는 자"를 "가상통화 취급업소"로 정의한다.[633] 금융회사는 금융거래 상대방이 "가상통화 취급업소"인지를 식별하기 위하여 특별한 주의를 기울여야 하며, 「금융실명거래 및 비밀보장에 관한 법률」 제4조 제1항 제5호에 의거하여 금융회사 간 취급업소 정보 등을 전산적 방법으로 공유한다. 금융회사가 상대방을 취급업소로 식별한 경우, 「특정금융거래정보의 보고 및 이용 등에 관한 법률」 제5조의2 제1항 제2호의 규정 및 금융정보분석원장의 고시에 따라 위험성에 비례하여 합리적으로 강화된 범위 내에서 강화된 고객확인 의무를 진다. 추가적인 고객확인은 현지실사 방법으로 실시해야 하며 확인해야 하는 정보의 내용은 다음과 같다.

---

632) 이하의 내용 중 가이드라인을 구체적으로 설명하기 위하여 필요한 내용은 「가상통화 관련 자금세탁방지 가이드라인」 및 금융위원회, 앞의 보도자료("가상통화 투기근절을 위한 특별대책(17.12.28) 중 금융부문 대책 시행")에서 인용하였음.

633) 금융위원회 보도자료, "「가상통화 관련 자금세탁방지 가이드라인」 개정", 2018.6.27., https://www.fsc.go.kr/downManager?bbsid=BBS0030&no=127331 (2019년 11월 4일 최종접속) 참조.

1. 취급업소가 제공하는 서비스의 내용
2. 취급업소의 실명확인 입출금계정서비스 이용여부 및 이용계획
3. 취급업소가 이용자의 생년월일, 주소, 연락처 등을 포함한 신원사항 확인 여부
4. 취급업소가 취급업소의 고유재산과 이용자의 예탁·거래금을 분리하여 관리하고 있는지 여부
5. 취급업소가 이용자별 거래내역을 구분하여 관리하고 있는지 여부
6. 취급업소가 이용자를 상대로 가상통화는 법정 화폐가 아니라는 사실과 가상통화의 내용, 매매 및 그 밖의 거래에 따르는 위험 등을 이용자가 이해할 수 있도록 설명하고 그 의사를 확인하는지 여부
7. 취급업소가 가상통화거래 관련 집금을 위해 임직원 계좌 등 별도의 계좌를 운용하는지 여부
8. 대한민국 정부에서 발표하는 가상통화와 관련한 정책의 준수 여부
9. 기타 금융회사등이 자금세탁등의 방지를 위해 필요하다고 인정하는 사항

또한 취급업소가 실명확인 입출금계정 이외의 계정으로 가상통화관련 금융거래를 하는 경우 금융회사 등은 자금세탁 등을 방지하기 위하여 다음의 사항을 이행하여야 한다.

1. 취급업소의 임직원 계좌가 가상통화관련 금융거래에 활용되는 것으로 의심되는 경우 임직원 명의 계좌에 대한 강화된 고객확인 및 금융거래모니터링 강화
2. 금융회사등의 고객 중 민법상 미성년자, 외국인 등의 가상통화관련 금융거래를 식별
3. 금융회사등은 취급업소 이용자의 금융거래내역 관리를 대행하거나 실시간 관리가 가능하도록 하는 등 취급업소의 가상통화관련 금융거래내역 관리에 편의성을 제공하는 용역 행위를 자제
4. 기타 금융회사등에서 자금세탁등의 방지를 위해 필요하다고 인정되는 사항

금융기관은 취급업소를 자금세탁 등의 위험이 높은 고객으로 고려해야 하며 6개월 이하의 주기마다 지속적으로 확인해야 한다. 실명확인 입출금계정을 이용하지 않는 경우에는 3개월 이하의 주기마다 확인해야 하며, 정보제공을 거부하거나 허위의 자료를 제출하는 경우 취급업소와의 거래를 거절해야 한다.

또한 금융회사는 다음 유형에 해당하는 경우 자금세탁으로 의심되는 근거가 있는지 여부를 적극적으로 판단하여 FIU에 보고하여야 한다.

〈의심거래보고 대상 주요 유형〉

㉠ 가상통화 취급업소 이용자의 금융거래가 의심스러운 경우

- 금융회사의 거래상대방 중 법인 또는 단체가 취급업소와 금융거래를 하는 경우

- 금융회사의 거래상대방(취급업소의 이용자)이 취급업소와 거액(1일 1,000만원, 7일 2,000만원)의 금융거래를 하거나 단시간 내에 빈번한(1일 5회, 7일 7회) 금융 거래를 하는 경우

  * 금융회사를 통한 입·출금 등 금융거래 기준이며, 취급업소를 통한 가상통화 매매가 아님 (거래소에 이미 입금한 돈으로 가상통화를 구입하는 것은 보고 대상이 아님)

  ** 금융회사가 금액을 산정할 때는, 동일인 명의로 입금한 금액을 합산하거나, 출금한 금액을 합산함 (예:500만원 입금 후 400만원 출금시 500만원으로 산정)

㉡ 가상통화 취급업소의 거래가 의심스러운 경우

- 취급업소가 취급업소의 임직원으로 추정되는 자와 지속적으로 송금 등 금융거래를 하는 경우

금융위원회는 가이드라인 제정 후 2018.4. 실시한 은행권 현장 점검 결과를 반영하고 미비점을 개선하기 위하여 2018.7.10. 가이드라인을 강화하는 개정안을 만들어 시행하였다. 주요 개정의 주요 내용은 다음과 같다.[634]

① 취급업소의 '비집금계좌'에 대한 금융회사의 모니터링 강화
② 해외 가상통화 취급업소의 목록도 금융회사 간에 공유
③ 금융회사가 취급업소에 대한 거래를 거절할 경우, 거절시점을 명시하고 거절 사유를 추가

이후 금융규제를 혁신하기 위하여 금융위원회는 2019.5.3. 「금융규제혁신 통합 추진회의」를 개최하였다. 이 회의에서 금융위원회는 기존 금융규제의 합리성과 투명성, 책임성을 강화하기 위하여 불필요한 내용은 폐지하고 필요한 내용은 법규화하기로 결정하였다. 이 회의에서 「가상통화 관련 자금세탁방지 가이드라인」은 법규화 대상으로 정해졌으며 1년의 기한을 두고 법령 제정을 추진하기로 하였다. 그러나 「특정금융거래정보의 보고 및 이용 등에 관한 법률」 등의 개정이 지연되면서 2019.6. 금융위원회는 가이드라인의 유효기간을 2020.7.9.까지로 1년 연장하였다.

그러나 이 가이드라인은 금융기관을 통하여 간접적으로 거래소를 규제하는 것을 내용으로 하고 있어 그 실효성에 대하여 지속적으로 의문이 제기되고 있다. 아울러 거래소를 통하지 않는 개인간 직접거래의 경우, 또는 영세한 불법거래소나 불법 믹서 등을 이용하는 경우에 대해서는 현실적으로 이를 사전에 확인하여 대처할 수 있는 방법이 없는 것이 사실이다.

634) 개정된 가이드라인에 대하여 상세한 내용은 금융위원회, 앞의 보도자료("「가상통화 관련 자금세탁방지 가이드라인」 개정") 참조.

8) 시세조종

암호화폐도 거래소에 '상장'되어 거래되므로 현금으로 환전되는 시세가 수시로 변하며, 오히려 암호화폐를 이용한 대금지급보다 시세의 변화를 이용한 차액을 거두기 위한 투자목적 매매가 훨씬 더 빈번하게 이루어지고 있다. 마치 상장된 주식의 매매와 같은 상황임에도 불구하고 암호화폐 시세조종이나 내부정보 이용행위에 대한 제재 방법이 전혀 없는 형편이다. 실제 암호화폐 시세조종 또는 특정 거래소 내부의 불법적인 행위들이 다수 발생하고 있을 것으로 추정된다. 그러나 처벌규정이 없으므로 일부 사기죄 등에 해당하는 경우를 제외하고는 실제 수사된 바도 찾기 어렵다.

물론 만약 암호화폐의 작동원리에 비추어 「자본시장과 금융투자업에 관한 법률」상의 지분증권, 채무증권, 투자계약증권 등에 해당될 가능성이 전혀 없는 것은 아니라고 할 수 있을지도 모르나, 법리적으로 「자본시장과 금융투자업에 관한 법률」을 직접 적용하는 것은 불가능할 것으로 생각된다. 입법적 대응이 시급하다.

9) 기타

공개되면 치명적인 인격적 훼손을 초래하는 개인정보 등을 이용하여 암호화폐를 갈취하는 사례가 발생하고 있다. 2015년에는 애슐리 매디슨(Ashley Madison)이라는 커플매칭 사이트가 해킹당해 정보가 유출되었는데, 이를 이용하여 결혼한 남성에게 암호화폐를 보내지 않으면 정보를 공개하겠다고 협박하기도 했다.[635] 우리나라에서도 2017년에는 특정한 개인정보를 포털사이트에 게시한 후 암호화폐를 지불해야 삭제해주겠다고 협박한 범죄자가 공갈미수 및 정보통신망법 위반죄로 처벌되기도 하였다.[636] 우크라이나에서는 거래소 임원이 납치된 후 몸값으로 거액의 암호화폐를 지불하고 풀려난 경우도 있다고 한다.[637] 이 외에도 테러자금을 암호화폐로 모금하기도 하는 등 암호화폐는 다양한 범죄의 수단으로 활용되고 있다.

---

635) 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 73면 참조.

636) "[토요이슈]거래 과정 철저히 감춰져… "달러 대신 비트코인 내놔라"", 동아일보 2017년 6월 17일자, http://news.donga.com/3/all/20170617/84906550/1 (2019년 11월 8일 최종접속) 참조.

637) 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 46면 참조.

제3절 | 블록체인 및 암호화폐 관련 법적 현황 및 그 한계

1. 법률 적용과 법규 정비에 관한 현황

현재 블록체인 기술을 이용한 암호화폐를 직접적으로 규율하는 법은 없다. 이에 암호화폐의 발행(ICO)과 거래에 대해 다른 유사법률을 적용하려는 시도가 있다.

가. ICO의 개념과 현행법상 법적 성격

ICO(Initial Coin Offerings)는 새로운 기술 또는 서비스를 개발하기 위해서 블록체인(blockchain)을 기반으로 한 가상화폐(virtual currency) 또는 암호화폐(crypto currency)를 발행함으로써 온라인에서 자금을 모으는 방법을 말한다.[638] 즉 실물이 아닌 가상화폐 형식의 "코인 또는 토큰(coin or token)"을 발행하는 것인데, 주식을 발행하고 상장하여 자금을 모집하는 것과 유사하기 때문에 주식을 상장하는 IPO(Initial Public Offering)에 비유하여 ICO라고 부르고 있다.[639] 이러한 ICO는 투자자들에게 투자의 대가로 통상적인 증권을 제공하는 것이 아니라 디지털 형태의 토큰을 제공한다는 점에서 기존의 법제도에 의한 IPO와 구별되는 것이고, 이 때 제공되는 토큰은 그 형태와 성격이 다양[640]하여 일률적으로 법적 성격을 규정하기가 쉽지 않다.

현재 ICO에 대해서는 이를 직접적으로 규율하는 국내 법제는 존재하지 않는다. 그러나 이미 큰 규모의 시장이 성립되어 있는 상황[641]이므로 법적인 관리나 감독의

---

638) 김병연, "ICO의 법적 개념 및 각국의 규제동향에 관한 연구", 일감법학 제43호, 건국대학교 법학연구소, 2019, 32면.

639) 김준영/김계정/문준호, "ICO(Initial Coin Offering)에 대한 주요 이슈 및 시사점", 증권법연구 제19권 제2호, 한국증권법학회, 2018, 203면. 또 다른 용어로 '토큰(Token)판매', '크라우드(Crowd) 세일' 등으로 불린다.

640) ICO에서 제공되는 토큰은 크게 '지급수단형 토큰(payment tokens)', '서비스이용형 토큰(utility tokens)', '자산형 토큰(asset tokens)' 등으로 분류할 수 있다. 이에 대한 상세한 내용은 김병연, 앞의 글, 33-35면 참조.

641) 우리나라의 경우 ICO를 법적으로는 '금지'하고 있는 상황이기 때문에 정확한 시장규모에 대한 통계자료를 찾아보기 어렵다. 한편 전 세계적으로는 2018년 한 해만 약 12조원에 달한다는 보고가 있으며, 2019년에도 9월말까지 10억 8천 3백만 달러(약 2조원)의 ICO가 성공적으로 행해졌다고 한다. 자세한 내용은 ICO bench, "ICO Market Monthly Analysis September 2019", https://icobench.com/reports/ICObench_ICO_Market_Analysis_September_2019.pdf (2019

필요성은 현저하다고 할 수 있고, 이에 따라 현행법 하에서는 일단 유사수신행위규제법 상의 유사수신행위에 해당될 가능성과 자본시장법상 집합투자업 또는 크라우드펀딩 관련규제의 적용가능성 등이 논의되고 있다.[642]

1) 자본시장과 금융투자업에 관한 법률의 적용 가능성

자본시장법 제444조 제12호에 의하면 "제119조(증권모집의 신고의무[643])를 위반하여 증권을 모집 또는 매출한 자"는 5년 이하의 징역 또는 2억 원 이하의 벌금형으로 처벌된다. ICO를 투자자금을 모집하기 위하여 증권을 발행하는 행위의 일종으로 간주한다면, 발행되고 투자자에게 지급된 암호화폐는 자본시장법상의 투자계약증권(제4조 제6항)[644]에 해당[645]할 가능성이 있다. 그러나 암호화폐의 재산적 가치가 투자계약증권의 성립요소인 "공동사업의 결과에 따른 손익을 귀속 받는 계약상의 권리"에 해당할 수 있는지에 대해서는 의문이 있다. 기업이 사업의 시작과 성장을 위하여 필요한 자금을 조달받는 통로와 그에 대한 대가라는 점에서는 IPO와 유사한 면이 있고 암호화폐는 IPO에서의 증권과 구조적 지위 상 유사한 면이 있지만, ICO를 통하여 발행되는 '코인'에 대하여 주식과 같은 지분의 개념보다는 '가상화폐'라는 측면이 주목받고 있고, 투자자들은 암호화폐의 가치가 상승되는 것에 관심이 있을 뿐 정작 '코인'을 발행한 기업의 성장에는 무관심하다는 점에서 사모투자에 불과하다는 지적[646]이 있다. 물론 이러한 특성은 통상적인 증권의 경우에도 일반인 투자자에 의한 경우에는

년 11월 8일 최종접속) 참조. 한편, 대통령직속 4차산업혁명위원회는 ICO에 대한 제도적 허용을 건의하면서 전 세계 일간 코인거래량은 약 80조원으로 추산하고 있다. 자세한 내용은 ""ICO·코인 거래면허제 검토해야", 4차위 '파격제안'에 文 응답할까", NEWS1 2019년 10월 25일자, https://news.v.daum.net/v/20191025161023785 (2019년 11월 8일 최종접속) 참조.

642) 유주선/강현구, 앞의 글, 238면.

643) 자본시장법 제119조 ① 증권의 모집 또는 매출(대통령령으로 정하는 방법에 따라 산정한 모집가액 또는 매출가액 각각의 총액이 대통령령으로 정하는 금액 이상인 경우에 한한다)은 발행인이 그 모집 또는 매출에 관한 신고서를 금융위원회에 제출하여 수리되지 아니하면 이를 할 수 없다.

644) 자본시장법 제4조 ⑥ 이 법에서 "투자계약증권"이란 특정 투자자가 그 투자자와 타인(다른 투자자를 포함한다. 이하 이 항에서 같다) 간의 공동사업에 금전 등을 투자하고 주로 타인이 수행한 공동사업의 결과에 따른 손익을 귀속받는 계약상의 권리가 표시된 것을 말한다.

645) 유주선/강현구, 앞의 글, 239면.

646) "[홍기훈의 블록체인과 핀테크] ICO? IPO? 크라우드펀드(Crowdfund)? 정확한 이해 필요하다", IT Chosun 2017년 9월 19일자, http://it.chosun.com/site/data/html_dir/2017/09/19/2017091985017.html (2019년 11월 8일 최종접속).

마찬가지의 측면이 있지만[647], 비트코인과 같은 전형적인 지급수단형 토큰의 형태이고 발행 이후 거래소에서 암호화폐로서 거래되는 대상으로서의 실질을 가지는 경우 이를 '발행동기'의 측면에만 집중하여 현행법상의 '증권'의 일종으로 파악하는 것은 다소 무리가 있어 보인다. 특히 발행자와 투자자의 법적인 관계를 정리하면 암호화폐 투자자의 투자는 암호화폐 발행자에 대한 호응이고 해당 암호화폐의 취득을 선호하는 것일 뿐 자체로 회사에 어떠한 지분이나 권리를 취득하지 않는다(즉 가상화폐 발행자와 투자자의 관계는 가상화폐의 발행으로 종료한다).[648] 그러므로 발행 당시에는 증권과 유사한 기능을 수행하지만 발행되어 시장에 나온 상태에서는 화폐와 같은 교환수단의 성격을 강하게 가지며, 이 글에서 주된 논의의 대상이 되는 형사법 관련 현상들도 '토큰'의 '수익배당증권'으로서의 성격보다는 암호화되고 익명성이 보장되는 교환수단이라는 성격에 따라 발생하는 것임을 고려하면, 현재의 상태에서 자본시장법을 직접 적용하여 ICO를 법적으로 관리·규제하는 것은 타당성을 인정받기 어려워 보인다.

2) 유사수신행위의 규제에 관한 법률 적용 가능성

ICO가 스타트업 기업 등의 법제도 외적인 자금조달의 통로가 되고 있다는 점에서 '비인가 자금조달'의 성격에 주목하여 이를 법이 금지하고 있는 '유사수신'으로 간주할 가능성도 있다. 「유사수신행위의 규제에 관한 법률」(이하, '유사수신행위법'이라 한다)에 의하면 "인가 등 없이 자금을 조달하는 것을 업으로 하는 행위"(제2조)[649]를 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금(제6조)으로 처벌하도록 하고 있는데, 유사수신행위법의 세부 규정에 의하면 이러한 자금조달행위가 유사수신에 해당하기 위해서는 "① 장래에 출자금의 전액 또는 이를 초과하는 금액을 지급할 것을 약정하고 출자금을 받거나, ② 장래에 원금의 전액 또는 이를 초과하는 금액을 지급할 것을 약정하고 예금·적금·부금·예탁금 등의 명목으로 금전을 받거나, ③ 장래에 발행가액 또는 매출가액 이상으로 재매입 할 것을 약정하고 사채를 발행하거나 매출하는 행위

647) 그래서 이를 ICO만의 특성으로 보기는 어렵다는 의견으로 김병연, 앞의 글, 38면 각주 39.
648) 정해상, "가상화폐발행(ICO)의 특성과 규제의 쟁점", 법학논총 제43권 제1호, 단국대학교 법학연구소, 2019, 11면.
649) 유사수신행위법 제2조(정의) 이 법에서 "유사수신행위"란 다른 법령에 따른 인가·허가를 받지 아니하거나 등록·신고 등을 하지 아니하고 불특정 다수인으로부터 자금을 조달하는 것을 업(業)으로 하는 행위로서 다음 각 호의 어느 하나에 해당하는 행위를 말한다.

를 하거나, ④ 장래의 경제적 손실을 금전이나 유가증권으로 보전하여 줄 것을 약정하고 회비 등의 명목으로 금전을 받는 행위"를 하여야 한다. 그런데 현재의 ICO가 이러한 유사수신행위법에 의한 규제의 대상이 될 가능성은 낮아 보인다. 우선 유사수신행위법은 규제의 대상을 자금조달 그 자체에 두는 것이 아니라 이를 '업'으로 하는 행위, 즉 자금조달을 영업적 행위로 하는 경우를 그 대상으로 하는 것이어서 기술개발자 혹은 스타트업 사업주가 1회에 한하여 직접 ICO를 하는 경우에는 유사수신행위법에 의한 규제의 대상이 되지 않음이 명백하다. 또한 자금조달의 방식에 있어서도 장래에 대한 지급, 재매입, 손실보전 등의 약정이 필요한데, ICO에서 투자자의 출자금을 보장하지 않는 한 발행자가 사업자금을 받는 것은 유사수신행위에 해당하지 않는다고 할 수 있다.[650]

나. ICO와 암호화폐 거래에 대한 법정책적 동향

1) 정부정책 동향의 개관

우리나라에서 블록체인 기술을 이용한 ICO와 암호화폐 거래에 대한 법정책은 초기 금융위원회를 주무부처로 하여 관련 산업의 육성차원으로 접근하였다가 비트코인으로 대표되는 암호화폐에 대한 '투기'의 문제가 부각되면서 규제에 중점을 두는 정책으로 급선회하였다고 할 수 있다.[651] 2017년 9월 금융위원회는 보도자료[652]를 내고 암호화폐 거래의 과열에 따른 불법성, 사기관련성, 재산손실의 우려 등을 중점적으로 강조하면서 규제 중심의 법제 정비에 나서겠다는 것을 표명하였다. 이어 주무부처는 법무부로 변경이 되었고 법무부는 2018년 1월 암호화폐 거래소에 대한 폐쇄를 추진하겠다고 발표하였다.[653] 이후 관련부처 간 여러가지 이견이 있고 논의[654]가 계속되고

650) 같은 의견으로 정해상, 앞의 글, 17면. 그러므로 ICO를 빙자한 사기와 ICO 자체의 유사수신행위로서의 성격은 구별해야 할 문제이다.

651) 2017년 12월까지 정부의 관련 법정책 동향에 대한 상세한 내용은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 102-114면 참조.

652) 금융위원회 보도자료, "「가상통화 관계기관 합동 TF」 개최 - 가상통화 현황 및 대응방향", 2017.9.4., https://www.fsc.go.kr/downManager?bbsid=BBS0030&no=119483 (2019년 11월 4일 최종접속) 참조.

653) "법무부 "가상화폐 거래소 폐쇄 추진". 개인투자자 반발", 전자신문 2018년 1월 11일자, https://news.v.daum.net/v/20180111151304156 (2019년 11월 8일 최종접속).

654) 일부 부처에서 가상통화 거래소 운영을 위한 고객 자산의 별도 예치, 설명의무 이행, 이용자

는 있으나 결과적으로 현재까지 정부는 ICO 관련 아무런 정보제공이나 가이드 없이 실효성 없는 금지방침으로 일관하고 있다고 할 수 있다.

2) ICO와 암호화폐 거래에 대한 법정책적 요구 동향

반면 ICO와 암호화폐 거래소에 대한 법정책의 마련과 관련하여 학계나 민간영역에서의 제안이나 요구는 꾸준히 이어지고 있다. 2017년 12월 블록체인협회는 12개의 거래소에 대한 자율규제안에 기한 심사, 자기자본 20억원 이상인 경우에만 거래소 운영가능, 투자정보 제공, 상장절차 건전성, 민원관리, 콜드월렛, 이용자 자산보호체계, 시세조종금지, 내부자거래금지, 자금세탁방지 등을 내용으로 하는 자율규제안을 발표[655]하였다. 학계[656]에서도 암호자산에 대한 투기성 거래 수요와 암호자산 거래소의 난립 등 거래소의 부실 및 오용으로 인한 이용자의 피해 및 시장의 건전성이 훼손될 위험이 커 최소한의 설립 및 운영 요건에 대한 입법적 조치가 있어야 한다는 요구가 계속되었다.

한편 2019년 10월, 대통령직속 4차산업혁명위원회는 대정부권고안을 발표하면서 암호화폐 발행과 거래를 법적으로 정의하고 제도화할 것을 권고하였다.[657] 즉 "암호자산의 정의와 제도권 편입 등을 포함하여 블록체인과 관련된 정책방향을 명확히 해야 한다. 우리 정부는 국제사회 조류에 뒤쳐지는 일이 없도록 암호자산에 대한 법적 지위를 조속히 마련하고 이에 대한 조세, 회계 처리 방안도 강구해야 할 것이다. 또한 우리나라 금융업계가 글로벌 금융업계에 현저히 뒤처지는 일이 없도록 금융기관의 암호자산 취급을 허용하고 금융권에 준하는 안전한 인프라와 자금세탁방지 규제를 도입해 국제 논의를 주도해야 한다."[658] 이것은 자본시장법 등 암호화폐 관련법 마련, 암호화폐 거래소에 대한 거래업 라이센스 발급 또는 가이드라인 도입, 암호화폐 파생

실명확인, 암호키 분산 보관, 가상통화 매도매수 호가·주문량 공개 등 의무화 검토 등 거래소의 준수사항에 대한 입법논의는 있었으나 구체적인 입법은 진행되지 않고 있다.

655) ""암호화폐 분쟁조정委 만든다"...블록체인협회, 자율규제안 마련", 이데일리 2017년 12월 15일자, https://news.v.daum.net/v/20171215115748997 (2019년 11월 8일 최종접속).

656) 암호화폐에 대한 규제정책이 본격화된 2018년 이후 지금까지 만 2년이 안 되는 기간 동안 ICO와 암호화폐 거래에 대해 적절한 법적 대책이 필요하다는 학계의 의견은 한국교육학술정보원이 제공하는 논문검색 사이트(RISS)에서만 30여 건이 넘게 검색된다.

657) 대통령직속 4차산업혁명위원회 보도자료, "4차위, 4차 산업혁명 대정부 권고안 발표", 2019.10.25., https://www.4th-ir.go.kr/article/download/602 (2019년 11월 8일 최종접속) 참조.

658) 대통령직속 4차산업혁명위원회, 4차 산업혁명 대정부 권고안, 2019.10, 72면.

상품 개발 허용 등의 의미를 담고 있는 것으로, 비록 당해 위원회가 법적 권한을 가진 기관은 아니지만 대통령 직속기구로 정부의 정책에 실질적인 영향력을 미칠 수 있음을 감안하면 이와 같은 정책권고는 향후 입법적 논의와 현실화에 긍정적 기대를 가질 수 있도록 하는 요인이라고 평가할 수 있을 것이다.[659]

다. 국회의 관련 입법안 현황

암호화폐에 대한 법적 근거의 마련과 정비가 필요하다는 사회정책적 요구와 함께 국회에서의 입법적 방안마련을 위한 노력도 꾸준히 이어지고 있는 것으로 보인다. 2018년 이후[660] 제출된 관련 법안은 총 6개[661]로, 암호화폐의 발행과 거래에 관한 별도의 특별법을 만들자는 취지가 2건이고 이미 존재하는 법률에 내용을 추가하는 방식으로 규율하고자 하는 것이 4건이다. 자금세탁에 관한 규제에 집중하는 제윤경 의원안 및 김병욱 의원안이나 소비자보호에 집중하는 채이배 의원안은 ICO와 암호화폐 거래의 직접적 부작용을 규율대상으로 하는 법안이고, 나머지 3건은 형식은 다소 차이가 있지만 공히 암호화폐와 암호화폐거래업을 정의하고 이에 대한 인가나 허가 등의 요건을 규정하며, 거래의 안전성과 소비자보호를 위해 금융당국의 규제와 관리가 가능하도록 하고 시세조종, 자금세탁 등 불건전거래행위에 대한 금지규정을 두는 등, 종합적인 암호화폐 발행 및 거래제도에 대한 설정과 관리, 규제를 골자로 하고 있다.

1) 정태옥 의원 대표발의 '가상화폐업에 관한 특별법안'

정태옥 의원이 대표발의한 '가상화폐업에 관한 특별법안'은 2018년 2월 2일 발의되었다.[662] 이 법률안은 "가상화폐의 정의와 관련업에 대한 인가규정, 실명확인, 안전한

---

659) 그럼에도 현재까지 나온 정부의 입장은 여전히 부정적이다. "금융위 '가상통화·ICO 관련 입법 추진하지 않을 것'", 연합인포맥스 2019년 10월 4일자, http://news.einfomax.co.kr/news/articleView.html?idxno=4050654 (2019년 11월 8일 최종접속) 참조.

660) 2017년 말까지의 관련 법률안에 대한 소개와 설명은 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 115-120면 참조.

661) 2019년 5월의 이언주 의원안까지 갯수로는 총 7개이나, 이언주 의원안은 2018년 9월의 하태경 의원안과 내용상 거의 동일하므로 별도의 법안으로 계산하지 않았다.

662) 의안번호 11752. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_F1R8A0R2N0W2N1H8D1W1Q3N8I9T6I4 (2019년 11월 8일 최종접속) 참조.

거래를 위한 보안조치, 이용자 피해 배상의무, 자율규제 등을 규정하는 특별법을 제정하여 가상화폐에 대한 영업의 자유를 보장하는 한편 투자자를 보호하여 가상화폐업을 건전하게 육성하고자 한다"는 취지로 제안되었다.

법률안은 제2조에서 '가상화폐'와 '가상화폐업' 등에 대해 다음과 같이 정의하는 규정을 두었다.

> 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
> 1. "가상화폐"란 불특정 다수인 간에 재화 또는 용역의 제공과 그 대가의 지급을 위하여 사용할 수 있거나 불특정 다수인이 매도·매수할 수 있는 재산적 가치(전자기기 혹은 그 외의 것에 전자적 방법에 의해 기록되어 있는 것에 한하며, 내국통화, 외국통화와 가상화폐 이외의 「전자금융거래법」 제2조에 따른 전자지급수단 등을 제외한다)로서 전자적 방법으로 이전 가능한 정보를 말한다.
> 2. "가상화폐업"이란 다음 각 목의 어느 하나에 해당하는 업을 말한다.
> 가. "가상화폐거래업"은 가상화폐 매매를 위한 시장을 개설하여 운영하는 업을 말한다.
> 나. "가상화폐계좌관리업"은 타인을 위하여 가상화폐를 보관하는 계좌를 관리하는 업을 말한다.
> 다. "가상화폐보조업"은 가상화폐업을 보조하거나 그 일부를 대행하는 업무를 행하거나 그 밖에 대통령령으로 정하는 가상화폐업과 관련된 업을 말한다.

법률안은 가상화폐업에 대한 금융위원회의 '인가'제를 규정하면서 인가요건으로 다음과 같은 내용을 규정하고 있다.

> 제3조(가상화폐거래업 등의 인가) ② 가상화폐거래업의 인가를 받으려는 자는 다음 각 호의 요건을 모두 갖추어야 한다.
> 1. 자본금이 30억원 이상으로서 대통령령으로 정하는 금액 이상일 것
> 2. 이용자에 대한 보호가 가능하고 가상화폐거래업을 수행하기에 충분한 인력과 전산체계 및 그 밖의 물적 설비를 갖출 것
> 3. 사업계획이 타당하고 건전할 것
> 4. 건전한 재무상태와 사회적 신용을 갖출 것[663]

663) 동 법률안은 제3항에서 가상화폐계좌관리업의 인가요건도 동일한 내용으로 규정하고 있다.

법률안은 가상화폐거래에 대한 주요 금지사항으로 다음과 같이 불건전영업행위, 불공정거래행위, 자금세탁행위 등을 규정하고 있다.

제11조(불건전 영업행위 금지) 가상화폐거래업자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다. 다만, 이용자 보호 및 건전한 거래질서를 해할 우려가 없는 경우로서 대통령령으로 정하는 경우에는 그러하지 아니하다.

1. 이용자로부터 가상화폐의 가격에 중대한 영향을 미칠 수 있는 매수 또는 매도의 청약이나 주문을 받거나 받게 될 가능성이 큰 경우 이를 체결시키기 전에 그 가상화폐를 자기의 계산으로 매수 또는 매도하거나 제3자에게 매수 또는 매도를 권유하는 행위
2. 특정 가상화폐의 가치에 대한 주장이나 예측을 담고 있는 자료를 이용자에게 공표함에 있어서 그 조사분석자료의 내용이 사실상 확정된 때부터 공표 후 24시간이 경과하기 전까지 그 조사분석자료의 대상이 된 가상화폐를 자기의 계산으로 매매하는 행위
3. 그 밖에 이용자 보호 또는 건전한 거래질서를 해할 우려가 있는 행위로서 대통령령으로 정하는 행위

제12조(불공정거래행위 금지 등) 가상화폐를 이용한 불공정거래행위에 대해서는 「자본시장과 금융투자업에 관한 법률」 제174조부터 제178조까지, 제178조의2, 제178조의3 및 제179조의 규정을 준용한다.

제13조(자금세탁행위 등의 금지) 누구든지 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조 제3호에 따른 불법재산의 은닉, 같은 조 제4호에 따른 자금세탁행위 또는 같은 조 제5호에 따른 공중협박자금조달행위 및 강제집행의 면탈, 그 밖에 탈법행위를 목적으로 가상화폐의 매매·중개·교환·발행·관리를 하여서는 아니 된다.

법률안은 가상화폐거래의 안전성을 확보하고 이용자를 보호하기 위하여 다음과 같은 규정을 두고 있다.

제15조(안전성 확보의무) ① 가상화폐업자는 가상화폐거래 및 가상화폐계좌관리 등이 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

② 가상화폐업자는 가상화폐거래 및 가상화폐계좌관리 등의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적장치, 소요경비 등의 정보기술부문, 가상화폐거래업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.

③ 금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.

④ 가상화폐업자는 안전한 가상화폐거래 및 가상화폐계좌관리를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하여야 한다.

⑤ 가상화폐거래의 안전성 확보에 관하여 제1항부터 제4항까지에서 정한 사항 외에는 「전자금융거

래법」 제21조의4부터 제21조의6까지 및 제26조를 준용한다.

제16조(가상화폐예치금 관리) ① 가상화폐거래업자는 가상화폐예치금을 고유재산과 구분하여 대통령령으로 정하는 기관에 예치하거나 「자본시장과 금융투자업에 관한 법률」에 따른 신탁업자에게 신탁하여야 한다.

② 가상화폐거래업자는 제1항에 따라 가상화폐예치금을 예치 또는 신탁하는 경우에는 그 가상화폐예치금이 가상화폐 이용자의 재산이라는 뜻을 밝혀야 한다.

③ 누구든지 제1항에 따라 예치 또는 신탁한 가상화폐예치금을 상계·압류(가압류를 포함한다)하지 못하며, 가상화폐예치금을 예치 또는 신탁한 가상화폐거래업자는 대통령령으로 정하는 경우 외에는 예치기관 또는 신탁기관에 예치 또는 신탁한 가상화폐예치금을 양도하거나 담보로 제공하여서는 아니 된다.(중략)

제17조(가상화폐업자의 책임) ① 가상화폐업자는 다음 각 호에 해당하는 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다.

1. 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고
2. 가상화폐거래를 위한 전자적 장치 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체 등의 이용으로 발생한 사고(후략)

그 밖에 법률안은 "금융감독원은 금융위원회의 지시를 받아 가상화폐거래업자 및 가상화폐계좌관리업자에 대하여 이 법 또는 이 법에 의한 명령의 준수 여부를 감독"하도록 하고(안 제5조), "가상화폐거래업자 및 가상화폐계좌관리업자가 업무상 모든 기록을 생성하여 대통령령으로 정하는 기간 동안 보존"하게 하며(안 제6조), "가상화폐업자는 가상화폐거래 및 가상화폐계좌관리 등이 안전하게 처리될 수 있도록 정보기술부문 등에 금융위원회가 정하는 기준을 준수"하도록 하고(안 제15조), "가상화폐업자 등을 회원으로 하는 협회를 설립하고 자율규제기관으로서 영업질서 유지 및 이용자 보호를 위한 자율규제업무를 행하도록" 하는(안 제6장) 규정을 두었다.

2) 정병국 의원 대표발의 '암호통화 거래에 관한 법률안'

정병국 의원이 대표발의한 '암호통화 거래에 관한 법률안'은 2018년 2월 6일 발의되었다.[664] 이 법률안은 "암호통화의 정의규정을 마련하고, 암호통화취급업의 등록 등에 관한 규정을 신설함과 동시에 암호통화거래의 안전성 확보 및 이용자 보호를 위한 의무와 금지행위 등 블록체인 등 기술혁신은 장려하고, 기존 이용자는 보호하는

664) 의안번호 11786. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_B1E8S0G2Z0Y6S1O6G5M6R4M2E9A9E4 (2019년 11월 8일 최종접속) 참조.

방향으로 반드시 필요한 최소한의 부분만을 법으로 규율해 암호통화 시장에서의 기술혁신과 공정한 경쟁을 촉진하고 이용자를 보호하며 암호통화취급업을 건전하게 관리해 암호통화 시장의 공정성·신뢰성 및 효율성을 높이겠다"는 취지로 제안되었다.

법률안 제2조는 다음과 같은 정의규정을 두고 있다.

> 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
>
> 1. "암호통화"란 컴퓨터 기술이나 생산 노력에 의하여 창조하거나 획득할 수 있는 교환의 매개수단 또는 디지털 가치저장방식으로 사용되는 모든 종류의 디지털 단위로서, 분산된 비중앙집중식 저장소 및 관리자 방식의 컴퓨터 암호학 기술에 기반을 둔 것을 말한다. 다만, 다음 각 목의 어느 하나에 해당하는 것은 제외한다.
>
> 가. 오직 온라인 게임 플랫폼 내에서만 사용되어 그 게임 플랫폼 외에 시장이 없거나 사용할 수 없는 디지털 단위
>
> 나. 화폐·전자화폐·재화·용역 등으로 교환될 수 없는 디지털 단위
>
> 다. 「전자금융거래법」에 따른 전자화폐
>
> 2. "암호통화취급업"이란 다음 각 목의 어느 하나에 해당하는 업(業)을 말한다.
>
> 가. 암호통화매매업: 암호통화를 판매하거나 구입하는 행위(암호통화의 판매를 대행하거나 구입을 권유하는 행위를 포함한다. 이하 "매매"라 한다)를 영업으로 하는 것. 다만, 재화나 용역을 판매하고 그 대가로 암호통화를 받는 경우는 제외한다
>
> 나. 암호통화거래업: 암호통화의 매매를 위한 시장을 개설하고 운영하는 행위를 영업으로 하는 것
>
> 다. 암호통화중개업: 암호통화의 매매를 중개하거나 알선하는 행위를 영업으로 하는 것
>
> 라. 암호통화발행업: 암호통화를 발행하거나 고안하여 암호통화의 생성체계 또는 거래체계를 만드는 행위를 영업으로 하는 것
>
> 마. 암호통화관리업: 타인을 위하여 암호통화를 보관·관리하는 행위를 영업으로 하는 것
>
> 바. 외국암호통화취급업: 외국의 법령상 그 나라에서 같은 종류의 등록(행정처분을 포함한다)을 받아 국내에서 가목부터 마목까지 중 어느 하나 이상의 행위를 영업으로 하는 것

법률안은 제4조와 제5조를 통해 암호통화취급업의 등록의무를 규정하고 미등록 영업행위에 대해 처벌하고자 하였으며, 암호통화취급업의 등록요건으로 다음의 내용을 규정하고 있다.

> 제5조 ② 제1항에 따라 등록하려는 자는 다음 각 호의 요건을 모두 갖추어야 한다.
>
> 1. 1억원 이상으로서 대통령령으로 정하는 금액 이상의 자기자본을 갖출 것
> 2. 사업계획이 타당하고 건전할 것

3. 암호통화를 중개·교환·매매 등을 하는 자(이하 "암호통화이용자"라 한다)에 대한 보호가 가능하고 그 영위하고자 하는 암호통화취급업을 수행하기에 충분한 인력과 전산설비, 그 밖의 물적 설비를 갖출 것
4. 경영건전성기준 등 대통령령으로 정하는 건전한 재무상태와 법령 위반사실이 없는 등 대통령령으로 정하는 건전한 사회적 신용을 갖출 것
5. 암호통화취급업자와 이용자 간, 특정 이용자와 다른 이용자 간의 이해상충을 방지하기 위한 체계로서 대통령령으로 정하는 요건을 갖출 것
6. 외국암호통화취급업자의 경우 국내에 영업소를 두어야 하며, 국내에 주소를 둔 자를 영업소의 대표로 선임할 것

법률안은 다음과 같이 암호통화예치금에 대한 별도예치에 관한 규정을 두고 있다.

제8조(암호통화예치금의 별도예치) ① 암호통화거래업을 영위하는 자(이하 "암호통화거래업자"라 한다)는 암호통화예치금(암호통화이용자로부터 암호통화의 매매, 그 밖의 거래와 관련하여 예치받은 금전을 말한다. 이하 같다)을 고유재산과 구분하여 대통령령으로 정하는 기관(이하 "예치기관"이라 한다)에 예치하여야 한다.

② 암호통화거래업자는 제1항에 따라 예치기관에 암호통화예치금을 예치하는 경우에는 그 암호통화예치금이 암호통화이용자의 재산이라는 뜻을 밝혀야 한다.

③ 누구든지 제1항에 따라 예치기관에 예치한 암호통화예치금을 상계·압류(가압류를 포함한다)하지 못하며, 암호통화예치금을 예치한 암호통화거래업자는 대통령령으로 정하는 경우 외에는 예치기관에 예치한 암호통화예치금을 양도하거나 담보로 제공하여서는 아니 된다.

그리고 법률안은 시세조종행위와 자금세탁에 대한 금지규정을 두고 있다.

제11조(시세조종행위의 금지) ① 누구든지 암호통화의 매매·중개·교환·발행·관리(이하 "매매등"이라 한다)에 관하여 그 매매등이 성황을 이루고 있는 듯이 잘못 알게 하거나, 그 밖에 타인에게 그릇된 판단을 하게 할 목적으로 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 자기가 매도하는 것과 같은 시기에 그와 같은 가격 또는 약정수치로 타인이 그 암호통화를 매수할 것을 사전에 그 자와 서로 짠 후 매도하는 행위
2. 자기가 매수하는 것과 같은 시기에 그와 같은 가격 또는 약정수치로 타인이 그 암호통화를 매도할 것을 사전에 그 자와 서로 짠 후 매수하는 행위
3. 그 암호통화의 매매등을 함에 있어서 그 권리의 이전을 목적으로 하지 아니하는 거짓으로 꾸민 매매등을 하는 행위
4. 제1호부터 제3호까지의 행위를 위탁하거나 수탁하는 행위

② 누구든지 암호통화의 매매등을 유인할 목적으로 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 그 암호통화의 매매등이 성황을 이루고 있는 듯이 잘못 알게 하거나 그 시세(암호통화를 교환하거나 거래하는 시장에서 형성된 시세 또는 그 밖에 대통령령으로 정하는 시세를 말한다. 이하 같다)를 변동시키는 매매등 또는 그 위탁이나 수탁을 하는 행위
2. 그 암호통화의 시세가 자기 또는 타인의 시장 조작에 의하여 변동한다는 말을 유포하는 행위
3. 그 암호통화의 매매등을 함에 있어서 중요한 사실에 관하여 거짓의 표시 또는 오해를 유발시키는 표시를 하는 행위

제12조(자금세탁행위 등의 금지) ① 누구든지 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조 제3호에 따른 불법재산의 은닉, 같은 조 제4호에 따른 자금세탁행위 또는 같은 조 제5호에 따른 공중협박자금조달행위 및 강제집행의 면탈, 그 밖에 탈법행위를 목적으로 암호통화의 매매등을 하여서는 아니 된다.

② 암호통화취급업자는 대통령령으로 정하는 바에 따라 매매등의 상대방이 본인임을 확인하여야 한다.

그밖에 법률안은 "암호통화거래의 안전성 및 신뢰성 확보를 위하여 기술적·물리적·관리적 보안대책을 수립·시행"하도록 하고(안 제10조), 암호통화이용자에 대하여 "매매권유 등을 하는 경우에 설명의무를 부과하며, 방문판매 등의 방법으로 매매·중개하는 것을 금지"(안 제13조 및 제14조)하는 규정을 포함하고 있다.

3) 제윤경 의원 대표발의 '특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안'

제윤경 의원이 대표발의한 '특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안'은 2018년 3월 21일 발의되었다.[665] 이 법률안은 "가상통화취급업소에 대해서도 자금세탁행위 및 공중협박자금조달행위의 효율적 방지를 위한 의무를 부과하고, 금융회사가 가상통화취급업소와 금융거래를 수행할 때 준수할 사항을 규정하기 위한다"는 취지로 제안되었다.

이 법률안은 '특정 금융거래정보의 보고 및 이용 등에 관한 법률'이 암호화폐의 발행과 거래에까지 적용되어 자금세탁 및 기타 불법행위가 규제될 수 있도록 하기 위해 관련 내용과 표현을 추가하는 방식으로 되어 있으며, 구체적으로 동법 적용의 대상인 '금융거래'를 '금융거래등'으로 변경하고 아래와 같은 내용을 추가하였다.

665) 의안번호 12592. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T1A8E0M3M2J1E1F8Z1J0U0N0Q8E6B8 (2019년 11월 8일 최종접속) 참조.

제2조 제2호 라목 1) 화폐·재화·용역 등으로 교환될 수 없는 전자적 증표 또는 그 증표에 관한 정보로서 발행인이 사용처와 그 용도를 제한한 것
2) 「게임산업진흥에 관한 법률」 제32조 제1항 제7호에 따른 게임물의 이용을 통하여 획득한 유·무형의 결과물
3) 「전자금융거래법」 제2조 제14호에 따른 선불전자지급수단 및 같은 법 제2조 제15호에 따른 전자화폐
4) 거래의 형태와 특성을 고려하여 대통령령으로 정하는 것

그리고 법률안은 "금융회사등이 자금세탁행위 및 공중협박자금조달 행위를 방지하기 위하여 내부의 절차 및 업무지침에 반영·운용해야 할 사항"을 규정하고(안 제5조 제2항), "가상통화 취급업소와 금융거래를 하는 금융회사등은 가상통화 취급업소의 신고의무(안 제10조) 이행 여부 등을 추가적으로 확인"하도록 하며(안 제6조), 금융회사등은 "의심거래보고, 고액현금거래보고, 고객확인 등 의무이행과 관련한 금융거래 자료 및 정보를 5년간 보존"하도록 규정하고(안 제8조), "가상통화 취급업소에 대해서 금융정보분석원의 장에게 상호 및 대표자의 성명 등을 신고"하도록 하는 한편, "이용자별 거래내역 분리" 등 자금세탁행위 및 공중협박자금조달행위를 방지하기 위하여 이행해야하는 조치를 규정하였으며(안 제10조 및 제11조), 금융회사등에 대하여 부과할 수 있는 과태료의 한도를 1억원으로 상향하는 한편, 과태료 부과사유로 "금융회사등이 이행해야 할 조치의무(안 제5조) 위반, 자료보관의무(안 제8조) 위반" 등을 추가하였다(안 제24조 제1항·제2항).

4) 채이배 의원 대표발의 '전자상거래 등에서의 소비자보호에 관한 법률 일부개정법률안'

채이배 의원이 대표발의한 '전자상거래 등에서의 소비자보호에 관한 법률 일부개정법률안'은 2018년 4월 6일 발의되었다.[666] 이 법률안은 "대부분의 암호화폐 거래소가 이 법상의 통신판매업자 등으로 신고하고 영업을 하는 현실을 반영하여, 암호화폐의 제도화가 이루어지는 동안에도 소비자 피해는 방지할 수 있도록 제도적 근거를 마련하고자 한다"는 취지로 제안되었다.

법률안은 암호화폐 거래소가 고객재산을 다량 보관하는 특성을 고려하여, 암호화폐

666) 의안번호 12961. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_D1H8F0Q4X0L6F2L1L0B6G0H4C4J9O0 (2019년 11월 8일 최종접속) 참조.

를 거래하는 업자에게 망분리를 하는 등 보관 중인 고객재산의 보호를 위한 조치를 하여야 하고, 이러한 조치를 이행하지 않았다가 해킹사고 등이 발생한 경우에는 손해에 대해 무과실책임을 지게 하자는 취지로 다음의 규정을 신설하였다.

> 제20조의4(소비자의 재산을 보관하는 통신판매업자등의 책임) ① 통신판매업자 또는 통신판매중개업자로서 소비자의 재산을 대통령령으로 정하는 규모 이상 보관하는 등 대통령령으로 정하는 기준에 해당하는 자는 보관 중인 소비자의 재산을 보호하기 위하여 대통령령으로 정하는 기술적·관리적·물리적 조치를 취하여야 한다.
>
> ② 제1항에 따른 조치의무를 이행하지 아니한 자는 멸실, 도난, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제7호의 침해사고 등으로 인하여 소비자에게 발생한 재산상 손해에 대해 고의 또는 과실이 없음을 들어 손해를 배상할 책임을 면하지 못한다.

암호화폐 거래소는 금융상품의 거래와 유사한 형태의 거래를 하고 있고, 따라서 높은 보안수준을 갖출 필요가 인정된다. 그리하여 법률안은 공정위가 금감원이나 한국인터넷진흥원과 합동으로 조사를 실시할 근거 규정을 만드는 한편, 소비자보호를 위한 시스템이 충분히 갖추어졌는지를 점검할 수 있도록 하는 근거 규정을 개정안(제26조의 개정)에서 제시하였다.

5) 하태경 의원 대표발의 '전자금융거래법 일부개정법률안'

하태경 의원이 대표발의한 '전자금융거래법 일부개정법률안'은 2018년 9월 27일 발의되었다.[667] 이 법률안은 "암호통화의 매도·매수·중개·교환·관리 등 암호통화취급업을 허가 대상으로 하고, 암호통화 발행은 금융위원회의 승인을 받아 할 수 있도록 하며, 보안대책 수립·시행, 시세조종행위 등의 금지, 금융위원회 및 금융감독원의 감독 및 검사 등 암호통화의 안전성, 신뢰성 및 이용자 보호에 관한 규정을 마련한다"는 취지로 제안되었다.

법률안은 전자금융거래법에 다음과 같은 규정을 신설하는 것을 주요 내용으로 한다.

---

667) 의안번호 15745. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_K1M8Z0M9X2L7E1H2S5P3N4H9V1V7Q0 (2019년 11월 8일 최종접속) 참조.

제2조 23. "암호통화"란 분산원장 기술(거래에 참여하는 사람들이 동기화된 거래 내역을 공동으로 관리하여 위조 등을 방지하는 기술을 말한다)을 사용하여 이전 가능한 재산적 가치 등을 전자적으로 저장된 형태로 발행한 것으로서 교환의 매개수단 및 가치의 저장수단으로 사용되는 증표 또는 그 증표에 관한 정보를 말한다. 다만, 화폐·전자화폐·재화·용역 등으로 교환될 수 없는 전자적 증표 또는 그 증표에 관한 정보 및 전자화폐는 제외한다.

24. "암호통화취급업자"란 제38조의2 제1항에 따라 허가를 받은 자를 말한다.

25. "암호통화거래"란 암호통화의 매도·매수·중개·교환·관리, 그 밖에 대통령령으로 정하는 거래를 말한다.

26. "암호통화기반시설"이란 암호통화거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호에 따른 정보통신망을 말한다.

27. "암호통화거래보조업자"란 암호통화취급업자를 위하여 암호통화거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

28. "암호통화이용자"란 암호통화취급업자와 체결한 계약에 따라 암호통화거래를 이용하는 자를 말한다.

제5장 암호통화취급업의 허가 및 업무

제38조의2(암호통화취급업의 허가) ① 다음 각 호의 업무를 행하고자 하는 자는 금융위원회의 허가를 받아야 한다. 다만, 「은행법」에 따른 은행 그 밖에 대통령령이 정하는 금융회사는 그러하지 아니하다

1. 암호통화매매업: 암호통화를 매도하거나 매수하는 업무(이를 대행하거나 권유하는 행위를 포함한다. 이하 "매매"라 한다)

2. 암호통화거래업: 암호통화의 매매를 위한 시장을 개설하고 운영하는 업무

3. 암호통화중개업: 암호통화의 매매를 중개하거나 알선하는 업무

4. 암호통화관리업: 타인을 위하여 암호통화를 보관·관리하는 업무

5. 그 밖에 대통령령으로 정하는 암호통화취급업무

② 제1항 제2호에 따른 허가를 받은 경우에는 같은 항 제3호 및 제4호에 따른 허가를 받은 것으로 본다.

제38조의3(허가의 요건) ① 제38조의2 제1항에 따라 허가를 받고자 하는 자는 다음 각 호의 요건을 모두 갖추어야 한다.

1. 업무의 종류별로 자본금 또는 출자총액이 20억원 이상으로서 대통령령으로 정하는 금액 이상일 것

2. 암호통화이용자의 보호가 가능하고 행하고자 하는 업무를 수행함에 있어서 충분한 전문인력과 전산설비 등 물적 시설을 갖추고 있을 것

3. 대통령령이 정하는 재무건전성 기준을 충족할 것

4. 사업계획이 타당하고 건전할 것

5. 대통령령이 정하는 주요출자자가 충분한 출자능력, 건전한 재무상태 및 사회적 신용을 갖추고 있을 것

② 허가의 결격사유, 신청, 예비허가 등에 관하여는 제32조, 제33조, 제33조의2를 준용한다.

③ 제1항의 규정에 따른 허가의 세부요건에 관하여 필요한 사항은 금융위원회가 정한다.

제38조의4(암호통화발행의 승인) ① 누구든지 암호통화의 발행(외국에서 발행된 암호통화를 국내에

서 취급하는 것을 포함한다)을 하려는 자는 대통령령으로 정하는 바에 따라 금융위원회의 승인을 받아야 한다.

② 제1항에 따른 승인의 기준은 암호통화의 위조 방지 및 거래의 안전성 등에 관하여 금융위원회가 정하여 고시한다.

③ 금융위원회는 제1항에 따른 승인을 한 때에는 지체 없이 그 내용을 관보에 공고하고 컴퓨터통신 등을 이용하여 일반인에게 알려야 한다.

④ 금융위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 승인을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다.

1. 허위 그 밖의 부정한 방법으로 승인을 받은 경우

2. 제2항의 기준에 미달하게 된 경우

3. 1년 이상 계속하여 해당 암호통화의 거래가 없는 때

제38조의5(암호통화발행심사위원회) ① 제38조의4 제1항에 따른 승인 및 그 기준을 심의하기 위하여 금융위원회에 암호통화발행심사위원회(이하 "심사위원회"라 한다)를 둔다.

② 심사위원회는 위원장 1명을 포함한 9명의 위원으로 구성하되, 위원장은 금융위원회 부위원장이 되고 위원은 암호통화 및 분산원장 기술 분야의 전문성을 고려하여 금융위원회 위원장이 위촉한다. 이 경우 공무원이 아닌 위원이 5명 이상이 되어야 한다.

③ 심사위원회의 위원 중 공무원이 아닌 위원은 「형법」 제127조 및 제129조부터 제132조까지의 규정을 적용할 때에는 공무원으로 본다.

④ 심사위원회의 위원은 공정한 심의를 기대하기 어려운 사정이 있다고 인정될 때에는 대통령령으로 정하는 바에 따라 위원회 회의에서 제척되거나 회피하여야 한다.

⑤ 심사위원회의 조직과 운영, 심의사항과 그 밖에 필요한 사항은 대통령령으로 정한다.

제38조의6(암호통화거래의 안전성 확보) ① 암호통화취급업자는 암호통화거래의 안전성 및 신뢰성을 확보할 수 있도록 그가 구축·운영하는 시스템에 대한 제3자의 불법적인 접근, 입력된 정보의 변경, 훼손, 파괴, 해킹, 유출, 서버 과부화 등에 대비하여 다음 각 호의 기술적·물리적·관리적 조치를 하여야 한다.

1. 암호통화거래를 안전하게 처리하기 위한 내부관리계획의 수립·시행

2. 시스템에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영

3. 접속기록의 위조·변조 방지를 위한 조치

4. 암호통화거래정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치

5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치

6. 그 밖에 암호통화거래의 안전성 확보를 위하여 필요한 보호조치

② 암호통화취급업자는 금융위원회의 인가를 받아 제1항에 따른 조치를 법인에 위탁할 수 있다.

③ 제1항에 따른 조치의 기준 및 제2항에 따른 인가에 필요한 사항은 금융위원회가 정한다.

④ 그 밖에 암호통화취급업자의 안전성 확보의무에 관하여는 제8조, 제21조, 제21조의2, 제21조의3, 제21조의5, 제21조의6을 준용한다. 이 경우 "금융회사"는 "암호통화취급업자"로, "전자금융보조업자"는 "제2항에 따른 위탁을 받은 자"로, "전자금융거래"는 "암호통화거래"로, "이용자"는 "암호통화이용자"로, "전자금융기반시설"은 "암호통화기반시설"로 본다.

제38조의7(암호통화이용자 피해보상계약) ① 암호통화취급업자는 제38조의6 제1항에 따른 정보의 변경, 훼손, 파괴 등에 의한 암호통화이용자(암호통화취급업자인 암호통화이용자를 제외한다)의 피

해를 보상하기 위하여 다음 각 호의 어느 하나에 해당하는 계약(이하 "피해보상계약"이라 한다)을 체결하여야 한다. 다만, 해당 피해보상계약의 유효기간이 만료된 경우에는 그러하지 아니하다.

1. 「보험업법」에 따른 보험계약
2. 암호통화이용자의 피해보상금의 지급을 확보하기 위한 「금융위원회의 설치 등에 관한 법률」 제38조에 따른 기관의 채무지급보증계약

② 제1항에 따라 피해보상계약을 체결한 암호통화취급업자는 지체 없이 그 사실을 금융위원회에 신고하여야 한다.

③ 그 밖에 피해보상계약에 대하여 필요한 사항은 대통령령으로 정한다.

제38조의8(시세조종행위의 금지) ① 누구든지 암호통화거래가 성황을 이루고 있는 듯이 잘못 알게 하거나, 그 밖에 타인에게 그릇된 판단을 하게 할 목적으로 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 자기가 매도하는 것과 같은 시기에 그와 같은 가격 또는 약정수치로 타인이 그 암호통화를 매수할 것을 사전에 그 자와 서로 짠 후 매도하는 행위
2. 자기가 매수하는 것과 같은 시기에 그와 같은 가격 또는 약정수치로 타인이 그 암호통화를 매도할 것을 사전에 그 자와 서로 짠 후 매수하는 행위
3. 그 암호통화의 매매등을 함에 있어서 그 권리의 이전을 목적으로 하지 아니하는 거짓으로 꾸민 매매등을 하는 행위
4. 제1호부터 제3호까지의 행위를 위탁하거나 수탁하는 행위

② 누구든지 암호통화거래를 유인할 목적으로 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 그 암호통화거래가 성황을 이루고 있는 듯이 잘못 알게 하거나 그 시세(암호통화를 교환하거나 거래하는 시장에서 형성된 시세 또는 그 밖에 대통령령으로 정하는 시세를 말한다. 이하 같다)를 변동시키는 암호통화거래 또는 그 위탁이나 수탁을 하는 행위
2. 그 암호통화의 시세가 자기 또는 타인의 시장 조작에 의하여 변동한다는 말을 유포하는 행위
3. 그 암호통화거래를 함에 있어서 중요한 사실에 관하여 거짓의 표시 또는 오해를 유발시키는 표시를 하는 행위

제38조의9(시장질서 교란행위의 금지) ① 다음 각 호의 어느 하나에 해당하는 자(이에 해당하지 아니하게 된 날부터 1년이 경과하지 아니한 자를 포함한다)는 암호통화거래와 관련된 미공개중요정보(암호통화거래에 중대한 영향을 미칠 수 있는 정보로서 대통령령으로 정하는 방법에 따라 불특정 다수인이 알 수 있도록 공개되기 전의 것을 말한다. 이하 이 항에서 같다)를 해당 암호통화거래에 이용하거나 타인에게 이용하게 하여서는 아니 된다.

1. 암호통화취급업자 및 해당 법인의 임직원·대리인으로서 그 직무와 관련하여 미공개중요정보를 알게 된 자
2. 암호통화취급업자에 대하여 법령에 따른 허가·인가·지도·감독, 그 밖의 권한을 가지는 자로서 그 권한을 행사하는 과정에서 미공개중요정보를 알게 된 자
3. 암호통화취급업자와 계약을 체결하고 있거나 체결을 교섭하고 있는 자로서 그 계약을 체결·교섭 또는 이행하는 과정에서 미공개중요정보를 알게 된 자
4. 제2호 또는 제3호에 해당하는 자의 대리인(이에 해당하는 자가 법인인 경우에는 그 임직원 및 대리인을 포함한다)·사용인, 그 밖의 종업원(제2호 또는 제3호에 해당하는 자가 법인인 경우에는 그 임직원 및 대리인)으로서 그 직무와 관련하여 미공개중요정보를 알게 된 자

5. 제1호부터 제4호까지의 어느 하나에 해당하는 자(제1호부터 제4호까지의 어느 하나의 자에 해당하지 아니하게 된 날부터 1년이 경과하지 아니한 자를 포함한다)로부터 미공개중요정보를 받은 자

② 제1호에 해당하는 자는 제2호에 해당하는 정보를 암호통화거래에 이용하거나 타인에게 이용하게 하는 행위를 하여서는 아니 된다. 다만, 투자자 보호 및 건전한 시장질서를 해할 우려가 없는 행위로서 대통령령으로 정하는 경우는 제외한다.

1. 다음 각 목의 어느 하나에 해당하는 자

가. 제1항 각 호의 어느 하나에 해당하는 자로부터 나온 미공개중요정보 또는 미공개정보인 사실을 알면서 이를 받거나 전득(轉得)한 자

나. 자신의 직무와 관련하여 제2호에 해당하는 정보(이하 이 호에서 "정보"라 한다)를 생산하거나 알게 된 자

다. 해킹, 절취(截取), 기망(欺罔), 협박, 그 밖의 부정한 방법으로 정보를 알게 된 자

라. 나목 또는 다목의 어느 하나에 해당하는 자로부터 나온 정보인 사실을 알면서 이를 받거나 전득한 자

2. 다음 각 목의 모두에 해당하는 정보

가. 그 정보가 암호통화거래의 조건에 중대한 영향을 줄 가능성이 있을 것

나. 그 정보가 암호통화이용자들이 알지 못하는 사실에 관한 정보로서 불특정 다수인이 알 수 있도록 공개되기 전일 것

③ 누구든지 암호통화거래와 관련하여 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 거래 성립 가능성이 희박한 호가를 대량으로 제출하거나 호가를 제출한 후 해당 호가를 반복적으로 정정·취소하여 시세에 부당한 영향을 주거나 줄 우려가 있는 행위

2. 권리의 이전을 목적으로 하지 아니함에도 불구하고 거짓으로 꾸민 매매를 하여 시세에 부당한 영향을 주거나 줄 우려가 있는 행위

3. 손익이전 또는 조세회피 목적으로 자기가 매매하는 것과 같은 시기에 그와 같은 가격 또는 약정수치로 타인이 그 암호통화를 매수할 것을 사전에 그 자와 서로 짠 후 매매를 하여 시세에 부당한 영향을 주거나 영향을 줄 우려가 있는 행위

4. 풍문을 유포하거나 거짓으로 계책을 꾸미는 등으로 암호통화의 수요·공급 상황이나 그 가격에 대하여 타인에게 잘못된 판단이나 오해를 유발하거나 암호통화의 가격을 왜곡할 우려가 있는 행위

제38조의10(설명의무) ① 암호통화취급업자는 암호통화이용자(암호통화이용자가 되려는 자를 포함하되, 암호통화취급업자인 암호통화이용자를 제외한다. 이하 이 조에서 같다)를 상대로 암호통화의 매매를 권유하는 경우에는 암호통화의 내용, 매매에 따르는 위험, 그 밖에 대통령령으로 정하는 사항을 암호통화이용자가 이해할 수 있도록 설명하여야 한다.

② 암호통화취급업자는 제1항에 따라 설명한 내용을 암호통화이용자가 이해하였음을 서명, 기명날인, 녹취, 그 밖의 대통령령으로 정하는 방법 중 하나 이상의 방법으로 확인을 받아야 한다.

③ 암호통화취급업자는 제1항에 따른 설명을 함에 있어서 암호통화이용자의 합리적인 판단 또는 해당 암호통화의 가치에 중대한 영향을 미칠 수 있는 사항(이하 "중요사항"이라 한다)을 거짓 또는 왜곡(불확실한 사항에 대하여 단정적 판단을 제공하거나 확실하다고 오인하게 할 소지가 있는 내용을 알리는 행위를 말한다)하여 설명하거나 중요사항을 누락해서는 아니 된다.

이 법률안은 전자금융거래법에 대한 일부개정의 형식을 취하고 있지만 사실상 위와

같이 암호화폐에 대한 근거규정과 요건, 규제의 내용 등을 대폭 신설하는 것을 내용으로 하고 있다.[668]

6) 김병욱 의원 대표발의 '특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부개정법률안'

김병욱 의원이 대표발의한 '특정 금융거래정보의 보고 및 이용 등에 관한 법률(이하 '특금법'이라 한다) 일부개정법률안'은 2019년 3월 18일 발의되었다.[669] 이 법률안은 "주요 20개국(G20) 정상회의와 자금세탁방지기구(FATF) 등 국제기구에서는 자금세탁방지 및 공중협박자금조달금지를 위한 국제기준을 제정하고, 회원국들에게 이를 이행할 것을 요구하고 있는데, 이에 가상자산 취급업소에 대해서도 자금세탁행위 및 공중협박자금조달행위의 효율적 방지를 위한 의무를 부과하고, 금융회사가 가상자산 취급업소와 금융거래를 수행할 때 준수할 사항을 규정하기 위한다"는 취지로 제안되었다.

법률안은 다음과 같은 가상자산에 대한 정의규정을 두었다.

> 제2조 제3호 하. 가상자산과 관련하여 다음 중 어느 하나에 해당하는 행위를 영업으로 하는 자(이하 "가상자산 취급업소"라 한다)
>
> 1) 가상자산을 매도, 매수하는 행위
>
> 2) 가상자산을 다른 가상자산과 교환하는 행위
>
> 3) 가상자산을 이전하는 행위 중 대통령령으로 정하는 행위
>
> 4) 가상자산을 보관 또는 관리하는 행위
>
> 5) 1) 및 2)의 행위를 중개, 알선하거나 대행하는 행위
>
> 6) 그 밖에 가상자산과 관련하여 자금세탁행위와 공중협박자금조달행위에 이용될 가능성이 높은 것으로서 대통령령으로 정하는 행위
>
> 라. 가상자산 취급업소가 수행하는 제1호 하목의 어느 하나에 해당하는 것(이하 "가상자산거래"라 한다)
>
> 3. "가상자산"이란 전자적으로 거래 또는 이전될 수 있는 가치의 전자적 증표(그에 관한 일체의 권리를 포함한다)를 말한다. 다만, 다음 각 목에 해당하는 것은 제외한다.

---

668) 이 법률안에 대해서는 동일한 내용에다 ICO의 허용이 추가된 수정법률안이 이언주 의원의 대표발의로 2019년 5월 8일에 다시 발의(의안번호 20245. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_E1H9S0V5I0P8S1J5O3X8X1H1F5G5P6 (2019년 11월 8일 최종접속) 참조)되었다.

669) 의안번호 19288. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_A1S9N0C3T1Q8D1N9S1P4P2G1M6Q7S8 (2019년 11월 8일 최종접속) 참조.

가. 화폐·재화·용역 등으로 교환될 수 없는 전자적 증표 또는 그 증표에 관한 정보로서 발행인이 사용처와 그 용도를 제한한 것

나.「게임산업진흥에 관한 법률」 제32조 제1항 제7호에 따른 게임물의 이용을 통하여 획득한 유·무형의 결과물

다.「전자금융거래법」 제2조 제14호에 따른 선불전자지급수단 및 같은 법 제2조 제15호에 따른 전자화폐

라. 거래의 형태와 특성을 고려하여 대통령령으로 정하는 것

법률안은 가상자산 취급업소에 대한 다음과 같은 의무사항을 규정하였다.

제7조(신고) ① 가상자산 취급업소(이를 운영하려는 자를 포함한다. 이하 이 조에서 같다)는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 금융정보분석원장에게 신고하여야 한다.

1. 상호 및 대표자의 성명
2. 사업장의 소재지, 연락처 등 대통령령으로 정하는 사항

② 제1항에 따라 신고한 자는 신고한 사항이 변경된 경우에는 대통령령으로 정하는 바에 따라 금융정보분석원장에게 변경신고를 하여야 한다.

③ 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자에 대하여는 대통령령으로 정하는 바에 따라 가상자산 취급업소의 신고를 수리하지 아니할 수 있다.

1. 정보보호 관리체계 인증을 획득하지 못한 자
2. 실명확인이 가능한 입출금 계정[동일 금융회사등(대통령령으로 정하는 금융회사등에 한한다)에 개설된 가상자산 취급업소의 계좌와 그 가상자산 취급업소의 고객의 계좌 사이에서만 금융거래등을 허용하는 계정을 말한다]을 통하여 금융거래등을 하지 않는 자. 다만, 가상자산거래의 특성을 고려하여 금융정보분석원장이 정하는 자에 대해서는 예외로 한다.
3. 이 법,「범죄수익은닉의 규제 및 처벌 등에 관한 법률」 및 대통령령으로 정하는 법령에 따라 벌금 이상의 형을 선고받고 그 집행이 끝나거나(집행이 끝난 것으로 보는 경우를 포함한다) 면제된 날부터 5년이 지나지 아니한 자(가상자산 취급업소가 법인인 경우 대표자와 임원을 포함한다)
4. 제4항에 따라 신고가 말소되고 5년이 지나지 아니한 자

④ 금융정보분석원장은 다음 각 호의 어느 하나에 해당하는 자에 대해서는 대통령령으로 정하는 바에 따라 제1항 및 제2항에 따른 신고를 직권으로 말소할 수 있다.

1. 제3항 각 호의 어느 하나에 해당하는 자
2. 이 법 또는 이 법에 따른 명령을 위반하여 다음 각 목의 어느 하나에 해당하는 자

가. 제15조 제2항 제1호에 따른 시정명령을 이행하지 아니한 경우

나. 제15조 제2항 제2호에 따른 기관경고를 3회 이상 받은 경우

다. 제15조 제1항부터 제3항까지 또는 제6항에 따른 명령·지시·검사에 따르지 아니하거나 이를 거부·방해·기피하여 금융정보분석원장(제15조 제6항에 따라 업무를 위탁받은 자를 포함한다)으로부터 제재를 받은 자

라. 그 밖에 고의 또는 중대한 과실로 자금세탁행위와 공중협박자금조달 행위를 방지하기 위하여

필요한 조치를 하지 아니한 경우로서 대통령령으로 정하는 경우

3. 「부가가치세법」 제8조에 따라 관할 세무서장에게 폐업신고를 하거나 관할 세무서장이 사업자등록을 말소한 자

⑤ 금융정보분석원장은 제1항부터 제4항까지에 따른 가상자산 취급업소의 신고에 관한 정보를 대통령령으로 정하는 바에 따라 공개할 수 있다.

⑥ 제1항에 따른 신고의 유효기간은 신고를 수리한 날부터 5년 이하의 범위에서 대통령령으로 정하는 기간으로 한다. 신고 유효기간이 지난 후 계속하여 같은 행위를 영업으로 하려는 자는 대통령령으로 정하는 바에 따라 다시 신고하여야 한다.

⑦ 금융정보분석원장은 이 조에 따른 가상자산 취급업소의 신고와 관련한 업무로서 대통령령으로 정하는 업무를 「금융위원회의 설치 등에 관한 법률」에 따른 금융감독원의 원장(이하 "금융감독원장"이라 한다)에게 위탁할 수 있다.

제8조(가상자산 취급업소의 조치) 가상자산 취급업소는 제4조 제1항 및 제4조의2에 따른 보고의무 등을 위하여 고객별 거래내역을 분리하여 관리하는 등 대통령령으로 정하는 조치를 하여야 한다.

그 외에도 법률안은 금융회사등은 가상자산 취급업소와 금융거래를 할 때 가상자산 취급업소의 신고의무 이행 여부 등을 추가적으로 확인하도록 하고, 가상자산 취급업소가 신고의무를 미이행한 것이 확인되는 등의 경우에는 금융거래를 거절하도록 하는 (안 제5조의2 제4항) 규정을 두었다.

이 법률안은 암호화폐의 거래 등을 통한 자금세탁을 방지하기 위한 국제기구의 권유 등을 국내법상 실현하기 위한 이행입법의 성격을 가지고 있다.

라. 국제자금세탁방지기구(FATF)의 자금세탁방지 관련 입법권고

FATF는 2019년 6월 21일 '가상자산(Virtual Asset)'을 이용한 자금세탁방지를 위한 권고지침(Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers)[670]을 발표하였다. 이 권고에서 FATF는 "가상자산은 디지털로 거래 또는 전송될 수 있고 지불이나 투자의 수단으로 이용될 수 있는 가치로, FATF 권고가 규정한 기존의 현실통화, 유가증권, 자산의 디지털 표상을 의미하는 것이 아니다."라고 가상자산에 대한 정의를 하면서 거래소 및 ICO 관련 서비스 제공자(Virtual Asset Service Providers)에게 자금세탁 방지 의무 부과하도록 하였다. 관련하여 본 지침에서

670) Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019.6., http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (2019년 11월 8일 최종접속).

는 '가상자산 서비스 제공자'를 가상자산과 현실화폐의 교환, 가상자산 간의 교환, 가상자산의 전송, 보관, 관리, 발행 등의 서비스를 제공하는 자연인 또는 법인이라고 정의[671]하였다.

FATF는 가상자산 서비스 제공자에 대한 인·허가(license) 또는 신고·등록(register)을 의무화하도록 하고(자율규제기관 등에 의한 허가 등은 불인정), 정부의 감독기구를 통한 자금세탁방지 관련 규제·감독(Regulation and supervision)이 이루어지도록 감독기구는 가상자산 취급업소의 의무위반에 대해 허가 등을 취소·제한·중지시킬 수 있는 권한을 보유하여야 한다고 하였으며, 가상자산 취급업소에 대해서는 금융회사에 준하는 자금세탁방지를 위한 예방조치(preventive measures) 이행의무를 부여하여 고객확인의무(Customer Due Diligence), 의심거래보고(Suspicious Transaction Report) 등의 의무를 법제화하도록 권고하였다.[672]

2. 현행법과 법정책적 동향에 대한 평가와 한계

암호화폐의 발행과 거래에 대한 명시적인 법규정이 없는 현재의 상태에서는 암호화폐와 관련하여 발생하고 있는 대부분의 사례에 대해 법적 대처가 불가능한 상황이라고 할 수 있다. 전술한 바와 같이 ICO는 전통적인 IPO와의 형식상의 유사점으로 인하여 자본시장법에 의한 규율의 대상이 될 수 있을지에 대한 검토가 행해졌지만 그 실질의 상이함으로 인해 암호화폐가 자본시장법에 의한 '증권'의 일종으로 취급될 수는 없는 상황이다. 특히 암호 '화폐'라는 명칭의 사용에서도 유추할 수 있는 바와 같이 ICO는 벤처기업들의 투자금을 모집하는 수단으로 사용되고 있기는 하지만 투자

671) "Virtual asset service provider" as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
i. Exchange between virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets;
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

672) FATF는 2019년 6월의 권고지침에 대한 회원국의 입법적 조치를 위한 시한으로 1년의 유예기간을 두었으며, 2019년 10월 총회에서는 구체적인 평가지침을 마련하였다.

자 혹은 거래참여자들의 주된 관심과 동기는 ICO에 의하여 발행된 '토큰'의 유통성과 교환성에 집중되고 있고, 법정책의 중심에도 ICO 자체보다는 '토큰거래소'의 인가와 운영의 문제가 자리하고 있다. 따라서 자본시장법의 취지와 암호화폐 거래의 문제는 이미 상당한 거리가 있는 것으로 평가할 수 있고, 현행 자본시장법에 의한 규제의 시도는 분명한 한계를 가지고 있다고 할 수 있다. 한때 정부가 시도한(다고 언론에 알려졌던) 유사수신행위법을 통한 규제도 마찬가지의 상황이다. 유사수신행위법 자체가 자금모집을 무단으로 하는 행위에 대해 금융시장의 질서를 유지한다는 차원에서의 규제입법의 취지를 가지고 있는 법이고, 이 역시 암호화폐의 거래보다는 암호화폐의 발행 그 자체가 대상이 될 수밖에 없는 법이다. 이미 거대한 시장으로 발달한 ICO와 암호화폐의 거래에 대해 단순히 무인가 자금조달의 규제라는 측면으로 접근할 수는 없는 시점이다. 여러 가지 면에서 현행법은 ICO와 암호화폐의 거래에 대해서 '법적 진공의 상태'[673]에 있다는 표현이 정확한 것으로 보인다.

ICO에 대한 법적 근거를 만들고 암호화폐의 거래와 거래소에 대한 관리 및 규제규정을 입법적으로 정비할 필요가 있다는 업계와 학계의 여러 주장과 제언은 이러한 현실을 직시하면서 '법적 진공상태'를 타파하기 위한 여러 노력의 일환으로 볼 수 있다. 그리고 이러한 여러 제언은 ICO와 암호화폐 거래시장을 (여러 문제점과 파생되는 부작용에도 불구하고) 사회적으로 인정하고 받아들일 수밖에 없다는 인식이 근저에 자리하고 있는 것이다. 문제는 금융정책기구를 비롯한 정부나 입법부의 구성원들은 아직까지는 암호화폐 거래가 가지는 여러 문제점과 파생되는 부작용을 더 크게 인식하고 있는 것 같다는 점이다. 암호화폐와 '투기'라는 단어의 연관성이 현저한 상황에서 암호화폐 거래의 합법화에 대한 정책적 부담감이 큰 것으로 보인다. 그러나 FATF에 의한 가상자산의 법적 관리를 위한 구체적 권고지침의 발표라는 외적 요인과 대통령직속 4차산업혁명위원회에 의한 암호화폐 발행과 거래에 대한 법적 정의 마련과 제도화를 내용으로 하는 대정부권고안 발표라는 내적 요인 등은 적어도 가까운 시일 내에 암호화폐를 중심으로 하는 가상자산에 대한 법적 정의와 이에 대한 금융감독기관의 관리와 감독을 내용으로 하는 입법적 조치는 이루어질 수 있을 것으로 전망

673) 2019년 10월 7일 개최된 블록체인법학회와 한국형사정책연구원이 공동으로 주최한 '블록체인과 형사사법' 학술대회 제1세션 지정토론자로 참석한 한국형사정책연구원 전현욱 연구위원의 토론내용 중 일부분.

된다. 따라서 국회에 발의되어 있는 여러 관련 법안들 중에서 가상자산과 가상자산 취급업에 대한 정의규정을 두고 자금세탁방지를 위하여 가상자산 취급업자에게 금융기관에 준하는 의무를 부여하며 아울러 금융감독기관의 감독기능 등을 규정하는 특금법 일부개정법률안(김병욱 의원안)이 일차적인 심의검토 및 입법적 처리의 대상이 될 것으로 예상한다.

그렇지만 이러한 입법적 조치는 문제의 해결이 아니라 출발점에 불과하다. 국회에 발의된 여러 입법안의 종류와 차이가 보여주듯 ICO와 암호화폐 거래에 대한 (형사)법적 대처 방식의 방향성에 대해서는 현저한 인식의 차이가 존재한다. 암호화폐 시장을 금융이나 자본거래의 일종으로 보아 기존 금융상품이나 은행규제의 법체계를 암호화폐 거래시장에 확장 적용하는 방식을 취할 것인지, 이와 달리 암호화폐의 발행과 거래를 기존에 존재하지 않았던 완전히 새로운 개념으로 받아들여 새로운 법적 관념과 체계를 형성하는 방식을 취할 것인지의 문제이다. 국회의 법률안들은 이 점에 대해 정리되지 않은 입법자들의 인식을 드러내고 있다. 또한 암호화폐에 대한 형사법적 대처의 목적에는 암호화폐 거래 자체에 대한 규제와 이에 대한 처벌의 문제보다는 암호화폐의 거래에서 파생되는 형사법적 문제들 즉, 암호화폐를 이용한 형법상의 신종범죄현상들에 대한 법적 대처방안의 마련이 더욱 크게 자리하고 있다. 암호화폐를 이용한 자금세탁의 방지를 위한 법률안은 형사법적 대처의 작은 일부분이다. 암호화폐에 대한 형사법적 대처를 위한 입법활동은 암호화폐 자체의 민형사법적 개념정의, 암호화폐에 대한 재산범죄의 해결을 위한 해석기준, 암호화폐를 이용한 범죄의 수사를 위한 절차법적 개선방향 등의 내용을 담아야 한다.

네트워크 혁신 시대의 형사법적 대응 방안

윤지영·류부곤·이원상

제5장

네트워크 혁신 시대의 형사법적 대응 방안

제1절 | 형사법적 대응 방안

1. 형사실체법적 대응 방안

가. 사물인터넷 기술 발달에 따른 형법 규정 정비

1) 기술적 수단을 이용한 사생활 침해

(1) 문제의 현황

사물인터넷 등 네트워크와 정보통신 기술의 비약적 발전은 컴퓨터라는 특정 전자기기를 넘어 일상에서 사용되는 생활 도구들을 정보통신 네트워크에 포섭시켜 다양하고 편리하게 활용할 수 있는 가능성을 열어주었지만, 그렇게 '넓게 열려진' 네트워크는 타인으로부터 공격받을 수 있는 길 또한 넓게 열려져 있다는 것을 의미한다. 일정한 주거에 대한 사생활의 자유를 누리는 주체가 사물인터넷을 이용하여 자신의 주거에 있는 여러 가전기기들을 관리하고 조종하며 관찰할 수 있다는 것은 그 정보통신망에 해킹 등의 방법을 통하여 들어올 수 있는 타인도 똑같이 집주인의 의사에 반하여 가전기기들을 관리, 조종, 통제할 수 있다는 것이다.

이러한 행위는 물론 현행법상으로 정보통신망에 대한 침해행위[674]가 성립되어 범

674) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
9. 제48조 제1항을 위반하여 정보통신망에 침입한 자

죄가 성립하고 처벌의 대상이 된다. 그런데 정보통신망법에 의한 정보통신망침해죄의 피해자는 해당 정보통신망을 운영하는 주체(즉 정보통신서비스 제공자)가 되는 것이고, 그러한 해킹과 망 침해 행위를 통하여 실제로 피해를 보는 집주인은 이 범죄의 명목상 피해자가 아니라는 문제가 발생한다. 예컨대 타인이 사물인터넷 망을 해킹하여 사생활이 보장되는 주거 내에 설치된 영상촬영장치나 음향수집장치를 조종할 수 있는 권한을 얻은 후 주거자가 알지 못하는 상태에서 영상이나 음향[675]을 취득한 경우 실질적인 피해자는 의도치 않게 자신의 모습이나 소리가 타인에게 공개되어진 주거자라고 할 수 있다. 그럼에도 불구하고 현재의 정보통신망법에 따른 정보통신망 침해행위는 정보통신망의 안전한 이용 자체를 보호하기 위한 범죄구성요건이어서 이러한 사인의 실질적 사생활 침해를 대상으로 하는 범죄라고 볼 수 없다. 그리고 이러한 행위는 현행 형법에서 사생활의 평온과 안전을 보호법익으로 하는 주거침입죄에 해당한다고도 보기 어렵다. 형법상의 주거침입죄는 주거자나 관리자의 의사 또는 추정적 의사에 반하여 주거 안으로 들어가는 '침입행위'[676]를 구성요건으로 하는 것인데, 정보통신망을 이용한 전자기기의 원격조종을 '침입'이라는 개념으로 포섭하기는 어렵다.[677]

(2) 형법상 보호법익의 재정립: 기술적 수단을 이용한 사생활침해로부터의 보호

사생활의 자유를 보호법익으로 하여 규정된 형법상의 범죄는 비밀침해죄와 주거침입죄이다. 비밀침해죄는 비밀장치된 문서 등의 내용이 타인에게 누설되는 것을 방지하고자 하는 것으로 비밀장치된 문서 등의 내용 그 자체를 보호의 대상[678]으로 하는

---

675) 음향의 경우 통신비밀보호법에 의한 비밀감청에 해당한다면 규제와 처벌의 대상이 될 수 있지만 통신비밀보호법에서 보호하고자 하는 대상은 타인간의 '대화'이기 때문에 음향의 내용이 대화에 해당하지 않는다면 이를 규제할 수 있는 법률은 없다. 얼마 전 모텔에서 투숙객들의 성관계 소리를 몰래 녹음한 모텔 직원의 행위에 대해 통신비밀보호법위반으로 처벌했다고 언론에 보도된 사안("수십차례 투숙객 성관계 소리 녹음한 모텔 직원 실형", KBS 2019년 4월 9일자, https://news.v.daum.net/v/20190409162631066 (2019년 11월 4일 최종접속))에서 통신비밀보호법이 적용된 이유는 투숙객 간의 대화가 함께 녹음되어서이고 '성관계 소리' 자체가 통신비밀보호법의 적용대상이 되었다고 보기는 어렵다.

676) 김성돈, 형법각론 제4판, 성균관대학교출판부, 2016, 254면.

677) 강학상 이는 죄형법정주의의 원칙 중 유추해석금지의 원칙에 반한다. '침입'이라는 용어는 기본적 문리해석상 물리적 진입행위를 필요로 하는 것이고 전자신호의 전송행위는 물리적 진입이라고는 도저히 볼 수가 없다. 과거 교과서 사례에서 '한밤중에 전화를 계속 거는 행위'에 대해 지속적으로 소음을 발생시키므로 이를 폭행이라고 볼 수 있고 이는 가능한 확장해석이지만, 이를 주거침입으로 보는 것은 전형적인 '유추해석'이라고 설명된 바 있다.

구성요건이고, 주거침입죄의 경우 종래에는 견해의 대립이 있었지만, 현재는 사생활의 평온이 보호법익이라는 것이 학설[679]과 판례[680]의 대체적인 입장이다. 주거침입죄의 보호법익인 사생활의 평온은 주거공간 내에서 주거자의 의사에 따라 주거에 들어오거나 존재하는 사람이 결정될 수 있도록 하여 그에 따라 주거자가 주거 내에서 향유하는 안전과 평온한 상태라고 할 수 있다. 그런데 이러한 범죄의 보호법익에는 기술적 수단으로 인해 사실상 침해될 수 있는 사생활의 이익은 포함되지 않는 것으로 보인다. 우선 비밀침해죄는 비밀의 주체가 비밀로 처리한 특정의 문서나 기록 등을 대상으로 하는 것이므로 여기서 문제되는 주거 내의 일반적 사생활 자체는 그 대상이 아님이 명백하다. 그리고 주거침입죄의 보호법익인 사생활의 평온도 타인의 주거침입에 대한 통제를 통해 얻어지는 물리적인 의미의 공간적 평온함을 의미하는 것이기 때문에 기술적 수단을 통해 침해되는 사생활의 노출 그 자체를 보호의 대상으로 하고 있다고 보기 어렵다. 이는 주거침입죄가 '침입'을 전제로 한 규정이라는 점에서 도출되는 해석상의 한계인데, 다른 건물에서 망원경 등을 통해 주거의 열려진 창문 안쪽의 모습을 살펴보는 것이나 무선으로 조종하는 드론을 통해 고층아파트의 베란다 창문 밖 상공에서 창문 안쪽을 촬영하는 행위 역시 물리적 침입은 없으므로 이를 주거침입죄로 의율할 수는 없다. 사생활이 타인에게 의도치 않게 노출되는 것을 규제하는 현행법규로 통신비밀보호법상의 불법감청규제를 들 수 있으나 이는 보호의 대상이 대화에 한정된다. 따라서 현행법상으로 기술적 수단을 이용한 영상촬영, 음향녹음으로 인한 사생활의 노출 그 자체를 침해의 결과로 하는 구성요건은 존재하지 않는 상황이다.

사생활 자유의 주체가 의도치 않게 사생활이 노출당하는 것에 대해 이를 보호법익으로 하는 범죄구성요건이 존재하지 않는 것은 종래의 상황에서는 비밀로 설정된 문서 등의 개봉이나 탐지 등에 대한 규제와 물리적 침입에 대한 규제로 대상 법익이 충분히 보호되었다는 점에 기인한다고 볼 수 있다. 쉽게 말해 문을 닫고 못 들어가게

678) 김성돈, 앞의 책, 242면. 이에 대해 보호법익을 넓게 보아 '사생활의 평온'이라고 해석하는 견해(김일수/서보학, 새로쓴 형법총론 제6판, 박영사, 2005, 225면)도 있다.

679) 김성돈, 앞의 책, 250면 각주27 참조.

680) 「야간에 타인의 집의 창문을 열고 집 안으로 얼굴을 들이미는 등의 행위를 하였다면 피고인이 자신의 신체의 일부가 집 안으로 들어간다는 인식하에 하였더라도 주거침입죄의 범의는 인정되고, 또한 비록 신체의 일부만이 집 안으로 들어갔다고 하더라도 사실상 주거의 평온을 해하였다면 주거침입죄는 기수에 이르렀다.」 대법원 1995. 9. 15. 선고 94도2561 판결.

하면 문 안쪽의 사생활은 자연스럽게 보호가 되는 상황이었다는 것이다. 그러나 기술의 발달은 문을 닫아도 타인이 들어갈 수 있는 방법이 다변화되었다는 것을 의미한다. 이러한 상황의 변화는 사생활의 자유를 보호하기 위한 형사정책도 다양화된 접근과 그에 따른 피해발생을 염두에 두고 사생활의 의도치 않은 노출방지를 보호법익으로 하는 입법정책을 강구할 필요가 있다. 이에 대해서는 현재도 정보통신망 자체에 대한 침입을 규제하고 처벌하는 법이 존재하고, 기술적 수단에 의한 침입사례의 경우에도 정보통신망에 대한 침입규제는 주거침입죄와 같은 '출입규제'의 기능을 할 수 있으므로 굳이 사생활 자체를 직접적 보호법익으로 하는 형사정책이 필요한 것인가 하는 반론이 있을 수 있다. 그러나 정보통신망의 침해에 대한 규제는 정보통신망 자체의 안정성을 확보하기 위한 행정형법적인 성격이 강한 것이고, 전술한 바와 같이 실제로 사생활의 침해를 당하는 피해자를 직접적인 보호의 대상으로 하는 것이 아니어서 개인이 가지는 사생활의 비밀과 자유를 보호하는 형사입법으로는 부족하다고 보여진다. 더구나 여기서 중요한 것은 정보통신망의 침해행위 그 자체의 해악성이 문제가 아니라 그렇게 해서 개별 피해자에게 실제로 발생한 사생활 침해의 해악성이 중점적으로 다루어져야 한다는 점이므로 형법상의 보호법익으로 기술적 수단으로부터의 사생활 보호가 직접 고려되어야 한다는 것이다. 이에 다음과 같이 형법 제319조의2를 신설하여 기술적 수단을 이용한 사생활 침해를 처벌할 수 있는 형법적 근거를 마련할 것을 제안한다.

[표 5-1] 형법 제319조의2 신설안

현 행	개정안
제319조(주거침입, 퇴거불응) ① 사람의 주거, 관리하는 건조물, 선박이나 항공기 또는 점유하는 방실에 침입한 자는 3년 이하의 징역 또는 500만원 이하의 벌금에 처한다. ② 전항의 장소에서 퇴거요구를 받고 응하지 아니한 자도 전항의 형과 같다.	제319조(주거침입, 퇴거불응) (현행과 같음)
〈신 설〉	제319조의2 (기술적 수단을 이용한 사생활 침해) 기술적 수단을 이용하여 사람의 주거, 관리하는 건물, 선박이나 항공기 또는 점유하는 방실에 있는 전자기기나 통신기기 등을 조작, 통제하거나 이를 통하여 사생활에 대한 정보를 획득한 자는 제319조의 예에 의한다.

2) 사물인터넷을 이용한 방화

(1) 문제의 현황

사물인터넷 기술 발전으로 인해 자동차, TV, 냉장고는 물론이고 난방시설이나 방범시설 등도 네트워크로 연결되고 있다. 만약 차량을 해킹하여 브레이크가 작동하지 않도록 해서 사람을 살해하였다면, 범죄의 수단은 첨단화되었더라도 현행 형법상 살인죄로 처벌하는 데에는 큰 어려움이 없다. 그러나 네트워크에 연결되어 있는 보일러 온도조절장치나 전기레인지 등을 조작해서 과열로 인한 화재를 일으킨 경우에는 형법상 방화죄가 적용될 수 있는지 논란이 일고 있다. 현행법상 현주건조물방화죄의 행위는 '불을 놓아' 목적물을 소훼하는 것이라고만 규정되어 있는바, 사람이 직접 불을 놓지 않고 사물인터넷을 이용하여 화재를 일으킨 경우에도 동 규정을 적용할 경우 죄형법정주의의 명확성 원칙에 위배될 우려가 있는 것이다.

(2) 형법상 구성요건의 명확화: 사물인터넷을 이용한 방화죄 인정

현재 방화죄 규정에서 '불을 놓아'라는 행위는 '목적물을 소훼시키는 일체의 행위'라고 해석되고 있는데, 방화의 방법에는 제한이 없으며 직접 목적물에 방화한 것이든, 매개물을 이용하여 방화한 것이든 불문한다.[681] 그러므로 사물인터넷을 이용해 원격으로 불을 일으킨 것도 누전을 시켜 불을 내는 것과 같이 직접적인 '불'이 없더라도 방화의 방법으로 인정될 수 있는바 현행 형법으로도 충분히 처벌할 수 있다고 본다.

그러나 '불을 놓아'라는 문언은 그 행위 태양을 '불을 놓는 행위'로 특정하고 있는바, 사물인터넷을 조작해서 과열로 인한 화재를 일으킨 경우까지 포섭하는 것으로 해석한다면 이는 명확성의 원칙에 반할 수 있다. 더욱이 사물인터넷 디바이스 해킹을 통한 방화는 형법 제정 당시에는 미처 상정하지 못한 범죄 상황이고, 기술이 적용된 이후에도 아직 발생하지 않았다. 그러나 컴퓨터 상용화 이후에 기존 조문으로는 처벌의 공백이 발생했던 경험을 떠올린다면, 사물인터넷을 이용한 방화죄도 목적론적 해석으로 처벌할 수 있다고 쉽게 결론지으며 넘어갈 일은 아니다. 이에 현행 방화죄의 구성요건 중 '불을 놓아'라는 부분을 '직접 또는 도구나 통신 등을 이용해 불을 놓아'로 개정해야 한다는 의견이 제시된 바 있다.[682] 다만 이 경우 도구나 통신 등을 이용하는

681) 이재상/장영민/강동범, 형법각론 제11판, 박영사, 2019, 519면.

것으로 수단이 특정되면서 방화의 다양한 행위태양이 포섭되지 못할 우려도 제기된다. 이에 '불을 놓아'를 '불을 내어'라는 말로 바꾸는 방안도 모색될 수 있다. 나아가 사물인터넷을 이용한 방화는 범죄자가 화재 현장에서 떨어진 곳에서 자신의 안전을 확보한 상태로 범하고, 인터넷이라는 확장적 수단을 이용하여 대규모 피해를 야기할 수 있다는 점에서 별도의 구성요건을 신설하는 방안도 고려될 수 있을 것이다.

[표 5-2] 형법 제164조 개정안(1안)

현 행	개정안
제164조(현주건조물등에의 방화) ① 불을 놓아 사람이 주거로 사용하거나 사람이 현존하는 건조물, 기차, 전차, 자동차, 선박, 항공기 또는 광갱을 소훼한 자는 무기 또는 3년 이상의 징역에 처한다.	제164조(현주건조물등에의 방화) ① 직접 또는 도구나 통신 등을 이용해 불을 놓아----------.
② 제1항의 죄를 범하여 사람을 상해에 이르게 한 때에는 무기 또는 5년 이상의 징역에 처한다. 사망에 이르게 한 때에는 사형, 무기 또는 7년이상의 징역에 처한다.	② (현행과 같음)

[표 5-3] 형법 제164조 개정안(2안)

현 행	개정안
제164조(현주건조물등에의 방화) ① 불을 놓아 사람이 주거로 사용하거나 사람이 현존하는 건조물, 기차, 전차, 자동차, 선박, 항공기 또는 광갱을 소훼한 자는 무기 또는 3년 이상의 징역에 처한다.	제164조(현주건조물등에의 방화) ① 불을 내어----------.
② 제1항의 죄를 범하여 사람을 상해에 이르게 한 때에는 무기 또는 5년 이상의 징역에 처한다. 사망에 이르게 한 때에는 사형, 무기 또는 7년이상의 징역에 처한다.	② (현행과 같음)

682) 국회 법제실, 4차 산업혁명 입법과제, 2017.12, http://likms.assembly.go.kr/law/lawsLawyInqyList1011.do?mappingId=%2FlawsLawyInqyList1011.do&genActiontypeCd=2ACT1010&genDoctreattypeCd=DOCT2041&procWorkId=&workstepId=&repFlowId=&flowId=&workId=&workSno=&winWd=&winHg=&winTypeAttr=M&nextWinWd=&nextWinHg=&nextWinTypeAttr=&nextMappingId=&nextGenActiontypeCd=&dispNum=233&pageSize=10&genMenuId=menu_serv_nlaw_lawt_5010&srchNm=&pageNum=2&boardNo=4&articleNo=382471&srchType=title&back_dispNum=233&back_pageSize=10&back_genMenuId=menu_serv_nlaw_lawt_5010&back_srchNm=&back_pageNum=2&back_boardNo=4&back_articleNo=382471&back_srchType=&dumy=&orderType=&orderObj= (2019년 10월 23일 최종접속).

[표 5-4] 형법 제164조 개정안(3안)

현 행	개정안
제164조(현주건조물등에의 방화) ① 불을 놓아 사람이 주거로 사용하거나 사람이 현존하는 건조물, 기차, 전차, 자동차, 선박, 항공기 또는 광갱을 소훼한 자는 무기 또는 3년 이상의 징역에 처한다.	제164조(현주건조물등에의 방화) ① (현행과 같음)
② 제1항의 죄를 범하여 사람을 상해에 이르게 한 때에는 무기 또는 5년 이상의 징역에 처한다. 사망에 이르게 한 때에는 사형, 무기 또는 7년이상의 징역에 처한다.	② 전자기기나 통신기기 등을 조작, 통제하거나 이를 통하여 불을 내어 사람이 주거로 사용하거나 사람이 현존하는 건조물, 기차, 전차, 자동차, 선박, 항공기 또는 광갱을 소훼한 자도 제1항의 형과 같다.
③ 〈신 설〉	③ 전2항의 죄를 범하여 사람을 상해에 이르게 한 때에는 무기 또는 5년 이상의 징역에 처한다. 사망에 이르게 한 때에는 사형, 무기 또는 7년 이상의 징역에 처한다.

나. 암호화폐의 범죄적 이용에 대한 형법적 의미 규명

1) 암호화폐의 법적 성격

(1) 암호화폐의 화폐성(금전성)

블록체인 기술에 기반하여 전자적 형태로 발행되고 거래되는 암호화폐는 명칭상 '화폐(currency)'라는 표현이 사용되고 있어서 이것이 법적으로도 통화나 화폐와 같은 효력을 부여받을 수 있는 것인지가 논의될 수 있다. 비트코인을 비롯하여 대규모로 발행하는 암호화폐는 그 본질에 있어서 법정화폐 혹은 '명목화폐(fiat currency)'를 대체하는 지급수단의 기능을 추구한다.[683] 일단 암호화폐가 우리의 현행법상 법적으로 강제통용력을 가지는 '법화(法貨)'가 될 수 없음은 분명하다. 한국은행법 제47조는 "화폐의 발행권은 한국은행만이 가진다"고 하여 민간사업자는 화폐의 발행권을 가질 수 없다. 그런데 개념적인 정의에서의 화폐는 법화만이 해당하는 것이 아니라 시장에서 실질적으로 교환과 지급의 수단이 될 수 있고, 이에 대한 법적인 보호나 규율이

683) 비트코인의 경우 전 세계적으로 상당수 오프라인 매장에서 결제수단의 하나로 사용되고 있으며 비트코인으로 결제할 수 있는 상점을 찾아주는 인터넷 서비스(coinmap.org)도 존재한다. 한편 비트코인을 현금으로 인출해주는 비트코인 ATM도 2019년 10월 현재 전 세계에 5,800여 개가 설치되어 있다고 한다. Coin ATM Radar 웹페이지, https://coinatmradar.com/ (2019년 11월 4일 최종접속) 참조.

될 수 있는 것이라면 모두 포함되므로 이러한 점에서의 검토가 추가로 요구된다.

암호화폐는 한국은행이 발행하는 실물법정화폐와 달리 금전적 가치가 전자적 형태로 만들어지고 존재 내지는 이전하며, 종래의 물리적 재물개념에 의하면 실체가 없는 화폐이기 때문에 '가상지급수단' 혹은 '가상화폐'의 일종으로 볼 수 있으며, 이에 대해서는 전술한 바와 같이 법적 규율이 아직 이루어지고 있지 않은 상황이다. 관련하여 현행 전자금융거래법에는 '전자지급수단'의 일종으로 '전자화폐'라는 개념이 있다.

전자금융거래법

제2조(정의)

15. "전자화폐"라 함은 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보로서 다음 각 목의 요건을 모두 갖춘 것을 말한다.
    가. 대통령령이 정하는 기준(500개) 이상의 지역 및 가맹점에서 이용될 것
    나. 제14호 가목의 요건(발행인(대통령령이 정하는 특수관계인을 포함) 외의 제3자로부터 재화 또는 용역을 구입하고 그 대가를 지급하는데 사용될 것)을 충족할 것
    다. 구입할 수 있는 재화 또는 용역의 범위가 5개 이상으로서 대통령령이 정하는 업종 수(5개) 이상일 것
    라. 현금 또는 예금과 동일한 가치로 교환되어 발행될 것
    마. 발행자에 의하여 현금 또는 예금으로 교환이 보장될 것

전자금융거래법에 의해 전자화폐로 인정되기 위해서는 환금성과 일정 수 이상의 사용처 등이 확보되어야 한다. 보다 근본적으로 "전자화폐는 일반적으로 현실세계의 통화를 디지털로 표현한 것에 불과하며 단순히 진정한 통화로 표시되는 가치를 전자적으로 전송하기 위해 사용되는 수단을 의미하는 것으로 해석된다"[684]는 점에서 암호화폐를 전자화폐의 일종으로 포섭하기는 어렵다.

법원도 비트코인에 대해서 "가상화폐의 경우 일반적으로 재화나 용역을 구입하는 데 이용될 수 없고 가치의 변동 폭이 커서 현금 또는 예금으로의 교환이 보장되지 않으며, 주로 투기적 수단으로 이용되고 있으므로 전자금융거래법상의 '전자화폐'에 해당한다고 볼 수 없다"고 판시[685]하여 암호화폐의 화폐성을 부정하고 있다.[686]

---

684) 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 17면; 최호진, 앞의 글, 73면.
685) 서울중앙지법 2018. 12. 20. 선고 2017가합585293 판결.

(2) 암호화폐의 (민·형법상) 재산적 가치성

암호화폐는 디지털 정보의 형태로 존재하기 때문에 일단 민법상 물건이나 형법상 재물에 해당할 수는 없다.[687] 하지만 암호화폐가 일정하게 정해지는 시세 등으로 인하여 경제적으로 측정될 수 있는 재산적 가치를 가지고 있고, 실제로 거래의 대상이 되고 있으므로 민·형법상으로 재산적 권리 혹은 재산적 이익이나 가치로서는 평가될 수 있는 가능성이 있다.

우선 민법적으로는, 암호화폐에 대해 소유권에 준하는 민법적 권리를 부여할 수 있다는 주장이 있다. '공개형 블록체인(public blockchain)에 기반한 가상화폐는, 시스템 제공자와의 관계로부터 자유롭게 되어 지배의 제한이나 훼손 없이 존재하고 거래도 가능하다는 점에 주목하는 것이다. 그러므로 가상화폐를 보유한 자의 지배력은 비록 사이버공간에 한정하는 것이지만, 소유권과 유사한 독립적인 지배력으로 볼 수 있다고 한다.[688] 이는 가상화폐가 기존의 사이버 재화와는 달리 제공자를 벗어나 물건처럼 전면적으로 대세적인 지배가 가능한 새로운 형태의 사이버 재화가 되는 법리적 근거가 되기도 하고, 법정화폐의 대체가능성 주장의 근거로도 볼 수 있다.[689]

그러나 민법적 논의에서 (아직은) 암호화폐에 대해 물권적 권리객체성을 인정하는 입장이 주류로 받아들여지고 있지 않는 것으로 보인다.[690] 다만 현행법상 암호화폐가 개인 간의 거래대상이 될 수 있는 재화가 될 수 있는 것은 분명하고 암호화폐의 취득이나 소지가 법적으로 금지되어 있지 않는 이상 계약자유의 원칙 및 민법에 의해 당사자

---

686) 참고로 미국판례에는 화폐성을 인정한 경우가 있다. United States v. Anthony R. Murgio, S215 Cr. 769 (AJN) (S.D. N. Y. 2015), https://www.Justice.gov/usao-sdny/file/830616/download (2019년 10월 26일 최종접속). 이는 피고인들이 비트코인을 중개하는 회사를 설립하여 2013년 10월부터 2015년 7월 사이에 고객들로 하여금 수백만 달러 상당의 비트코인을 교환하도록 한 사건에서 피고인들의 이러한 행위를 허가 없이 자금이체업을 행한 혐의, 전신환 사기 혐의, 자금세탁 혐의 등을 유죄로 인정한 판결이다.

687) 이에 대해서는 형법상 재물에 대한 기준인 '관리가능성'을 물리적 관리가능성이 아닌 '동등관리가능성'이라는 개념으로 확장하여 현행법의 해석상으로도 암호화폐를 '재물' 개념에 포섭시킬 수 있다는 주장이 있다. 백대열/송희권, "형법상 재물과 재산상의 이익 간 구분 기준으로서의 관리가능성", 서울대 법학평론 제9권, 서울대학교 법학평론 편집위원회, 2019, 527면 이하.

688) 片岡 義広, "仮想通貨の私法的性質の論点", Libra Vol.17 No.4, 東京弁護士会, 2017.4., 12頁. (윤배경, "가상화폐의 법적 성질과 민·형사상 강제집행", 인권과 정의 474호, 대한변호사협회, 2018.6., 10면에서 재인용) 이 견해는 암호화폐에 '준물권'과 같은 법적 지위를 부여하자는 입장이다.

689) 박선종, "가상화폐의 법적 개념과 지위", 일감법학 제42호, 건국대학교 법학연구소, 2019, 149면. 박 교수는 이를 "종이에 인쇄된 신문이 아닌 인터넷 신문도 신문으로 인정받을 수 있는 것"에 비유한다.

690) 윤배경, 앞의 글, 10-11면 참조.

의 급부내용으로 허용될 수 있기 때문에[691] 당사자 간의 암호화폐에 대한 일정한 급부계약을 통해 형성되는 채권의 목적물로서의 성격은 충분히 가질 수 있을 것으로 보인다.[692]

민법상 채권의 목적물이 될 수 있다는 것은 형법상으로도 (비록 재물성은 가질 수 없다고 하더라도) 재산상 이익으로는 평가될 수 있음을 의미한다. 형법상 재산상 '이익'의 개념에 대해서는 이것이 순수한 경제적 이익을 의미하는 것인지, 아니면 법적으로 인정되고 승인된 것이어야 하는지에 대한 논란이 있지만 다수의 학설은 법적 승인의 여부와 관계없이 순수하게 경제적인 가치가 있으면 이익으로 인정하는 입장[693]이고, 판례[694] 또한 "재산상의 이득은 반드시 사법상 유효한 재산상의 이득만을 의미하는 것이 아니라 외견상 재산상의 이득을 얻을 것이라고 인정할 수 있는 사실관계만 있으면 된다"고 판시하여 경제적 이익설의 입장을 취하고 있다. 따라서 민법상 채권의 목적물이 될 수 있고 현실적으로 거래소에서의 시세에 따른 환금성을 가질 수 있는 암호화폐를 형법상으로도 일정한 재산적 가치를 가지는 재산적 이익으로 평가할 수 있고, 따라서 암호화폐는 형법상 '이득죄'의 객체가 될 수 있다.

2) 암호화폐에 대한 범죄와 법적 해석

이하에서는 암호화폐와 암호화폐의 거래행위에 대해 발생 가능한 혹은 이미 발생한 침해유형을 중심으로 현행법에 따른 형사실체법적 쟁점에 대하여 기술한다. 암호화폐를 이용한 각종거래행위(다크넷 등에서 암호화폐를 지급수단으로 사용하는 마약, 무기, 음란물 등의 거래)는 암호화폐가 범죄의 수단으로 이용되는 것일 뿐, 암호화폐 자체의 법적 성격이 해당 행위의 범죄구성요건해당성에 영향을 주는 것은 아니다. 암호화폐의 법적 성격과 관련하여 해석이 요구되는 새로운 유형의 범죄에 해당하는 경우는 암호화폐 자체를 탈취한 경우와 암호화폐 거래소에서의 소위 시세조종행위 사례이다.

---

691) 최호진, 앞의 글, 73면.
692) 윤배경, 앞의 글, 11면.
693) 타법제도와 관계없이 현실을 독자적으로 평가하는 형법의 독자성의 반영이다. 오영근, 형법각론 제4판, 박영사, 2017, 222면; 이영란, 형법학-각론강의-제3판, 형설출판사, 2013, 266면; 손동권, 형법각론 제3개정판, 율곡출판사, 2010, 316면; 정성근/박광민, 형법각론 전정판, 성균관대학교출판부, 2012, 281면 등.
694) 대법원 1987. 2. 10. 선고 86도2472 판결.

(1) 개인지갑의 암호화폐를 탈취하는 경우

개인지갑에 보관된 암호화폐 계정정보를 알아내어 피해자의 암호화폐를 자신 또는 제3자의 계정으로 이체하는 방식으로 암호화폐를 탈취하는 경우이다. 예를 들어[695] A가 직장 동료인 B의 지갑 주소(공개키) 및 프라이빗 키를 알게 되었고 이후 해당 지갑 주소에 접속하여 프라이빗 키를 통해 비트코인을 3개의 거래소를 경유하여 전액 이체하는 방식으로 탈취하였다면 A에게 적용되는 범죄는 무엇인가 하는 문제이다. 앞에서 살펴본 바와 같이 암호화폐는 민법상 금전 혹은 그에 준하는 소유권의 객체나 형법상 재물로 볼 수는 없기 때문에 이 사안을 형법상 절도죄(제329조)로 의율할 수는 없다고 할 수 있다.[696] 하지만 암호화폐를 재산상 이익으로 볼 수 있다면 이 사안의 경우 일정한 행위를 통해 타인에게 재산상 손해를 야기하고 자기 또는 제3자로 하여금 재산상 이익을 취득하도록 한 것으로는 볼 수 있다. 그리고 여러 대의 컴퓨터 등 전자적 처리장치를 이용하여 구현되는 블록체인기술의 특성상 타인의 계정정보를 이용하여 암호화폐를 거래하는 행위는 '권한없이 정보를 입력'하여 정보처리를 하게 한 경우에 해당할 수 있기 때문에 형법 제347조의2 컴퓨터등 사용사기죄로는 의율할 수 있을 것으로 생각된다. 만약 행위자가 몰래 알아낸 타인의 계정정보를 거래소에 제출하여 거래를 요청·위탁하는 방식으로 이체가 이루어졌다고 하더라도 이것이 거래소에 대한 일반적인 사기죄로 성립하는 경우는 드물 것이다. 거래소는 거래의 중계 역할만을 할 뿐 결국 재산적 이익의 이전은 블록체인 분산원장에 해당 블록이 생성되는 방식으로 이루어지는 것이므로 (간접적 방식으로) 컴퓨터에 권한 없이 정보를 입력하고 그에 따라 정보처리가 이루어지는 동일한 구조로 이해할 수 있다.[697] 정리하면 이 사안의 경우는 타인의 은행 계좌 정보를 이용하여 무단으로 타인의 은행예금을

695) 예시된 사례는 한서희, "가상자산 관련 범죄에 대한 연구 – 실제 사례를 중심으로", 한국형사정책연구원/블록체인법학회 공동학술대회 발표자료집, 2019.10.7., 24면의 사안을 재구성한 것임.

696) 이에 대해서는 전술한 바와 같이 '재물성'을 인정하여 절도죄의 객체로 볼 수 있다는 주장이 있으며, 한서희 변호사도 학술대회(2019.10.7.)에서 기본적으로는 절도죄로 의율해야 하는 사안인 것 같다는 견해를 구두로 피력한 바 있다.

697) 이 점에서 은행에 예치된 금전을 직접 지급받는 타인통장이용 인출행위와는 차이가 있다. 다만 현재 제출된 암호화폐 거래소에 대한 법률안에는 대부분 이용자 보호를 위하여 암호통화거래예치금 제도를 두도록 하고 있는데, 이 경우의 법률관계는 다소 달라질 수도 있을 것으로 보인다.

인터넷뱅킹이나 ATM기를 이용하여 자기 또는 제3자의 계좌로 이체하는 행위와 구조적으로 다르지 않다고 할 수 있고, 이는 형법상 컴퓨터등 사용사기죄로 의율될 수 있을 것이다.

(2) 암호화폐 거래소에서 담합에 의한 시세조종행위를 하는 경우

암호화폐 거래소에서의 시세는 기본적으로 일반적인 유가증권 거래시장과 마찬가지로 수요와 공급의 원리에 의하여 결정된다. 즉 수요보다 공급이 많으면 가격이 하락하고 그 반대의 경우면 가격이 오르는 식이다. 그리고 이에 더하여 이러한 시장은 수요자나 공급자가 각각 희망하는 매수, 매도 가격을 명시하여 요청하는 방식으로 거래가 이루어지기 때문에 수요와 공급의 단순한 숫자뿐만 아니라 수요와 공급의 다수가 원하는 가격, 즉 다수의 적정가격에 대한 의사의 내용이 중요한 시장이다. 따라서 이러한 시장은 시장의 방향성을 결정할 수 있을 정도의 다수 혹은 시장상황에 대한 정보우위에 있는 사람들이 의사의 합치에 이른 경우에는 그들의 의사에 의해 쉽게 시장의 가격을 결정할 수 있다. 현재 법적으로 적절한 관리와 감독이 이루어지고 있지 않고, 암호화폐 종류의 다양성만큼이나 다양한 규모의 거래소들이 난립하고 있는 상황에서 이른바 '작전세력'에 의한 가격의 의도적 형성, 즉 시세조종행위의 가능성과 위험성은 매우 높다고 할 수 있다. 더군다나 시세의 흐름이 기업의 가치와 거시경제적 지표 및 상황에 기반한 주식시장과 달리 암호화폐의 경우에는 순수하게 암호화폐 자체의 가치에 대한 투자자와 참여자들의 기대심리에 따라 시세가 결정되므로 거래참여자들의 심리에 영향을 줄 수 있을 만한 '세력'의 영향은 시세에 단기간에 크게 작용할 수 있고, 이러한 시세조종행위의 폐해는 기존의 자본시장과는 비교도 안 될 만큼 현저할 수 있다.[698]

현재 암호화폐 거래가 자본시장법의 적용을 받지 못하고 있는 상황에서 이러한 행위를 시세조종행위에 대한 처벌규정(제176조 및 제443조)으로 의율할 수는 없다. 이에 우선 해당 행위가 거래소에 대한 형법상 위계에 의한 업무방해죄(제314조)로 처벌될 수 있는지 검토할 수 있다. 시장의 원리에 의하여 형성되어야 할 거래소 시세를

698) 최근의 사건에서는 특정 코인 거래소의 협력회사 직원이 카톡방을 개설하여 참여자를 모집한 후 의도적으로 일시에 낮은 가격으로 매도하였는데 단 하루만에 해당코인의 가격이 1/10로 폭락했다고 한다(한서희, 앞의 발표자료, 17면에서 인용).

행위자들의 의도에 따라 인위적으로 변경되도록 하였다는 점에서 거래소에 대한 업무방해의 결과가 발생하였다고 볼 여지가 있다. 특히 업무방해죄의 성립에는 "업무방해의 결과가 실제로 발생함을 요하지 않고 업무방해의 결과를 초래할 위험이 발생하는 것이면 족하며, 업무수행 자체가 아니라 업무의 적정성 내지 공정성이 방해된 경우에도 업무방해죄가 성립"[699]하는 것이므로 시세의 비정상적 형성은 거래소의 업무를 방해하였다고는 볼 수 있을 것이다. 그런데 위계에 의한 업무방해죄가 성립하기 위해서는 시세조종행위에 가담한 자들이 담합하여 매도 혹은 매수 주문을 내는 행위가 허위사실 유포 혹은 위계행위에 해당해야 한다. 가담자들의 매도 혹은 매수 주문 자체는 허위의 의사표시가 아니므로 허위사실의 유포에 해당할 수는 없을 것이고, 이것이 상대방에게 오인, 착각 또는 부지를 일으키게 하는 것인 위계행위에 해당하는지 여부가 문제될 수 있을 것인데, 이때의 위계 역시 단순히 상대방의 판단력을 흐리게 하거나 행위자의 의도대로 판단하도록 하는 일체의 행동이라고 넓게 볼 수 있는 것은 아니고,[700] 허위사실의 유포에 준하여 일정한 사실관계를 왜곡, 축소, 은폐하는 등의 조작행위가 있어야 할 것으로 생각된다. 그러므로 단순히 담합에 의하여 다수가 일정한 의사표시를 동시다발적으로 하는 행위를 거래소에 대한 위계행위라고 보기는 어렵다.

한편 시세조종행위의 실질적 피해자는 거래소의 거래에 참여한 다른 참여자들이라고 할 수 있는데, 설령 시세조종행위를 위계에 의한 업무방해행위의 성격을 가진 것이라고 하더라도 여기서의 업무 주체는 거래소에 한정될 것이고 거래에 참여한 사람들에게는 해당 업무의 주체성을 인정하기는 사실상 곤란하기 때문에 역시 업무방해죄를 성립시키기는 어려울 것으로 생각된다.[701][702]

다만 이러한 담합을 통한 매도, 매수 주문을 내기 위해 가담자들은 사전에 동일인이

699) 대법원 2008. 1. 17. 선고 2006도1721 판결.

700) 위계의 개념을 이렇게 넓히면 단순한 설득이나 유혹 등의 행위도 위계에 해당할 수 있어서 부당하다.

701) 이러한 해석상의 난점으로 인해 자본시장법은 별도의 시세조종행위에 대한 구성요건과 처벌규정을 두고 있는 것이라고 이해할 수 있다.

702) 추가로 시세조종을 위한 매도 주문 등을 내는 행위가 거래소 서버 등에 전자적 정보의 형태로 전송되어 입력되므로 형법 제314조 제2항의 컴퓨터등에 대한 장애 업무방해죄의 성립 여부도 검토해 볼 수 있으나, 역시나 이러한 행위가 '부정한 명령'이나 '정보처리에 대한 장애'에 해당한다고는 보기 어려우므로 해당 조문으로 의율할 수 없을 것이다.

(명의자가 다른) 다수의 계정을 만들고 그러한 계정들을 이용한 활동을 (계정주인의 직접적 활동인 것처럼 가장하여) 동일인 혹은 몇몇 소수인이 수행하였다면 이는 정보통신망법 위반행위에 해당할 가능성이 있다. 정보통신망법 제48조 제1항은 "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다."라는 규정을 두고, 이를 위반한 경우 5년 이하의 징역이나 5천만원 이하의 벌금으로 처벌(정보통신망법 제71조 제1항 제9호)할 수 있도록 하고 있다. 이 규정에서 '접근권한이 없는 경우'의 해석에 대해서 대법원 판례는 다음과 같이 판시하여 이는 해당 계정이나 접근수단의 명의자가 아니라 정보통신서비스를 제공하는 서비스제공자의 의사에 따라 판단되어야 한다는 입장이다.

> "정보통신망 이용촉진 및 정보보호 등에 관한 법률은 그 보호조치에 대한 침해나 훼손이 수반되지 않더라도 부정한 방법으로 타인의 식별부호(아이디와 비밀번호)를 이용하거나 보호조치에 따른 제한을 면할 수 있게 하는 부정한 명령을 입력하는 등의 방법으로 침입하는 행위도 금지하고 있다고 보아야 한다. (중략) (해당 규정은) 이용자의 신뢰 내지 그의 이익을 보호하기 위한 규정이 아니라 정보통신망 자체의 안정성과 그 정보의 신뢰성을 보호하기 위한 것이라고 할 것이므로, 위 규정에서 접근권한을 부여하거나 허용되는 범위를 설정하는 주체는 서비스제공자라 할 것이고, 따라서 서비스제공자로부터 권한을 부여받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우 그에게 접근권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단하여야 한다. 이용자가 자신의 아이디와 비밀번호를 알려주며 사용을 승낙하여 제3자로 하여금 정보통신망을 사용하도록 한 경우라고 하더라도, (중략) 사회통념상 이용자가 직접 사용하는 것에 불과하거나, 서비스제공자가 이용자에게 제3자로 하여금 사용할 수 있도록 승낙하는 권한을 부여하였다고 볼 수 있거나 또는 서비스제공자에게 제3자로 하여금 사용하도록 한 사정을 고지하였다면 서비스제공자도 동의하였으리라고 추인되는 경우 등을 제외하고는, 원칙적으로 그 제3자에게는 정당한 접근권한이 없다고 봄이 상당하다."[703]

이러한 해석에 의하면 담합에 따른 집단적 행위를 실행하기 위하여 타인명의의 계정을 동일인이 다수 생성하고 이를 이용하여 실행한 행위는 정보통신망법 제48조 제1항에 의한 정보통신망 침해행위로 평가될 수 있다.

(3) 소결

암호화폐 자체에 대한 전자적 방식의 탈취행위는 컴퓨터등을 이용한 권한 없는 자금의 이체 등과 같은 구조로 보아 절도죄가 아닌 형법상 컴퓨터등 사용사기죄로

703) 대법원 2005. 11. 25. 선고 2005도870 판결.

의율할 수 있을 것으로 보인다. 그러나 암호화폐 거래나 거래소에 대한 시세조종행위 등은 현행 형법의 범죄구성요건으로는 포섭하기에는 난점이 있다. 암호화폐 거래나 거래소의 특성상 비교적 소수의 담합만으로도 거래시장에 큰 혼란을 야기할 수 있으므로 암호화폐 거래소에 대한 근거법령을 입법하는 과정에서 시세조종행위나 미공개정보이용행위에 해당하는 시장교란행위 등에 대한 금지 및 처벌규정이 마련될 필요가 있다. 아울러 담합행위를 통한 시세조종행위의 과정에서 다수 타인의 계정 등을 이용하는 행위는 현행 정보통신망법에 의해서도 규제와 처벌의 대상이 될 수 있으나 이러한 행위의 위법성을 보다 명확히 하기 위해서 암호화폐 발행과 거래에 대한 근거법령에 관련 규정을 추가할 필요가 있어 보인다.

3) 암호화폐에 대한 형벌의 부과 – 몰수의 대상

(1) 2018년 대법원 판결 이전의 논의

암호화폐나 암호화폐 거래를 대상으로 하는 재산범죄 뿐만 아니라 암호화폐를 불법거래의 수단으로 사용한 경우, 그러한 행위를 통하여 범죄자가 취득한 암호화폐는 범죄의 수익으로 평가될 수 있고 형법상 부가형인 몰수의 대상이 될 수 있다. 그러나 종래는 암호화폐의 발행과 거래에 대한 법적 근거가 없고 암호화폐에 대해 법적으로 재산적 가치가 인정될 수 있는 것인지가 모호하다는 점으로 인해 범죄자들이 범죄행위를 통하여 취득하였고 특정되어 있는 암호화폐가 형법상 몰수의 대상이 될 수 있는지에 대해서는 논란이 있었다. 학설은 대체로 형법상 몰수에 대한 근거규정인 형법 제48조는 '물건'을 그 대상으로 하고 있으므로 디지털 형태의 전자정보인 암호화폐는 재산적 가치를 인정할 수 있다고 하더라도 형법상 몰수의 대상이 되지는 않는다고 보는 입장이었다.[704] 그런데 몰수에 관한 특별법인 「범죄수익은닉의 규제 및 처벌 등에 관한 법률」(이하 '범죄수익은닉법'이라 함)에서는 '중대범죄'를 대상으로 하여 범죄수익이 '재산'인 경우에도 몰수할 수 있는 것으로 규정하고 있다. 이에 종래의 논의는 범죄수익은닉법에 의한 암호화폐의 몰수는 가능할 수 있을 것으로 해석하는 입장이 많았다.[705]

---

704) 최호진, 앞의 글, 66면 참조. 반면 형법 제48조 제3항의 반대해석상 전자기록 등의 전부가 몰수대상인 경우에는 폐기가 아닌 몰수가 가능하다고 해석하는 입장도 있다. 정성근/박광민, 형법총론 전정판, 성균관대학교출판부, 2013, 294면.

(2) 암호화폐의 몰수를 인정한 2018년 대법원 판결의 내용과 의미

2018년 5월 대법원은 아동음란물을 유포하는 인터넷사이트를 운영하면서 음란물 유포죄와 도박개장방조죄를 범하는 대가로 비트코인을 취득한 범죄자들에 대해 그들이 취득한 비트코인을 몰수할 수 있다는 취지로 판결[706]하였다. 종래 학설상으로 논의되던 범죄수익인 암호화폐의 몰수 대상성 여부에 대해 사법부가 내린 최초의 확정적 판단으로, 그동안 암호화폐의 발행과 거래에 대해 소극적이고 무대응으로 일관해 온 우리나라 암호화폐 법정책에 의미 있는 전환점을 마련해 준 것으로 평가할 수 있다. 이 판결은 판시사항을 통해 암호화폐의 한 종류인 비트코인을 몰수의 대상으로 볼 수 있는 이유를 다음과 같이 설시했다.

> "비트코인은 경제적인 가치를 디지털로 표상하여 전자적으로 이전, 저장 및 거래가 가능하도록 한, 이른바 '가상화폐'의 일종인 점, 피고인은 위 음란사이트를 운영하면서 사진과 영상을 이용하는 이용자 및 음란사이트에 광고를 원하는 광고주들로부터 비트코인을 대가로 지급받아 재산적 가치가 있는 것으로 취급한 점에 비추어 비트코인은 재산적 가치가 있는 무형의 재산이라고 보아야 하고, 몰수의 대상인 비트코인이 특정되어 있다."

정리하면 대법원이 비트코인을 몰수의 대상이 될 수 있다고 보는 근거는 크게 세 가지이다.[707]

첫째는 비트코인이 가상화폐의 일종이라는 점이다. 비트코인을 비롯한 암호화폐는 우리나라의 현행법상으로는 실체적 근거가 없는 것이지만 인터넷과 같은 가상세계에서 화폐와 같은 지급수단으로 기능할 것을 목적으로 만들어지고 사람들 간에 거래의 대상이 되고 있다는 현실적 모습을 형사법적으로도 인정할 수 있다는 것이다.

둘째는 비트코인의 재산적 가치가 인정된다는 점이다. 해당 비트코인은 당사자들이 일정한 재산적 거래관계의 대가로 실제로 지급하고 지급받은 것이어서 거래의 대가라는 측면에서 재산적 가치성이 인정되는 무형의 재산으로 볼 수 있다는 것이다.[708]

---

705) 2018년 대법원 판결이 나오기 이전까지의 암호화폐 몰수와 관련한 논의의 상세한 내용으로는 연성진/전현욱/김기범/신지호/최선희, 앞의 보고서, 124-128면 참조.

706) 대법원 2018. 5. 30. 선고 2018도3619 판결.

707) 이 판결에 대한 평석으로는 최호진, 앞의 글, 60면 이하.

708) 이 점에 대해서 원심판결은 게임머니를 부가가치세법상의 '재화'에 해당한다고 본 다음의 대법원 판결을 참고하였다고 한다. 대법원 2012. 4. 13. 선고 2011두30281 판결: 과세관청이,

셋째는 비트코인은 특정성이 있다는 것이다. 비트코인을 비롯하여 블록체인 분산원장 기술을 이용한 암호화폐의 경우에는 한번 생성되면 기록이 (블록체인 전체를 말소하지 않는 한) 변경되지 않고 조작이 불가능하여 영구적인 동일성이 인정되고, 암호화된 개인키로 접근할 수 있는 암호화폐의 정보는 다른 정보와는 구별되는 특정성을 가지며, 암호화폐가 이체(이전)된 경우에도 일반적인 전자정보처럼 복사되는 것이 아니라 정보의 고유성과 동일성은 유지되는 것이라는 점에서 전자기록임에도 유형물과 같은 특정성을 가진다는 것이다.

암호화폐의 형태와 종류 등이 매우 다양하고 변형된 형태가 계속 개발되고 있는 시점에서 비트코인이 몰수의 대상이 될 수 있다고 판단한 대법원의 판결이 암호화폐의 발행과 거래에 대한 법적인 차원에서의 전면적 수용으로 이어진다고 보기는 어렵다.[709] 그러나 법적인 판단의 영역에서 암호화폐의 실체 자체를 긍정적으로 인정하고 이에 대한 재산적 가치의 존재를 인정했다는 점은 어떤 식으로든 암호화폐의 발행과 거래에 대한 법적 규율이 필요하다는 신호로서의 의미는 충분히 부여할 수 있으며, 형사절차법적인 측면에서도 현재 아무런 규정이 없는 암호화폐의 몰수에 관련한 실무적 절차나 방법 그리고 몰수된 암호화폐를 처분하기 위한 절차규정 등에 대한 입법적 과제를 연구자들과 입법자들에게 부과하고 있는 것이다.

2. 형사절차법적 대응 방안

가. 온라인 수색 제도 도입

인터넷을 기반으로 하는 사이버공간은 물리적 제약을 뛰어넘는 연결성을 핵심으로

게임아이템 중개업체의 인터넷 사이트를 통해 온라인 게임 '리니지'에 필요한 게임머니를 게임제공업체나 게임이용자에게서 매수한 후 다른 게임이용자에게 매도하고 대금을 중개업체를 경유하여 지급받은 갑이 사업자로서 게임머니를 판매하면서도 매출신고를 누락하였다는 이유로 갑에게 부가가치세 부과처분을 한 사안에서, 게임머니는 구 부가가치세법상의 '재화'에 해당하고, 갑의 게임머니 매도거래는 재화의 '공급'에 해당하며, 갑은 부가가치를 창출해 낼 수 있는 정도의 사업형태를 갖추고 계속적이고 반복적인 의사로 재화인 게임머니를 게임이용자에게 공급하였다고 봄이 타당하므로 구 부가가치세법상의 '사업자'에 해당한다고 보아 부가가치세 부과처분이 적법하다고 한 원심판단을 수긍한 사례.

709) 이 판결이 나온 직후 금융위원회의 관계자는 "대법원은 범죄수익으로 얻은 비트코인을 몰수할 수 있을지를 판결한 것일 뿐"이고 "암호화폐 및 거래소 제도화와 관련한 정부 입장에는 영향을 미치지 않는다."고 발언하면서 판결의 의미에 대해 선을 긋는 태도를 보였다. "대법 "비트코인도 재산" 시장은 기대, 정부는 "화폐 아니다"", 중앙일보 2018년 5월 31일자, https://news.v.daum.net/v/20180531005521406 (2019년 11월 4일 최종접속).

하지만 네트워크는 모든 참여자에게 자유로운 접근성이 허용되는 것이 아니다. 접근을 위한 여러 가지 조건을 부가하여 참여자에게 접근성을 선별적으로 부여할 수 있으며, 애초부터 접근을 위한 방식을 기술적으로 특화하여 네트워크 참여자들이 해당 사이버 영역의 존재 자체를 모르게 할 수도 있다. 그런데 사이버 공간에서의 범죄를 비롯한 대부분의 불법행위는, 범죄를 은폐하고자 하는 인간의 본성상 너무나도 당연하게도, 접근성이 제한된 영역이나 일반적인 참여자들이 인지할 수 없는 영역에서 이루어진다. 이른바 딥웹(Deep Web) 혹은 다크넷(Darknet) 이라고 불리는 영역으로, 이러한 영역과 같이 익명성과 비밀성이 보장된 인터넷을 이용한 불법거래 등에서는 마찬가지로 거래의 익명성이 보장되는 암호화폐가 주된 거래의 수단이 된다. 암호화폐와 관련한 다수범죄의 양상은 필연적으로 딥웹이나 다크넷에서의 범죄양상과 연결되어 있으며 따라서 암호화폐와 관련한 형사적 대책은 딥웹이나 다크넷에서의 범죄를 수사하기 위한 법적, 정책적 대책과 긴밀한 연관성을 가질 수밖에 없다. 이하에서는 딥웹이나 다크넷과 같이 폐쇄형 가상공간상에서 일어나는 행위를 수사하기 위한 새로운 수사방법의 필요성과 함께, 이러한 수사방법의 도입과 활용을 위해서는 형사소송법 등 관련법규의 정비가 수반되어야 하므로 비교법적 자료를 바탕으로 하는 법제도적 논의도 함께 검토한다.

1) 온라인 수색의 정의와 현황

온라인 수색이란 수사기관이 여러 가지 기술적 수단을 이용하여 당사자의 IT 시스템에 비밀리에 접근하여 대상시스템의 이용을 비밀리에 감시하거나 절차상 중요한 저장매체의 내용을 열람하기 위해 거기에 저장된 데이터를 수사기관이 비밀리에 전달하는 것을 의미한다.[710] 온라인 수색은 범죄혐의자의 컴퓨터 등에 스파이웨어를 설치하는 등의 방식을 이용하여 범죄혐의자가 수색을 당한다는 사실을 알지 못한다는 점에 그 특징이 있다. 온라인 수색은 일회에 한하여 타인의 컴퓨터시스템에 저장된 데이터를 복제하기 위해서 비밀리에 접근하는 '온라인 검열'과 다수 장기간 작동 중인 컴퓨터시스템의 이용 상황을 비밀리에 감시하는 '온라인 감시'로 구분된다.[711] 온라인

710) 박희영, "예방 및 수사목적의 온라인 비밀 수색의 허용과 한계", 원광법학 제28권 제3호, 원광대학교 법학연구소, 2012, 154면; 박웅신/이경렬, 앞의 글, 237면.
711) 박희영, 앞의 글, 154면.

수색은 '트로이 목마'[712] 프로그램을 범죄혐의자의 컴퓨터에 심는 방식으로 이루어지고, 프로그램을 침투시키는 방법은 이메일의 첨부파일을 이용하는 방식[713]과 컴퓨터 운영체제의 보안상 취약점을 이용하는 방식[714]이 있다.[715]

현재도 수사기관에서는 현실적 필요성으로 인해서 실무상 특정한 범죄에 한해 관련자의 진술, 악성코드나 소스코드 분석을 통해 계정과 비밀번호를 알아내 수색을 집행하고 있는 듯하다.[716] 현행법상으로는 온라인 수색은 비밀수사[717]의 한 형태이기 때문에 원칙적으로 영장의 사전제시를 요건으로 하는 압수수색에 관한 형사소송법 규정이 적용될 수 없다.[718] 그러므로 이러한 방식의 온라인 수색을 정당화하기 위해서는 형사소송법에 온라인 수색의 허용요건과 절차에 관한 규정을 명문화하는 것이 필요하다.

2) 독일 형사소송법상 온라인 수색 규정

독일은 2017년에 아래와 같이 온라인 수색을 실시할 수 있는 근거규정과 이에 대한 대상, 절차 등을 명시하는 규정을 형사소송법에 신설하였다.

독일 형사소송법 제100조b(온라인 수색)[719]

① 다음 각 호의 어느 하나에 해당하는 경우 당사자가 이를 알지 못하더라도 당사자가 이용하는 정보기술적 시스템에 침입할 수 있고 이로부터 정보를 수집할 수 있다.

1. 제2항에 열거된 중범죄의 정범 또는 공범으로서 수행했다는 혐의 및 미수를 처벌하는 사례에서 실행에 착수하였다는 혐의의 근거가 되는 사실이 있는 경우
2. 개별사례에 비추어 범행의 중대성이 인정되는 경우
3. 사실관계의 조사나 피의자의 소재에 대한 수사가 다른 방법으로는 현저히 어려움을 겪거나 불가능할 것으로 예상되는 경우

712) 줄여서 'Trojaner'라고도 한다.
713) 전통적인 방식으로, 수신인이 첨부된 파일을 열었을 때 컴퓨터에 스파이웨어가 심어진다.
714) 윈도우의 보안상 취약한 부분에 바이러스 프로그램을 삽입하여 사용자가 시스템에 접속하기만 해도 바이러스가 침투되는 방식이다. 2017년 전 세계 약 23만대의 컴퓨터를 공격한 랜섬웨어 '워너크라이(Wanna-Cry)'도 이런 방식으로 전파되었다.
715) 이에 대한 상세한 설명으로 허 황, "최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신감청에 관한 연구", 형사법의 신동향 제58호, 대검찰청, 2018, 101-103면 참조.
716) 정대용/김기범/권헌영/이상진, "디지털 증거의 역외 압수수색에 관한 쟁점과 입법론-계정 접속을 통한 해외서버의 원격 압수수색을 중심으로-", 법조 제65권 제9호, 법조협회, 2016.12., 146면 참조.
717) 수사의 대상자가 수사가 이루어진다는 것을 알지 못하는 방식의 수사를 말한다.
718) 박희영, 앞의 글, 167면; 허 황, 앞의 글, 125면.

② 제1항 제1호에 해당하는 중범죄는 다음과 같다.

1. 형법
   a) (세부조문번호 생략. 이하 같음) 내란죄, 민주적 법치국가를 위협하는 죄, 외환죄와 공적 안전을 위협하는 범죄
   b) 범죄단체조직죄와 테러단체조직죄
   c) 화폐 및 유가증권 위조의 죄
   d) 성적 자기결정권을 침해한 죄
   e) 아동 및 청소년이 등장하는 음란물의 유포, 취득, 소지
   f) 모살과 고살
   g) 인신매매, 강제성매매와 강제노역죄, 자유박탈 이용하의 착취
   h) 범죄단체구성절도와 범죄단체구성중절도
   i) 중강도와 강도치사
   j) 강도공갈죄와 특별히 중한 경우의 공갈죄
   k) 영업적인 장물취득, 범죄단체구성 장물취득 및 영업적인 범죄단체구성 장물취득
   l) 특히 중한 경우의 금전세탁 및 불법영득재산의 은닉; 단 중범죄 중 하나로부터 대상물이 취득되었을 때
   m) 특별히 중한 경우의 수뢰와 증뢰죄
2. 망명절차법
   a) 망명신청남용을 목적으로 하는 호도행위
   b) 망명신청남용을 목적으로 하는 영업적 및 범죄단체구성을 통한 호도행위
3. 외국인체류법
   a) 외국인의 불법유입
   b) 인명의 손실을 야기한 불법유입과 영업적 및 범죄단체 구성을 통한 불법유입
4. 마약류법
5. 전쟁무기통제에 관한 법률
6. 국제형법
   a) 인종학살
   b) 인간성에 반하는 죄
   c) 전쟁범죄
   d) 공격죄
7. 무기법

③ 이러한 처분은 피의자에 대해서만 허용된다. 타인의 정보기술시스템에 대한 침입은 특정사실에 의거 다음 각 호가 인정될 때 허용된다.

1. 제100조e 제3항의 영장에 표시된 피의자가 타인의 정보기술시스템을 이용하고 있고,
2. 피의자의 정보기술시스템에 대한 침입의 집행만으로는 공동피고인의 사실 또는 현재지의 조사로 이어지지 않는다는 점
   타인이 불가피하게 개입된 경우에도 동 조치는 집행될 수 있다.

독일의 온라인 수색 규정에 의하면 중대한 범죄를 저질렀거나 시도하려는 현저한 사실상의 근거가 있는 범죄자(공범 포함)에 대한 수사가 다른 방법으로는 현저히 곤란하거나 전망이 없는 경우, 대상자가 알지 못하는 상태에서 기술적 수단들로 대상자에 의해 이용되는 정보기술시스템에 침입할 수 있고, 데이터를 수집할 수 있다.

독일 연방헌법재판소는 현행과 같은 형사소송법의 입법이 있기 전인 2008년 기술적 수단을 통한 온라인 수색을 허용한 노르트라인 베스트팔렌주의 헌법보호법 규정에 대해 위헌취지의 결정을 내리면서 이러한 온라인 수색이 정당화되기 위한 요건을 다음과 같이 설시하였다. 우선 아주 중요한 법익에 대한 구체적인 위험이 발생했다고 볼 수 있는 실제의 근거가 있어야 한다. 여기서 중요한 법익으로 신체, 생명, 인간의 자유 그리고 국가의 기초와 존립 및 인간존재의 기초에 있어 중요한 일반적 이익을 들 수 있고, 생존을 보장하는 공공급부시설의 본질적인 부분의 기능도 여기에 포함된다고 한다.[720] 정보기술적 시스템에 대한 은밀한 침투는 개별 사안에서 특정 인물들에 의해 앞서 말한 법익에 대한 위험이 야기되었음이 특정 사실에 의해 뒷받침되는 한 그 위험이 근래에 실현될 것이라는 점이 충분한 개연성을 가지고서 확정되지 않더라도 정당화될 수 있다고 한다.[721] 이 경우에 온라인 수색명령은 전적으로 독립적이고 중립적인 법관에 의해서 이루어져야 하고 이러한 처분권한을 부여하는 법률은 반드시 개인적 생활형성의 핵심영역을 보호하기 위한 장치를 마련해야 한다고 하였다.[722] 이후 독일연방헌법재판소는 2016년 온라인 수색에 대한 근거규정을 둔 독일연방수사청법에 대한 일부위헌 취지의 판결을 하면서 온라인 수색에 대한 정당화요건으로 다음의 내용을 제시하였다.

---

719) 번역은 허 황, 앞의 글, 118-119면에서 인용.

720) BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. 247.(번역은 허 황, 앞의 글, 110면에서 인용)

721) BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. 251(번역은 허 황, 앞의 글, 111면에서 인용)

722) BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. 257 ff.(번역은 허 황, 앞의 글, 111면에서 인용)

"입법자는 데이터의 선별·이용단계에서 안전장치를 확보함으로써 그러한 부작용을 최소화하여 당사자를 보호해야만 한다. 다시 말해 본 조항에는 수집된 데이터를 선별하는 기관의 독립성이 충분히 보장되어 있지 않으며, 데이터의 선별은 본질적으로 수사기관 내부의 보안업무를 맡은 직원이 아니라 외부의 자에게 그 임무가 부여되어야 한다는 것이다."[723]

3) 온라인 수색 규정의 도입 필요성

온라인 수색은 디지털증거의 수집을 위해 매우 효과적인 것은 사실이지만 이에 대해 법적으로 제도화하는 것에 대해서는 반대의 의견도 적지 않다. 근본적으로 온라인 수색을 도입하려는 논의에 대해서는 "디지털 정보에 의한 감시와 분석 기술이 더 강력해지고 효율적으로 될수록 국가는 영장주의나 다른 절차적 기본권 보장 장치를 잠탈하고서라도 문제 발생 이전에 잠재적인 문제아들을 더 효과적으로 잡아내고자 하는 욕구를 강하게 갖게 된다"[724]는 문제제기가 있다. 온라인 수색을 반대하는 입장의 주된 논거는 관련성을 좁게 해석하는 전제에서 영장주의의 침탈을 초래한다는 데에 있다.[725] 정보통신망의 수색을 가능하게 하는 영장을 발부받아 이를 집행한다고 하더라도 그 영장은 위헌적인 영장이 되어 그로 인해 수집한 전자증거의 증거능력이 위법수집증거로서 배제될 수 있다고 해야 한다고 주장하며,[726] 나아가 설령 법관의 영장을 발부받아 행해진다고 하더라도 온라인 수색은 밀행적으로 이루어지는 수사활동으로서 형사소송법 제121조 및 제123조에 의해 보장되는 피의자, 변호인, ISP 등 전자정보 저장장치의 소유자, 보관자 또는 관리자의 참여권을 배제하는 위법한 수사가 된다는 입장이다.[727]

하지만 디지털 증거의 압수방법에 대한 '원칙적 선별압수, 예외적 매체압수' 원칙이 실제로는 역전현상이 많이 발생하고 있는 현실에서 온라인 수색만이 국민의 기본권

723) BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09, Rn. 223f.(번역은 이상학, "테러방지 수권규정과 기본권침해의 한계 - 독일연방수사청법의 테러방지권한에 대한 연방헌법재판소의 판결(2016.4.20.) 검토를 중심으로", 공법학연구 제17권 제3호, 한국비교공법학회, 2016, 120면에서 인용).

724) Jack M. Balkin, "The Constitution in the National Surveillance State", Minnesota Law Review, Vol.93 No.1, University of Minnesota Law School, 2008.11., p.16.

725) 오기두, "정보통신망 모니터링에 의한 범죄통제의 적합성", 형사정책연구 제27권 제4호, 한국형사정책연구원, 2016, 25-26면.

726) 오기두, 앞의 글, 27면.

727) 오기두, 앞의 글, 27면.

침해를 증대시키는 것은 아니다. 이는 대량성과 네트워크 관련성을 가지는 디지털 정보에 대한 압수수색의 숙명이라 볼 수 있다.[728] 다방면으로 확산되어 많은 범죄자들이 딥웹과 다크넷을 무대로 범죄를 실행하고 있는 상황에서 온라인 수색이 가지는 밀행성과 일방성으로 인해 그 방법 자체가 헌법적으로 허용될 수 없다는 견해는 국가가 범죄에 적절히 대처해야 하는 기능 자체를 부정하지 않는 이상 적절하다고 할 수 없다. 수사비례의 원칙에 비추어 보더라도 비밀의 영역에 대한 수사를 공개적 방식만을 사용하라는 것은 타당하지 않다. 헌법적 원칙에 충실하여 국가의 처분으로부터 국민의 기본권 보호에 충실한 독일의 경우에도 이러한 온라인 수색을 입법화한 것에 비추어, 독일의 입법과정에서 독일헌법재판소가 제시한 원칙을 같이 고려하여, 우리나라에도 온라인 수색에 대한 근거와 절차규정이 입법될 필요가 있다고 보여진다. 다만 온라인 수색 규정을 우리나라에 도입하더라도 이러한 강제처분이 아니면 수사나 예방활동이 도저히 불가능한 경우가 도대체 어떤 경우인지에 대한 해석론상의 확인과 정리가 선행되어야 할 것이다.[729]

나. 비밀수사관 제도 도입

1) 다크넷과 함정수사

사물인터넷이나 암호화폐 범죄의 주된 실행무대가 다크넷 등의 인터넷 사이버 공간이고 범죄실행의 단서, 범죄행위의 증거도 모두 네트워크에 연결된 사이버 공간과 전자통신기기에서 찾을 수 있는 상황이므로 이에 대한 (범죄예방활동을 포함한) 수사활동도 네트워크와 사이버 공간을 직접 대상으로 하여 이루어질 수 있어야 한다. 특히 다크넷과 연계된 암호화폐범죄 수사를 위해선 함정수사방식이 필수적이라고 할 수 있다. 다크넷은 딥웹[730]의 영역 중 의도적으로 숨겨져 있으며 구글과 같은 검색엔진으로 접속할 수 없는 인터넷의 숨겨진 영역이다. 다크넷은 익명성을 요구하

728) 박웅신/이경렬, 앞의 글, 241면.
729) 같은 취지로 허 황, 앞의 글, 134면.
730) 딥웹(Deep Web)은 '표면웹(Surface Web)'에 반대되는 개념으로 인터넷 영역 중 일반인의 공개적 검색과 접속이 가능하지 않고, 접속을 위해서는 일정한 절차나 요건이 별도로 요구되는 영역을 말한다. 즉 접속을 위해서는 로그인 등의 절차가 필요한 경우 등과 같은 폐쇄적 인터넷 영역을 일컫는다.

는 이용자들을 위한 영역[731]이며, 이를 위해 해당 영역의 정보들은 암호화되고 그 접속에 특별한 프로그램[732]을 이용하고 있으며, 접속의 과정에서도 해당 영역의 개설과 이용 취지에 부합하는 이용자인지 여부를 검증하는 절차를 거치도록 한다. 이러한 다크넷의 특성, 특히 '인증절차'를 요구하는 폐쇄성은 다크넷에 대해 "조직범죄단체가 수사권으로부터 자유로운 영역을 구축하기에 매력적인 장소"[733]라는 평가가 이루어지도록 하고 있다.

한편 우리나라에서는 신분을 위장하고 수사하는 이른바 함정수사에 대해 명문의 근거규정은 없다. 다만 단순히 범죄자에게 범행의 기회를 제공하는 이른바 기회제공형 수사의 경우 허용[734]되는 것이 일반적이고 범의를 유발한 경우에는 수사의 신의칙에 반하여 허용되지 않는다고 하고 있다.[735]

2) 독일 형사소송법의 비밀수사관 제도

독일은 1992년 "조직범죄방지법"을 통해 형사소송법 제110조의 a 내지 e항을 신설하고, 비밀수사관 제도를 도입하였다. 이처럼 독일은 형사소송법에서 신분을 위장하고 활동하는 비밀수사관에 대한 근거 및 활동절차를 규정함으로써 신분위장을 통한 함정수사가 법적으로 허용되도록 하고 있다.

독일 형사소송법 제110조a(비밀수사관)[736]

① 다음의 범죄 행위가 행해졌음이 유력하다는 실질적인 증거가 있는 경우, 비밀수사관을 이용하여 범죄를 조사할 수 있다.

---

731) 다크넷의 특징에 대한 상세한 설명으로 박웅신/이경렬, 앞의 글, 222-225면 참조.

732) 대표적으로 TOR(The Onion Router)라는 프로그램이 있다.

733) 박웅신/이경렬, 앞의 글, 226면.

734) 「함정수사라 함은 본래 범의를 가지지 아니한 자에 대하여 수사기관이 사술이나 계략 등을 써서 범죄를 유발케 하여 범죄인을 검거하는 수사방법을 말하는 것이므로, 범의를 가진 자에 대하여 범행의 기회를 주거나 범행을 용이하게 한 것에 불과한 경우에는 함정수사라고 할 수 없다.」 대법원 2004. 5. 14. 선고 2004도1066 판결.

735) 「수사기관과 직접 관련이 있는 유인자가 피유인자와의 개인적인 친밀관계를 이용하여 피유인자의 동정심이나 감정에 호소하거나, 금전적·심리적 압박이나 위협 등을 가하거나, 거절하기 힘든 유혹을 하거나, 또는 범행방법을 구체적으로 제시하고 범행에 사용할 금전까지 제공하는 등으로 과도하게 개입함으로써 피유인자로 하여금 범의를 일으키게 하는 것은 위법한 함정수사에 해당하여 허용되지 아니한다.」 대법원 2007. 7. 12. 선고 2006도2339 판결.

736) (1) Verdeckte Ermittler dürfen zur Aufklärung von Straftaten eingesetzt werden, wenn

1. 마약이나 무기 거래, 위조 또는 위조
2. 국가보호에 대한 죄 (제74a조, 제120조)
3. 직업적 혹은 상습적인 범죄행위이거나
4. 범죄조직이나 다른 방식에 의한 조직범죄

또한 비밀수사관들은 특정 사실이 재발을 일으킬 위험이 있는 한 범죄를 조사하는 데 이용될 수 있다. 이러한 이용은 다른 방법으로 수사가 불가능하거나 현저히 곤란한 경우에만 허용된다. 또한 범죄의 특수성이 인정되고 다른 조치들이 실패한다면 비밀수사관을 이용하여 범죄를 조사할 수 있다.

② 비밀수사관은 그에게 부여된 영구적이고 변경된 신분(위장신분)하에 수사하는 경찰관이다. 비밀수사관은 위장신분에 따라 합법적으로 활동할 수 있다.

③ 비밀수사관은 위장신분의 구성 또는 유지 관리에 없어서는 안되는 증명서를 생성, 수정 및 사용할 수 있다.

이 규정에 의하여 특정한 중범죄를 대상으로 필요한 경우에는 수사관에게 위장신분을 부여하여 합법적으로 범죄수사를 위한 활동을 할 수 있도록 한다. 무기, 마약거래, 위폐 및 국가위협범죄, 집단적 조직적 범죄의 경우 비밀수사관의 이용이 가능하다. 수사관은 범죄수사 목적달성을 위해 가상의 신원을 창출하거나 유지하기 위해 필요한 각종 문서를 작성하거 변경 또는 사용하는 것이 허가된다.

3) 비밀수사관제도의 도입 필요성

사이버 영역의 접근에 있어서 일정한 자격요건과 그에 대한 검증을 요구하는 일반

---

zureichende tatsächliche Anhaltspunkte dafür vorliegen, daß eine Straftat von erheblicher Bedeutung

1. auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
2. auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes),
3. gewerbs- oder gewohnheitsmäßig oder
4. von einem Bandenmitglied oder in anderer Weise organisiert begangen worden ist. Zur Aufklärung von Verbrechen dürfen Verdeckte Ermittler auch eingesetzt werden, soweit auf Grund bestimmter Tatsachen die Gefahr der Wiederholung besteht. Der Einsatz ist nur zulässig, soweit die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Zur Aufklärung von Verbrechen dürfen Verdeckte Ermittler außerdem eingesetzt werden, wenn die besondere Bedeutung der Tat den Einsatz gebietet und andere Maßnahmen aussichtslos wären.

(2) Verdeckte Ermittler sind Beamte des Polizeidienstes, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln. Sie dürfen unter der Legende am Rechtsverkehr teilnehmen.

(3) Soweit es für den Aufbau oder die Aufrechterhaltung der Legende unerläßlich ist, dürfen entsprechende Urkunden hergestellt, verändert und gebraucht werden.

적인 다크넷에 대한 수사활동을 위해서는 그러한 자격요건에 대한 가장이 필수적으로 요구된다. 그것이 만약 단순히 수사관이라는 신분을 공개하지 않는 부작위[737]에 그치지 않고 적극적으로 일정한 신분을 가공하여 증명해야 하는 작위를 요구하는 것이라면 일반적으로 허용되는 임의수사로 평가되기는 어렵고 일종의 함정수사나 위법한 비밀수사로 평가될 수 있으므로 그에 대한 법적 근거가 요구된다고 할 수 있다.

이와 관련해서는 한자마켓(Hansa Market) 수사사례[738]를 참고할 필요가 있다. 한자마켓은 비트코인을 이용하는 불법거래 인터넷사이트였고 Silk Road, Alphabay와 함께 그 규모에 있어서 3대 불법거래사이트로 평가되고 있었다. 이 사례는 유로폴과 독일, 네덜란드의 경찰이 공조를 한 사례로, 사이트의 운영자는 독일인이었고 사이트의 서버는 네덜란드, 룩셈부르크, 독일 등에 두고 있었다. 유로폴의 기술지원을 받아 네덜란드 경찰이 서버를 발견하였고, 2017년 6월 20일 네덜란드 법원의 허가를 받아 해당 서버를 접수한 후 네덜란드 경찰이 사이트를 폐쇄하지 않고 그대로 운영하였는데, 이 부분은 인터넷상 가장(비밀)수사를 가장 적극적인 형태로 허용한 것으로 볼 수 있다. 마침 동일한 시점에 유로폴과 미국 FBI가 공조하여 미국을 중심으로 운영되던 불법거래사이트 Alphabay를 폐쇄시켰는데, 그러자 다크넷 불법거래상들이 대거 한자마켓으로 이동하는 현상을 보였다(신규회원 수 약 8배 증가). 그리하여 2017년 7월 20일까지 네덜란드 경찰은 한자마켓의 운영과 감시를 통해 약 38,000건의 불법거래를 확인하고 10,000여 건의 불법거래상 정보를 알아냈으며, 유로폴은 이 정보를 전 세계 협력국가와 공유하였다. 한편 네덜란드 경찰에 의하여 체포된 운영자들은 독일로 보내져서 독일검찰에 의해 기소되었고 그들이 소지한 비트코인은 모두 몰수 및 환매처분되었다.

또한 최초의 다크넷 폐쇄 사례인 실크로드 사건[739]은 잠입수사관 제도의 도입 여부

737) SNS나 인터넷 채팅방에서 가명으로 범죄혐의자와 채팅을 하면서 단지 자신이 경찰이라는 사실을 밝히지 않고 일반인인 것처럼 대화를 이어나가는 방식을 말한다. 이 경우는 대화의 내용이 중요하며 경찰이 범죄혐의자에게 적극적으로 범죄를 권하거나 유도하여 '범의를 형성'하였다고 볼 만한 사정이 없고 단순히 범죄의 기회를 제공한 정도에 그친 것이라면 현재와 같이 법적 근거가 없어도 일반적인 임의수사의 한 방식으로 허용될 수 있다.

738) "Massive blow to criminal Dark Web activities after globally coordinated operation", Europol News 2017.7.20., https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (2019년 11월 4일 최종접속).

739) 실크로드 사례에 대해서는 박웅신/이경렬, 앞의 글, 227-228면 참조.

에 대해 의미있는 시사점을 준다. 연방수사국의 잠입수사관이 실크로드에 잠입해 운영자인 DPR의 살인청부를 수주하여 DPR에 수사기관이 접근할 수 있는 단서를 제공했기 때문이다. 다크넷과 같은 인터넷에서 인적 비밀수사조치를 취할 수 있는 기준으로는 다음과 같은 것이 제시되고 있다.[740]

- 해당 사이트의 통제의 정도는 수사목적상 허위의 신분으로 진입이 가능하고,
- 그 허위의 신분으로 수사가 장시간 지속되어야 하며,
- 소극적 내지 적극적으로 대화포럼에 참가하여야 한다.

다. 암호화폐 몰수·처분 및 거래정보 획득 관련 규정 정비

1) 암호화폐 몰수와 처분에 관한 절차

(1) 암호화폐의 몰수(압수)절차

암호화폐를 몰수할 수 있다는 대법원의 판결에도 불구하고 사건에서 암호화폐가 범죄수익으로 판명되어 몰수의 대상이 되었더라도 구체적인 몰수의 절차와 방법에 대한 규정이 존재하지 않아서 실무적인 혼선이 있을 수밖에 없다. 일반적인 물건에 대한 몰수의 절차와 방법은 형사소송법상의 압수에 준한다.[741] 즉 이미 압수영장이나 임의제출에 의하여 압수되어 수사기관에 보관 중인 물건은 법원의 몰수결정에 의하여 몰수물로 그 성격이 전환되는 것이고, 만약 아직 압수되어 있지 않다면 법원의 몰수결정에 의하여 대상물을 압수하는 방법으로 몰수가 이루어진다. 그러므로 암호화폐에 대한 몰수 절차는 곧 암호화폐에 대한 압수의 절차와 방법에 대한 논의이다.

2018년 비트코인을 몰수할 수 있다는 대법원 판결이 이루어진 해당 사건에서는 규정이나 지침상의 근거 없이 수사기관이 임의로 수사관 명의의 개인지갑(wallet)과 계정을 만들고 범죄자들의 계정에서 수사관 개인지갑으로 송금받는 방식으로(즉 임의제출의 방식으로) 해당 비트코인을 압수하였다. 물리적인 실체가 없이 전자정보의 형태로 존재하는 암호화폐의 특성상 암호화폐에 관한 전자적 정보 자체를 거래이전의

740) 민영성/강수경, "독일의 인터넷 비밀수사에 관한 논의와 그 시사점", 국민대 법학논총 제31권 제2호, 국민대학교 법학연구소, 2018, 371면.
741) 형사소송법 제106조.

방식으로 압수하는 것은 불가피한 면이 있어 보이지만, 여기에는 두 가지의 구체적인 문제가 있다.

첫째는 위와 같은 계정생성과 이체의 방식으로 암호화폐를 압수하려면 법원 혹은 수사기관 명의의 계정을 만들고 이에 대한 관리의 절차가 마련되어야 한다. 법원이나 수사기관의 계정과 지갑(wallet)은 해킹이나 거래소의 파산 등으로 인한 손실 등을 방지하기에 적절한 방식으로 마련되어야 하며,[742] 이체의 과정에서 발생하는 수수료 등에 대한 처리 규정과 이체의 과정을 공식적으로 기록하고 문서화하여 일정기간 유지하는 절차에 관한 규정이 마련되어야 한다.[743] 그런데 주지하다시피 우리나라의 경우 비트코인 등 암호화폐의 발행과 거래 자체에 대한 법적 근거가 마련되어 있지 않고 있어서 국가기관인 법원이나 수사기관이 이러한 비법적(非法的) 수단을 사용하여도 되는 것인가의 문제가 있다. 물론 암호화폐의 발행이나 거래행위가 법적으로 금지되는 불법행위는 아니며 암호화폐가 금제품(禁制品)이 아니라는 점에서 수사기관의 이러한 행위도 '임의적' 방법의 하나로 취급될 수 있다. 그러나 암호화폐의 발행과 거래에 대해 법적으로 그 존재를 인정할 수 없다는 정책적 태도를 취하고 있는 현재의 법정책적 상황에서는 법원이나 수사기관이 계정을 생성하는 것 자체가 정책적인 의미에서는 국가정책에 반하는 것 내지는 암호화폐를 사실상 승인하는 듯한 태도로 해석될 여지가 충분히 있어서 법정책적 혼란을 야기할 수 있다는 이유로 이러한 것을 허용할 수 없다는 주장도 가능한 상황이라고 할 수 있다. 이러한 문제상황은 정부가 암호화폐에 대한 법정책을 (긍정적으로) 전환하면 금방 해결될 문제이긴 하지만, 현재의 암호화폐에 대한 법정책이 유지된다고 하더라도 이미 대법원이 (일정한 종류의) 암호화폐에 대한 몰수가 가능함을 해석론으로 확정한 이상 그에 관한 압수절차를 정비하는 것은, 법정책의 문제와 상관없이, 시급한 과제라고 할 수 있다. 암호화폐에 대한 몰수를 인정한 대법원의 판결이 암호화폐에 대한 법정책과는 무관하다는 판단이 받아들여질 수 있는 것이라면 이에 대해 법원이나 수사기관이 압수에 관련한 공식적

742) 소위 'Cold Wallet' 방식을 말한다. 형사소송법 제131조(주의사항) 압수물에 대하여는 그 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 한다.

743) 참고로 독일 Hessen주의 경우 수사기관 명의의 비트코인 계정을 개설하고 여기에 이체하는 방식으로 압수하고 있으며 이에 대해서는 검찰이 자체 메뉴얼(내규)을 제정하여 운용하고 있다고 한다.(이 내용은 필자가 2019년 8월 20일, 독일 Hessen주 검찰청을 방문하여 검찰공보담당관으로부터 직접 청취한 내용임)

인 절차를 만드는 것 또한 가능하고 필요한 상황이라고 할 수 있다.

둘째는 법원이나 수사기관이 암호화폐의 계정을 만들고 이에 관한 절차를 마련하더라도 피의자나 피고인이 임의제출을 하지 않는 경우에는 이를 강제처분의 방식으로 압수할 방법이 마땅치 않다는 문제가 있다. 암호화폐는 소유자만이 알 수 있는 고유의 비밀키가 존재하는 것이 본질적인 특징인데, 이와 같이 거래에 필요한 비밀키 등의 정보를 피의자나 피고인이 제공하지 않으면 압수를 진행하기가 사실상 곤란하다. 암호화폐의 소유자가 거래에 필요한 비밀키 등의 정보를 거래소에 위탁하여 거래에 사용한 경우에는 해당 거래소에 대한 압수수색영장을 집행하는 방식으로 법원이나 수사기관이 그 정보를 취득할 수 있으나, 피의자나 피고인이 개인지갑을 통한 개인간 거래를 통하여 취득한 경우에는 그 정보는 일종의 인적 인식내용(개인의 지식과 같은 것)이므로 직접적으로 확보할 방법이 없다. 몰수를 위한 압수수색영장은 어디까지나 대물적 효력을 가지는 것이고 개인에 대해 일정한 진술을 강요할 수 있는 성질의 것은 아니기 때문이다.[744] 따라서 이는 압수수색영장의 대물적 효력에 의한 간접적인 방법을 사용하는 수밖에 없다. 압수수색영장의 효력범위에 피의자나 피고인의 개인기록(PC, 휴대전화, 메모 등)을 포함하도록 하여 거기서 얻어진 정보들을 이용하여 법원이나 수사기관이 암호화폐의 거래에 필요한 정보를 찾아내는 방법을 사용해야 할 것이다.[745] 이와 관련하여 이러한 정보를 자발적으로 제공한 경우에는 수사협조자에 준하여 책임을 감경하거나 임의적인 감형사유로 규정하는 방식[746] 등으로 그러한 협조를 유도하는 방식 등도 생각해 볼 수 있으나, 수사협조자에 대한 형벌감면을 제도화하는 것 자체에 대한 비판이 적지 않고[747] 일반적인 수사협조자와는 달리 이 경우는 자신의 범죄와 직접적으로 관련한 정보를 대상으로 한다는 점에서 플리바게닝(plea-bargaining)을 제도적으로 인정하지 않고 있는 상황에서 이러한 방법을 도입하

744) 설령 피의자나 피고인의 인식에 존재하는 것을 그대로 진술하도록 할 수 있는 기술적인 방법이 있다고 하더라도 이는 곧바로 위헌적인 수사방법이 될 것이다.

745) 이러한 문제는 피압수자의 스마트폰에 패턴이나 비밀번호 등의 방식으로 잠금장치가 되어있는 경우에도 마찬가지로 발생하고 있다. 스마트폰 제조사 등의 기술적인 지원 등 이를 기술적으로 해제할 수 있는 방법이 없는 경우에는 실무상 피압수자로부터 이를 직접적으로 알아낼 수는 없다.

746) 주로 조직범죄를 대상으로 범죄신고 등을 한 수사협조자에 대해 감형이나 형사면책 등의 제도를 도입하자는 논의가 있다. 이에 대해서는 최병각, "조직범죄수사의 협조자에 대한 양형과 형사면책", 비교형사법연구 제5권 제2호, 한국비교형사법학회, 2003, 503면 이하 참조.

747) 대표적으로 윤동호, "수사협조범죄자 기소면제 및 형벌감면 법제화 비판", 비교형사법연구 제13권 제2호, 한국비교형사법학회, 2011, 325면 이하.

는 것은 현 시점에서는 적절하지 않다고 보여진다.

(2) 몰수된 암호화폐의 처분

압수의 방식으로 몰수한 암호화폐의 처분에 대해서도 현재는 명확한 절차규정이 존재하지 않는다. 현행 형사소송법은 몰수물의 처분에 대해 단순히 처분의 주체를 검사로 명시하고 있을 뿐[748] 몰수물의 처분에 대한 구체적인 절차와 방법을 규정하고 있지는 않고, 몰수물의 구체적 처분방법에 대해서는 검찰압수물사무규칙에 규정되어 있다. 검찰압수물사무규칙 제28조는 "검사는 몰수물이 유가물인 때에는 공매에 의하여 국고납입 처분을 하여야 한다."고 규정하고 있다. 만약 암호화폐의 몰수를 인정한 대법원 판결의 취지를 그대로 인정하여 암호화폐를 '유가물'로 볼 수 있다면 동 규칙에 의하면 압수하여 수사기관 등의 계정에 보관된 암호화폐를 '공매절차'를 통하여 법정통화로 환가한 후 이를 국고에 납입하는 방식으로 처분해야 하는 것이다. 그러기 위해서는 특정 거래소를 통하여 압수된 암호화폐를 공매할 수 있는 절차에 관한 별도의 규정이 마련되어야 할 것이지만, 이것은 암호화폐의 이체라는 임의적 방식으로 암호화폐를 압수하는 것과는 다르게 암호화폐가 공적으로 거래될 수 있는 '시장'을 제도적으로 인정해야 한다는 점에서 암호화폐의 거래소를 법적으로 인정하지 않는 현재의 법정책 하에서는 제도화하기 어려운 상황이라고 할 수 있다.[749]

만약 몰수된 암호화폐를 유가'물'이라고 보지 않고 채권의 일종으로 보는 민법상의 해석을 반영하여 '유가증권'으로 간주한다면 검찰압수물사무규칙 제33조에 따라 그 자체를 국고납입처분해야 한다. 이 경우 해당 암호화폐를 국고계정으로 이체하는 것으로 이해할 수 있으나 이 경우에도 국가가 암호화폐의 국고계정을 개설하여 운용할 수 있느냐는 근본적인 법정책적 문제가 해결되어야 할 것이다.

이 밖에 현재 암호화폐의 발행과 거래를 인정하지 않는 법정책을 적극적으로 반영하여 몰수한 암호화폐를 폐기의 대상으로 보아 폐기처분하기로 결정하는 방식도 생각해 볼 수 있으나, 이 경우 한 번 생성된 블록체인은 수정과 폐기가 불가능하다는

748) 형사소송법 제483조(몰수물의 처분) 몰수물은 검사가 처분하여야 한다.

749) 이러한 이유로 2018년 대법원 판결로 몰수 결정된 비트코인은 현재까지 처분되지 못하고 여전히 검찰이 보관하고 있다. "몰수 비트코인 1년째 처분 못하는 검찰..가치만 15억→6억→19억 '널뛰기'", 세계일보 2019년 5월 30일자, https://news.v.daum.net/v/20190530060242843 (2019년 11월 4일 최종접속).

고유의 특성을 이용하는 암호화폐의 본질적 특성상 기술적으로 폐기가 가능한 것인지 의문이다. 해당하는 암호화폐의 정보를 특정하여 영구 거래정지 등의 처분으로 폐기에 갈음할 수도 있겠지만 이러한 처분은 거래소 등에 대한 행정적인 효력만을 가질 수 있을 뿐 개인 대 개인 간의 직접 거래는 실질적으로 규제할 수 없어서 폐기라는 실효성을 가지기 어려울 것이다.

결론적으로 암호화폐에 대한 몰수를 법적으로 인정하고 실제로 몰수처분이 이루어진 이상 현실적으로는 (암호화폐에 대한 법정책의 전환과 아울러) 유가물로 간주하여 공매한 후 국고에 귀속시킬 수 있도록 하는 것이 타당하고, 이에 대한 제도적 규정[750]을 정비하는 것이 필요할 것으로 생각된다.

2) 암호화폐 거래정보 획득 및 증거능력

(1) 암호화폐 거래정보의 획득을 위한 절차

암호화폐의 거래를 이용한 주요한 범죄의 양상에는 자금세탁, 금지물품의 거래 등이 있음은 전술한 바와 같다. 그런데 이러한 범죄는 실행행위의 밀행성을 주된 특징으로 하고 '피해자 없는 범죄(victimless crime)'로서의 속성을 가지고 있다는 점에서 이러한 행위를 찾아내고 규제[751]해야 하는 국가의 입장에서는 적절히 대처하기 어려운 유형이라고 할 수 있다. 이러한 유형은 거래의 대가나 대상인 암호화폐의 거래행위가 범죄실행행위의 주요 부분이라고 할 수 있는데, 주지하다시피 암호화폐의 거래는 소위 '오프라인'이라고 불리는 현실세계에서는 행해지지 않고 가상의 세계인 '온라인' 상으로만 이루어지며 이러한 온라인상에서의 거래행위는 익명화된 당사자 간의 전자적 정보의 전송행위이기 때문에 거래에 참여한 당사자가 아닌 제3자는 그러한 온라인 공간에 개념적으로 함께하고 있다고 하더라도 거래가 이루어졌다는 사실 자체도 파악하기 어렵다. 또한 거래소 등을 통해서 이루어지는 규모가 큰 비트코인과

---

750) 공매에 이용될 거래소의 지정방법, 공매의 시기와 구체적 매수대상자의 선정방법 등에 대한 규칙의 제정이 필요하다.

751) 물론 이러한 피해자없는 범죄의 경우 형사적인 규제 자체가 타당하냐, 법경제학적 관점에서 정당성이나 효율성을 가질 수 있는 것이냐에 대한 논의가 존재한다. 특히 밀행성을 가지는 피해자없는 범죄의 경우, 이에 대한 규제정책이 사회적으로 효과를 기대할 수 있는 것이냐에 대한 근본적인 물음이 존재하는 것이 사실이다. 이에 대해서는 김혜정/조상희, "피해자없는 범죄의 규제에 관한 소고", 피해자학연구 제23권 제1호, 한국피해자학회, 2015, 94면 이하 참조.

같은 암호화폐의 경우에는 일일 거래량이 관찰자가 일일이 식별할 수 있는 규모를 훨씬 뛰어넘는 다량이기 때문에 거래 당시에 불법정황이 있는 거래를 실시간으로 식별해 내는 것은 불가능에 가깝다. 따라서 암호화폐의 거래를 수단으로 하여 행해지는 자금세탁이나 금지물품거래에 대해 국가의 사법기관이 적절히 대처하기 위해서는 단순한 참여자에게 관찰자가 얻을 수 있는 정보의 한계를 넘어서는 거래정보에 대한 접근방법과 절차가 마련되어야 한다.

우선은 암호화폐 거래 자체를 실시간으로 모니터링할 수 있는 제도를 생각해 볼 수 있다. 이른바 '사이버 순찰'[752]이라고 부를 수 있는 거래소 거래정보를 실시간으로 감시, 식별할 수 있는 시스템을 구축하자는 것이다. 사이버 순찰 시스템은 함정수사, 표현의 자유 침해, 프라이버시권의 침해 등의 문제에 대한 우려가 있으나 사이버 공간의 본질적인 기본권을 침해하지 않도록 공개된 정보에 한정하고 필요최소한도로 접근하는 등의 세부적인 설계를 통해 가능할 수 있을 것[753]으로 생각되며, 실제로 몇몇 인터넷 커뮤니티 사이트 등에서 불법거래 등을 감시하고 적발하기 위하여 구현된 사례가 있다.[754] 해당 인터넷 사이트를 모니터링하다 불법거래가 의심되는 상황을 발견하면 수사기관 담당자는 최대한 신속히 해당 게시판 사이트로 접속하여 관련 증거 스크린샷 등을 수집·저장하고, 해당 게시글과 관련된 주소로 인터넷 서비스 제공업체 등에 조회 의뢰하여 관련자의 인적사항 및 주소를 알아낸 후 즉시 현장 조사 등의 조치를 취하도록 하는 체계[755]이다. 그러나 이러한 체계는 거래소에 이루어지는 암호화폐의 거래를 감시하는 수단으로는 충분하지 않다. 인터넷 게시판의 게시글에서는 글의 제목 등에서 범죄혐의에 대한 단서 자체를 찾을 수 있지만 단순히 숫자의 증감으로 이루어지는 암호화폐의 거래에 대해 이러한 관찰방식의 모니터링은 효과를 기대하기 어렵다.

---

752) '사이버 순찰'은 인터넷 공간에서 게시글 등을 모니터링하여 이에 대한 경찰차원의 즉각적인 대응조치가 가능하도록 하는 일련의 활동을 말한다. 이에 대해서는 장준원, "실시간 디지털증거 수집기법을 이용한 사이버 순찰 체계 구축 및 활용사례", 디지털포렌식연구 제8권 제2호, 한국디지털포렌식학회, 2014, 35면 참조. 특정 범죄정보에 국한하지 않고 광범위하고 포괄적인 감시활동을 하며 범죄관련 사항이 발견되었을 경우 현장초동조치에 유사한 즉각적인 강제조치가 행해질 수 있다는 점에서 단순 '모니터링'이나 '수사'가 아닌 '순찰'이라는 용어를 사용한다고 한다.

753) 장준원, 앞의 글, 42-49면.

754) 장준원, 앞의 글, 53-57면.

755) 장준원, 앞의 글, 53면.

그러므로 거래소의 거래 내역을 (꼭 실시간이 아니어도) 거래당사자의 인적 사항과 거래의 규모, 거래의 빈도 등을 종합적으로 제공받아 분석할 수 있는 체계가 필요하다. 일반적인 거래소는 가입자 성명, 이메일, 휴대전화번호, 금융계좌번호, 가상통화 구매 정보(신용카드 정보 등), 가상통화 지갑 주소 및 비밀키, 거래 내역 등의 정보를 보유하고 있다. 암호화폐를 기능하도록 하는 블록체인 분산원장 그 자체는 공개성을 가지고 있어 거래된 내역에 해당하는 전자정보 자체는 누구나 접근할 수 있지만, 블록체인 분산원장에 기록된 전자정보는 특정 암호화폐 자체의 존재와 거래정보에 불과하여 거래자의 정보나 거래의 불법성 여부에 대한 정보를 제공하지 않는다. 따라서 불법거래를 발견하고 대응하기 위해서는 거래소에 보관된 거래 관련 정보에 대한 접근과 수집이 반드시 필요한데, 이는 사실 거래소의 사적개인정보에 해당하므로 계좌추적과 유사한 강제수사적 성격을 가질 수밖에 없다. 따라서 거래소의 정보를 수집하기 위해서는 영장주의의 원칙이 적용되어야 한다. 암호화폐를 이용한 불법거래의 정황이 다른 자료를 통해 객관적으로 드러난 경우에는 현행 압수수색 영장을 이용해서 관련 자료에 접근할 수 있겠지만, 거래소의 거래 내역의 감시와 분석을 통한 범죄혐의의 발견이 필요한 대부분의 경우에 있어서는 일반적인 범죄혐의사실에 기초한 현행 영장 제도를 이용하기 어렵다.

암호화폐 거래정보를 적시에 효율적으로 수집·분석하기 위해서는 현재 금융기관에 대해 제도화되어 있는 포괄적인 금융거래 정보제공제도를 암호화폐의 거래소에 대해서도 확대 적용할 필요성이 있다. 현행 「금융실명거래 및 비밀보장에 관한 법률」 제4조[756]는 법원의 영장이 발부되었거나 국세청, 금융감독기구 등에서 조세탈루나

---

756) 제4조(금융거래의 비밀보장) ① 금융회사등에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 금융회사등에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우로서 그 사용 목적에 필요한 최소한의 범위에서 거래정보등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다.

1. 법원의 제출명령 또는 법관이 발부한 영장에 따른 거래정보등의 제공
2. 조세에 관한 법률에 따라 제출의무가 있는 과세자료 등의 제공과 소관 관서의 장이 상속·증여 재산의 확인, 조세탈루의 혐의를 인정할 만한 명백한 자료의 확인, 체납자의 재산조회, 「국세징수법」 제14조 제1항 각 호의 어느 하나에 해당하는 사유로 조세에 관한 법률에 따른 질문·조사를 위하여 필요로 하는 거래정보등의 제공
3. 「국정감사 및 조사에 관한 법률」에 따른 국정조사에 필요한 자료로서 해당 조사위원회의 의결에 따른 금융감독원장(「금융위원회의 설치 등에 관한 법률」 제24조에 따른 금융감독

불법거래, 이상거래 등의 정황을 조사하기 위하여 거래정보의 제공이 요청된 경우에는 금융기관이 해당 기관이 보유한 거래정보를 제공하도록 하는 제도를 두고 있다. 물론 이러한 방안이 제도화되기 위해서는 거래소에 대한 인허가와 관리·감독 등에 대한 포괄적인 법제도가 마련되는 것이 선결되어야 하겠지만, 그러한 법제도의 내용에 금융기관에 준하여 금융거래정보의 제공에 대한 위와 같은 특례규정을 반드시 포함하여 불법거래에 대한 정보에 수사기관이나 감독기관이 시의 적절하게 접근할 수 있는 방안을 마련해야 한다. 또한 이와 관련하여 거래소에 대해서도 인허가나 운영유지의 요건으로 거래정보의 제공·분석에 대한 일정한 협력의무를 부여하는 방안도 고려될 수 있다. 불법거래에 대한 명확한 정황이 드러나지 않은 상황에서 불법거래를 포착하기 위해서는 방대한 거래정보를 세밀하게 분석하는 작업이 필요한데 이는

원의 원장을 말한다. 이하 같다) 및 예금보험공사사장(「예금자보호법」 제3조에 따른 예금보험공사의 사장을 말한다. 이하 같다)의 거래정보등의 제공

4. 금융위원회(증권시장·파생상품시장의 불공정거래조사의 경우에는 증권선물위원회를 말한다. 이하 이 조에서 같다), 금융감독원장 및 예금보험공사사장이 금융회사등에 대한 감독·검사를 위하여 필요로 하는 거래정보등의 제공으로서 다음 각 목의 어느 하나에 해당하는 경우와 제3호에 따라 해당 조사위원회에 제공하기 위한 경우
   가. 내부자거래 및 불공정거래행위 등의 조사에 필요한 경우
   나. 고객예금 횡령, 무자원(無資源) 입금 기표(記票) 후 현금 인출 등 금융사고의 적발에 필요한 경우
   다. 구속성예금 수입(受入), 자기앞수표 선발행(先發行) 등 불건전 금융거래행위의 조사에 필요한 경우
   라. 금융실명거래 위반, 장부 외 거래, 출자자 대출, 동일인 한도 초과 등 법령 위반행위의 조사에 필요한 경우
   마. 「예금자보호법」에 따른 예금보험업무 및 「금융산업의 구조개선에 관한 법률」에 따라 예금보험공사사장이 예금자표(預金者表)의 작성업무를 수행하기 위하여 필요한 경우
5. 동일한 금융회사등의 내부 또는 금융회사등 상호간에 업무상 필요한 거래정보등의 제공
6. 금융위원회 및 금융감독원장이 그에 상응하는 업무를 수행하는 외국 금융감독기관(국제금융감독기구를 포함한다. 이하 같다)과 다음 각 목의 사항에 대한 업무협조를 위하여 필요로 하는 거래정보등의 제공
   가. 금융회사등 및 금융회사등의 해외지점·현지법인 등에 대한 감독·검사
   나. 「자본시장과 금융투자업에 관한 법률」 제437조에 따른 정보교환 및 조사 등의 협조
7. 「자본시장과 금융투자업에 관한 법률」에 따라 거래소허가를 받은 거래소(이하 "거래소"라 한다)가 다음 각 목의 경우에 필요로 하는 투자매매업자·투자중개업자가 보유한 거래정보등의 제공
   가. 「자본시장과 금융투자업에 관한 법률」 제404조에 따른 이상거래(異常去來)의 심리 또는 회원의 감리를 수행하는 경우
   나. 이상거래의 심리 또는 회원의 감리와 관련하여 거래소에 상응하는 업무를 수행하는 외국거래소 등과 협조하기 위한 경우. 다만, 금융위원회의 사전 승인을 받은 경우로 한정한다.
8. 그 밖에 법률에 따라 불특정 다수인에게 의무적으로 공개하여야 하는 것으로서 해당 법률에 따른 거래정보 등의 제공

수사기관이나 법원의 역량만으로 해결하기에는 부담이 클 수 있다. 거래소 자체의 감시감독 시스템이나 블록체인거래를 추적하는 감시프로그램[757]을 의무적으로 구축하도록 하고 의심거래에 대한 조사 시 거래정보에 대한 분석에 협조하도록 하는 방안이 고려되어야 할 것이다.

(2) 암호화폐 거래기록의 증거능력

암호화폐 거래기록은 블록체인 기술에 기반한 분산원장에 기록되어 있고, 수사기관이 입수한 관련 기록도 블록체인에 전자적 형태로 존재한다. 즉 이 기록은 거래당사자가 직접 작성한 기록이라기보다는 블록체인 시스템의 작동원리에 의하여 전자적으로 형성된 간접적 기록이다. 그러한 면에서 이 기록이 혹시 전문증거이고 전문법칙의 적용을 받게 되는 것은 아닌지 하는 의문이 제기될 수 있다. 특히 전자적 형태로 존재하는 사적 정보에 대해 증거능력을 부여하기 위해서는 입수된 해당 전자정보가 원본과의 동일성과 무결성 요건을 충족해야 한다는 일반적인 법리[758]로 인하여 블록체인 분산원장에 존재하는 암호화폐에 대한 전자기록의 경우도 이러한 법리에 따라 무결성 등에 대한 검증이 필요한 것이 아닌가 하는 논란이다.

여기에 대해서는 블록체인이 기술적인 측면에서 자동적으로 생성되며 참여자의

---

757) 암호화폐의 거래를 감시, 분석하는 프로그램으로, 대표적으로 'Chainalysis'를 들 수 있다. 다음은 Chainalysis 홈페이지(https://www.chainalysis.com/government-agencies/ (2019년 11월 4일 최종접속))에서 제공하는 프로그램의 설명이다.
"Cryptocurrency gives criminals new ways to evade detection. Our leading investigation tools allow you to understand the real-world entities behind every transaction and combat serious crimes such as money laundering, terrorism financing, and human trafficking. Chainalysis makes it easy to see where cryptocurrency funds are going. Follow the money, chart it on an intuitive visual graph, and share your findings in multiple formats. Enrich your investigations with contextual information scraped from thousands of clear and darknet forums."

758) 대법원 2015. 1. 22. 선고 2014도10978 전원합의체 판결
"파일 등의 전자매체는 성질상 작성자나 진술자의 서명 혹은 날인이 없을 뿐만 아니라, 녹음자의 의도나 특정한 기술에 의하여 내용이 편집·조작될 위험성이 있음을 고려하여 대화 내용을 녹음한 원본이거나 혹은 원본으로부터 복사한 사본일 경우에는 복사 과정에서 편집되는 등 인위적 개작 없이 원본의 내용 그대로 복사된 사본임이 입증되어야만 하고, 그러한 입증이 없는 경우에는 쉽게 그 증거능력을 인정할 수 없다. 그리고 증거로 제출된 녹음파일이 대화 내용을 녹음한 원본이거나 혹은 복사 과정에서 편집되는 등 인위적 개작 없이 원본 내용을 그대로 복사한 사본이라는 점은 녹음파일의 생성과 전달 및 보관 등의 절차에 관여한 사람의 증언이나 진술, 원본이나 사본 파일 생성 직후의 해쉬(Hash)값과의 비교, 녹음파일에 대한 검증·감정 결과 등 제반 사정을 종합하여 판단할 수 있다."

조작이나 제거 등이 원천적으로 불가능하도록 한 것이라는 그 특성에 비추어 비록 전자적 형태의 기록이나 형사소송법에서 당연히 증거능력이 있는 서증[759]인 상업장부[760] 혹은 기타 신용할만한 정황에 의하여 작성된 문서로 취급하면 된다는 설명이 유력한 것으로 보인다. 관련해서 언론보도에 의하면 미국의 버몬트주[761]나 중국[762]에서는 블록체인 전자기록에 대해 무결성을 인정하여 증거능력을 긍정한다는 취지의 법규범을 제정한 것으로 보인다.

라. 영장제도 개선

사이버 범죄에 대한 대처에 있어 현행 영장제도는 여러 가지 면에서 개선이 검토되어야 한다.

첫째는 암호화폐 등의 거래정보를 거래소 등을 통해 효과적으로 입수·분석하기 위해서는 금융거래정보에 대한 특별영장[763]과 같은 제도를 암호화폐 거래소 등에도

---

759) 형사소송법 제315조(당연히 증거능력이 있는 서류) 다음에 게기한 서류는 증거로 할 수 있다.
1. 가족관계기록사항에 관한 증명서, 공정증서등본 기타 공무원 또는 외국공무원의 직무상 증명할 수 있는 사항에 관하여 작성한 문서
2. 상업장부, 항해일지 기타 업무상 필요로 작성한 통상문서
3. 기타 특히 신용할 만한 정황에 의하여 작성된 문서

760) 대법원 2015. 7. 16. 선고 2015도2625 판결.
"업무상 필요로 작성한 통상문서에 해당하는지 여부를 판단하기 위해서는, 당해 문서가 정규적·규칙적으로 이루어지는 업무활동으로부터 나온 것인지 여부, 당해 문서를 작성하는 것이 일상적인 업무 관행 또는 직무상 강제되는 것인지 여부, 당해 문서에 기재된 정보가 취득된 즉시 또는 그 직후에 이루어져 정확성이 보장될 수 있는 것인지 여부, 당해 문서의 기록이 비교적 기계적으로 행하여지는 것이어서 기록 과정에 기록자의 주관적 개입의 여지가 거의 없다고 볼 수 있는지 여부, 당해 문서가 공시성이 있는 등으로 사후적으로 내용의 정확성을 확인·검증할 기회가 있어 신용성이 담보되어 있는지 여부 등을 종합적으로 고려"

761) "Vermont is Close to Passing a Law That Would Make Blockchain Records Admissible in Court", Coindesk 2016.5.17., https://www.coindesk.com/vermont-blockchain-timestamps-approval (2019년 11월 4일 최종접속) 참조.

762) "중국 대법원, 블록체인 증거 법적 구속력 인정", 코인데스크코리아 2018년 9월 8일자, https://www.coindeskkorea.com/28353/ (2019년 11월 4일 최종접속) 참조.

763) 금융실명거래 및 비밀보장에 관한 법률 제4조(금융거래의 비밀보장) ① 금융회사등에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 금융회사등에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우로서 그 사용 목적에 필요한 최소한의 범위에서 거래정보등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다.
1. 법원의 제출명령 또는 법관이 발부한 영장에 따른 거래정보등의 제공

마련할 필요가 있다. 일종의 '일반영장'[764]이라고 할 수 있는 금융실명법상의 영장제도를 암호화폐 거래소의 거래정보에 대해서도 이용할 수 있도록 해야 한다는 것이다. 암호화폐 거래소의 설립인가, 관리·감독에 관한 법령의 제정에 있어 거래소에 대한 '특정 금융정보에 대한 보고의무'[765]를 부과함과 동시에 거래소의 거래정보에 대해서는 법원의 영장으로 거래기록을 수사기관이 즉시 입수할 수 있도록 하는 규정이 마련되어야 한다.

둘째는 온라인 수색이나 네트워크 수사기법(NIT)에서 문제될 수 있는 관할의 문제를 해결하기 위해 온라인 수색활동의 정당성이 법원의 관할 혹은 역외에도 적용될 수 있도록 하는 영장의 효력범위에 대한 특례규정을 마련할 필요가 있다. 앞서 본 바와 같이 미국의 연방형사소송규칙은 치안판사의 영장에 따른 NIT에 대한 근거규정을 두면서 NIT에 대한 영장의 효력은 관할구역을 벗어난 곳에 존재하는 네트워크 기기에 대해서도 유효함을 규정하고 있다(the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both). 미국의 연방형사소송규칙이 이렇게 규정하는 것에 대해서는 "비록 피고인의 컴퓨터가 치안 판사 관할구역 외부에 위치했지만, 추적 장치를 설치하기 위한 영장을 발부하였는데, NIT는 피고인이 다운로드 하고자 하는 중요한 매체에 삽입되었고, 서버가 피고인의 컴퓨터에 접속하였다고 보기보다는 피고인이 자료를 얻기 위해 전자적으로 치안 판사 관할권 내의 서버로 접속했다고 평가한다."[766] 고 설명하며 그 정당성을 인정하고 있다. 이러한 문제와 논리는 추적의 대상이 된 네트워크 기기가 국외에 있는 경우에도 마찬가지일 수 있다. 우리나라에 온라인 수색에 대한 규정이 도입될 경우에는 영장효력의 역외적용에 대한 특례규정이 함께 규정되어야 할 것이다.

셋째는 보다 근본적인 문제로, 물리적 영장의 발부를 전제로 하는 현행 형사소송법

764) 형사소송법의 일반원칙상 영장은 '피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여' 발급되어야 하며 포괄적인 것을 대상으로 하는 '일반영장'의 발급은 원칙적으로 금지된다.

765) 특정 금융거래정보의 보고 및 이용 등에 관한 법률 제4조 등.

766) United States v. Lough, United States District Court, N.D. West Virginia. November 18, 2016, 221 F. Supp. 3d 770: "although defendant's computer was located outside of magistrate judge's district; NIT was imbedded in material defendant sought to download, and defendant went electronically to server within magistrate judge's jurisdiction to get material, rather than server reaching out to defendant's computer unsolicited."

의 영장발부와 제시에 대한 규정이 정비될 필요가 있다. 현행 형사소송법은 영장이 종이의 형태로 발부되는 것을 전제로 영장의 원본을 수사대상자에게 '물리적으로' 제시할 것을 요구하고 있다.[767] 그리고 현행 법조실무도 이를 매우 엄격하게 해석하고 있다.[768] 그런데 사이버 공간 상에서 이루어지는 암호화폐 거래나 네트워크 침해범죄의 경우에 그 특성상 해당 수색 대상자에게 물리적인 영장을 제시하는 것이 곤란하거나 현저한 시간과 비용이 드는 경우가 대부분일 것이다. 물론 온라인 수색이나 네트워크 수사기법이 법적 근거를 가지고 도입될 경우 영장제시의 요건이 완화되어 수사대상자에게 영장의 제시 자체가 불필요하도록 하는 방식으로 설정될 것이지만 이는 특정 개인에 대한 비공개 수사의 경우에만 한정적으로 정당한 방식이라고 할 수 있고, 암호화폐의 거래소와 같은 정보제공의 주체에 대해서는 영장제시의 요건은 원칙적으로 충족되어야 할 것이다. 그런데 오로지 사이버 공간을 기반으로 운영되는 거래소와 같은 정보제공자에 대해 물리적 방식으로 영장을 제시하도록 하는 것은 방법적인 측면에서 비효율성이 크고 때로는 소재파악에 대한 곤란함으로 인해 적절한 시점을 놓치게 되어 수사에 지장을 초래하는 경우를 충분히 예상할 수 있다. 따라서 적법하고 정확한 영장의 집행이라는 절차적 정당성을 훼손하지 않는 보완조치와 함께 전자적 방식으로도 영장의 발부와 제시가 이루어질 수 있도록 하는 형사소송법의 정비가 필요한 시점이라고 생각한다. 영장의 전자적 발부와 관련해서는 일정부분 블록체인 기술이 활용될 여지가 있을 것이다. 영장의 발부는 전자정보의 빠른 처리보다는 정확성과 투명성이 중요한 것이므로 전자영장 발부시스템은 법원에 의한 공적 블록체인시

767) 형사소송법 제118조(영장의 제시) 압수·수색영장은 처분을 받는 자에게 반드시 제시하여야 한다.

768) 대법원 2017. 9. 21. 선고 2015도12400 판결.

"대한민국헌법 제12조 제3항 본문은 '체포·구속·압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다'고 규정하고, 형사소송법 제219조, 제118조는 '수사기관이 압수·수색영장을 집행할 때에는 처분을 받는 자에게 반드시 압수·수색영장을 제시하여야 한다'는 취지로 규정하고 있다. 그리고 형사소송법 제219조, 제114조 제1항 본문, 형사소송규칙 제58조는 압수·수색영장에 피의자의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지 및 압수·수색의 사유를 기재하고 영장을 발부하는 법관이 서명날인하도록 규정하고 있다. 형사소송법이 압수·수색영장을 집행하는 경우에 피압수자에게 반드시 압수·수색영장을 제시하도록 규정한 것은 ① 법관이 발부한 영장 없이 압수·수색을 하는 것을 방지하여 영장주의 원칙을 절차적으로 보장하고, ② 압수·수색영장에 기재된 물건, 장소, 신체에 대해서만 압수·수색을 하도록 하여 개인의 사생활과 재산권의 침해를 최소화하는 한편, ③ 준항고 등 피압수자의 불복신청의 기회를 실질적으로 보장하기 위한 것이다."

스템의 방식으로의 구축을 검토해 볼 가치가 있다고 보여진다.

마. 국제수사공조 활성화

암호화폐 관련 범죄는 범죄 발생 후 수 분 내에 피해금이 국외로 유출이 가능하며, 범죄의 발생과 실행 단계에서도 여러 나라를 경유하여 거래가 이루어지는 경우가 많다. 암호화폐를 이용한 자금세탁의 대부분은 대게 국외의 서버나 거래소를 이용하게 된다. 사실상 암호화폐 거래에 국경은 의미가 없는 상황이다. 그런데 블록체인의 특성상 대부분의 암호화폐는 송금경로의 추적이 가능하다.[769] 그리고 종국적으로는 법정통화로 환가하기 위해 KYC(Know Your Customer: 고객 신원 인증)를 거친 암호화폐 거래소를 이용할 수밖에 없으므로 신속한 국제공조가 이루어진다면 대응이 가능하다는 특징이 있다. 암호화폐 거래를 이용한 범죄에 대한 형사적 대응책으로 국제공조가 강조되는 이유이다.

범죄수사에 있어 국제협력을 의미하는 국제형사사법공조는 일반적으로 국가간 협정에 의한 형사사법공조조약에 의하는데, 형사사법공조조약에 의하면 국가간 형사공조가 필요한 경우 외교경로를 통한 공조의 요청에 의하는 것이 원칙이고 개별적으로 형사사법공조조약에 근거규정을 두어 중앙기관간 직접 공조를 요청하는 것도 가능하다. 이러한 조약에 의한 국제공조는 사람 또는 물건의 소재에 대한 수사, 증거수집, 압수·수색 또는 검증, 증거물 등의 인도 등이 가능하도록 하고 있다. 조약에 의한 국가간 형사공조는 공신력은 높으나 절차가 복잡하고 신속한 처리가 곤란하다는 단점이 있으며 정보통신망 등을 통한 증거확보 방법에 대해서는 일정한 한계가 있다.

그러므로 앞의 한자마켓이나 알파베이 사례와 같이 유로폴이나 인터폴과 같이 전체적인 지휘와 기술지원의 중심이 되는 조직을 두고 각국의 실제 수사기관들이 직접적으로 수사활동을 실행할 수 있도록 하는 공조시스템이 구축될 필요가 있다. 현재는 개별적인 사건에 대해서는 일시적으로 그러한 공조체계가 구축되어 작동하는 사례가 나오고 있으나, 암호화폐의 거래를 수단으로 하는 범죄가 어느 한 국가의 문제는

769) 암호화폐를 추적하는 프로그램에 대한 정보와 기술을 제공하는 곳으로는 Etherscan(http://etherscan.io), Blockchain.com(http://blockchain.com), Chainalysis(http://chainanalysis.com) (2019년 11월 4일 최종접속) 등이 있다.

분명히 아니고 암호화폐 거래의 시장은 앞서 보았듯이 전지구적으로 거대한 시장이 되어가고 있으므로 암호화폐와 같은 가상자산에 한정하더라도 국가 간 수사기구를 아우르는 특별공조체계를 마련할 필요성은 더 강조할 필요가 없어 보인다. 특히 이러한 공조체계는 정보의 신속한 공유와 추적을 가장 우선시할 필요가 있으며, 그러한 정보의 공유와 통제가 사설 거래소와 수사기관 간에도 이루어질 수 있도록 거래소의 참여와 협조를 함께 고려해야 한다.

한편 비공식적 국제공조로 취득한 증거는 위법수집증거가 되어 형사재판에서 사용하지 못하는 것이 아닌가 하는 의문이 있을 수 있으나, 이미 대법원은 형사사법공조가 적법한 절차에 따라 이루어졌는지 여부와 그 활동에 의해 수집된 증거의 증거능력은 무관하다는 입장을 표명한 바 있으며,[770] 외국의 서버에 존재하는 전자기록의 증거능력과 관련하여 무결성 요건을 어떻게 충족시킬 수 있을 것인가 등에 대한 실무적 문제점이 제기될 수도 있지만, 이 역시 대법원은 "피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 해쉬(Hash) 값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피' 또는 '이미징' 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 등으로 이를 증명할 수 있다"[771]고 하여 국제공조로 인한 증거능력의 문제는 특별히 발생하지 않을 것으로 생각된다.[772]

---

770) 대법원 2011. 7. 14. 선고 2011도3809 판결 참조.
771) 대법원 2013. 7. 26. 선고 2013도2511 판결 참조.
772) 물론 블록체인 분산원장 기술이 가지는 조작불가능성이라는 특성에 의해서도 이 문제는 쉽게 해결이 될 수 있을 것으로 보인다.

제2절 | 형사정책적 대응 방안

1. 사이버보안 강화 방안

가. 사이버보안 법제 현황

1) 문제의 상황

사이버공간의 헤게모니를 잡기 위한 선진국들의 경쟁이 점점 더 치열해 지고 있다. 미국과 중국, 유럽연합, 러시아, 일본 등 아날로그 세상의 맹주들은 사이버공간에서도 그 자리를 유지하기 위해서 많은 노력을 기울이고 있다. 그 뿐 아니라 그들은 사이버공간의 보안을 위해서도 강력한 정책을 펼치고 있는데, 사이버공간의 보안능력이 사이버공간의 헤게모니를 위해 매우 중요한 역할을 하기 때문이다.[773] 사이버공간은 이미 영토, 영공, 영해, 우주 등과 함께 국가의 안보 영역으로 여겨지고 있다.[774] 그래서 미국은 2010년 '국방검토보고서'에 사이버공간을 영토, 영해, 영공, 우주에 이어 제5의 전장으로 규정하고,[775] 사이버공간에 대해 공격을 하는 것은 미국 본토를 공격하는 것이므로 물리적 공격까지 취하겠다는 엄포를 놓기도 하였다.[776] 한국도 2010년 사이버사령부가 창설되었고, 2012년 사이버공간을 군사작전영역에 포함시켰다.[777] 이에 따라 사이버공간에서의 침해행위는 단순히 범죄행위를 넘어서서 테러행위, 더 나아가

773) 영어의 'Security'의 개념은 그 활용에 따라 한국에서는 외국으로 부터 국가의 안전을 유지하고 확보하는 '안보'라는 개념과 기밀을 보호한다는 '보안'으로 사용되기도 한다. 다만, 두 개념은 동전의 양면과 같아서 안보가 되어야 보안이 지켜지고, 보안이 되어야 안보가 지켜지게 되기 때문이다. 더욱이 'Cybersecurity'의 개념에서는 안보와 보안의 개념이 수렴하게 된다. 따라서 Security의 개념을 국방에서는 '안보'로, 사이버범죄 등과 관련해서는 주로 '보안'으로 사용되는데, 이는 사용 영역에 따른 기능적인 구분이며, 그 내포적인 의미에 큰 차이가 있는 것은 아니다. 따라서 본 보고서에서도 사이버범죄와 관련성을 고려하여 '보안'이라는 개념을 사용하고, 국방과 관련된 맥락에서는 '안보'라는 개념을 사용하고자 한다.

774) 문인철, "사이버공간의 특성과 안보화 문제", 국가안보와 전략 제17권 4호(통권 68호), 국가안보전략연구원, 2017, 158면.

775) Department of Defense, Quadrennial Defense Review Report, 2010.2, p.32, https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf (2019년 11월 3일 최종접속).

776) "미 국방부, "사이버 공격에 무장 대응하겠다"", IT World 2011년 6월 1일자, http://www.itworld.co.kr/news/70284#csidx5a9cbf7ffb89e28b56abdb6175857b8 (2019년 11월 3일 최종접속) 참조.

777) 강석구/이원상, 사이버범죄 관련 법령 정비방안, 한국형사정책연구원, 2014, 27면.

전쟁행위와도 연관을 맺게 된다.[778]

그런 맥락에서 최근 주요 선진국들은 사이버보안을 위해 기술적, 인적, 제도적, 법적, 국제 협력적 노력을 기울이고 있다. 사이버공간을 보호하기 위해서는 공격하는 자에 비해 기술적 수단이 우월해야 하고, 공격에 대응하기 위한 사이버전문가들이 준비되어 있어야 하며, 그를 위한 각 부처의 협력 및 예산 지원들의 제도적 장치가 필요하고, 대응 및 처리에 근거가 되는 법률이 마련되어야 하며, 사이버공간이 글로벌하게 펼쳐진 관계로 국제협력이 반드시 필요하기 때문이다. 사이버보안을 위해서는 모든 요소들이 중요하지만, 여기에서는 사이버보안의 근거가 될 수 있는 규정들에 대해서 좀 더 살펴보고자 하는데, 나머지 요소들이 모두 규정에 의해서 작동하기 때문이다.

근래 들어 미국, 유럽연합, 중국, 일본 등 주요 선진국들은 사이버보안 관련 규정들을 앞다투어 강화하고 있다. 심지어 미국은 중국의 통신장비 업체인 화웨이의 5G 통신장비 제품이 사이버안보에 위협이 된다는 이유로 동맹국들에게 화웨이 장비에 대해 보이콧을 하라는 요청을 하기도 하였다.[779] 사실 이는 단순히 사이버보안만을 위한 것은 아니다. 사이버보안은 산업과도 연관을 맺고 있기 때문이다. 따라서 표면적으로 사이버보안 관련 규정의 강화는 자국의 사이버안보를 위한 조치라고 할 수 있지만, 그 이면에는 자국의 사이버 관련 산업에 대한 보호막을 설정하는 것이기도 하다.[780] 그러므로 사이버보안 규정을 단순히 국가의 사이버안보를 위한 규정으로만 해석해서는 안 된다. 따라서 주요 선진국의 사이버보안 관련 규정에 대해서는 한국의 국가기관 뿐 아니라 기업들도 관심을 기울일 필요성이 있다. 그러므로 아래에서는 한국의 사이버보안 관련 법제 현황을 검토하고, 미국, 유럽연합, 중국, 일본 등 주요 국가들의 사이버보안 관련 규정을 살펴본 후 그 시사점을 도출하고자 한다.

---

778) 강석구/이원상, 앞의 보고서, 29면.

779) "화웨이: 서구는 왜 화웨이를 두려워 하는가?", BBC 코리아 2019년 3월 20일자, https://www.bbc.com/korean/international-47608166 (2019년 11월 3일 최종접속).

780) 직접적인 산업인 사이버보안 시장만 보더라도 전 세계 사이버보안 시장은 2017년 1,378억 달러로 추산되지만, 매년 11%의 성장을 하여 2022년에는 2,319억 달러에 이를 것으로 예상되고 있다. 넥스텔리전스, 2018 글로벌 정보보호 산업시장 동향조사, 한국인터넷진흥원, 2018, 3-4면.

2) 한국의 사이버보안 관련 법제 현황

미국, 유럽연합, 중국, 일본 등 주요 선진국들은 사이버공간의 보안에 대해 지대한 관심을 보이고 있다. 따라서 자국의 사이버공간을 보호하기 위한 다양한 노력을 기울이고 있다. 그 근간이 되는 것이 사이버보안 관련 법령을 제정하는 것이다. 물론 사이버보안 법률에 따라 구체적으로 실현하는 것도 중요하다. 그러나 우선 법적인 근거가 있어야 전문인력, 기술, 장비, 기관 간 협력, 재정 등 사이버보안을 구현하기 위한 필요한 요소들을 요청할 수 있게 된다. 그러므로 최근 주요 국가들은 사이버보안 관련 법령을 통해 사이버보안 체계를 구축하고 실현하고 있다.

그런 상황에서 한국도 사이버보안 관련 법률을 재정비할 필요성이 증대하고 있다. 이는 그 동안 한국이 하드웨어적으로는 세계 최고의 수준에 도달해 있지만, 법제적인 측면에서는 매우 더딘 발걸음을 걷고 있기 때문이다. 우선 사이버보안 관련 법령들을 살펴보면 다음과 같다.

- 정보통신망법 및 동 시행령, 시행규칙
- 정보통신기반 보호법 및 동 시행령, 시행규칙
- 국가정보화 기본법 및 동 시행령, 시행규칙
- 전자정부법 및 동 시행령
- 개인정보 보호법 및 동 시행령, 시행규칙
- 위치정보의 보호 및 이용 등에 관한 법률 및 동 시행령
- 정보보호산업의 진흥에 관한 법률 및 동 시행령, 시행규칙

이는 사이버보안 법령의 범위를 넓게 설정하였을 경우이며, 사실상 사이버보안과 관련된 법령은 정보통신망법과 정보통신기반 보호법, 개인정보 보호법, 위치정보보호법 정도라고 할 수 있다. 1992년 제14대 국회부터 지금까지 사이버보안과 관련된 법률안을 살펴보면 다음과 같다.

- 2006년 의안번호 175884 : 사이버위기 예방 및 대응에 관한 법률안(공성진의원등 17인)(임기만료 폐기)
- 2008년 의안번호 1801619 : 국가 사이버위기관리법안(공성진의원등 17인)(임기만료 폐기)

- 2013년 의안번호 1904286 : 국가 사이버안전 관리에 관한 법률안(하태경의원 등 11인)(임기만료 폐기)
- 2013년 의안번호 1904459 : 국가 사이버테러 방지에 관한 법률안(서상기의원 등 13인)(임기만료 폐기)
- 2015년 의안번호 1915185 : 사이버위협정보 공유에 관한 법률안(이철우의원 등 22인)(임기만료 폐기)
- 2015년 의안번호 1915777 : 사이버테러 방지 및 대응에 관한 법률안(이노근의원 등 13인) (임기만료 폐기)
- 2016년 의안번호 1918583 : 국가 사이버테러 방지 등에 관한 법률안(서상기의원 등 24인)(임기만료 폐기)
- 2016년 의안번호 2000032 : 국가 사이버안보에 관한 법률안(이철우의원 등 122인)(소관위 접수)
- 2017년 의안번호 2004955 : 국가사이버안보법안(정부안, 소관위 접수)

20대 국회 이전에 발의 되었던 사이버보안 관련 규정들은 제대로 된 논의도 되지 못하고 임기만료로 폐기 되었고, 20대 국회 들어서는 이철우 의원안과 정부안만이 존재하고 있다. 더욱이 2018년과 2019년에는 법률안조차도 제기되지 않고 있다. 아래에서는 우선 두 법률안에 대해서 살펴보고자 한다.

3) 사이버보안 관련 법률안 검토

(1) 국가 사이버안보에 관한 법률안[781]

① 제안이유

법률안에서는 한국의 사이버공간에 대한 사이버공격이 2009년 7.7디도스 사건 이후 꾸준히 증가하고 있으며, 피해범위가 공공역역 뿐 아니라 민간영역까지 전방위적으로 확대되고 있다고 지적하고 있다. 그에 반해 현행 법령에 따르면 공공부문과 민간부문이 분리되어 있어 적절한 대처가 어렵고, 대통령훈령인 「국가사이버안전관리규정」은 행정기관에만 초점을 두고 있기 때문에 민간부문 뿐 아니라 입법 및 사법기관 조차도 그 대상에서 제외되고 있어서 사이버공격에 대한 대처가 용이하지 않다고 하고 있다. 그러므로 해당 법률은 민간과 함께 정부가 체계적이고 통합적인 체계를 구축하여 사이버공격의 탐지 및 조기차단 등에 신속하게 국가 역량을 집중하기 위한

781) 의안번호 32. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_L1Z6M0L5M3W0U1W4T2M8K4L3S5I0Y2 (2019년 11월 3일 최종접속).

것을 목적으로 하고 있다고 밝히고 있다. 해당 법률안의 제안 취지를 보면 사이버보안을 위해 국가의 통합체계를 구축한다는 취지는 적절하다고 판단되지만, 최근 문제가 되고 있는 사물인터넷이나 A.I., 암호화폐, 자율주행자동차, 5G 등이 충분히 고려된 법률안으로는 보이지 않는다.

② 주요내용

해당 법률안의 주요내용을 살펴보면 다음과 같다.

- 사이버안보에 심의를 위한 대통령 소속 "국가사이버안보정책조정회의" 설치(안 제4조)
- 한국의 통합적인 사이버안보 업무 수행을 위해 국가정보원장 소속 "국가사이버안보센터" 설치(안 제6조)
- 국가정보원장은 사이버안보 기본계획을 수립 및 시행계획을 작성하여 책임기관의 장에게 배포(안 제7조)
- 책임기관의 장은 사이버공격에 대비한 "보안관제센터" 구축(안 제10조)
- 책임기관의 장은 국가정보원장과 다른 책임기관 장에게 사이버위협정보를 제공하고, 국가정보원장은 "국가사이버위협정보공유센터"를 구축·운영함(안 제11조)
- 책임기관의 장은 사이버공격 시 사고조사 결과를 중앙 행정기관 장 및 국가정보원장에 통보(안 제12조).
- 국가정보원장은 사이버위기경보 발령을 하고, 책임기관의 장은 피해 최소화 및 피해복구(안 제14조).
- 정부는 경계단계에 따라 "사이버위기대책본부" 구성·운영(안 제15조).
- 정부는 능력을 고려하여 사이버안보 전문업체 지정·관리(안 제16조).
- 정부는 사이버안보를 위한 기술개발·산업육성·인력양성 등 시책추진(안 제19조, 제20조 및 제21조).

③ 법률안 평가

일단 본 법률안은 현행 대통령훈령인 "국가사이버안전관리규정"을 법률로 규정하는 것 이상의 내용이 존재하지 않고 있다. 따라서 최근의 사이버범죄 관련 문제들을 규정하고, 새로운 환경에 맞는 국가적인 체계를 구축하기 위한 내용 보다는 현재 국가정보원이 담당하고 있는 업무를 법률로 격상시켜 주는 이상의 내용이 보이지 않고 있다. 무엇보다 국가정보원은 정보기관이기 때문에 국가 사이버보안체계를 총괄하는 것에는 한계가 있다. 그리고 조문을 살펴보면 사실상 사이버보안과 관련된 문제는 각 책임단체의 장에게 책임과 권한이 분산되어 있기 때문에 결국 통합된 사이버보안 체계가 적절하게 운영될 수 있을지는 의문이다.

(2) 국가 사이버안보법안[782]

① 제안이유

"국가 사이버안보법안"은 정부안으로 제출되었다. 제안이유를 살펴보면 사이버공격이 민간영역과 공공영역에 걸쳐 광범위하게 발생하고, 그로 인한 경제피해와 사회혼란도 크기 때문에 "국가사이버안보위원회"를 설치하고, 국가기관 등을 책임기관으로 정하여 사이버보안 임무를 부여하고, 사이버위협정보 공유 및 사이버공격 탐지와 대응 등의 절차를 명확히 하여 한국의 사이버안보 체계를 강화하는 것을 목적으로 삼고 있다. 다만, 제안이유에서도 간략히 살펴볼 수 있는 것처럼, 해외 주요 국가들은 이미 사이버보안에 대해서 2.0으로 넘어서고 있는데, 한국은 여전히 과거의 사이버보안 의식에 정주하고 있는 것으로 보인다. 그 이유는 사이버보안에 대한 구체적이고 세밀한 사고 보다는 기존의 나이브하고 추상적인 사고에서 사이버보안 체계를 구축하려는 경향이 보이기 때문이다. 이는 사이버보안에 대한 위험성은 알고 있지만, 지속적이고 체계적이며, 통합적인 연구가 미흡하기 때문으로 여겨진다. 무엇보다 권한 있는 주무기관이 지속적으로 사이버보안에 대한 관심을 가지고 체계를 구축할 필요성이 있어 보인다.

② 주요내용

해당 법률안의 주요내용은 크게 사이버안보 추진기구, 사이버안보를 위한 예방활동, 사이버안보를 위한 대응활동 등으로 구성되어 있다. 여기서 핵심은 사이버안보 추진기구라고 할 수 있다. 이는 해외 주요 국가들이 사이버보안을 담당하기 위해 통합적인 기관을 구축하는 것에 비견될 수 있다. 본 법률에서는 "국가사이버안보위원회"의 설치(안 제5조)를 규정하고 있는데, "사이버안보와 관련된 국가의 정책 및 전략 수립에 관한 사항 등을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회를 두되, 위원회는 위원장을 포함하여 20명 이내의 위원으로 구성하고, 위원장은 국가안보실장으로, 위원은 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관의 차관급 공무원 중 대통령령으로 정하는 사람과 사이버

782) 의안번호 4955. 국회 의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=ARC_C1J7Y0Z1J0B3I1K6D4K6M4X8X9W8W1 (2019년 11월 3일 최종접속).

안보에 관하여 전문적인 지식과 경험을 갖춘 사람 중에서 국가안보실장이 임명하거나 위촉"하도록 하고 있다. 그리고 국가기관 및 지방자치 단체 등에 책임기관을 지정하고, 국가정보원장이 지원하도록 구성하고 있다(안 제6조 및 제7조).

사이버안보를 위한 예방활동으로 국가정보원장이 사이버안보 기본계획 및 시행계획을 수립하도록 하고 있다(안 제10조). 그리고 국가정보원장은 중앙행정기관 등을 대상으로 사이버안보 실태 평가를 하게 되고(안 제11조), 사이버위협정보에 대해서는 국가정보원장 소속으로 "사이버위협정보공유센터를 두어 공유하도록 하고 있다(안 제12조). 그리고 사이버안보를 위한 대응활동으로 책임기관의 장은 "보안관제센터"를 구축하거나 위탁하여 사이버공격의 탐지 등을 하고(안 제14조), 또한 사이버공격으로 인한 사고를 통보 및 조사하는데(안 제15조), 경우에 따라서는 국가정보원장이 조사할 수 있다. 그리고 국가정보원장은 사이버위기경보의 발령 및 사이버위기대책본부를 구성하여 운영할 수 있다(안 제16조 및 제17조). 정부안의 내용을 살펴보면 앞의 법률안과 큰 차이가 보이지 않는다.

③ 소결

위의 법률안에 대해서 국회의 검토보고서를 살펴보면 여러 부분에서 미흡한 부분들이 드러나고 있다. 우선 책임기관을 통해서 사이버보안의 권한과 책임을 분산시키는 문제이다. 책임기관의 숫자가 공공기관이 11,178개, 민간이 256개로 대부분의 인터넷 사용이 민간부문인 것을 고려하면 실효성이 의심될 수밖에 없다.[783] 더욱이 국가가, 그것도 국가정보원이 민간기관까지 사이버보안을 이유로 점검하도록 하고 있는 것은 그 취지와 상관없이 민간에 대한 통제로 비춰질 수 있게 된다.[784] 무엇보다 해당 법률안은 사이버보안을 위해 너무도 많은 계층이 존재하고 있고, 추진과 계획은 국가정보원이 하게 되는데 사이버보안에 대한 책임은 책임기관에서 지게 되고, 지원은 한국인터넷진흥원을 비롯해 산재되어 있는 기관에서 하게 되고, 상위에는 위원회가 있는 구조이다. 해외 주요 국가들이 사이버보안과 관련해서 조직의 층위를 줄이고,

783) 「국가사이버안보법안」 검토의견서, 국회의안정보시스템, http://likms.assembly.go.kr/bill/billDetail.do?billId=ARC_C1J7Y0Z1J0B3I1K6D4K6M4X8X9W8W1 (2019년 11월 3일 최종접속) 25-26면.

784) 앞의 「국가사이버안보법안」 검토의견서, 28면.

권한과 책임을 집중하고, 인력 및 기술의 지원도 통합하는 경향에 비하면 너무나도 아날로그적인 조직체계라고 할 수 있다.

나. 국제사회의 입법 대응 현황

1) UN차원에서의 논의

(1) UN 및 CCPCJ 결의

UN차원에서는 사이버보안을 포함하여 사이버범죄에 대한 글로벌 프로그램을 가동 중에 있다. 유엔총회 결의 65/230호와[785] 범죄예방 및 형사사법위원회(CCPCJ) 결의 22/7[786] 및 22/8에[787] 따르면 UN차원의 사이버범죄에 관한 글로벌 프로그램을 통해서 회원국들에 대한 기술 지원 및 역량강화를 통해 사이버범죄에 적극 대응하도록 노력하고 있다. 따라서 글로벌 프로그램을 시행하기 위한 전단계로서 UNODC는 '개방형 정부 간 전문가 그룹(open-ended intergovernmental expert group)'을 만들어서 사이버 범죄 문제의 현황과 회원국, 국제사회 및 민간부문의 대응을 종합적으로 연구하고 있다. 해당 연구에서는 국가 법률, 모범사례, 기술지원 및 국제 협력 등에 대한 내용이 포함되어 있다.[788]

UN 총회결의가 보다 구체화된 CCPCJ결의 내용을 살펴보면, CCPCJ 결의 22/7에서는 살바도르 선언을 근거로 해서 사이버범죄에 대한 포괄적인 연구를 수행하기로 한다. 그 가운데에는 사이버보안과 관련된 내용이 포함된다. 결의문에서는 전문가 그룹 회의의 결과물인 '사이버 범죄에 관한 포괄적 연구'에 대해 지속적인 논의를 하고, CCPCJ의 주도로 계속해서 사이버범죄에 대한 관심 및 사이버범죄에 대한 종합적인 연구가 수행되어야 하며, UNODC에서는 연구결과물을 6개의 공식언어로 번역하여 배포하고, 회원국들은 전문가 그룹 업무를 지원하기 위해 추가적인 자원을 제공

785) Resolution 65/230, https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/230 (2019년 11월 3일 최종접속)

786) Resolution 22/7, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf (2019년 11월 3일 최종접속).

787) Resolution 22/8, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf (2019년 11월 3일 최종접속).

788) UNODC, Cybercrime, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (2019년 11월 3일 최종접속).

하며, 업무추진 상황을 지속적으로 CCPCJ에 보고하도록 하고 있다.[789]

CCPCJ 결의 22/8에서는 좀 더 내용이 구체화 된다. 유엔범죄마약국(United Nations Office on Drugs and Criminal)으로 하여금 회원국들과 협력하여 다양한 유형의 사이버범죄를 예방, 탐지, 수사 및 기소하고, 컴퓨터 네트워크의 보안을 강화하기 위해 회원국의 관련 법규를 개선하도록 권고하는 한편, 회원국의 담당기관의 역량을 구축 및 강화하기 위해 회원국에 대한 기술지원 및 훈련을 활성화하도록 요청하였다.[790] 그에 대한 추진계획으로서 CCPCJ 결의안 20/7에서 기술지원 및 역량강화를 위해 노력해야 한다는 것을 연계시키고 있다. 그래서 2차 전문가 그룹 회의 결과를 토대로 UNODC로 하여금 회원국과 협력하여 '사이버 범죄에 관한 글로벌 프로그램(Global Programme on Cybercrime)'의 이행을 촉진하도록 요청하고, 더 나아가 정부 간 상설 실무그룹을 요청하고 있으며, 사이버범죄에 대응하기 위해서 회원국 및 관련 단체, 그리고 민간부문 및 시민 사회와 기술지원 및 역량강화를 위한 파트너십 강화를 요청하고, 회원국들이 보다 적극적으로 추가 자원을 제공하도록 하고 있다.[791]

(2) UN 차원의 사이버보안 관련 법제

유럽연합에는 '유럽 사이버범죄 방지협약(Convention on Cybercrime)'이 존재하고 있다. 해당 규정에서는 일부 사이버보안과 관련된 실체법 조항이 부분적으로 존재하고 있다. 또한 'EU 사이버보안법'에도 주무기관과 사이버보안 인증을 위한 근거 규정이 존재하고 있다. 한편 본 보고서에서는 비중 있게 다루고 있지 않지만, 아프리카 연합차원에서도 이미 사이버보안과 관련된 초안이 만들어지기도 하였다.[792] 이처럼 지역단위나 국가단위에서는 사이버보안과 관련된 법제가 만들어지고 있는 상황이다. 그에 반해 UN차원에서는 아직까지 사이버보안 관련 법제는 마련되어 있지 않다. 현재

---

789) Resolution 22/7, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf (2019년 11월 3일 최종접속).

790) Resolution 22/8, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf (2019년 11월 3일 최종접속).

791) Resolution 22/8, https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf (2019년 11월 3일 최종접속).

792) DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBER SECURITY IN AFRICA, https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf (2019년 11월 3일 최종접속).

기본적인 논의가 진행되고 있으며, 회원국들 간의 의견을 조율하고 있는 상황이다. 앞서 언급한 전문가 그룹 회의는 2019년 3월 비엔나에서 5차 회의를 진행하였다. 2013년에 초안이 만들어진 이후,[793] 지금까지 해당 내용을 검토하고 있다. CCPCJ에서도 지속적으로 관심을 보이고 있으며, 주무기관으로서 UNODC가 관련 업무를 계속해서 수행하고 있다. 사이버보안과 관련된 주요 사항 역시 회원국들의 사이버보안 역량강화 및 기술지원이라고 할 것이다. 회원국별로 사이버보안에 대한 역량이 서로 다르고, 사이버공격 기술이 발전함에 따라 그에 상응하는 대응기술이 마련되어야 하기 때문이다. 다만, 개발도상국들은 역량강화 및 기술지원을 위해서 선진국들이 보다 많은 재정적 노력을 할 것을 요구하고 있는 반면, 선진국들도 계속적인 재정지원에 대해 어려움을 표시하고 있기 때문에 논의가 다소 더디게 진행되고 있다. 더 나아가 사이버보안에 대한 중국과 러시아의 입장과 미국, 유럽연합, 일본 등의 입장이 대립하는 양상을 보이기도 한다. 특히 미국을 비롯한 유럽연합, 일본 등은 유럽 사이버범죄 방지협약을 국제협약으로 확대하려고 노력하는 것에 반하여 중국과 러시아는 국제적으로 새로운 사이버 질서를 마련하고, 그들이 그 중심이 되려고 노력하고 있다. 따라서 UN 차원에서의 사이버범죄 및 사이버보안에 대한 규정이 만들어지기 까지는 많은 어려움이 있을 것으로 예상된다.

2) 미국

(1) 사이버보안 관련 규정 개관

전 세계에서 사이버보안 규정에 있어 가장 선두에 있다고 볼 수 있는 것이 미국이다. 미국의 사이버공간은 전 세계의 수많은 공격자들의 대상이 되고 있기 때문이다.[794] 따라서 현실공간에서 세계 최강인 미국은 사이버공간에서도 최강의 지위를 유지하기 위해서 노력하고 있다. 사이버보안 기술이나 인력, 체계, 실무 등 실질적인 사이버보안 능력뿐 아니라 사이버보안과 관련된 강력한 정책과 법률들을 마련하고 있다. 미국의

793) Comprehensive Study on Cybercrime Draft—February 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (2019년 11월 3일 최종접속).

794) "2018년 미국 사이버범죄 현황, "보안 지출 증가하고, 위험도 증가"", IT World 2018년 11월 7일자, http://www.itworld.co.kr/insight/111396#csidx976fdb63579871aa5114b7cbf260aed (2019년 11월 3일 최종접속).

사이버보안과 관련된 종래의 법률들을 살펴보면, 국토안보법(Homeland Security Act of 2002), 컴퓨터 보안법(Computer Security Act(1987년)), 애국법(USA Patriot Act), 연방정보보안관리법(Federal Information Security Management Act, FISMA(2002년)), 사이버보안 강화법(Cyber Security Enhancement Act of 2002), 해외정보 감시법(Foreign Intelligence Surveillance Act, FISA(2007년)), 법집행기관을 위한 통신지원법(Communications Assistance for Law Enforcement Act, CALEA(1994년)) 등이 있다.[795] 해당 법률들은 주로 미국이 9.11 테러를 당한 이후, 2002년에 '국토안보를 위한 국가전략(National Strategy for Homeland Security)'이 수립되면서 사이버공간에 대한 보호가 국가의 주요 전략으로 포섭됨에 따라 도입된 규정들이다.[796]

그러다 근래 들어 사이버공격의 형태가 보다 다양해지고, 그 피해도 증가하는 추세를 보이고 있으므로 사이버보안에 대한 중요성이 다시금 강조되면서 '연방 정보보안 현대화법', '국가 사이버보안 보호법', '사이버보안 강화법', '국토안보부 사이버보안 인력채용 및 유지법', '사이버보안 인력 평가법', '사이버보안 정보공유법' 등이 새롭게 제정되기에 이르렀다.[797] 더 나아가 2018년 말에는 기존의 '국토안보부법'을 개정하여 사이버보안 및 기반시설보안청법(Cybersecurity and Infrastructure Security Agency Act of 2018, 이하 'CISA법'이라고 함)을 만들면서 사이버보안에 대한 주무기관과 그에 대한 물리적 및 사이버위협 대처방안, 민간조직과의 협력방안이 법률로 보다 구체화 되었다.[798] 해당 법률의 핵심은 사이버보안 및 기반시설보안청(Cybersecurity and Infrastructure Security Agency, 이하 'CISA'라고 함)이 기존에 사이버보안 정책을 담당하던 '국가보호프로그램위원회(NPPD)'를 대체하는 상설기관이 된 것이다.[799] 이는 아래의 유럽연합 법률에서도 ENISA가 상설화 되어 유럽연합의 사이버보안 관련 사무를 관장하게 된 것과 같은 맥락이라고 할 것이다. 즉, 사이버보안을 위한 실질적인 권한과 능력을 가진 컨트롤타워를 구축한 것이다. 그에 따라 앞으로 미국의 사이버보안 정책은 CISA를 중심으로 이루어지게 될 것이다.

---

795) 이연수/이수연/윤석구/전재성, "주요국의 사이버안전 법·조직체계 비교 및 발전방안 연구", 국가정보연구 제1권 제2호, 한국국가정보학회, 2008, 65면.
796) 이연수/이수연/윤석구/전재성, 앞의 글, 64-65면.
797) 양천수/지유미, "미국 사이버보안법의 최근 동향 - '사이버보안 정보공유법'을 중심으로 하여'", 법제연구 제54호, 한국법제연구원, 2018, 161-162면.
798) 국회도서관, 현안관련 외국입법례, 제51호, 2018, 2면.
799) CYBERSECURITY, https://www.cisa.gov/cybersecurity (2019년 11월 3일 최종접속).

(2) 기존 사이버보안 규정들의 개관

미국의 경우 사이버보안과 관련해서 여러 법률들이 제정되어 있다. 특히 2014년경에는 2기 오바마 정부가 사이버보안의 중요성을 강조함에 따라[800] 사이버보안과 관련된 법률들이 다수 제정되었는데, 그에는 '국가 사이버보안 보호법(National Cybersecurity Protection Act of 2014)', '연방 정보보안 현대화법(Federal Information Security Modernization Act of 2014)', '사이버보안 강화법(Cybersecurity Enhancement Act of 2014)', '국토안보부 사이버보안 인력채용 및 유지법(DHS Cybersecurity Workforce Recruitment and Retention Act)', '사이버보안 인력평가법(Cybersecurity Workforce Assessment Act)' 등이 있다.[801] 2기 오바마 정부 들어 미국이 지속적으로 사이버공격을 받게 되면서 사이버공간에서의 보안문제가 주요 정책으로 떠오르게 되었고, 그에 따라서 오바마 대통령은 사이버보안과 관련된 앞의 법률에 서명을 하게 되었다.[802]

해당 법률들의 특징은 크게 사이버보안에 있어 연방정부로의 권한 집중, 공공부문과 민간부문의 정보공유 강화, 사이버보안 인력 관련 시스템의 강화 등으로 평가되기도 한다.[803] 그런 맥락에서 다섯 개의 법률을 살펴보면 다음과 같은 특징들이 보이게 된다. 첫째로, '국가 사이버보안 보호법'의 핵심은 '국가 사이버보안 및 통신 통합센터(National Cybersecurity and Communications Integration Center, 이하 'NCCIC'라고 함)'의 권한강화이다. 국토안보부 차관이 센터를 맡게 되어 정부기관들뿐 아니라 민간기관에 대한 통합적 권한이 부여되고, NCCIC가 정부와 민간부분의 사이버보안 조정자의 역할을 수행하게 되었다.[804] 이를 위해 NCCIC는 사이버보안에 대한 정부기관과 민간부분에 대한 정보공유 및 조정을 하게 되고, 보안위협을 방지하는 역할을 수행하며, 그러한 업무가 프라이버시보호나 법률에 따라 이루어 질 수 있도록 권한과 책무를 갖게 되었다.[805]

---

800) 송은지/강원영, "미국 오바마 정부 2기의 사이버보안 강화정책", INTERNET & SECURITY FOCUS 2014년 9월, 한국인터넷진흥원, 2014, 9면.

801) Congress Passes Five Cybersecurity Bills, https://www.insideprivacy.com/united-states/congress-passes-four-cybersecurity-bills/ (2019년 11월 3일 최종접속).

802) 양천수/지유미, 앞의 글, 161면.

803) 양천수/지유미, 앞의 글, 162면.

804) S.2519 - National Cybersecurity Protection Act of 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2519 (2019년 11월 3일 최종접속).

둘째로, '연방 정보보안 현대화법'의 핵심은 사이버보안 정책의 감독 및 관리 강화이다. '연방 정보보안 현대화법'은 예산관리국장이 정보보안 및 실행을 감독하도록 함으로서 국토안보부의 사이버보안 관리기능을 강화시켰던 기존의 '연방 정보보안 관리법(Federal Information Security Management Act of 2002)'을 보다 강화시키는 방향으로 개정된 것이다.[806] 따라서 국토안보부가 비국가 보안 연방 행정각부 시스템에 대해서도 기술지원 및 해당 시스템에 대한 기술구현을 포함하여 정보보안 정책을 구현하는 것을 관리하는 권한을 갖게 되었고, 연방기관의 정보보안 실행에 대한 예산관리국장의 감독 권한을 수정하고 보다 명확하게 하였다. 또한 예산관리국장에 대해 비효율적이며 소모적일 수 있는 보고를 없애기 위해 'OMB A-130'을 수정 및 개정할 것도 요구하고 있다.[807]

셋째로, '사이버보안 강화법'의 핵심은 민관협력 강화 및 사이버보안 인식강화이다.[808] 그에 따라 법률의 내용도 사이버보안에 대한 민관협력(제1절), 사이버보안 연구 및 개발(제2절), 교육 및 인력개발(제3절), 사이버보안에 대한 인식 및 준비(제4절), 사이버보안 기술표준 강화(제5절) 등으로 구성되어 있다.[809] 해당 법률에서는 국립표준기술원(National Institute of Standards and Technology, 이하 'NIST'라고 함)의 역할이 상당히 강조되고 있다. 그래서 NIST의 장에게 민간분야와의 조정임무, 국가안보기관의 장들과 협의, 정보보안 대책 및 통제를 위한 효과적이고 효율적인 방안 모색, 표준과 모범 사례 통합 및 국제기준과의 정합 문제와 규제의 중복여부 등에 대한 관리와 방법 모색 등의 책무를 부과하고 있다.[810]

넷째로, '국토안보부 사이버보안 인력채용 및 유지법'과 '사이버보안 인력평가법'의 중점은 국토안보부 장관이 사이버보안 인력을 채용하고, 강화시키는 권한을 갖고 사이버보안 인력을 지속적으로 양성하고 충원 및 유지하는 것이다. 따라서 전자의 법률

805) 양천수/지유미, 앞의 글, 164면.
806) H.R.3844 - Federal Information Security Management Act of 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844 (2019년 11월 3일 최종접속).
807) Federal Information Security Modernization Act, https://www.dhs.gov/cisa/federal-information-security-modernization-act (2019년 11월 3일 최종접속).
808) 양천수/지유미, 앞의 글, 165면.
809) S.1353 - Cybersecurity Enhancement Act of 2014, https://www.congress.gov/bill/113th-congress/senate-bill/1353 (2019년 11월 3일 최종접속).
810) S.1353 - Cybersecurity Enhancement Act of 2014, https://www.congress.gov/bill/113th-congress/senate-bill/1353 (2019년 11월 3일 최종접속).

에서는 국토안보부 장관이 매년 정해진 기간에 미의회에 사이버보안 직원의 채용과 유지를 위한 계획, 해당 계획이 국토안보부 인력충원 계획과 통합되는 방식, 채용인력 및 퇴직인력 현황, 상관의 새로운 보안인력에 대한 훈련 방식 등에 대한 보고를 해야 한다.[811] 그리고 후자의 법에서는 국토안보부 장관이 중요한 사이버보안업무의 범주와 전문분야를 결정하고, 인력관리국장에게 그와 관련된 내용과 함께 새롭고 시급한 기술부족 상황 등을 확인하며 그 지침에 대한 내용을 보고하도록 하여 대책을 세우도록 하고 있다.[812]

이처럼 미국의 기존의 사이버보안 관련 법률들은 국토안보부를 중심으로 다른 국가기관이나 민간기관 등이 협력하고, 국토안보부의 NCCIC가 허브의 역할을 하는 형국이었다. 그런 가운데 2018년 CISA법이 발효되면서 국토안보부는 사이버보안에 대한 권한은 한층 더 강력해 지게 되었으며, CISA를 통해서 사이버보안에 대한 허브 역할을 넘어 실질적인 컨트롤타워로서의 역할을 수행할 수 있게 되었다. 그러므로 아래에서는 CISA법에 대한 내용을 좀 더 살펴보고자 한다.

(3) CISA 업무개관

CISA는 사이버보안 및 기반시설보안을 위해 연방네트워크 보호, 종합적인 사이버공간 보호, 기반시설 복원 및 현장 운영, 사이버보안 위협에 따른 긴급통신 등 사실상 미국 국가차원에서의 사이버보안 업무 전반을 관할하는 역할을 수행하는 기관이다.[813] 한국에는 그와 비슷한 역할들을 '한국인터넷진흥원'과 '방송통신위원회', '과학기술정보통신부', '청와대 비서실', '국가정보원' 등이 나누어서 수행하고 있는데 반해, CISA는 포괄적인 권한을 가지고 수행하게 되어 형식상 및 사실상 미국 사이버보안 컨트롤타워 역할을 수행한다고 할 수 있다. CISA는 트럼프 대통령이 2018년 11월 16일 CISA법에 서명을 하게 되면서 탄생하게 되었다. 그를 통해 미국 국토안보부(Department of Homeland Security) 내의 NCCIC를 포함해서 국가보호 및 프로그램 관리국(NPPD)의 업무가 CISA를 통해 인계되는데, 이를 위해 NCCIC는 2017년 조직

811) S.1353 - Cybersecurity Enhancement Act of 2014, https://www.congress.gov/bill/113th-congress/senate-bill/1353 (2019년 11월 3일 최종접속).

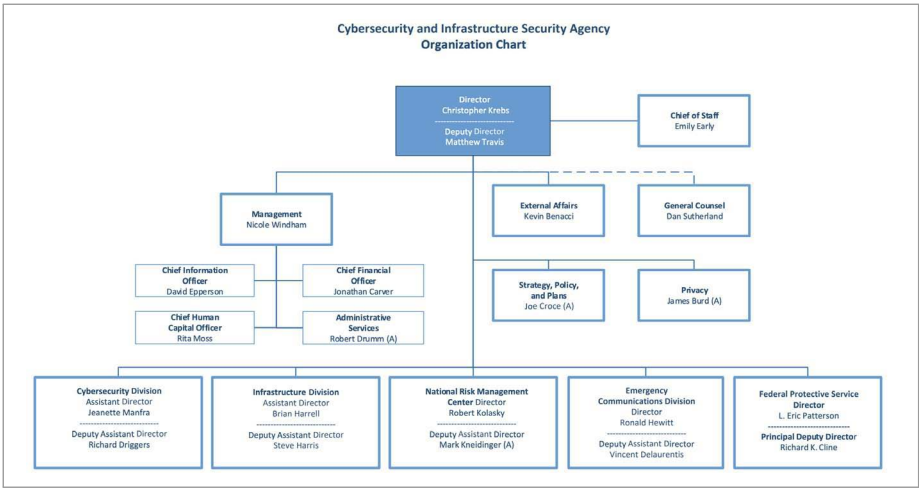
812) S.2354 - DHS Cybersecurity Workforce Recruitment and Retention Act of 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2354 (2019년 11월 3일 최종접속).

813) CISA 홈페이지, https://www.us-cert.gov/about-us (2019년 11월 3일 최종접속) 참조.

구조를 정비하여 이전의 '미국 컴퓨터 비상대응팀(US-CERT)'과 '산업 제어시스템 사이버 비상대응팀(ICS-CERT)'에 의해 독립적으로 수행되던 기능을 통합하였다.[814]

이전까지 미국 국토안보부의 산하기관으로는 미국 이민국(U.S. Citizenship and Immigration Services, USCIS), 미국 연안경비대(United States Coast Guard, USCG), 미국 세관(United States Customs and Border Protection, CBP), 미국 재난관리청(Federal Emergency Management Agency, FEMA), 미국 법집행관 훈련 센터(Federal Law Enforcement Training Center, FLETC), 미국 이민세관집행국(United States Immigration and Customs Enforcement, ICE), 미국 국토안보부 비밀수사국(United States Secret Service, USSS), 미국 교통안전국(Transportation Security Administration, TSA) 등이 있었는데, CISA도 미국 국토안보부 내의 산하기관으로서 크게 사이버보안, 기반시설보안, 비상통신, 국가위험관리 등의 업무를 수행하게 되었다.[815] 그에 따른 CISA의 조직도는 아래와 같다.

[그림 5-1] CISA 조직도[816]



조직도를 살펴보면 CISA의 업무가 크게 다섯 가지로 구분되고 있는 것을 알 수 있다. 사이버보안 관련 업무(Cybersecurity Division), 기반시설 관련 업무(Infrastructure

814) CISA 홈페이지, https://www.us-cert.gov/about-us (2019년 11월 3일 최종접속) 참조.
815) Operational and Support Components, https://www.dhs.gov/operational-and-support-components (2019년 11월 3일 최종접속).
816) 이미지출처: CISA 홈페이지, https://www.us-cert.gov/about-us (2019년 11월 3일 최종접속).

Division), 사이버공간과 관련된 국가 위기관리 업무(National Risk Management Center), 긴급통신 전달업무(Emergency Communication Division), 그리고 연방 보호를 위해 지원해 주는 업무(Federal Protective Service) 등이다. 이와 같은 조직이 구성되고 있는 것은 CISA법에서 CISA의 역할을 구체적으로 명시하고 있기 때문이다. 그러므로 아래에서는 CISA법의 내용에 대해서 좀 더 살펴보고자 한다.

(4) CISA법 분석

CISA법을 보면 우선 제2201조에서는 주요기반시설 정보(CRITICAL INFRASTRUCTURE INFORMATION), 사이버보안 위험(CYBERSECURITY RISK), 사이버보안 위협(CYBERSECURITY THREAT), 국가 사이버보안 자산에 대한 대응 활동(NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.), 특별전담 에이전시(SECTOR- SPECIFIC AGENCY), 공유(SHARING) 등 해당 법률 규정에 나오는 용어들에 대한 정의를 내리고 있다.

이어서 제2202조에서는 사이버보안 및 기반시설보안청(이하 '보안청'이라고 함)에 대한 규정을 하고 있다. 해당 규정을 살펴보면 보안청의 책임가운데 가장 주요한 것은 연방기관들과의 조정자로서의 역할을 수행하는 것이다(제2202조 (c)). 그와 함께 보안청과 특별전담 에이전시와의 협업(제2202조 (c) (6)), 보안청 내부 부서들의 협의와 협업(제2202조 (c) (7), 전략계획 및 위험에 대한 평가(제2202조 (c) (8)) 등의 업무를 수행하게 된다. 또한 보안청은 사이버보안 및 기반시설보안에 대한 주무기관으로서 보안 취약성에 대한 포괄적인 평가(제2202조 (e) (1) (B)), 평가를 바탕으로 다른 기관들에 대한 권고(제2202조 (e) (1) (C)), 국가 차원의 종합적인 조정 계획 수립(제2202조 (e) (1) (E)), 보안 위험 분석을 통해 다른 기관들에게 국가의 주요 자원 및 기반시설 보호 방안 권고(제2202조 (e) (1) (F)), 검토와 분석 및 권고 등을 통해 향상된 국가의 정책 및 절차 마련(제2202조 (e) (1) (G)), 국가 기관 등에 대한 적절한 컨설팅(제2202조 (e) (1) (I)), 다른 기관들과 훈련 등에 대한 조정(제2202조 (e) (1) (M)) 및 국가의 주요 법집행기관들과의 관련 업무 조정(제2202조 (e) (1) (N)) 등 사이버보안과 관련된 다양한 업무를 수행하게 된다. 그 내용들을 살펴보면 사이버보안에 대해서 사실상 허브역할과 함께 컨트롤타워 및 정책설정의 역할도 수행하는 것으로 보인다.

무엇보다 눈에 띄는 것은 보안청에 '프라이버시 담당관'을 두어 프라이버시와 관련

된 문제들을 별도로 취급하도록 하는 것이다(제2202조 (h)). 프라이버시 담당관은 보안청이 기술적인 수단을 사용할 때, 프라이버시가 침해되지 않는지 등을 살펴보게 되며(제2202조 (h) (A)), 해당 수단과 관련된 법적 평가나(제2202조 (h) (C)) 그로 인한 프라이버시 영향평가(제2202조 (h) (C)) 등의 업무를 수행하게 된다. 이는 사이버보안 문제가 프라이버시와 깊은 연관이 있으며, 대응을 위해서는 프라이버시가 침해될 수 있을 가능성이 존재한다는 것을 의미하기도 한다.

제2203조에서는 보안청 내에 사이버보안 부서를 두어 보안청 내에서의 사이버보안 업무와 '2015년 사이버보안법' 등에 부합하는 사이버보안 활동을 수행하게 된다(제2203조 (b)). 제2204조에서는 보안청 내에 기반시설보안 부서를 두도록 하고 있다. 기반시설보안 부서는 기반시설보안을 위한 노력을 기울이게 되는데, 화학시설 테러방지 표준 프로그램이나 질산암모늄 프로그램 등에 따라 안전을 보장하는 역할을 하게 된다(제2204조 (b)). 그리고 기반시설보안 부서는 관련 법률에 따라서 다양한 지위를 갖게 되는데, 2002년 국토안보법에서는 차관으로서의 지위를(6 USC 652), 긴급 통신 전달에 있어서는 책임자로서의 지위를(6 USC 571), 사이버보안과 통신전달에 있어서는 차관보로서의 지위를(6 USC 653), 기반시설 보호에 있어서도 차관보로서의 지위를(6 USC 654) 갖게 된다(제2204조 (b)).[817] 이처럼 다양한 지위를 부여하는 것을 통해 여러 관련 업무를 수행하는 것에 있어 상당한 실무적 권한을 부여하고 있는 것을 알 수 있다.

보안청 책임자는 미국 의회에 법률에 의해 요구되는 보고를 해야 한다. 따라서 보안청 책임자는 정해진 기간 내에 미국 의회에 운영에 관한 사항 등 보안청과 관련된 다양한 정보를 보고해야 하고(제2204조 (d)), 사이버보안 인력평가법(Cybersecurity Workforce Assessment Act)에 따라 해당 기관이 인력을 어떻게 충원하고 있는지에 대해 의회에 보고해야 한다(제2204조 (d)). 그 뿐 아니라 보안청의 시설과 관련된 사항에 대해서도 의회에 보고해야 한다(제2204조 (d)). 이는 보안청이 기본적으로 국회의 감시 및 감독을 받기 때문이다.

그 외에도 CISA법에서는 기술 및 구성요소와 관련해서 2002년 국토안보법 규정(제2204조 (g))뿐 아니라 2015년 사이버보안법(제2204조 (h) (1)), 중소기업법(제2204조

817) 제2204조에서는 동일한 수준에서 (b) 조항이 두 개가 나타나게 된다. 입법상의 오류로 판단된다.

(h) (2)), USC 제5편(제2204조 (h) (3)), 국토안보법 목차(제2204조 (i)) 등 해당 법률과 연관이 될 수 있는 여러 법률들의 규정들을 개정하고 있다. 이는 독일의 'Artikelgesetz' 또는 'Mantelgesetz'와 같이 하나의 법률이 개정될 경우 그 법률과 관련된 다른 법률들을 함께 개정하는 방식을 취하고 있는 것이다.

결론적으로 볼 때, CISA법은 보안청의 지위를 설정하고, 보안청의 업무범위와 책무 등을 규정해 놓은 법률로서, 사이버보안 및 기반시설보안에 있어 정책설정의 역할과 함께 실질적인 컨트롤타워를 설정하고, 해당 컨트롤타워가 기존의 사이버보안 관련 법률에서는 어떤 역할을 수행하게 되는지, 그리고 국회로부터 감시 및 감독을 받도록 하는 근거 규정을 두고 있다.

(5) 미국의 사이버보안 관련 최근 동향

CISA는 설립 이후 최근 국가 사이버보안과 관련된 전략을 발표하였다.[818] CISA는 "미국민을 위한 핵심 기반시설의 보안과 복원"을 비전으로 삼고, 리더십과 협업, 위험의 우선 순위화, 결과중심, 국가가치의 존중, 목표와 조직의 단일화를 지도 원칙으로 삼고 있다.[819] 그를 바탕으로 단기적 전략으로 "사이버보안 위험분석 및 관리 계획 수립 강화, 사이버위협 정보 공유 확대, 관계기관 및 지방정부 등 이해관계자와 협력 강화, 사이버보안 위험 대응 기술 지원 강화, 사이버보안 사고에 대한 대응 능력 향상"을 제시하여 긴급한 사이버위협에 대응하고 있다.[820] 그리고 중장기적 전략으로는 "사이버보안 위험 모델 개발 및 기술적 지원 제공, 원활한 협업을 위한 조직 운영, 교육훈련 강화 보조금 지원 강화"를 제시하여 국가 사이버 기반시설의 사이버보안 수준을 높이는 것을 목표로 삼고 있다.[821] 그를 위한 중점추진 정책과제를 "5G 네트워크 공급망 위험 제거, 선거 사이버보안 강화, 공공 공간의 사이버보안 위험 완화, 연방기관 사이버보안 강화, 산업용 제어 시스템 보안 강화"로 설정하여 추진해 나가고 있다.[822] 앞으로 CISA의 전략과 중점추진 정책과제에 따라 추진되는 내용들에 대해서

---

818) CISA Strategic Intent - Defend Today, Secure Tomorrow, https://www.dhs.gov/sites/default/files/publications/cisa_strategic_intent_s508c_0.pdf (2019년 11월 3일 최종접속).

819) CISA Strategic Intent - Defend Today, Secure Tomorrow, https://www.dhs.gov/sites/default/files/publications/cisa_strategic_intent_s508c_0.pdf (2019년 11월 3일 최종접속).

820) 한국인터넷진흥원, "미국 국토안보부, 국가 중요 인프라에 대한 사이버보안 전략 보고서 발표", 인터넷 법제동향 제144호, 한국인터넷진흥원, 2019.9, 15면.

821) 한국인터넷진흥원, 앞의 글, 16면.

는 한국도 지속적으로 주의 깊게 살펴볼 필요가 있다. 한국에도 좋은 모델을 제시해 줄 수 있기 때문이다.

(6) 소결 및 시사점

미국도 아래에서 살펴볼 다른 국가들과 같이 사이버보안 및 기반시설보안과 관련된 업무를 단일화 하고 집중화 하는 경향을 보이고 있다. CISA를 통해서 미국 사이버보안과 관련된 업무를 통합적이고 종합적으로 처리하며, 사이버보안의 컨트롤타워의 역할을 수행하도록 하고 있다. 미국은 이미 사이버보안과 관련된 여러 법률들이 있었고, 해당 법률의 집행을 위해 여러 기관들이 연관되어 있었지만, 이제는 CISA를 통해 일원화 되었다. 더욱이 CISA는 단순히 사이버보안 위협을 감지하고, 정보를 공유하거나 수동적으로 대처하는 것을 넘어서 적극적으로 복원(Resilience)시키는 기능까지 갖고 있다. 한국의 경우 CISA와 같은 업무가 한국인터넷진흥원을 비롯해서 방송통신위원회 등 다양한 기관들에 분산되어 있고, 관련 법령들도 각기 달라 통합적이고 종합적인 사이버보안이 용이하지 않다. 이에 대해서는 이미 수 년 동안 지적되어 오고 있지만 여전히 개선되지 않고 있다. 사이버보안의 위험성을 고려해 볼 때, 한국인터넷진흥원과 같은 사이버보안 집행기관에게 보다 적극적인 의사결정과 신속한 집행이 가능할 수 있는 체계와 권한이 주어져야 한다.

CISA법에서 눈에 띄는 것은 프라이버시 담당관을 두고 있는 것이다. 사이버보안은 필연적으로 프라이버시 침해 문제를 동반하게 된다. 따라서 법집행기관이 사이버보안을 위한 활동을 하는 경우 프라이버시 침해 문제에 대해 보다 주도면밀하게 살펴보아야 한다. 이는 기업이 기업 업무를 할 때, 법적인 절차를 고려하는 준법감시인을 두고 있고, 건물을 지을 때 교통영향평가를 하는 것과 같은 기능을 합하여 놓은 것과 같다. 따라서 프라이버시 담당관은 법집행기관이 사이버보안을 위한 활동을 할 때, 프라이버시와 관련된 법률을 검토하고, 해당 활동이 프라이버시에 어떠한 영향을 미치게 되는지를 판단하여 비례적인 법집행을 돕는 역할을 하게 된다. 매우 중요하고 필요한 기능이라고 할 수 있다. 이는 한국도 적극적으로 고려할 필요가 있다.

또한 사이버보안과 관련해서는 여러 가지 법률들이 복잡하게 얽히게 된다. 이는

822) 한국인터넷진흥원, 앞의 글, 16면.

사이버보안법 체계가 처음부터 체계적으로 구축된 것이 아니기 때문이다. 이는 미국을 비롯해서 대부분의 국가들이 겪는 모습니다. 이에 대해 아래에서 살펴볼 일본처럼 기본법 체계로 해결할 수도 있지만 미국의 CISA법에서 보이는 것과 같이 사이버보안 관련 법률을 제정할 때, 유관 법률들을 모두 확인하여 한 번에 개정하는 방식을 취해야 한다. 예를 들어, 한국은 개인정보 보호법이 제정되면서 정보통신망법 제4장 개인정보 보호의 제4절(제33조~제40조 규정)이 전체적으로 삭제되었다. 그런데 해당 개정이 치밀한 개정이 아니라는 것이 엿보이는 대표적인 이유로 동법 제44조의10 명예훼손의 분쟁조정부 관련 규정의 제3항에서는 아직도 분쟁조정절차에 대해서 "제33조의2 제2항, 제35조부터 제39조까지의 규정을 준용한다"라는 규정이 남아 있다. 2011년 정보통신망법상의 규정이 개인정보 보호법으로 이관되어 삭제되었고, 이미 9년의 시간이 흘렀으며, 그 간에도 그에 대한 지적과 비판이 있었지만[823] 잘못된 규정이 여전히 개정되지 않고 있다. 이와 같은 문제가 발생하는 이유는 법률이 개정될 때, 유관 규정들을 함께 개정하는 작업이 미흡하기 때문이다. 그러므로 사이버보안과 관련된 한국법의 규정들의 관계성을 제대로 파악해서, 관련 규정이 개정될 때 함께 개정하는 작업이 수행되어야 법률의 정합성이 깨지는 문제점이 발생하지 않을 수 있다.

사이버보안과 관련해서는 상당한 권한이 해당 기관에 부여될 필요가 있다. 하지만 그 만큼 권한이 남용될 여지도 발생한다. 따라서 미국은 의회를 통한 통제가 강화되어 있다. 따라서 CISA는 다양한 조직관련, 사이버보안 관련 정보 등을 미국 의회에 보고할 의무를 가지고 있다. 의회를 통한 통제가 강화되려면 의회는 해당 보고를 정치적인 관점에서만 판단하고 논의해서는 안 된다. 그를 위해서는 의회도 사이버보안과 관련해서 전문성을 키울 필요가 있다. 의원들의 정치적 관점에 따라 사이버보안 문제를 판단하는 것이 아니라 사이버보안 체계의 전문적인 관점에서 해당 문제를 분석하고 결정을 내려야 한다. 그러므로 사이버보안 기관을 적절하고 제대로 통제하기 위해서는 의회에서도 사이버보안의 전문성을 강화시킬 수 있는 방안을 반드시 모색할 필요가 있다.

---

823) 강석구/이원상, 앞의 보고서, 183면.

3) 유럽연합

(1) 사이버보안 관련 규정 개관

① 사이버보안법 재정경위

2019년 3월 12일 스트라스부르에서 열린 유럽의회(the European Parliament) 회의에서는 찬성 586표, 반대 44표, 기권 36표로 '유럽 사이버보안법'이 채택되었다. 유럽에서는 사이버공간을 보호하는 법률로서 (한국에서 '유럽 개인정보 보호법'으로 소개되고 있는) '일반 데이터 보호 규정(General Data Protection Regulation, 이하 'GDPR'이라 함)'과 함께 '사이버보안법(the Cybersecurity Act, 이하 'EU 사이버보안법'이라고 함)'이 시행되게 된 것이다. 'EU 사이버보안법'은 EU의 사이버보안 기구인 '유럽연합 사이버보안 기구(The European Union Agency for Cybersecurity, 이하 'ENISA'라고 함)'에 의해서 수행되며, 사이버보안 인증을 통해 유럽 내 디지털 제품과 서비스에 대한 안전을 강화하기 위해서 만들어진 규정이다.[824] 따라서 'EU 사이버보안법'의 제정 취지를 볼 때, ENISA에게 유럽의 사이버보안과 관련된 영구적인 권한을 부여하고, 그를 위해 재정 및 인적 자원을 강화하는 등 강력한 지원을 통해 ENISA의 능력을 향상 시키고, EU 차원의 사이버보안 인증 프레임워크를 확립하는 것을 주요 목적으로 하고 있다.[825]

제정과정을 간략하게 요약해 보자면, 2017년 9월에 유럽연합 집행위원회(European Commission)는 EU가 사이버공격에 대해 적절하게 대처하고, 강력한 사이버보안을 구축하기 위해 사이버보안법을 제안하게 된다.[826] 그리고 2018년 7월 유럽의회의 산업·연구·에너지위원회(ITRE)는 해당 제안에 대한 보고서를 채택한다. 이후, 2018년 12월 10일 유럽의회, 유럽평의회(Council of Europe), 유럽연합 집행위원회는 제5차 3국 회의에서 정치적 합의에 도달하게 되었고,[827] 그 결과 'EU 사이버보안법'이 시행

824) The Cybersecurity Act strengthens Europe's cybersecurity, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity (2019년 11월 3일 최종접속).

825) The Cybersecurity Act strengthens Europe's cybersecurity, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity (2019년 11월 3일 최종접속).

826) State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks, https://europa.eu/rapid/press-release_IP-17-3193_en.htm (2019년 11월 3일 최종접속).

827) Cybersecurity Act, https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

되게 되었다.

② EU 사이버보안법의 수행기관

앞서도 언급하였지만 'EU 사이버보안법'은 ENISA를 개편하고 그 권한을 강화함으로서 EU의 사이버보안에 대한 주도적인 기관으로 발전시키고, 디지털 제품, 서비스 및 프로세스에 대한 EU 차원의 사이버보안 인증 프레임워크를 구축하여 EU의 사이버 공간을 보다 강력하게 보호하는 것에 그 주요 목적을 두고 있다.[828] 그에 따라 ENISA는 특정 인증제도에 대한 기술적 기반을 마련하고, 전용 웹사이트를 통해 인증서를 발급해 주는 것은 물론 인증 제도를 EU 시민들에게 홍보하는 등 EU 사이버보안 인증 프레임워크의 설정과 유지에 핵심적인 역할을 수행하게 된다.[829] 또한 ENISA는 '네트워크 및 정보시스템 보안에 관한 지침(The Directive on security of network and information systems, 이하 'NIS Directive'라고 함)에 의해[830] 설립된 '국가 컴퓨터 보안사고 대응팀(national Computer Security Incidents Response Teams, 이하 'CSIRTs'라고 함)' 네트워크의 사무국으로서의 지위에서 EU 차원의 보안사고 대응팀 운영에 있어 협력을 증대하고, EU 회원국들의 사이버보안 사고에 대한 대응을 지원하며, 초국가적인 사이버공격이나 위기가 발생하는 경우 EU 차원에서의 조정업무도 수행하게 된다.[831]

ENISA는 유럽차원에서의 사이버보안업무를 다루는 기관으로서 범유럽 사이버보안 훈련, 국가 사이버보안 전략의 개발 및 평가, CSIRT의 협력 및 역량 구축, IoT 및 스마트인프라 구축·데이터 보호 문제 현황·개인정보 보호 강화 기술 및 새로운 기술에 의한 개인정보 보호·eIDs 및 신뢰 서비스·사이버 위협 환경 파악 등에 관한 연구 등을 수행하고 있다.[832] 그 뿐 아니라 ENISA는 유럽차원의 네트워크 및 정보보안(NIS)

(2019년 11월 3일 최종접속).

828) The EU Cybersecurity Act, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (2019년 11월 3일 최종접속).

829) he EU Cybersecurity Act, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (2019년 11월 3일 최종접속).

830) NIS 지침은 사이버보안과 관련된 유럽차원의 첫번째 규정이다. 이에 대한 규정은 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (2019년 11월 3일 최종접속).

831) The EU Cybersecurity Act, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (2019년 11월 3일 최종접속).

에 관해서 유럽연합의 정책 및 법률을 개발하고, 그 이행을 지원하며, 회원국과 유럽연합 기관, 기관 대 기관이 자발적으로 사이버공격의 취약성에 대해 공개적인 정책을 수립 및 시행할 수 있도록 지원하고 있다.[833]

무엇보다 2019년부터 'EU 사이버보안법'이 발효됨에 따라 ENISA는 EU의 단일 디지털 시장에서 출시되는 제품들, 프로세스, 서비스에 대해 인증의 기준이 되는 '유럽 사이버보안 인증제도'를 마련하는 과제를 수행하고 있다.[834] 따라서 ENISA의 활동영역이 보다 확대되어 그 업무도 사이버보안 및 독자적인 조언에 따른 권고 사항, 사이버 정책 수립 및 구현을 지원하는 활동, ENISA가 EU 전체의 운영팀과 직접 협업하는 '핸즈 온(Hands On)' 업무, EU 차원의 대규모 사이버보안 사고에 대해 EU 커뮤니티들과의 협업 및 대응방안 조정, 사이버보안 인증 계획 작성 등의 업무도 수행하게 되었다.[835]

③ 사이버보안 인증 프레임워크

새로 발효된 EU 사이버보안법의 핵심은 디지털 제품 및 서비스, 프로세스에 대한 유럽차원에서의 사이버보안 인증 프레임워크를 구축하는 것이다.[836] 사이버공간은 이어져 있는 공간이고, 더욱이 유럽은 단일 시장을 형성하고 있기 때문에 사이버보안 인증은 디지털 제품과 서비스 등에 대한 신뢰와 보안을 강화하는 데 매우 중요한 역할을 한다. 물론 현재 EU에는 다양한 유형의 사이버보안 인증 체계가 존재하고 있긴 하지만 공통의 프레임워크가 없는 경우 유럽의 단일 시장에서 디지털 제품이나 서비스 등은 단편화되고, 새로운 장벽이 될 수 있는 위험이 있다.[837] 그러므로 사이버보안 인증 프레임워크는 사이버공간에서 유럽을 구분하고, 유럽 내부의 사이버보안을 강화시켜 통일되고 안전한 사이버공간을 유지할 수 있도록 해 준다.

그를 위해 사이버보안 인증 프레임워크는 EU 차원의 합의에 기반해서 일반적인

832) About ENISA, https://www.enisa.europa.eu/about-enisa (2019년 11월 3일 최종접속).
833) About ENISA, https://www.enisa.europa.eu/about-enisa (2019년 11월 3일 최종접속).
834) About ENISA, https://www.enisa.europa.eu/about-enisa (2019년 11월 3일 최종접속).
835) About ENISA, https://www.enisa.europa.eu/about-enisa (2019년 11월 3일 최종접속).
836) The EU cybersecurity certification framework, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (2019년 11월 3일 최종접속).
837) The EU cybersecurity certification framework, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (2019년 11월 3일 최종접속).

규정, 기술 요건, 표준 및 절차 등에 대한 EU의 인증 체계를 제공하게 된다. 그러한 해당 인증제도에 따라 인증된 ICT 제품과 서비스 a) 적용 제품 및 서비스의 범주, b) 사이버보안 요구사항(예: 표준 또는 기술 사양), c) 평가 유형(예: 자체 평가 또는 제3자 평가), d) 의도되는 보증 수준(예: 기본, 실질 및 실질, 실질) 등을 명기하게 되고, 그를 통해 해당 제품 및 서비스가 인증 요건을 준수한다는 것을 입증하게 된다.[838]

또한 제품이나 서비스 인증서에는 사고의 확률과 영향 측면에서 제품의 의도된 사용, 서비스 또는 프로세스와 관련된 위험 수준에 상응한 '보통, 상당함, 높음(Basic, Substantial, High)' 등과 같은 위험 정도가 표시되는데, 예를 들어, '높음'의 인증을 받은 제품은 가장 높은 보안 시험을 통과했다는 것을 의미하게 되고, 그 결과 해당 인증서는 모든 EU 회원국에 의해 인정받게 되어 인증서를 받은 기업은 유럽 국가들과 자유로운 거래를 할 수 있게 되는 것이다.[839]

2019년 6월 27일 사이버보안법 시행에 따라 유럽연합 집행위원회는 '이해관계자 사이버보안 인증 그룹(Stakeholder Cybersecurity Certification Group, 이하 'SCCG'라고 함)'의 회원을 선정하기 위해 각 회원들에게 신청을 요구하였다. 그 대상자는 학술기관, 소비자 단체, 적합성 평가기관, 표준 개발 기관, 기업, 무역협회 및 기타 회원 기관이며, SCCG는 사이버보안 인증과 관련된 전략적 문제에 대해 유럽연합 집행위원회와 ENISA에 조언을 하고, 지원을 하게 되는 전문가 그룹이다.[840] 그러므로 앞으로 EU 사이버보안 인증 체계의 모습과 방향성을 가늠하기 위해 SCCG의 활동에 대해서는 지속적으로 추적관찰을 할 필요가 있다.

(2) EU 사이버보안법의 내용

① 법률구조 개관

EU 사이버보안법은 크게 제1부, 제2부, 제3부 그리고 제4부로 나누어진다. 제1부는 일반규정으로 해당 법률의 목적과 범위(제1조), 해당 법률에서의 용어에 대한 정의가

838) The EU cybersecurity certification framework, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (2019년 11월 3일 최종접속).
839) The EU cybersecurity certification framework, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (2019년 11월 3일 최종접속).
840) The EU cybersecurity certification framework, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (2019년 11월 3일 최종접속).

(제2조) 규정되어 있다. 제1조에 따르면 EU 사이버보안법은 수준 높은 사이버보안, 사이버 복원력 및 유럽연합 내부의 신뢰형성을 목표로 하면서 동시에 유럽 내 시장 기능의 적절성을 보장하는 것을 목적으로 삼고 있다. 그를 위해 주무기관 역할을 수행하는 것이 ENISA이므로 (a) ENISA의 목표와 업무 및 조직에 대한 내용과 (b) 유럽연합 내에서 ICT 제품 및 서비스, 프로세스가 적합한 수준의 사이버보안을 확보하도록 하기 위해 사이버보안 인증 제도와 관련된 프레임워크를 구축하는 것에 대한 내용을 규정하고 있다. 그리고 해당 규정은 공공보안, 국방, 국가안보 및 국가 활동 등과 관련해서 회원국의 역량에 대한 편견 없이 적용된다고 선언하고 있다.

제2조에서는 동 법률에서 사용되고 있는 용어인 사이버보안(cybersecurity), 네트워크 및 정보시스템(network and information system), 네트워크 및 정보시스템 보안에 관한 국가전략(national strategy on the security of network and information systems), 필수 서비스 운영자(operator of essential services), 디지털 서비스 제공자(digital service provider), 사고(incident), 사고처리(incident handling), 사이버위협(cyber threat), 유럽 사이버보안 인증제도(European cybersecurity certification scheme), 국가 사이버보안 인증제도(national cybersecurity certification scheme), 유럽 사이버보안 인증서(European cybersecurity certificate), ICT 제품(ICT product), ICT 서비스(ICT service), ICT 프로세스(ICT process), 승인(accreditation), 국가 승인 기관(national accreditation body), 적합성 평가(conformity assessment), 적합성 평가기관(conformity assessment body), 표준(standard), 기술규격(technical specification), 보증수준(assurance level), 적합성 자체평가(conformity self-assessment) 등의 정의가 규정되어 있다. 해당 용어들은 이미 이전에 유사 법률들에서 사용하고 있던 개념들과 거의 유사하게 사용되고 있으며, 인증제도와 관련된 새로운 규정들은 새롭게 개념 규정하고 있다.

제2부는 제1장 권한과 목적(Mandate and objectives), 제2장 임무(Tasks), 제3장 ENISA 조직(Organisation of ENISA), 제4장 ENISA 예산구조 및 예산수립(Establishment and structure of ENISA's budget), 제5장 인력(Staff), 제6장 ENISA 일반규정(General provisions concerning ENISA) 등 총 6개의 장으로 구분되며 총 43개 조문으로 구성되어 있다. 사실 해당 규정은 ENISA 조직에 관한 규정이므로 다른 나라에는 큰 관련성이

있는 규정들은 아니라고 할 수 있다. 우리가 좀 더 주의 깊게 살펴볼 필요성이 있는 규정은 제3부이다. 제3부는 사이버보안 인증 프레임워크와 관련된 내용을 20개 조문에 걸쳐 담고 있다. 해당 조문들을 대략 살펴보면, 다음과 같다.

제46조 유럽 사이버보안 인증 프레임워크(European cybersecurity certification framework)
제47조 유럽 사이버보안 인증을 위한 유럽연합 롤링 워크 프로그램(The Union rolling work programme for European cybersecurity certification)
제48조 유럽 사이버보안 인증제도 요청(Request for a European cybersecurity certification scheme)
제49조 유럽 사이버보안 인증제도의 준비, 채택 및 검토(Preparation, adoption and review of a European cybersecurity certification scheme),
제50조 유럽 사이버보안 인증제도에 관한 웹사이트(Website on European cybersecurity certification schemes)
제51조 유럽 사이버보안 인증제도의 보안 목표(Security objectives of European cybersecurity certification schemes)
제52조 유럽 사이버보안 인증제도의 보증 수준(Assurance levels of European cybersecurity certification schemes)
제53조 적합성 자체평가(Conformity self-assessment)
제54조 유럽 사이버보안 인증제도의 요건(Elements of European cybersecurity certification schemes)
제55조 인증된 ICT 제품, 서비스 및 프로세스에 대한 사이버보안 정보 보충(Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes)
제56조 사이버보안 인증(Cybersecurity certification)
제57조 국가 사이버보안 인증제도 및 인증서(National cybersecurity certification schemes and certificates)
제58조 국가 사이버보안 인증기관(National cybersecurity certification authorities)
제59조 동료 평가(Peer review)
제60조 적합성 평가기관(Conformity assessment bodies)
제61조 통지(Notification)
제62조 유럽 사이버보안 인증 그룹(European Cybersecurity Certification Group)
제63조 이의제기권(Right to lodge a complaint)
제64조 효과적인 사법적 구제권(Right to an effective judicial remedy)
제65조 벌칙(Penalties)

마지막으로 제4부는 종결 규정(Final Provision)은 4개의 조문으로 구성되어 있다. 제66조 집행위원회 절차(Committee procedure), 제67조 평가 및 검토(Evaluation and review), 제68조 폐기 및 승계(Repeal and succession), 제69조 조약발효(Entry into force) 등에 대한 내용이 규정되어 있다. 해당 규정은 아직까지는 강제되고 있지 않지만 2023년까지 의무화 될 것이기 때문에 유럽에 진출하려는 한국 기업에도 큰 영향을 주게 된다. 따라서 이미 한국의 기업들이 EU 사이버보안법에 대한 세밀한 분석을 하고 대응해야 한다고 하는 주장도 제기되고 있다.[841] 다만 이는 한국 기업에만 국한되는 것은 아니다. 그러므로 EU 사이버보안 인증제도에 대해서는 미리 대비하여야 할 필요성이 있으므로 아래에서 좀 더 살펴보고자 한다.

② EU 사이버보안 인증제도 내용

㉮ 개관

EU 사이버보안법의 핵심은 그동안 임시기관이었던 ENISA를 상설기관화 시켜 EU의 사이버보안업무를 전담시킨 것과 EU 사이버보안 인증제도를 통해 ICT제품이나 서비스 및 프로세스 등을 설계할 때부터 사이버보안을 고려하도록 한 것이다. 이는 최근 ICT 제품 및 서비스가 증가하고 있으며, 더욱이 사물인터넷의 대중화로 인해 인터넷에 연결되고 있는 사물들이 증가하고 있지만, 사이버보안 수준이 미흡하기 때문에 잦은 보안사고가 발생하는 것에 대응하는 조치라고 할 수 있다.[842] 두 핵심 가운데 한국에서 주목해야 할 것은 사이버보안 인증제도이다. 이는 유럽의 GDPR과 함께 한국의 기관 및 기업 등에 직접적인 영향을 미치는 제도이기 때문이다. EU 사이버보안 인증제도의 대상은 ICT 제품과 서비스, 프로세스이며 사이버보안의 기본요건인 가용성(availability), 신뢰성(authenticity), 무결성(integrity) 및 기밀성(confidentiality)을 보장하기 위한 제도이다(제46조).

841) "[ICT광장] EU의 사이버보안 인증 규제에 대비해야", 정보통신신문 2019년 4월 15일자, http://www.koit.co.kr/news/articleView.html?idxno=75201 (2019년 11월 3일 최종접속).

842) 2025년 IoT의 숫자는 7백 5십만 개를 넘어설 것으로 예상되고 있다고 한다; EU Cybersecurity Act: how a little-known piece of legislation could transform the internet of things, https://tech.newstatesman.com/security/eu-cybersecurity-act-iot-legislation (2019년 11월 3일 최종접속).

㉯ EU 롤링 워크 프로그램

이를 위해 EU 집행위원회는 'EU 롤링 워크 프로그램'을 통해서 전략적 우선순위를 파악하게 되는데(제47조 제1항), 특정한 기준을 정하여(동조 제3항)[843] 사이버보안 인증제도의 범위에 포함될 ICT 제품과 서비스, 프로세스의 목록을 작성하게 된다(동조 제2항). EU 집행위원회는 유럽 사이버보안 인증그룹(European Cybersecurity Certification Group, 이하 'ECCG'라고 함)과 이해관계자 인증그룹(Stakeholder Certification Group)의 의견을 고려해야 하고(동조 제4항), 제1차 프로그램을 2020년 6월 28일까지 완성하며, 3년에 1회 이상 업데이트를 하게 된다(동조 제5항).

EU 집행위원회나 ECCG는 EU 롤링 워크 프로그램을 근거로 ENISA에 유럽 사이버보안 인증계획에 대한 것을 요청할 수 있다(제48조). 그러면 ENISA는 그에 따라 관련 요건(제51조, 제52조 및 제54조) 등을 검토하여 그에 충족하는 후보군을 준비하게 된다(제49조 제1항)(경우에 따라서는 거절 이유를 명시하여 거절할 수도 있다(동조 제2항)). 그를 위해 ECCG와 긴밀히 협력하고(동조 제5항), 이해관계자들과 협의하며(동조 제4항), 경우에 따라서는 구체적인 조언과 전문지식을 제공해 줄 수 있는 특별 워킹 그룹을 설립하게 된다(동조 제4항). 그렇게 해서 채택된 제도에 대해 ENISA는 5년마다 이해관계자들의 피드백을 받아 평가를 하고, 집행위원회나 ECCG는 해당 평가결과에 따라 다시금 제도의 개선을 요청할 수 있다(동조 제8항). 또한 ENISA는 유럽 사이버보안 인증제도와 관련해서 보안인증서, 보안 적합성 명세서, 국가 사이버보안 인증서 등의 정보를 제공하는 웹사이트를 운영하게 된다(제50조).

㉰ 인증계획의 설계

유럽 사이버보안 인증계획의 설계는 다음과 같은 보안 목표에 도달할 수 있게 설계되도록 명시하고 있다(제51조):

---

843) 특정한 기준에는 (a) ICT 제품과 서비스, 프로세스의 특정 카테고리와 특히 단편화 위험에 관한 국가 사이버보안 인증계획의 가용성 및 개발, (b) 유럽연합 또는 회원 국가의 법과 정책, (c) 시장 수요, (d) 사이버 위협 환경에서의 개발, (e) ECCG에 의해 특정한 후보계획의 준비 요청 등이 포함된다.

(a) ICT 제품이나 서비스, 프로세스의 전체 수명주기 동안 돌발적이거나 허가되지 않은 저장, 처리, 접근 또는 노출로부터 저장, 전송 또는 다른 방법으로 처리되는 데이터를 보호함

(b) ICT 제품이나 서비스, 프로세스의 전체 수명주기 동안 돌발적이거나 허가되지 않은 파괴, 손실 또는 변경 또는 가용성 부족으로부터 저장, 전송 또는 다른 방법으로 처리되는 데이터를 보호함

(c) 인가된 사람, 프로그램 또는 기계만이 자신의 접근권에 따라 데이터, 서비스 또는 기능에 접근하도록 함

(d) 알려진 종속성과 취약성의 식별 및 문서화함

(e) 언제, 누가 접근, 사용 또는 다른 방법으로 처리된 데이터, 서비스 또는 기능을 사용했는지에 대해 기록하도록 함

(f) 언제, 누가 접근, 사용 또는 다른 방법으로 처리된 데이터, 서비스 또는 기능을 사용했는지를 확인가능 하도록 함

(g) ICT 제품과 서비스, 프로세스에 알려진 취약성이 포함되어 있지 않은지 검증하도록 함

(h) 물리적 또는 기술적 사고 발생 시 신속하게 데이터, 서비스 및 기능에 대한 가용성과 접근성을 복구하도록 함

(i) ICT 제품과 서비스, 프로세스는 기본적으로 설계 시부터 보안을 고려함

(j) ICT 제품과 서비스, 프로세스는 공개적으로 알려진 취약성을 포함하지 않는 최신 소프트웨어 및 하드웨어와 함께 제공되며, 보안 업데이트를 위한 메커니즘을 제공함

이처럼 유럽 사이버보안 인증계획에서 요구하는 요소들은 기술의 발전에 따라서 함께 변화할 수 있게 된다. 특히 다른 나라에 있는 기업 등은 유럽에서 사용되는 ICT 제품이나 서비스, 프로세스에 대해 유럽 사이버보안 설계의 내용을 제품 설계단계부터 염두에 두어야 한다. 그렇지 않으면 유럽 사이버보안 인증을 획득할 수 없는 문제에 직면하게 되기 때문이다. 그런데 제품을 설계하면서 유럽만을 위한 제품을 설계하는 것은 쉽지 않기 때문에 유럽 사이버보안 규정은 전 세계 사이버보안에도 영향을 끼칠 수밖에 없는 것이다.

㉲ 인증제도의 보증 수준 및 포함요소

유럽 사이버보안 인증제도의 보증 수준은 그 위험 수준에 비례해서 '기본', '보통', '높음'으로 구분된다(제52조 제1항). 그에 따라 인증서 또는 EU 적합성 명세서는 그와 관련된 기술 규격, 표준 및 절차, 기술 통제, 사이버보안 사고의 위험을 줄이거나 사이버보안 사고를 예방하기 위한 목적 등이 포함된다(동조 제4항). '기본'에 해당하는 ICT 제품이나 서비스, 프로세스의 제조자 또는 제공자는 적합성 자체 평가를 할 수 있다(제53조 제1항). 그 결과를 가지고 EU 적합성 보고서를 발행할 수 있으며, 준수에

대한 책임도 지게 된다(동조 제2항). 또한 해당 명세서, 기술 문서, 관련 정보 등을 국가 사이버보안 인증기관에서 이용할 수 있도록 작성하고, 그 사본을 국가 사이버보안 인증기관과 ENISA에 제출해야 한다(동조 제3항). 즉, 기본에 해당하는 경우에는 사이버보안의 정도가 상대적으로 완화되는 것이다. 그에 반해 '높음'에 해당되는 경우에는 별도의 까다로운 절차들이 요구된다. 그에 대해서는 아래에서 설명하고 있다.

유럽 사이버보안 인증제도에는 최소한 다음의 요소를 포함하도록 하고 있다(제54조):

(a) ICT 제품이나 서비스 및 프로세스의 유형 또는 범주를 포함한 인증제도의 주제 및 범위

(b) 계획의 목적과 채택된 표준, 평가방법 및 보증 수준이 계획의 사용자의 요구에 얼마나 부합하는지에 대한 명확한 설명

(c) 평가에 적용되는 국제, 유럽 또는 국가 표준, 또는 해당 표준이 없거나 적절하지 않은 경우 (EU) No 1025/2012 규정의 부속문서 II에 명시된 요건을 충족하는 기술명세서, 또는 해당 명세서를 사용할 수 없는 경우 유럽 사이버보안 인증제도에 정의된 다른 기술명세서 또는 사이버보안 요구서 참조

(d) 해당되는 경우, 하나 이상의 보증 수준

(e) 본 제도에 의해 적합성 자체 평가가 허용되는지 여부에 대한 표시

(f) 해당되는 경우, 사이버보안 요건을 평가할 수 있는 기술적 역량을 보장하기 위해 적합성 평가기관에 적용되는 특정 또는 추가 요건

(g) 제51조에 언급된 보안목표의 달성을 입증하기 위해 평가 유형을 포함하여 사용할 구체적인 평가기준 및 방법

(h) 해당되는 경우, 인증을 위해 필요하고, 신청자가 적합성 평가기관에 제공 또는 제공해야 하는 정보

(i) 본 제도가 마크나 라벨을 제공하는 경우, 그러한 마크나 라벨을 사용할 수 있는 조건

(j) 특정 사이버보안 요건을 지속적으로 준수하는 것을 입증하는 메커니즘 포함하여 유럽 사이버보안 인증서 또는 EU 적합성 명세서의 요건에 따라 ICT 제품이나 서비스 및 프로세스의 준수를 감시하기 위한 규칙

(k) 해당되는 경우, 유럽 사이버보안 인증서의 발급, 유지, 지속 및 갱신 조건 및 인증 범위의 확대 및 축소 조건

(l) 인증 및 EU 적합성 명세서가 발행된 ICT 제품이나 서비스 및 프로세스의 결과에 관한 규칙(제도의 요건이 준수되지 않는 경우의 규칙)

(m) ICT 제품이나 서비스 및 프로세스에서 이전에는 탐지되지 않은 사이버보안 취약점을 보고하고 처리하는 방법에 대한 규칙

(n) 해당되는 경우, 적합성 평가기관에 의한 기록보유에 관한 규칙

(o) ICT 제품이나 서비스 및 프로세스, 보안 요구사항, 평가기준 및 방법, 보증 수준 등에 있어서 동일한 유형 또는 카테고리를 포함하고 있는 국가 또는 국제 사이버보안 인증제도의 확인

(p) 유럽 사이버보안 인증서 및 발행할 EU 적합성 명세서의 내용과 형식

(q) ICT 제품이나 ICT 서비스 및 프로세스의 제조업체 또는 제공자가 이용할 수 있도록 EU 적합성 명세서, 기술 문서 및 기타 모든 관련 정보 등을 이용할 수 있는 기간

(r) 본 계획에 따라 발행된 유럽 사이버보안 인증서의 최대 유효 기간
(s) 제도에 의해 발행, 개정 또는 철회된 유럽 사이버보안 인증서에 대한 정책 공개
(t) 제3국의 인증제도와 상호인정을 위한 조건
(u) 해당되는 경우, 제56조 제6항에 따른 보증수준 '높음'을 위해서 유럽 사이버보안 인증서를 발급하는 당국이나 기관이 제도로 확립한 동료 평가 메커니즘에 관한 규칙(그러한 메커니즘은 제59조에 규정된 동료 평가를 침해하지 않아야 함)
(v) 제55조에 따라 사이버보안 보충 정보를 제공하거나 업데이트할 때 ICT 제품이나 ICT 서비스 및 프로세스의 제조자나 제공자가 따라야 할 형식 및 절차

다만, 이런 내용들은 유럽연합의 법률요건에 부합해야 하고(동조 제2항), 법적으로는 유럽 사이버보안 인증서나 EU 적합성 명세서는 적법성이 추정될 수 있다(동조 제3항, 제4항).

㉮ 보충정보 및 재평가

또한 인증된 ICT 제품이나 서비스, 프로세스에 대해서는 사이버보안에 대한 보충정보가 요구되기도 한다(제55조 제1항). 보충정보의 내용으로는 (a) 최종 사용자가 ICT 제품이나 서비스의 안전한 구성·설치·구축·운영 및 유지보수를 지원하기 위한 지침 및 권고사항, (b) 특히 사이버보안 관련 업데이트의 가용성과 관련해서 최종 사용자에게 보안 지원이 제공되는 기간, (c) 제조업체 또는 공급자의 연락처 정보 및 최종 사용자 및 보안 연구자로부터 취약성 정보를 수신하기 위해 허용될 수 있는 방법, (d) ICT 제품이나 서비스, 프로세스와 관련해서 공개적으로 노출된 취약점에 대한 온라인 저장소 리스트 및 사이버보안 권고사항 레퍼런스 등이 해당된다. 해당 정보는 디지털 형태로 이용될 수 있어야 하며, 인증기간 만료 시까지 유지 및 갱신되어야 한다(동법 제2항).

사이버보안 인증을 받은 ICT 제품이나 서비스, 프로세스는 해당 제도의 요건을 준수하는 것으로 추정된다(제56조 제1항). 인증제도는 2년 마다 집행위원회의 평가를 받게 되는데(동법 제3항), 평가 내용으로는 (a) ICT 제품이나 서비스, 프로세스에 대해 예상되는 보안 수준 향상으로 인해 그에 적합한 조치를 취할 경우, 그로 인해 제조자 또는 제공자에게 사회적 또는 경제적 편익의 측면에서 어떠한 영향을 미칠 수 있는지, (b) 회원 국가 및 제3국 법률의 존재와 이행여부, (c) 모든 이해관계자 및 회원국과

개방적이고 투명하며 포괄적인 협의 프로세스 사용, (d) 특히 SME를 포함해서 ICT 제품이나 서비스, 프로세스의 제조업체나 제공자에게 미칠 영향을 고려한 이행 마감일 및 과도기적 조치 및 기간, (e) 자발적인 인증제도에서 의무적인 인증제도로의 전환이 시행되는 가장 빠르고 효율적인 방법 등이 포함된다(동조 제3항).

㉯ 인증서 발급기관 및 피발급자의 의무

인증서를 발급해 줄 수 있는 기관으로는 (a) 동 규정 제58조 제1항에 따른 국가 사이버보안 인증기관,[844] (b) 동 규정 제60조 제1항에 따른 적합성 평가기관으로 인가된 공공기관 등이다(동조 제5항). 하지만 유럽 사이버보안 인증제도에서 보증수준이 '높음'을 요구하는 경우에는 국가 사이버보안 인증당국 및 (a) 적합성 평가기관이 발행한 개별 유럽 사이버보안 인증서에 대한 국가 사이버보안 인증당국의 사전 승인, 또는 (b) 국가 사이버보안 인증당국의 적합성 평가기관에서 유럽 사이버보안 인증서를 발급하는 경우 해당 직무에 대해 개괄적 수권을 받은 평가기관에 의해서만 인증이 가능하다(동조 제6항).

인증서를 발급받은 자는 일정한 의무를 지게 된다. 따라서 인증서를 발급받은 자는 인증된 ICT 제품이나 서비스, 프로세스의 보안과 관련하여 이후에 탐지된 취약점 이상성을 발견한 경우 해당 기관이나 당국에 통보해야 한다(동조 제8항). 유럽 사이버보안 인증서는 유럽 사이버보안 인증제도에 규정된 기간 동안만 유효하며, 관련 요건이 계속적으로 충족될 경우에만 갱신될 수 있다(동조 제9항). 본 조항에 따라 발급된 유럽 사이버보안 인증서는 모든 회원국에서 인정을 받게 된다(동조 제10항). 따라서 회원국은 이미 시행 중인 유럽의 사이버보안 인증제도에 의해 적용되고 있는 ICT 제품이나 서비스, 프로세스에 대해 새로운 국가 사이버보안 인증제도를 도입해서는 안 된다(제57조 제2항). 이는 인증제도의 충돌로 인한 혼란을 방지하기 위한 것으로 판단된다.

---

844) 제58조 제1항에 따르면 각 회원국들은 하나 이상의 국가 사이버보안 인증기관을 지정하거나 다른 회원국의 합의에 따라 감독업무를 담당하는 하나 이상의 다른 회원국의 사이버보안 인증기관을 지정하여야 하며, 그 내용을 EU 집행위원회에 통보해야 한다(제58조 제2항).

㈏ 인증에 대한 적합성 평가

유럽 사이버보안 인증서 및 EU 적합성 명세서와 관련해서 EU 전체에서 동등한 표준을 달성하기 위해 국가 사이버보안 인증기관은 보안점검의 대상이 되는데(제59조 제1항), 특히 구조·인적자원 및 프로세스 요건·기밀성·불만사항에 관해 건전하고 투명한 평가 기준 및 절차를 위해서 '동료 평가'를 실시한다(동조 제2항).[845] 이 때, 동료 평가는 다른 회원국과 집행위원회의 국가 사이버보안 인증기관 2곳에서 실시하며, 최소 5년에 1회 이상 실시하여야 하고, ENISA도 보안 점검에 참여할 수 있다(동조 제4항). 그리고 보안 점검의 결과는 ECCG가 검토해야 하며, ECCG는 공개적으로 이용할 수 있는 요약을 작성해야 하고, 필요한 경우 해당 기관이 취해야 할 조치나 방법에 대한 지침이나 권고사항을 내도록 한다(동조 제6항).

적합성 평가기관은 '(EC) No 765/2008' 규정에 따라 임명된 국가 인증기관에 의해 인가되어야 하고, 해당 인가는 적합성 평가기관이 본 규칙 부속문서에 명시된 요건을 충족하는 경우에만 허용되어야 한다(제60조 제1항). 만일 유럽 사이버보안 인증서가 동 규정 제56조 제5항 및 제56조 제6항에 따라 국가 사이버보안 인증당국에서 발급되는 경우에는 국가 사이버보안 인증당국의 인증기관은 본조 제1항에 따른 적합성 평가기관으로 인정된다(동조 제2항). 그리고 유럽 사이버보안 인증제도가 동 규정 제54조 제1항의 (f)호에 따라 특정 또는 추가 요건을 정하는 경우, 그러한 요건을 충족하는 적합성 평가기관만이 해당 제도에 따라 업무를 수행할 수 있기 때문에 해당 평가기관은 국가 사이버보안 인증당국의 승인을 받아야 한다(동조 제3항). 그 결과 적합성 평가기관의 지위는 5년간 유지되며 동일한 조건에서 갱신되고, 더 이상 조건을 충족하지 못하는 경우에는 인가의 제한·보류·취소 등의 조치가 취해진다(동조 제4항).

---

845) 제3항에 따르면 동료 평가의 내용은 (a) 해당되는 경우, 제56조 제5항 및 제56조 제6항에 언급된 유럽 사이버보안 인증서의 발급과 관련된 국가 사이버보안 인증기관의 활동이 제58조에 규정된 감독 활동과 엄격히 분리되어 있는지 여부 및 그러한 활동이 서로 독립적으로 수행되고 있는지 여부, (b) 제58조 제1항에 따른 유럽 사이버보안 인증서의 ICT 제품이나 서비스 및 프로세스의 준수여부를 모니터링 하고 있는 규칙을 감독하고 시행하는 절차, (c) 제58조 제7항 (b)호에 따른 ICT 제품이나 서비스 및 프로세스의 제조자 또는 제공자의 의무를 감시하고 집행하는 절차, (d) 적합성 평가기관의 활동을 감시, 승인 및 감독하는 절차, (e) 해당되는 경우, 제56조 제6항에 따라 보증 수준 '높음'에 대한 인증서를 발급하는 당국의 직원이나 기관이 적절한 전문지식을 가지고 있는지 여부 등이다.

㉮ 유럽 사이버보안 인증 그룹의 설립

사이버보안 인증제도의 시행과 관련해서 '유럽 사이버보안 인증 그룹(European Cybersecurity Certification Group)'을 설립하도록 하고 있다(제62조 제1항). ECCG의 임무는 다음과 같다(동조 제4항):

> (a) 특히 'EU 롤링 워크 프로그램', 사이버보안 인증정책 문제, 정책 접근법의 조정 및 유럽 사이버보안 인증계획의 준비 등과 관련해서 일관성 있는 구현과 적용을 보장하기 위해 집행위원회에 대한 조언 및 지원
>
> (b) 제49조에 따른 후보 제도의 준비와 관련하여 ENISA에 대한 지원, 조언 및 협조
>
> (c) 제49조에 따라 ENISA가 작성한 후보 제도에 대한 의견 채택
>
> (d) ENISA에 제48조 제2항에 따른 후보 제도의 준비 요청
>
> (e) 기존의 유럽 사이버보안 인증제도의 유지 및 검토와 관련하여 집행위원회에 제출된 의견 채택
>
> (f) 사이버보안 인증분야 관련 개발을 검토하고 사이버보안 인증 체계에 대한 정보와 모범사례 교환
>
> (g) 특히 사이버보안 인증과 관련된 문제에 대해 효율적인 정보교환 방법을 확립함으로써 역량강화 및 정보교환을 통해 국가 사이버보안 인증당국 간의 협력촉진
>
> (h) 제54조 제1항의 (u)호에 따라 유럽 사이버보안 인증제도에 의해 확립된 규칙으로 보안 평가 메커니즘의 이행지원
>
> (i) 기존의 유럽 사이버보안 인증제도를 검토하고, 적절하다면, 유럽 사이버보안 인증제도를 국제표준화 기구와 협력하여 국제적으로 인정되는 표준과의 차이 및 결함을 해결할 수 있도록 ENISA에 권고하고, 유럽 사이버보안 인증제도를 국제적으로 공인된 표준과 연계촉진

각 회원국들에 설치되는 ECCG는 각 회원국의 창구와 같은 역할을 하면서 ENISA와 협력하여 유럽 사이버보안 인증제도와 관련된 업무를 함께 수행하게 되는 것이다.

㉯ 법적 장치

본 제도와 관련해서 몇몇 법적 장치가 마련되어 있다. 자연인 및 법인은 유럽 사이버보안 인증서의 발급자에게 이의를 제기하거나, 동 규정 제56조 제6항에 따라 행동할 때 적합성 평가기관이 발행한 유럽 사이버보안 인증서와 관련된 이의를 국가 사이버보안 인증기관과 함께 제기할 권리가 있다(제63조 제1항). 이의사항이 접수된 당국이나 기관은 소송 진행 상황 및 취해진 결정에 대해 정보를 제공하고, 동 규정 제64조에 명시된 '효과적인 사법적 구제권'을 이의 신청자에게 고지해 준다(동조 제2항). 여기서 '효과적인 사법적 구제권'은 (a) 제63조 제1항에 언급된 당국이나 기관이 취한 결정(해당되는 경우)은 해당 자연인 및 법인이 보유한 유럽 사이버보안 인증서의 부적절한

발급, 발급 실패 또는 인정과 관련하여, (b) 제63조 제1항에 언급한 당국이나 기관이 이의제기에 대해 조치를 취하지 않는 경우에 요구된다(제64조 제1항) 해당 소송은 사법처리가 필요한 당국이나 기관이 있는 회원국의 법원에다 제기한다(동조 제2항). 그를 위해 회원국은 침해 및 유럽 사이버보안 인증제도의 침해에 적용되는 벌칙에 관한 규칙을 정해야 하며, 이를 이행하기 위해 필요한 모든 조치를 취해야 한다. 제공되는 벌칙은 효과적이고, 비례적이며, 통제력이 있어야 한다. 그리고 회원국은 지체 없이 해당 규칙과 해당 조치여부에 대해 집행위원회에 통보해야 하며, 이에 영향을 미치는 후속 개정에 대해서도 통보해야 한다(제65조).

(3) EU의 사이버보안 관련 최근 동향

① 5G 사이버보안의 필요성

한국은 최근 세계 최초로 5세대 이동통신 서비스를 시작하게 되었다. 약자로 '5G'라고 표현하고 있는데, 국제전기통신연합(ITC)에서 정한 정식 명칭은 'IMT-2020'이다. 5G는 최대 속도가 20Gbps로서 4G에 비해 속도가 20여배 빠르고, 약 100배 많은 처리를 할 수 있기 때문에 4차 산업혁명의 가상현실이나 자율주행, 사물인터넷 기술 등이 원활하게 구현될 수 있도록 '초저지연성' 및 '초연결성'을 보장해 주는 기술이라고 한다.[846] 이처럼 한국은 언제나 하드웨어적으로 세계의 선두를 유지하고 있지만, 보안과 관련된 법률에 대해서는 여전히 미흡한 실정이다. 이에 반해 유럽은 이미 5G 서비스의 출현을 준비하고 있다. 앞서 살펴본 바와 같이 GDPR, EU 사이버보안법을 발효시켰으며, 5G와 관련해서도 집행위원회가 권고안을 마련하였다. 사이버공간이 지속적으로 발전하기 위해서는 하드웨어와 소프트웨어, 기관, 보안, 법제가 함께 유기적으로 움직여야 한다. 어느 하나라도 미흡하게 되면 안전한 사이버공간을 담보할 수 없게 된다. 그런 면에서 유럽연합은 법적 장치에 있어서 발 빠른 행보를 보이고 있다. 특히 최근 사이버공간과 관련된 과감한 법제화를 통해 사이버공간의 안전을 강력하게 추구하고 있다.

---

846) "5세대 이동통신" 검색결과, https://terms.naver.com/entry.nhn?docId=1968158&cid=43667&categoryId=43667 (2019년 11월 3일 최종접속).

② 5G 사이버보안을 위한 집행위원회 권고

5G 사이버보안과 관련해서 2019년 3월 26일 유럽연합 집행위원회가 발행한 권고안을 살펴보면 5G 서비스를 시작한 한국에 대한 시사점을 발견할 수 있을 것으로 보인다.[847] 집행위원회는 권고안에서는 5G 네트워크 사이버보안의 목적을 (a) 회원국들이 국가 차원에서 5G 네트워크에[848] 영향을 미치는 사이버보안 위험을 평가하고, 그에 필요한 보안조치를 취하도록 하며, (b) 회원국 및 유럽연합의 관련 기관, 에이전시 및 기타 기관이 국가위험평가에 기반해서 공동의 유럽연합 위험평가를 개발하고, (c) 디지털 생태계를 뒷받침하는 기반시설,[849] 특히 5G 네트워크에 관련된 사이버보안 위험을 완화시키기 위해 취할 수 있는 지침을 마련하는 것이다.[850]

이를 위해 크게 개별 회원국 수준에서 수행해야 할 활동과 유럽연합 수준에서 수행해야 할 활동들이 제시되고 있다. 먼저 개별 회원국 수준을 보면, 각 회원국들은 2019년 6월 30일까지 보안 위반으로 인해 중대한 부정적 영향이 발생할 수 있는 민감한 요소들을 포함해서 5G 네트워크 기반시설에 대한 위험평가를 실시해야 하고,[851] (i) 5G 네트워크의 특별한 기술적 특성과 같은 기술적 요소와 (ii) 정보 및 통신기술 장비의 제공자가 제3국에 속해 있는 경우의 법적·정책적 프레임워크와 같은 기타 요인들로부터 발생할 수 있는 사이버보안 위협을 고려하기 위해 국가 차원에서 적용되는 보안 요구사항과 위험관리 방법을 검토해야 한다.[852] 또한 회원국들은 해당 국가위험평가 및 검토에 근거하고, 유럽연합 수준에서 지속적으로 수행하고 있는 실행방안을

847) European Commission, COMMISSION RECOMMENDATION of 26.3.2019 - Cybersecurity of 5G network, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154 (2019년 11월 3일 최종접속).

848) 권고안에 따르면 '5G 네트워크'란 "서로간의 연결을 위해 사용되는 모바일 및 무선통신 기술에 있어 사용되는 관련 네트워크 기반시설 요소들의 집합을 의미하는데, 매우 높은 데이터 속도와 용량, 통신할 때의 짧은 지연시간, 초고도의 신뢰성 또는 수많은 연결 장치 지원 등 고급성능의 특성을 갖고 있는 부가가치 서비스이다. 여기에는 4G 또는 3G와 같은 이전 세대의 모바일 및 무선통신 기술에 기초한 기존 네트워크 요소가 포함될 수 있다. 그러므로 5G 네트워크는 네트워크의 모든 관련 부분을 포함하고 있는 것으로 이해될 수 있다"(European Commission, Ibid., p.5).

849) 본 권고안의 정의에 따르면 '디지털 생태계를 뒷받침해 주는 기반시설'이란 "경제와 사회에서 광범위한 영역에서 중요하게 취급되는 어플리케이션에 걸쳐 디지털화를 할 수 있도록 해 주는 기반시설"을 의미한다(European Commission, Ibid., p.5).

850) European Commission, Ibid., p.5.

851) 보고서 작성 시까지 그 결과가 공표되지 않아서 부득이 보고서에는 반영을 하지 못하게 되었다.

852) European Commission, Ibid., p.6.

고려해서 (a) 5G 네트워크에 적용되는 보안 요구사항 및 위험 관리 방법을 업데이트하고,(b) 2002/21/EC의 제13a조 및 제13b항에 따라 공공 통신망 또는 공공이 이용 가능한 전자통신서비스를 제공하는 사업에게 부과되는 의무를 업데이트 하며, (c) 공공 네트워크의 보안에 관한 일반인증에 있어 허가되지 않은 접근에 대해 조건을 부과하고, 2002/20/EC 지침에 따라 네트워크의 보안 요건 준수와 관련해서 향후 5G 대역의 무선 주파수에 대한 사용권 부여 절차에 참여할 것을 요청하며, 그와 함께 잠재적 사이버보안 위험을 완화하기 위해서 기타 예방 조치를 적용하도록 하고 있다.[853] 그에 해당하는 조치에는 전자통신망의 계획된 변경이나 국가의 감사 및 인증 연구소가 보안 및 무결성을 위해 특정 정보 기술요소와 시스템 등을 사전에 시험하도록 하는 요구조건 등에 관해서 권한 있는 국가기관에 관련 정보를 제공하는 것과 같이 네트워크의 민감한 부분의 보안을 보장하기 위해 공급자와 운영자에 대해 의무를 강화하는 내용이 포함되어야 한다.[854] 그 뿐 아니라 예를 들어, 동일한 사업으로 인해 둘 이상의 회원국에서 네트워크 기반시설이 운영되거나 구축되는 경우, 네트워크 구성에 주요한 유사점이 있는 경우와 같이 디지털 생태계와 5G 네트워크를 뒷받침하고 있는 기반시설과 관련해서는 적절한 기술적 전문지식과 시설을 사용하고 공유하는 등의 방법으로 2개 이상의 회원국이 공동보안검토를 실시하게 되는데, 이 때, ENISA나 EUROPOL 및 유럽 전자통신규제기구(Body of European Regulators for Electronic Communications, BEREC)는 이 지역 회원국들의 지원 요청에 우선순위를 두어야 하고, 해당 검토의 결과는 '협력단(Cooperation Group)'과 '컴퓨터 보안사고 대응팀 네트워크(Computer Security Incident Response Team Network)'로 전송하도록 하고 있다.[855]

다음으로 유럽연합 수준에서의 활동으로는 우선 5G 네트워크와 관련하여 사이버 보안 위험을 해결하기 위한 공통 접근방식을 개발하기 위해 회원국들은 2019년 4월 30일까지 협력 그룹의 업무 흐름에 맞추어 운영을 시작해야 하고, 협력 그룹의 작업에 자국의 관련 기관을 참여토록 해야 한다.[856] 5G 네트워크와 관련된 기존 및 잠재적

853) European Commission, Ibid., p.6.
854) European Commission, Ibid., p.6.
855) European Commission, Ibid., p.6.
856) European Commission, Ibid., p.6.

사이버보안 위험에 대한 공통의 인식을 구축하기 위해 회원국은 서로 또는 유럽연합의 관련 기관과 정보를 교환해야 하고, 국가위험 평가를 2019년 7월 15일까지 집행위원회와 ENISA에 전달해야 하며, ENISA는 '협력단' 및 '컴퓨터 보안사고 대응팀'의 지원을 받아 구체적인 5G 네트워크의 위협 환경 매핑을 완료해야 한다.[857] 그러고 나서 회원국들은 2019년 10월 1일까지 5G 네트워크의 위험에 대한 유럽연합 차원에서의 공동검토를 완료하게 된다. 여기서의 '공동 검토'는 산업용 어플리케이션에 사용되는 5G 접속 네트워크 요소뿐만 아니라 5G 네트워크의 핵심 요소에 포함된 특별히 민감하거나 취약한 요소에 적용되는 위험의 분석에도 중점을 두어야 하고, 이 후 디지털 가치 체인의 다른 전략적 요소로 확대하도록 하고 있다.[858]

권고안은 단순히 사이버보안 위협의 검토에 그치지 않고 그 해결 방안에 대해서도 설시하고 있다. 협력단 업무는 4번 지점에서 예견된 유형의 국가 수준에서 적용되는 모범사례의 대책을 모색하는 것이다. 이러한 국가 모범사례에 근거하여 2019년 12월 31일까지 국가 및 EU 수준에서 확인된 사이버보안 위험을 완화할 수 있는 적절하고 효과적이며 비례적인 위험 관리 조치를 위한 '툴박스(Toolbox)'를 합의하여, 높은 수준의 보안을 보장하기 위한 최소 공통 요구사항 개발과 관련된 사항을 위원회에 권고해야 한다. 그리고 5G 네트워크의 사이버보안에 대한 정보를 수집하도록 하고 있다. 그렇게 해서 만들어진 툴박스에는 (a) 5G 네트워크의 사이버보안에 영향을 미칠 수 있는 보안 위험 유형 목록,[859] (b) 위험평가 후 하나 이상의 회원국에서 확인된 모든 유형의 보안 위험을 다루어야 하는 가능한 완화 조치들[860] 등을 포함하도록 하고 있다.[861] 그리고 5G 네트워크와 관련된 유럽의 사이버보안 인증제도가 개발되면 회원국들은 해당 제도가 적용되는 통신기술 제품이나 서비스 및 시스템의 위험을 해결하기 위해 유럽연합의 법률을 채택해야 한다.[862] 그와 함께 회원국은 집행위원회와

857) European Commission, Ibid., p.7.
858) European Commission, Ibid., p.7.
859) 대표적인 예로 공급망 위험, 소프트웨어 취약성 위험, 액세스 제어 위험, 제3국에서 정보통신기술 장비 공급자가 대상이 될 수 있는 법적 및 정책 프레임워크에서 발생하는 위험 등을 들고 있다(European Commission, Ibid., p.7).
860) 대표적인 예로 하드웨어나 소프트웨어 및 서비스에 대한 제3자 인증, 공식적인 하드웨어 및 소프트웨어 테스트 또는 적합성 검사, 접근 제어가 존재한다는 것을 확인하거나 잠재적으로 안전하지 않은 것으로 간주되는 제품, 서비스 또는 공급업체를 식별하는 프로세스 등을 들고 있다(European Commission, Ibid., p.7).
861) European Commission, Ibid., p.7.

함께 5G 사업권을 가진 업체에 대한 요구조건에 대한 검토를 해야 하며, 5G 네트워크와 관련해서 공공 조달에 적용될 수 있는 구체적인 보안 요건을 개발하고, 그 경우 모든 공급자와 운영자에게 (현재는 구속력이 없지만 장차 의무화 될) 사이버보안 인증제도를 공공 조달의 필수 요건으로 포함되도록 해야 한다.[863] 그리고 회원국들은 2020년 10월 1일까지 해당 권고안의 효과를 평가하기 위해 위원회와 협력해야 하고, 향후 보다 적절한 방법을 결정하도록 하고 있다.[864]

(4) 소결 및 시사점

최근 유럽연합은 사이버보안과 관련해서 다양한 규정들을 내어놓고 있다. 유럽연합은 개별 국가가 아니기 때문이 각 회원국들의 협력 및 이행이 반드시 요구된다. 따라서 유럽연합의 규정은 각 회원국들의 상황에 따라 각 회원국별로 다소 다른 모습을 가질 수 있지만, 기본적인 프레임을 벗어나지는 않게 된다. 한국이 유럽연합을 주목해야 할 이유는 유럽연합의 사이버보안 관련 규정은 한국 기업 및 기관 등에 밀접한 영향을 미치기 때문이다. 이는 이미 유럽연합의 'GDPR'을 통해서도 경험한 바이다.

이번 유럽연합의 사이버보안법의 핵심은 ENISA를 상설화 하고, 사이버보안 인증체계를 구축하는 것이다. 즉, ENISA를 유럽 사이버보안의 허브 및 조정기관으로 삼고, 사이버보안 인증제도를 통해 유럽의 사이버공간의 안전을 보장하고자 하는 것이다. 그와 함께 최근 새롭게 부각되고 이는 기술인 5G와 관련된 문제에도 발 빠르게 대처하고 있다. 이처럼 유럽연합이 사이버보안을 위해 노력하고 있는 이유는 최근 사이버공격 등으로 인해서 그 피해가 증대되고 있는 것을 경험하고 있기 때문이다. 유럽의 경우에도 한국보다는 다소 느리지만 정보화 사회가 상당히 진전되면서 사이버공간의 중요성이 커지고 있다. 특히 정보통신망이 상대적으로 잘 갖추어진 독일이나 영국 등에서 많은 피해가 발생하고 있기 때문에 이들 국가를 중심으로 사이버보안에 대한 정책이 펼쳐지고 있다. 자율주행자동차나 A.I. 등 새로운 기술발전에 따른 규정에 대한 연구가 상대적으로 다른 국가들이나 지역, UN차원의 논의보다도 앞서 있는 것으로 보인다. 그러므로 앞으로도 지속적으로 유럽연합 차원에서의 사이버보안 관련 논

862) European Commission, Ibid., pp.7-8.
863) European Commission, Ibid., p.8.
864) European Commission, Ibid., p.8.

의를 추적 관찰할 필요성이 있다.

무엇보다 한국은 단순히 한국의 사이버보안에 치중하는 것을 넘어서 동북아시아, 동남아시아를 비롯하여 아시아지역 전반의 사이버보안에 관심을 기울여야 할 필요성이 있다. 이는 국제사회에서 사이버보안과 관련해서 한국의 중요성을 높이 사고 있는 이유이기도 하다. 따라서 유럽연합이 사이버보안과 관련된 규정들을 만들어 나아가는 프로세스는 한국에게 좋은 예가 될 수 있을 것이다. 비록 아시아가 유럽연합과 같은 연합체는 아니지만 앞으로 한국이 사이버보안 규정과 관련 문제에 있어 적어도 아시아지역에서 선도적인 역할을 수행하기 위해서는 유럽연합의 체계를 벤치마킹 하는 것도 많은 도움이 될 것이다.

4) 일본

(1) 사이버보안 관련 규정 개관

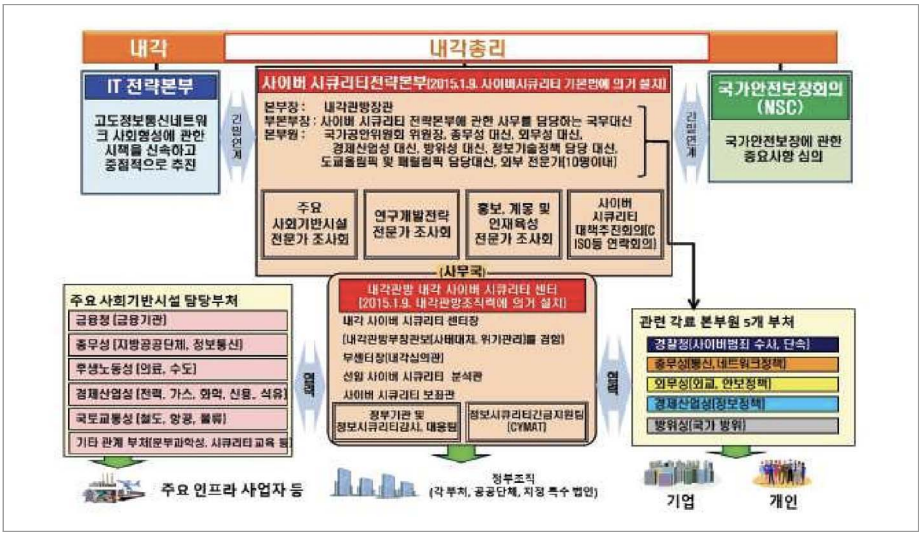
일본도 사이버보안의 중요성을 인식하게 되면서 사이버보안 정책에 많은 노력을 기울이고 있다.[865] 특히 일본 사회의 패러다임이 정보화 사회를 넘어 'Society 5.0'으로 바뀌고 있고, 2020년 도쿄 올림픽과 관련해서 사이버 위협이 증가할 것이라고 예상하고 있기 때문에 체계적인 전략이 필요한 상황으로 인식하고 있다.[866] 그래서 2018년의 'Cybersecurity Strategy'에서는 일본 사이버전략의 비전으로서 자유(free), 공정(fair), 보안(secure)이라는 기존의 사이버보안 전략의 기조를 유지하면서,[867] 사이버공간의 새로운 발전방향에 맞추어 서비스 제공자에 대한 임무와 위험관리, 참여·조정·협력이라는 새로운 접근방법을 모색하고 있다.[868] 그와 같은 일본의 전략은 일본정부가 정보보안에 대해 관심을 갖기 시작한 2007년부터 이어져 온 것이다.[869] 그와 같은 일본의 사이버보안 전략이 법률로서 구체화된 것이 '사이버시큐리티기본법'이다.

일본은 2014년 11월 '사이버시큐리티기본법'을 제정했으며, 2018년 12월에 개정하

865) NISC, Cybersecurity Strategy, 2018.7.27., https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf (2019년 11월 3일 최종접속).
866) NISC, Ibid., pp.1-2.
867) NISC, Ibid., p.9.
868) NISC, Ibid., pp.12-13.
869) NISC, Japanese Government's Efforts to Address Information Security Issues, 2007, https://www.nisc.go.jp/eng/pdf/overview_eng.pdf (2019년 11월 3일 최종접속).

였다. 사이버시큐리티기본법은 제1장 총칙, 제2장 사이버시큐리티전략, 제3장 기본 시책, 제4장 사이버시큐리티 전략본부, 제5장 벌칙 그리고 부칙으로 구성되어 있다.[870] 해당 내용을 요약해 보면 아래의 그림과 같다.

[그림 5-2] 일본 사이버보안 정책 대응체계[871]



해당 법률은 기본법이기 때문에 그를 바탕으로 보다 구체적인 개별법들이 만들어지게 될 것이다. 한국은 기본법의 역할이 실질적으로는 다른 개별법과 같은 지위에 있지만, 일본은 기본법을 바탕으로 개별법들이 체계적으로 만들어지는 입법구조를 가지고 있다. 그러므로 해당 법률을 살펴보게 되면 앞으로의 일본의 사이버보안 관련 법률의 방향을 알 수 있게 된다.

(2) 사이버시큐리티기본법 분석

일본 사이버시큐리티기본법을 살펴보면 앞서 살펴본 미국이나 유럽연합의 규정과는 달리 한국의 법률규정과 같은 구조와 내용을 담고 있다. 일본 사이버시큐리티기본

870) 한국인터넷진흥원, "일본 경제산업성, 사이버·물리보안 대책 프레임워크 개정안 발표", 인터넷 법제동향 제133호, 한국인터넷진흥원, 2018.10, 36면.
871) 이미지 출처: 배상균, "일본 사이버 보안 정책에 관한 검토-사이버 시큐리티 기본법의 성립과 개정을 중심으로-", 외법논집 제42권 제2호, 한국외국어대학교 법학연구소, 2018, 149면.

법 제1장 총칙은 총 11개의 조문으로 구성되어 있다. 제1조에서는 해당 법률의 목적을 밝히고 있으며,[872] 제2조에서는 사이버시큐리티의 정의를 내리고 있고,[873] 제3조에서는 기본이념, 제4조에서는 국가의 책무, 제5조에서는 공공단체의 책무, 제6조에서는 중요 사회기반사업자의 책무, 제7조에서는 사이버관련 사업자 및 기타 사업자의 책무, 제8조에서는 교육연구기관의 책무, 제9조에서는 국민의 노력, 제10조에서는 법제상의 조치, 그리고 제11조에서는 행정조직의 정비 등에 대한 내용을 규정해 놓고 있다.[874] 해당 규정들 가운데 눈에 띄는 것은 사이버 관련 사업자 및 기타 사업자의 책무를 명시적으로 밝히고 있다는 것이다. 대개의 법률은 주로 국가와 국가기관, 지방단체, 국민들의 책무를 규정해 놓는데, 사이버보안에 있어서는 사업자의 역할이 매우 중요하게 된다. 그러므로 해당 기본법에서도 그 부분을 명확히 하고 있는 것으로 보인다. 또한 제10조에서는 정부로 하여금 사이버시큐리티를 위한 법제, 재정, 세제, 그 외 필요한 조치를 강구하도록 하고 있다. 따라서 해당 법률이 기본법이기 때문에 앞으로 여러 개별 법률들이 제정될 것으로 보인다.

제2장에서는 사이버시큐리티 전략에 관한 내용을 규정하고 있다. 해당 전략은 앞서 살펴본 NISC의 문서에서 언급한 사이버시큐리티 전략과 관련을 맺게 된다. 그렇게 보면 일본의 사이버보안 정책은 '정부의 사이버시큐리티 전략 → 사이버시큐리티기본법 → 사이버시큐리티 개별 규정'의 구조로 규범화 되는 것으로 보인다. 그러나 제2장

872) 일본 사이버시큐리티기본법 제1조 이 법은 인터넷, 그 밖의 고도정보통신 네트워크의 정비 및 정보통신기술 활용의 진전에 따라 세계적 규모로 발생하는 사이버시큐리티에 대한 위협의 심각성, 그 밖의 국내외 정세의 변화에 따라 정보의 자유로운 유통을 확보하고, 사이버시큐리티를 확보하는 것이 긴급 과제인 상황에 비추어 우리나라의 사이버시큐리티 시책에 관하여 기본이념을 정하고, 국가 및 지방공공단체의 책무 등을 밝히며, 사이버시큐리티 전략의 책정, 기타 사이버시큐리티 시책의 기본 사항을 규정함과 동시에 사이버시큐리티 전략본부를 설치하여 고도정보통신 「네트워크 사회형성기본법」(평성12년 법률 제144호)과 더불어 사이버시큐리티에 관한 시책을 종합적이며 효과적으로 추진하고, 나아가 경제사회의 활력 향상, 지속적 발전 및 국민이 안심하고 안전하게 살 수 있는 사회를 실현하고 국제사회의 평화 및 안전의 확보, 우리나라의 안전보장에 기여하는 것을 목적으로 한다.

873) 일본 사이버시큐리티기본법 제2조에 따르면 사이버시큐리티란 "전자적 방식, 자기적 방식, 기타 사람의 지각으로는 인식할 수 없는 방식으로 기록되거나 발신·전달 또는 수신되는 정보의 누설, 멸실 또는 훼손의 방지, 그 밖에 해당 정보의 안전관리를 위하여 필요한 조치, 정보 시스템 및 정보통신 네트워크의 안전성 및 신뢰성 확보를 위하여 필요한 조치가 마련되고, 그 상태가 적절히 유지·관리되는 것"을 의미한다.

874) 본 법률의 내용은 세계법제정보센터에서 번역한 내용을 기본으로 사용하였다, http://world.moleg.go.kr/cms/commonDown.do?DLD_CFM_NO=MNPH3FOQ89J32FGWJPAR&FL_SEQ=47496 (2019년 11월 3일 최종접속).

의 내용을 살펴보면 사이버시큐리티기본법 제2장에 따라 일본 정부가 사이버시큐리티 전략을 마련하도록 되어 있다. 따라서 '사이버시큐리티기본법 → 정부의 사이버시큐리티 전략 → 사이버시큐리티 개별 규정'의 순환구조를 갖게 된다. 제2장은 제12조 한 개의 조문으로 구성되어 있다. 해당 조문에서 일본 정부는 사이버시큐리티 전략을 마련하되, "1. 사이버시큐리티 시책에 대한 기본 방침, 2. 국가 행정기관 등에서의 사이버시큐리티 확보에 관한 사항, 3. 중요사회기반사업자와 그가 조직하는 단체 및 지방공공단체에서의 사이버시큐리티 확보의 촉진에 관한 사항, 4. 제1호부터 제3호까지의 사항 외에 사이버시큐리티 시책을 종합적이며 효과적으로 추진하기 위하여 필요한 사항" 등이 내용에 포함되어야 하고, 결정된 정책은 지체 없이 국회에 보고하고, 그와 동시에 인터넷이나 그 밖의 방법 등으로 공표하도록 하고 있다.

제3장에서는 기본 시책에 대해 규정하고 있다. 제13조에서는 국가 행정기관 등에서의 사이버시큐리티 확보방안, 제14조에서는 중요사회기반사업자 등의 사이버시큐리티 확보촉진방안, 제15조에서는 민간사업자 및 교육연구기관 등의 자주적인 사이버시큐리티 확보방안, 제17조에서는 다양한 주체들의 연대방안 등을 강구하도록 규정하고 있다. 다만, 해당 규정은 방안에 대한 내용이 아닌 국가 및 사회의 다양한 주체들이 사이버시큐리티를 확보할 수 있도록 선언하는 의미에 불과 하다. 제18조에서는 사이버시큐리티 관련 범죄 단속 및 피해확대 방지를 위해 필요한 시책을 마련하도록 하고 있으며, 제19조에서는 사이버안전에 영향을 미칠 수 있는 사상에 대한 대응, 제20조에서는 사이버시큐리티 관련 산업을 진흥하고 국가경쟁력을 강화시킬 수 있도록 하고 있으며,[875] 제21조에서는 사이버시큐리티 관련 연구개발을 추진하고, 제22조에서는 사이버시큐리티 인재를 확보하는 방안, 제23조에서는 사이버시큐리티와 관련해서 대국민적 교육 및 학습의 진흥과 보급을, 그리고 제24조에서는 사이버시큐리티와 관련해서 국제협력을 강화할 수 있는 시책을 마련할 것을 규정하고 있다. 해당 장에서는 제17조와 제24조가 사이버보안과 관련된 형사정책과 직접적인 관련을 맺고 있다.

875) 한국의 업체들이 사이버보안과 관련해서 일본의 업체들보다 뛰어나다는 것은 일본도 인지하고 있다. 그러므로 2020년에 도쿄에서 열리는 올림픽에서 사이버보안과 관련된 업무를 한국 업체들이 담당하고 있기 때문에 일본에서는 한일갈등으로 인한 사이버보안의 공백을 우려하는 분위기도 있었다; "도쿄올림픽 앞둔 日, 韓보안업체들 등돌릴까 '발동동'", 아시아경제 2019년 7월 25일자, https://www.asiae.co.kr/article/2019072410072474645 (2019년 11월 3일 최종접속).

따라서 앞으로 해당 규정에 따라 어떤 법률적 조치들이 취해지는지를 지속적으로 살펴볼 필요가 있다.

제4장에서는 사이버시큐리티 전략본부에 대한 규정을 하고 있다. 해당 규정에 따르면 일본의 사이버시큐리티 시책을 위해서 내각에 사이버시큐리티 전략본부를 두도록 하고 있다(제24조). 그리고 전략본부장은 내각관방장관이 담당하고(제27조 제1항), 부본부장은 국무대신이 담당하도록 하고 있다(제28조 제1항). 그리고 본부원으로는 국가공안위원회위원장, 총무대신, 외무대신, 경제산업대신, 방위대신 뿐 아니라 내각관방장관이 필요하다고 인정하는 자 및 사이버시큐리티 전문가 중 내각관방장관이 임명하는 자 등이 해당된다(제29조 제2항). 이는 일본의 사이버시큐리티에 대한 관리감독을 강화하기 위한 조직적 방법으로 보인다. 전략본부는 사이버시큐리티 관련 사무를 전문기관에 위탁할 수 있으며(제30조), 관계 행정기관으로부터 관련 정보를 제공받을 수 있고(제31조), 소관사무 수행을 위해서 지방공공단체나 독립행정법인, 국립대학법인 등 여러 기관들의 장에게 협력을 요구할 수 있으며(제32조), 지방공공단체는 요구에 따르도록 노력하고 있다(제33조). 이는 조직을 통한 권한 확립과 함께 관련 업무를 수행함에 있어서도 다른 조직의 협력을 받아낼 수 있는 근거를 마련함으로써 전략본부의 장악력을 강화시키기 위한 방안이라고 할 것이다. 결국 일본은 사이버시큐리티 전략본부를 사이버시큐리티의 컨트롤타워로 두고, 전략본부를 통해 사이버공간에서의 보안을 유지하는 체계를 구축한 것이다.

제5장에서는 처벌규정을 두고 있는데, "제30조 제1항 규정에 따라 사무위탁을 받은 법인의 임원이나 직원 또는 이들의 직에 있는 자는 정당한 이유 없이 해당 위탁에 관련된 사무에 관하여 알게 된 비밀을 누설하거나 남용"한 경우에는 1년 이하의 징역이나 50만엔 이하의 벌금에 처해지도록 하고 있다.

(3) 일본의 사이버보안 관련 최근 동향

일본도 최근 5G와 관련된 사이버보안에 관심을 기울이고 있다. 따라서 일본 총무성은 최근 2017년의 "IoT 보안 종합대책"의 후속으로 IoT 보안대책, 5G 보안대책, 기타 보안대책으로 구성된 "IoT, 5G 보안 종합대책"을 제시하였다.[876] IoT 보안대책으로는

876) 한국인터넷진흥원, "일본 총무성, IoT·5G 보안 종합 대책 발표", 인터넷 법제동향 제144호, 한국인터넷진흥원, 2019.9, 22면.

IoT 기기를 설계 및 제조, 판매 시 사이버보안과 관련된 가이드라인 및 인증제도, IoT 기기를 설치 및 운용; 보수 시 사이버보안 취약성에 대처하기 위한 체계, 사이버공격에 취약한 IoT 기기들에 대한 조사, 전기통신사업자 사이의 사이버공격 관련 정보공유 강화 등이 있다.[877] 5G 보안대책으로는 5G 기술 이용과 관련된 SW 보안 취약성에 대한 대책, 빅데이터와 A.I. 등의 기술 활용에 따른 HW 보안 취약성에 대한 대책, 클라우드 서비스 안전성 평가제도 등을 통한 클라우드 서비스에 대한 대책, 스마트시티와 관련된 보안에 대한 대책, 공공 및 민간의 협력을 통한 중요 정보통신 기반시설 시스템의 보안에 대한 대책, 그리고 사이버보안 방어 훈련이나 사이버보안 전문가 양성, 지역 정보통신 서비스 지원을 통한 지역 정보통신 서비스 향상 등으로 범주화하여 대책을 마련하고 있다.[878]

(4) 소결 및 시사점

일본의 사이버시큐리티기본법은 용어 그대로 기본법이다. 일본의 사이버보안 규정이 구체적으로 어떻게 구현될지는 앞으로 제정되는 개별법을 살펴볼 필요가 있다. 다만 일본 사이버시큐리티기본법을 통해서 얻을 수 있는 시사점으로는 일본은 사이버시큐리티의 컨트롤타워를 내각관방장관으로 설정하여 통일적인 정책이 추진될 수 있는 체계를 마련하고 있다는 것이다. 다만, 일본이 한국과 유사한 점이 많다는 것을 고려해 볼 때, 총리가 아닌 내각관방대신이 컨트롤타워로서의 역할을 원활하게 수행할 수 있을지 의문이다. 그럼에도 불구하고 해당 기본법에 사실상 사이버보안 컨트롤타워를 규정함으로써 내각관방대신이 합법적으로 사이버보안의 컨트롤타워 역할을 수행할 수 있도록 하고 있다. 또한 총무성이 주관이 되어 기술변화에 따라서 발생할 수 있는 사이버보안 문제에 대해서 지속적으로 계획을 하고, 평가 및 국제협력, 민관협력 등을 통해 종합적인 대응을 하고 있다.

그에 반해 한국의 경우에는 기존의 사이버보안의 컨트롤타워조차 약화되고 있다. 이전 정부 때에는 그동안 학계 등에서 주장되었던 내용이 어느 정도 반영되었는데, 이번 정부에 들어와서는 오히려 정책이 후퇴하여 사이버안보 비서관이 폐지되었고,[879] 사이버안보와 정보융합을 통합하여 '사이버정보비서관'을 두고 있다.[880] 물론

877) 한국인터넷진흥원, 앞의 글("일본 총무성, IoT·5G 보안 종합 대책 발표"), 22-23면.
878) 한국인터넷진흥원, 앞의 글("일본 총무성, IoT·5G 보안 종합 대책 발표"), 23면.

국가안보실 제1차장이 사이버정보를 다루고 있기는 하다.[881] 그러나 국가안보실은 조직구조상 사이버보안의 컨트롤타워가 되기 어렵고, 사이버보안과 정보융합은 서로 반대 방향을 보고 있는 정책이기 때문에 한 바구니에 담아서 정책을 펼치기가 쉽지 않다. 더욱이 사이버공간의 진흥과 억제 수단인 보안을 한 바구니에 담는 것은 상대적으로 진흥을 위해서 보안이 희생될 수 있을 여지가 생긴다. 그러므로 사이버보안과 관련된 정책을 분리하여 지속적으로 추진하고, 사이버보안과 관련해서 사회의 변화를 이끌어내며, 보다 광범위하고 세밀한 정책구현을 위해서는 일본 사이버시큐리티기본법과 같이 확고한 사이버보안 컨트롤타워를 구축하고, 그를 법률을 통해 구체화 시키는 것이 필요하다.

5) 중국

(1) 사이버보안 관련 규정 개관

중국도 사이버보안과 관련해서 많은 관심을 기울이고 있다. 일반적으로 중국은 북한과 함께 사이버공격의 거점지로 알려져 있지만, 중국 역시 사이버공격의 대상이 되고 있기도 하다. 따라서 2014년에만 2.4억 명이 사이버범죄의 피해를 입었으며, 그 액수도 7,000억 위안에 이른다고 한다.[882] 그로 인해 중국도 사이버보안과 관련해서 2016년 11월에 '사이버보안법'을 제정하였고, 2017년에는 '네트워크제품 및 서비스 보안심사방법', '인터넷 뉴스정보서비스 관리규정', '인터넷 정보내용관리 행정집행법절차규정' 등을 새롭게 규정하였다.[883] 다만, 이보다 앞선 2016년 12월에 '국가사이버공간안전전략'을 반포하여 사이버공간에서의 안전에 대한 프레임을 제시하기도 하였다.[884]

---

879) 사이버안보 비서관은 박근혜 정부 때 사이버안보를 위해 만들어진 자리였다. "靑 사이버안보 비서관에 신인섭 준장", 매일경제 2015년 4월 1일자, https://www.mk.co.kr/news/society/view/2015/04/310034/ (2019년 11월 3일 최종접속).

880) "청와대 사이버안보비서관 폐지...한국 사이버안보 후퇴하나", 보안뉴스 2018년 7월 27일자, https://www.boannews.com/media/view.asp?idx=71783 (2019년 11월 3일 최종접속).

881) 청와대 조직도 참조, https://www1.president.go.kr/about/organization (2019년 11월 3일 최종접속).

882) 한국무역협회 북경지부, 중국 사이버보안법 관련 법규 해설, 2017.6., 2면, http://ebook.kita.net/ebookView.ez?cmd=&ebook_seq=00000000000000001497924078550000&category_seq=0204&category_name=%ED%95%B4%EC%99%B8%EC%A7%80%EB%B6%80%EB%B3%B4%EA%B3%A0%EC%84%9C&ftaYN=undefined (2019년 11월 3일 최종접속).

883) 한국무역협회 북경지부, 앞의 책, 2면.

2017년 새롭게 규정된 '네트워크제품 및 서비스 보안심사방법', '인터넷 뉴스정보서비스 관리규정', '인터넷 정보내용관리 행정집행법절차규정'은 기존의 사이버보안법에 대한 절차규정으로 이해되고 있다.[885] 그러므로 우선 이들 절차규정에 대해서 개관해 보고, 실체규정인 사이버보안법을 살펴보고자 한다. 첫째로, '네트워크제품 및 서비스 보안심사방법'은 사이버공간에서의 서비스의 안전에 주안점을 두고 있는 법률이다. 총 16조의 규정으로 되어 있으며, 사이버서비스의 심사범위, 심사내용, 심사기관, 제품 및 서비스제공자의 권리와 의무 및 법적 책임 등에 관해 규정을 하고 있다.[886] 해당 법률에 대해서는 국가안전에 영향을 미칠 수 있는 제품 및 서비스에 대해 경계를 구분하고, 안전심사 대상과 심사표준을 명확히 하였으며, 제품 및 서비스 제공자에 대한 구제수단을 두고 있다는 긍정적인 평가와 함께 대부분의 규정이 불명확하고, 구제수단도 부족하다는 비평도 제기된다.[887]

둘째로, '인터넷 뉴스정보서비스 관리규정'의 목적은 인터넷 뉴스에 대한 관리를 강화하는 것에 있다.[888] 총 6장 29개 조문으로 구성되어 있으며, 그 내용을 살펴보면 서비스 허가의 감독형태, 제공자의 자질과 사회적 책임 구체화 등으로 구성되어 있다.[889] 본 법률이 관리에 중점을 두고 있기 때문에 인터넷 서비스 제공자는 '발포서비스', '전재서비스', '전파 플랫폼 서비스'로 구분되어 반드시 '서비스 허가'를 얻어야 하고,[890] 인터넷사이트나 블로그, 공식계정 등 어떤 형식으로든 대중에게 뉴스를 제공하는 자는 반드시 허가를 얻도록 하고 있다.[891] 또한 뉴스 서비스 제공자도 "a. 중국에서 적법하게 설립된 법인, b. 주요 책임자 및 총 편집장이 중국공민, c. 전문 편집인원, 내용심사인원과 기술보장인원 구비, d. 건전한 네트워크뉴스정보서비스 관리제도 구비, e. 건전한 정보보안관리제도와 안전하고 통제 가능한 기술보장조치 구비, f. 서비스제공에 필요한 장소, 시설과 자금 구비" 등 매우 까다로운 조건을 요구하고 있다.[892]

---

884) 한국무역협회 북경지부, 앞의 책, 3면.
885) 한국무역협회 북경지부, 앞의 책, 2면.
886) 한국무역협회 북경지부, 앞의 책, 10-11면.
887) 한국무역협회 북경지부, 앞의 책, 12면.
888) 한국무역협회 북경지부, 앞의 책, 12-13면.
889) 한국무역협회 북경지부, 앞의 책, 13-14면.
890) 한국무역협회 북경지부, 앞의 책, 13면.
891) 한국무역협회 북경지부, 앞의 책, 13면.
892) 한국무역협회 북경지부, 앞의 책, 13-14면.

셋째로, '인터넷 정보내용관리 행정집행법절차규정'은 정보내용관리부서가 행정집행을 하는 절차를 규정하고 있다. 모두 8장 49개 조문으로 구성되어 있으며, 주요 내용으로는 집행주체와 집행범위를 확정하고, 관할, 집행감독, 법률 집행 체계 등을 규정하고 있으며, 집행절차에 대한 구체적인 요건, 당사자 권리 보호 등에 대한 규정을 두고 있다.[893] 절차규정을 통해 투명하고 공정한 절차집행에 기여할 것이라는 평가도 있지만,[894] 사실상은 관리감독의 편의를 위한 규정으로 보인다. 그럼에도 불구하고 해당 규정을 두고 있는 것 자체만으로도 일단은 긍정적인 평가를 줄 수 있을 것이다.

아래에서 살펴볼 사이버보안법과 함께 중국도 사이버보안과 관련된 법체계를 구축해 나가고 있는 것으로 보인다. 다만, 절차규정에서는 사이버보안의 목적과 함께 중국 사이버공간에 대한 관리감독을 강화하려는 시도도 엿보인다. 아래에서는 중국 사이버보안법 체계의 핵심이라고 할 수 있는 사이버보안법에 대해 좀 더 자세히 살펴보고자 한다.

(2) 중국 사이버보안법 분석

중국 사이버보안법의 본래 명칭은 '중화인민공화국네트워크안전법(이하 '네트워크안전법'이라고 함)'이다.[895] 네트워크안전법은 '제1장 총칙, 제2장 네트워크 지지 및 촉진, 제3장 네트워크 운영 안전, 제4장 네트워크 정보보안, 제5장 모니터링 경보와 비상 대응제, 제6장 법률 책임제, 제7장 부칙' 등으로 이루어져 있다. 우리가 주의 깊게 살펴볼 부분은 제3장~제6장까지 이다. 첫째로, 네트워크 운영 안전을 위한 규정들을 살펴보면, 먼저 국가는 안전등급 보호제도를 시행해야 하고, 네트워크 사업자는 해당 제도에 따라 보호 의무를 이행하도록 하고 있다(제21조). 그리고 네트워크 제품 및 서비스는 국가표준 및 업계표준을 준수해야 하며(제22조), 네트워크 사업자는 보안 비상 매뉴얼을 작성하여 보안사고 시 그에 따라 대처해야 한다(제25조). 특히 네트워크 사업자는 "공안기관, 국가안전기구가 법에 따라 국가의 안보를 지키고 범죄활동을 조사하도록 기술 지원과 협조를 제공해야 한다(제28조)"라고 규정하여 네트워크 사업

893) 한국무역협회 북경지부, 앞의 책, 15-16면.
894) 한국무역협회 북경지부, 앞의 책, 16면.
895) 본 법률에 대해서는 개인정보보호 종합포탈(www.privacy.go.kr)에 번역되어 있는 조문을 사용하고자 한다, https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000833946&fileSn=0 (2019년 11월 3일 최종접속).

자의 협조의무를 명시하고 있다. 또한 국가와 네트워크 사업자는 보안정보를 공유하고(제29조), 보안정보를 사용하는 유관부처는 안전 유지를 위해서만 해당 정보를 활용할 수 있도록 하고 있다(제30조). 또한 핵심 정보 인프라는 별도의 규정을 통해서 보다 강하게 보호하고 있다. 따라서 국무원이 핵심 정보 인프라와 관련된 보안정책과 책임분배를 담당하고(제31조~제32조), 핵심 정보 인프라 사업자는 보다 강화된 안전 보호 의무를 이행하도록 하고 있다(제34조~제38조). 그리고 국가 네트워크 정보부처는 다른 부처들과 협력하여 핵심 정보 인프라 보안 리스크 분석 및 개선, 정기 훈련 등으로 핵심 정보 인프라 사업자 협업 및 협력 능력 향상, 관련 기관과 핵심 정보 인프라 사업자 및 관련 연구기관 등과의 네트워크 보안 정보 공유 촉진, 그리고 네트워크 보안 사고에 대한 처리와 복구 등에 대한 기술지원과 협조를 제공(제39조) 등의 업무를 수행하도록 하고 있다.

둘째로, 네트워크 정보보안과 관련해서 네트워크 사업자의 개인정보 수집 및 활동 등에 책임을 강화하고 있다. 따라서 네트워크안전법 제4장의 규정의 기존에 한국의 정보통신망법에 개인정보보호 관련 규정이 있었던 것과 같이 개인정보와 관련된 규정들을 자세하게 규정하고 있다.

셋째로, 모니터링 경보와 비상대응과 관련된 규정들을 두고 있다. 따라서 국가는 네트워크 보안을 위한 모니터링 경보체계와 비상대응체계를 구축하여 운영하도록 하고 있다(제51조~제53조). 그에 따라 국가는 네트워크 보안사건 발생의 위험이 있는 경우 관련 부처 등에 모니터링 강화 요구, 관련 부처 등과 협조하여 위험 분석평가 및 발생가능성과 피해 예측, 네트워크 위험 경고 및 대응조치 전파를 해야 한다(제54조). 네트워크 보안사고 시 매뉴얼에 따라 조치하고(제55조), 성급 이상의 인민 정부 유관 부처는 네트워크 사업자 등과 면담할 수 있다(제56조). 무엇보다 눈에 띄는 규정으로는 제58조 규정으로서 "국가 안보와 사회 공공질서를 유지하고, 중대하고 돌발적인 사회 안전 사건을 처리하기 위해서 필요할 때, 국무원의 결정 혹은 비준에 따라, 특정 지역에서 네트워크 통신에 대하여 제한 등의 임시 조치를 취할 수 있다"라고 규정하고 있다. 즉, 해당 규정으로 인해 중국에서는 합법적으로 네트워크 통제가 가능하게 된 것이다.

넷째로, 법률책임에 있어서는 네트워크 사업자의 법적 책임을 상당히 강화하고

있다. 따라서 네트워크 사업자가 안전의무를 이행하지 않은 경우 그 위반 유형과 정도에 따라 벌금과 업무 일시중단, 영업중단, 사이트 폐쇄, 인허가 취소 등을 부과하고 있으며(제59조~제62조, 제64조~제66조, 제69조~제69조 등), 개인의 경우에는 네트워크 보안을 침해하는 활동을 하는 경우에 구류나 벌금형 등에 처해진다(제63조, 제67조 등). 다만, 제74조와 제75조를 보면 본 법률에서 법적 제재가 상당히 광범위해질 수 있는 위험이 있다. 제74조에서는 "본법의 규정을 어기고 타인에게 피해를 줄 경우 법에 의해 민사책임을 진다. 본법 규정을 어기고, 치안 관리 위반 행위를 구성한 경우, 법에 따라 치안 관리 처벌을 부과하고, 범죄를 구성한 경우, 법에 따라 형사책임을 추궁한다"라고 규정하고 있으며, 제75조에서는 "경외의 기구, 조직, 개인이 중화인민공화국의 핵심정보인프라를 공격, 침입, 방해, 파괴하는 등 위해를 가하는 활동에 종사하여 심각한 결과를 초래할 경우, 법에 따라 법률 책임을 추궁한다. 동시에 국무원 공안부문과 유관 부문은 해당기구, 조직, 개인에 대해서 재산 동결 또는 기타 필요한 제재 조치를 취할 수 있다"라고 규정되어 있다. 처벌을 위한 구성요건과 형벌이 매우 모호하기 때문에 앞서 살펴본 제58조와 함께 결합하게 되면 사실상 사이버공간의 보안뿐 아니라 사이버공간 자체를 합법적으로 통제할 수 있게 된다.

(3) 중국의 사이버보안 관련 최근 동향

중국은 한걸음 더 나아가 2019년 1월에 블록체인과 관련된 법률도 제정하였다.[896] 다만, 해당 법률은 블록체인을 촉진시키고 활성화 시키고자 하는 목적보다는 관리감독을 강화하는 것에 중점을 두고 있다. 따라서 블록체인 서비스제공자는 네트워크안전법에 따라 서비스를 제공해야 하며, 중국의 관련 법률을 위반하는 사용자에 대해서는 제재와 당국에 보고를 하도록 하고 있다.[897] 그 외에도 안전관리 책임을 부과하여 관련 정책을 마련하고, 기준에 부합하는 기술조치를 마련하며, 공개적인 관리규정 및 신규 제품 등에 대한 안전평가 의무를 부과하고 있다.[898] 그와 함께 블록체인 서비스제공자는 신고절차를 이행해야 하고, 관련 정보에 대해서는 6개월간 보존 및

896) 한국무역협회 베이징지부, 중국 블록체인 규정 해설, 2019.3, 1면, https://www.kita.net/cmmrcInfo/rsrchReprt/ovseaMrktReprt/FileDown.do?nIndex=1&nPostidx=39975&type=2 (2019년 11월 3일 최종접속).
897) 한국무역협회 베이징지부, 앞의 책, 3면.
898) 한국무역협회 베이징지부, 앞의 책, 4면.

조사기관에 제공해야 하며, 관련 부서의 정보제공에 따라 보유하는 정보를 제공해야 한다.[899] 그리고 의무를 어기거나 해당 서비스를 통해 국가안전을 위협하는 경우에는 처벌하는 규정도 두고 있다.[900] 이와 함께 '블록체인 정보서비스 신고관리 시스템'을 운영하여 실질적인 감시감독을 수행하고 있다.[901]

블록체인은 국가의 통제를 받지 않고 개인들 간의 거래를 위해서 고안된 제도임에도 중국은 관련 법률을 통해서 오히려 국가의 통제를 강화시키고 있다. 해당 법률이 현재는 중국 내 기업 및 중국인을 대상으로 하고 있기 때문에 해외 기업이나 외국인에게는 적용되지 않는 것과 같은 구조를 가지고 있지만, 구글의 사례를 볼 때, 사실상 해외 기업이나 외국인에게도 적용되는 법률이라고 할 수 있다.[902]

(4) 소결 및 시사점

중국의 경우 최근 관련 법령의 제정이 오히려 한국보다도 앞서고 있는 것으로 보인다. 물론 해당 법률의 정당성과 타당성에 있어서는 여전히 의문이 제기되고 있지만, 미국이나 유럽 등과 보조를 맞춰서 사이버보안과 관련된 법률생태계를 조성하는 속도는 상당히 빠르다고 할 수 있다. 이는 사이버공간에서도 중국의 영향력을 강화시키기 위한 '중국굴기'의 일환으로 볼 수 있다. 앞서 살펴본 미국이나 EU의 경우를 보더라도 자국이나 지역연합을 위해 만들어진 규정이 다른 나라에도 영향을 미치고 있으며, 강력한 사이버공간의 보호 장치로의 역할을 하고 있기 때문이다. 사이버공간의 중요성을 인식하고 있는 중국은 이미 UN차원에서 논의되고 있는 사이버공간에서의 국제적인 규범에 대한 논의에 대규모 인력을 파견하기도 하고, 중국의 알리바바와 같은 기업들이 옵서버로 참여하기도 한다. 그러므로 중국은 국제사회의 사이버공간에 대한 규범에 영향력을 미치면서도 자국에서 발 빠르게 관련 규정을 만들어 사이버공간에서의 국제사회의 리더라는 인상을 주고 있다고도 판단된다.

다만, 앞서 법률규정에도 확인되고 있는 것과 같이 중국의 사이버보안 관련 규정들이 관련 내용들을 모두 규정하고 있기 때문에 명확한 것처럼 보이지만, 사실상 중국정

899) 한국무역협회 베이징지부, 앞의 책, 4면.
900) 한국무역협회 베이징지부, 앞의 책, 5면.
901) 블록체인 신고 홈페이지, https://bcbeian.ifcert.cn/index (2019년 11월 3일 최종접속).
902) 한국무역협회 베이징지부, 앞의 책, 6면.

부의 정책이 법률에 우선해서 적용될 수 있도록 하는 모호한 규정들이 상당히 포함되어 있다. 또한 블록체인 관련 법률에서 보는 것과 같이 중국에서는 앞으로도 새로운 정보화 사회의 현상들에 부응해서 선제적인 법률들을 마련할 것으로 예견된다. 그러므로 미국, 유럽 등과 함께 중국의 사이버보안 관련 법률의 동향도 계속해서 주의 깊게 살펴볼 필요가 있다.

다. 개선 방안

이제까지 미국, EU, 중국, 일본, UN 등 사이버보안과 관련해서 한국이 참조할 필요성이 있는 국가들의 사이버보안 법제들에 대해서 살펴보았다. 앞서도 언급하였지만 사이버보안 규정은 단순히 국가의 사이버안보 확보를 위해 존재하는 것이 아니라 자국의 사이버 관련 콘텐츠 및 서비스, 기술 등을 보호하려는 목적도 함께 포함되어 있다. 실제로 중국은 사이버보안을 이유로 관련 규정을 내세워 중국에서 서비스를 제공하고 있는 한국의 네이버나 다음,[903] 미국의 구글[904] 등의 서비스를 제한하고 있다. 그 결과 바이두나 소후와 같은 자국 기업이 단기간에 괄목할 만한 성장을 하게 되었다. 유럽연합의 경우도 앞서 살펴본 바와 같이 사이버보안 규정이 유럽연합의 사이버 관련 산업의 장벽이 되어 주고 있다. 그러나 사이버보안 규정의 본래 목적은 사이버공간의 안전이므로 산업적인 측면을 배제하고 볼 때, 대체로 다음과 같은 공통점들이 나타나고 있다.

첫째로, 컨트롤타워의 설치 및 강화이다. 사이버보안 문제는 순간적으로 대량의 피해를 유발할 수 있으며, 그 복구에는 수많은 시간과 비용 등이 발생한다. 따라서 예방과 대응, 복구 등에 있어 절차를 최소화 하고, 효율적으로 운영할 필요가 있다. 그것을 위해 필요한 것이 컨트롤타워이다. 미국의 CISA, EU의 ENISA, 일본의 시큐리티 전략본부와 같이 실질적으로 의사결정을 하고, 정책을 수행할 수 있는 컨트롤타워는 사이버보안을 위한 필수요건이라고 할 것이다. 따라서 앞서 살펴본 국가들의 경우 법률에서 명확하게 해당 조직에 대한 권한을 부여하고, 업무를 규정하여 실질적인

903) "중국, 다음 이어 네이버 차단…'한국 포털' 통제 왜?", 서울신문 2019년 6월 11일자, https://www.seoul.co.kr/news/newsView.php?id=20190611500200 (2019년 11월 3일 최종접속).

904) "구글, 중국에 머리 숙인다…검열하는 검색 엔진 출시 검토", 중앙일보 2018년 8월 2일자, https://news.joins.com/article/22854486 (2019년 11월 3일 최종접속).

사이버보안 컨트롤타워의 역할을 수행할 수 있도록 하고 있다. 그에 비해 한국은 여전히 컨트롤타워의 문제가 지적되고 있다. 컨트롤타워의 핵심은 컨트롤타워가 부처 등을 아우르는 보안관련 의사결정권한과 수행권한 등을 갖는 것이다. 사이버보안 컨트롤타워는 형식적으로 운영되어서는 안 된다. 따라서 한국의 사이버보안 컨트롤타워가 실질화 되도록 법제와 실무가 함께 움직여야 할 것이다.

둘째로, 신속한 근거법률의 제정이다. 한국도 정보통신망법을 비롯해서 사이버보안과 관련된 법률들은 이미 마련되어 있다. 그러나 유럽의 5G 통신관련 보안법률, 중국의 블록체인 관련 법률 등과 같이 최근 사회적으로 보안이 이슈화 되고 있는 새로운 기술들과 관련된 법률에 대한 논의가 상대적으로 지지부진하다. 물론 새로운 기술에 대응하는 사이버보안 관련 법률이 선제적으로 제정되기는 쉽지 않다. 그러나 새로운 기술이 상용화되고 확산되는 경우에는 그에 맞추어 법적인 장치를 마련할 필요성이 크다. 따라서 이미 상용화가 되었거나 대중화가 되고 있지만 여전히 입법이 미비한 사이버보안 관련 사안에 대해서는 신속하게 근거법률을 마련해 줄 필요가 있다.

셋째로, 사이버보안 인력 및 기술력강화이다. 사이버보안은 사실상 보안기술과 전문인력이 8할이라고 할 수 있다. 그러므로 앞서 살펴본 국가들이 중점을 두고 있는 것이 바로 사이버보안 인력의 양성, 충원, 유지 및 사이버보안 기술력 개발이다. 사이버보안에 있어 한국의 사이버보안인력의 우수성은 이미 세계적으로도 입증되었다. 그러나 사이버보안인력의 층이 너무 얇고, 기술수단은 주로 해외 툴을 이용하고 있다. 이전에도 이미 오랫동안 경고를 하였지만 일본과의 경제전쟁을 통해서 비로소 국산소재개발이 발등의 불이 된 것처럼 사이버보안에 있어서도 그와 같은 일이 발생할 수 있을 개연성이 매우 크다. 더욱이 국내의 우수한 사이버보안인력조차도 그 처우나 사회적 대응 등으로 인해 해외로 유출되고 있는 상황이다. 그러므로 하루 빨리 국내의 사이버보안인력을 양성하고, 유지하며, 기술력을 지속적으로 강화시킬 수 있는 통합적인 제도가 마련되어야 하며, 그를 위한 법률 제정도 필요하다. 그를 위해 국회의 노력이 필요하게 되므로, 국회에서도 사이버보안에 좀 더 많은 관심을 기울이고, 입법에 집중할 필요가 있다.

우선 사이버보안 관련 법제 정비 및 개인정보 보호강화가 시급하다. 사물인터넷으로 인해서 많은 사물들이 사이버공간으로 연결되게 되었다. 문제는 사이버보안이 새

로운 환경에 적절하게 적응해야 하는 것이다. 스마트 냉장고를 해킹해서 대량의 스팸을 발송한 사건이 있었는바[905] 사이버보안이 취약한 스마트 기기를 이용한 사이버공격의 방법이다. 그런 것이 가능한 이유는 사물인터넷에 적합한 사이버보안체계가 적절하지 않았기 때문이다. 따라서 유럽은 사이버보안 인증제도를 강화해서 유럽지역의 사이버보안을 강화하고 있다. 물론 한국도 "국가정보화기본법"에 따라 행정규칙으로 "정보보호시스템 평가인증 지침"이 마련되어 있기는 하다. 하지만 해당 지침을 보면 평가대상이 '정보보호시스템' 및 '보호프로파일'로 한정되어 있다(제1장). 그 외에도 정보통신망법, 개인정보 보호법 등의 법령에 따라 다양한 고시들이 있기는 하지만 사물인터넷 등 새로운 스마트 환경을 목적으로 하고 있다고 보기는 어렵다.

사이버보안의 3요소로는 인가된 사용자만 접속할 수 있는 기밀성(confidentiality), 권한을 가진 사용자만이 인가된 방법으로 데이터를 변경할 수 있는 무결성(integrity), 원하는 정보에 원하는 때에 접근할 수 있는 가용성(Availability) 등이 있다. 이 요소 가운데 한 가지라도 깨어지면 보안이 침해되는 것이다. 이런 기본요소는 사이버보안의 전략적 요소이다. 그러므로 변경되지 않는 요소이다. 하지만 사이버보안을 구체적으로 어떻게 구축할 지에 문제는 전술적 요소라고 할 수 있다. 사물인터넷, A.I., 암호화폐 등 새로운 기술들에 대한 사이버보안 전략은 변함이 없다. 그러나 그 전술에 있어서는 변화가 필요하게 된다. 따라서 해외 주요 국가들은 사이버보안법을 통해서 전술을 변경하고 있는 것이다. 한국도 지금의 법령과 지침 등을 통해서 사이버보안의 전술에 변화를 주어야 한다.

또한 법률을 통해 사이버보안의 주무기관을 명확히 해야 할 필요가 있다. 해외 주요 국가들도 이미 법률을 통해서 구현하였다. 한국 정보통신망법의 주무기관은 과기정통부와 방송통신위원회이다. 한 법에 대해 두 기관이 관여하는 것이다. 그래서 한국인터넷진흥원은 과기정통부와 방송통신위원회의 지시를 받게 된다. 법률과 조직이 이렇게 여러 곳에 연관되어 있는 경우는 매우 많다. 이런 복잡한 체계에서는 책임소재가 모호하며, 지시의 충돌도 발생할 수 있다. 교통정리가 필요하다. 따라서 한국은 사이버보안을 전담할 수 있는 전권을 가진 기관과 그 근거가 되는 법률이 필요하다.

---

905) "냉장고 해킹해 스팸 발송…스마트가전 보안 비상", KBS 2014년 1월 18일자, http://news.kbs.co.kr/news/view.do?ncd=2792178 (2019년 11월 3일 최종접속).

2. 형사정책적 활용 및 기타 고려 사항

가. 형사정책적 활용 방안

1) 형사정책적 활용 가능 기술 및 분야 도출

(1) 형사정책적 활용 가능 기술

전술한 바와 같이 블록체인은 익명의 노드로만 구성된 네트워크에서 신뢰를 생성할 수 있지만 그에 대한 비용이자 대가로 일을 중복하도록 만든 비효율적인 방식이다. 블록체인은 절대 익명의 금융거래에 적합한 속성을 가지고 있고, 이에 비트코인 등으로 구현되어 범죄의 수단이나 돈 세탁 등에 이용되고 있다. 최근 IBM이 주도가 된 하이퍼 레저 패브릭(Fabric)과 같이 변형된 블록체인들이 주목을 받고 있으나 대부분 실명인증에 기반한 중앙화 시스템으로 구성된 경우가 많기 때문에 이는 진정한 의미에서의 '블록체인'이 아니라 '디지털화'일 뿐이라는 비판도 제기되고 있다. 즉 암호화폐 등의 기망행위를 배제하고, 기술로서의 블록체인을 부각하기 위해 하이퍼 레저 등이 등장하였지만, 엄밀한 의미에서 이는 블록체인의 정의에 부합하지 않고 아직은 그 효용성도 미지수라는 것이다. 그럼에도 불구하고 블록체인은 기록의 비가역성을 추구하고 있는바, 형사사법 분야의 각종 기록 생성 및 보관의 염결성을 담보하기 위해 이 기술을 활용할 수 있는 방안을 모색해볼 수 있다. 그러나 블록체인은 항상 같은 일을 수많은 노드가 반복하므로 중앙화 시스템에 비해 막대한 비용이 소모된다. 익명성이 담보되지 않아도 되는 네트워크에서는 엄청난 비용을 지불하면서 일을 중복처리할 필요가 없는바, 형사사법 분야에서 블록체인을 활용해야만 하는 분야를 도출해 내기란 쉬운 일이 아니다.

반면 사물인터넷의 경우 현실 세계의 다양한 정보를 수집하여 이를 전달 및 공유함으로써 형사사법 분야의 다양한 업무를 보다 스마트하게 수행할 수 있다. 다만 네트워크에 연결된 디바이스가 많아지면서 사이버 공격에 대한 취약성이 커지게 되었고, 그로 인해 대규모 피해가 발생할 수 있다는 점은 해당 기술 활용 시에 반드시 고려되어야 할 사항이다. 또한 데이터 생산이 방대해지고, 여러 데이터가 결합된 복합데이터가 생성되면서 정보 침해로 인한 피해가 더 커졌지만 정작 책임소재는 보다 불분명해질

수 있다는 문제도 간과되어서는 안 된다. 이러한 위협 요소를 감소시키기 위한 보안 강화 등을 전제하면서 사물인터넷 기술의 활용 방안이 모색되어야 할 것이다.

(2) 형사정책적 활용 분야

현재 사물인터넷은 이미 다양한 분야에서 활용되고 있다. 주로 범죄예방의 최적화를 도모하기 위해 도입되어 있지만, 해당 시스템은 범죄수사의 효율성 제고의 측면에서도 상당한 기여를 하고 있다. 이에 한걸음 더 나아가 사물인터넷 기반 모니터링은 구금의 대안이 될 수 있다.[906] 2019년 3월 6일, 불법 비자금 조성과 횡령 및 뇌물수수 등의 혐의로 1심에서 징역 15년에 벌금 130억 원과 추징금 82억 원 등을 선고받았던 전직 대통령이 보석으로 석방되었다.[907] 당시 재판부는 주거지를 자택으로 제한하고, 접견 및 통신의 대상도 일정 범위 내의 사람으로 한정했으며, 매주 시간활용내역을 보고한다는 조건 등을 부과하며 보석을 허가했다.[908] 사실상 가택구금과도 같은 이례적인 보석조건이 주목을 받았으나 조건 준수의 실효성에 대해서는 의문이 제기되기도 했다.[909] 사물인터넷은 재택구금이나 기타 지역사회 내 보호관찰 등의 영역에서 유용하게 사용될 수 있다. 특히 사물인터넷은 센서를 통해 건물 내부 상황에 대한 정보를 제공하는 방식으로 모니터링을 할 수 있고, 법집행을 수행하는 경찰이나 보호관찰관의 안전을 증진시킬 수 있다는 측면에서 유용하다.[910]

---

906) Berg Insight사가 발표한 보고서에 의하면 범죄자들의 전자감독(electronic monitoring)에 있어 구형인 RFID 시스템을 IoT 기반의 GPS 기술이 대체하고 있다. 미국이나 영국의 경우 교정시설의 과밀화가 심각한 상황이며 따라서 구금의 대체형으로 전자감독을 이용한다면 수감시설보다 비용적으로도 저렴하고 범죄자의 책임성도 강화시키며 재범률도 낮추어 공공안전을 강화시킬 수 있다고 한다. 전자감독의 경우 성범죄자 뿐만 아니라 재판 전 적용이나 가석방에 대한 추가 명령으로 사용이 증가될 것이라고 하고 있다. "IoT-based monitoring increasingly offers alternative to prison, says report", Internet of Business News 2017.5.23., https://internetofbusiness.com/tagging-offenders-increasingly-iot-issue-says-report/ (2019년 10월 23일 최종접속).

907) "이명박 보석 청구 조건부 허가…"구속 만기 전 선고 불가"", 국민일보 2019년 3월 6일자, http://news.kmib.co.kr/article/view.asp?arcid=0013119737&code=61121111&cp=nv (2019년 10월 23일 최종접속).

908) "이명박 전 대통령, 구속 349일 만에 보석 허가…'조건부 석방'", 매일경제 2019년 3월 6일자, https://www.mk.co.kr/news/politics/view/2019/03/134959/ (2019년 10월 23일 최종접속).

909) ""대포폰 사용 등 완전차단 불가능" 자택구금 조건 실효성 벌써 논란", 서울경제 2019년 3월 6일자, https://www.sedaily.com/NewsView/1VGHGFY0YU (2019년 10월 23일 최종접속); "MB 보석 석방 이틀째…'자택 구금' 실효성 있을까?", YTN 2019년 3월 7일자, https://www.ytn.co.kr/_ln/0103_201903071209011682 (2019년 10월 23일 최종접속).

910) John S. Hollywood/Dulani Woods/Richard Silberglitt/Brian A. Jackson, Using Future

한편 이미 우리나라에는 전자감독제도가 도입되어 있다. 2008년 도입 당시에는 전자발찌 부착자가 별도의 GPS수신기를 휴대해야 했는데, GPS가 내장된 위치추적장치가 전자발찌에서 발신되는 전자파를 감지하여 이동통신망을 통해 데이터를 재택감독장치로 전송하였다. 이로 인해 GPS수신기 유기로 인한 위치추적의 공백 문제가 발생했다. 기술의 발전은 종래의 문제를 해결할 수 있도록 해주었는바, 전자감독제도가 도입된 지 10주년이 되었던 지난 2018년, 발목에 착용하는 부착장치에 GPS기능이 탑재된 일체형 전자발찌가 개발되었다.[911]

우리보다 앞서 동 제도를 도입한 미국에서는 사물인터넷 기술이 사회내 처우를 확대할 수 있는 동력이 될 것이라는 전망이 나오고 있다. 수백 만 명에 이르는 보호관찰 대상자 및 가석방자에 대해서 사람의 개입이 거의 없거나 전혀 없는 경우라도 사물인터넷을 이용하여 실시간 위치 추적 및 모니터링이 이루어질 수 있는 것이다.[912] 한편 독일의 경우 2000년 5월 헤센주를 시작으로 보호관찰 대상자에게 무선주파수를 이용한 대상 식별(Radio Frequency IDentification, RFID) 방식의 전자감독이 시행되었고,[913] 2012년부터는 자유제한적 보안처분 부과 시에 그 준수사항으로서 GPS를 이용한 전자감독을 시행하고 있다.[914] 향후 사물인터넷을 적극적으로 활용할 경우

Internet Technologies to Strengthen Criminal Justice, Research Reports RR-928-NIJ, RAND Corporation, 2015, pp.15-16.

911) 법무부 보도자료, "전자감독제도 10년! 재범 억제 능력을 입증하고, 수용시설 과밀화 대안으로 주목받다", 2018.9.5., http://www.moj.go.kr/moj/221/subview.do?enc=Zm5jdDF8QEB8JTJGYmJzJTJGbW9qJTJGMTgyJTJGNDIxNDM1JTJGYXJ0Y2xWaWV3LmRvJTNGcGFzc3dvcmQlM0QlMjZyZ3NCZ25kZVN0ciUzRCUyNmJic0NsU2VxJTNEJTI2cmdzRW5kZGVTdHIlM0QlMjZpc1ZpZXdNaW5lJTNEZmFsc2UlMjZwYWdlJTNEMSUyNmJic09wZW5XcmRTZXElM0QlMjZzcmNoQ29sdW1uJTNEc2olMjZzcmNoV3JkJTNEJUVDJUEwJTg0JUVDJTlFJTkwJUVBJUIwJTkwJUVCJThGJTg1JTI2 (2019년 10월 23일 최종접속).

912) IJIS Institute, Correction Tech 2020. Technological Trends in Custodial & Community Corrections, 2017.3., p.12, https://www.justnet.org/pdf/Corrections_Tech_2020_FINAL_20170331.pdf (2019년 10월 23일 최종접속).

913) Günes Önel, Verfassungsmäßigkeit und Effektivität der „elektronischen Fußfessel", Jahrbuch des Kriminalwissenschaftlichen Instituts der Leibniz Universität Hannover Band 1, Leibniz Universität Hannover, 2012, S.14-22; Markus Mayer, Modellprojekt elektronische Fußfessel: Studien zur Erbrobung einer umstrittenen Maßnahme, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2004, S.1ff.

914) "68 Straftäter an der elektronischen Fußfessel", Hessisches Ministerium der Justiz 2014.2.26., https://www.hessen.de/pressearchiv/pressemitteilung/68-straftaeter-der-elektronischen-fussfessel (2019년 10월 23일 최종접속). 이는 시설 수용을 대체하는 것이 아니며, 성폭력범죄자나 고위험 폭력범죄자 중 재범위험성이 존재하는 경우에 부과된다. 김혜정, 전자감독제도의 장기 발전전략 수립을 위한 부착명령 대상범죄 및 부착기간 등의 적정성에 관한 연구, 법무부

가택구금 등 사회내 처우의 효율성을 제고시킬 수 있고, 이는 다시 시설내구금의 감소라는 선순환 구조를 만들어 낼 수 있을 것이다.

시계나 안경과 같은 웨어러블 기술의 발전은 형사사법 분야의 법집행 담당 인력을 지원하는 역할도 수행할 수 있다.[915] 앞서 살펴본 바와 같이 이미 중국이나 두바이에서는 안면인식 소프트웨어가 탑재된 스마트안경이 용의자 확인 등에 활용되고 있다. 물론 이들 국가에 비해 개별 국민의 프라이버시 보호라는 가치에 무게를 두고 있는 미국에서는 정작 자국에서 스마트안경이 개발되었음에도 불구하고 이를 활용하지 못하고 있다. 두 손을 자유롭게 쓰면서 각종 정보에 접근하거나 기록할 수 있다는 점에서 큰 매력을 가지는 스마트안경의 경우 현행범 추적 등 긴박한 상황에서 유용할 수 있다.

사물인터넷의 속성은 동일하더라도 해당 기술을 형사사법 분야에서 구현하는 형태는 다양할 것이다. 2019년 10월 22일 경찰청과 과학기술정보통신부는 과학치안 아이디어 공모전 시상식을 개최했는데, 사물인터넷 기반의 아이디어들도 일부 포함되어 있었다.[916] 대표적인 것이 '사물인터넷 연결 CCTV(IoT Connected CCTV: Angel Eyes)'였는데, 이는 사물인터넷 센서를 이용해서 사고를 당한 사람의 스마트폰과 주변에 있는 CCTV 및 블랙박스 등이 실시간 위치정보를 공유하도록 함으로써 사고의 증거가 될 영상자료와 목격자를 확보할 수 있게 만든다.[917] 그 이외에도 '세이프존 위치정보공유 지도앱'[918]과 '스마트가로등을 활용한 광역 안전시스템'[919] 등도 사물인터넷을 이용한 아이디어였다.[920]

정책연구보고서, 2015, 78면.

915) IJIS Institute, Ibid., p.21.

916) 과학기술정보통신부 보도자료, "제5회 과학치안 아이디어 공모전 시상식 개최", 2019.10.22., https://www.msit.go.kr/SYNAP/skin/doc.html?fn=9b9e71030ab0787a39b2b79983724a28&rs=/SYNAP/sn3hcv/result/201911/ (2019년 10월 23일 최종접속).

917) 과학기술정보통신부, 앞의 보도자료("제5회 과학치안 아이디어 공모전 시상식 개최") 참조.

918) 모든 세이프존(여성안심 귀갓길, 안심 골목길, 안심 부스, 가로등 비상벨, 범죄예방 환경설계를 적용한 거리 등)의 위치를 모아둔 지도 앱을 개발하여 거주지 주변 세이프존의 위치 파악이 용이하고 위급 상황 시 SMART 신고 기능으로 112 신고센터 및 1km 이내의 상점과 해당 지역 주민들에게 문자가 발송되어 신속한 신고가 이루어지도록 하는 등 범죄예방 효과를 제고할 수 있다.

919) 스마트 가로등(가로등에 열상감시기가 부착되어 야간 보행자 판별 및 보행자 무단횡단 판별 시 색 변경을 통해 접근 차량의 운전자에게 경고하고, CCTV 설치를 통한 영상인식으로 보행자가 교통약자로 판별되는 경우 보행신호를 조절할 수 있음)을 이용하여 야간에 운전자에게 보행자에 대한 정보를 전달하고, 파출소 관할 구역마다 드론을 할당하여 운영함으로써 치안 안전시스템을 구축하여 보행자의 안전을 강화하고 범죄를 예방할 수 있다.

920) 과학기술정보통신부, 앞의 보도자료("제5회 과학치안 아이디어 공모전 시상식 개최") 참조.

2) 도입된 제도의 활성화

현재 경찰은 웨어러블 폴리스캠이나 드론 등을 도입하였으나 네트워크에 연결되지 않은 형태로 장치를 운용하고 있다. 2015년 10월부터 시범 운영되고 있는 폴리스캠의 경우 2019년 초에 발생한 버닝썬 클럽 사건[921]이나 암사동 흉기난동 사건[922] 등을 계기로 하여 그 필요성을 주장하는 목소리가 커지고 있으나, 정작 폴리스캠의 활용 건수는 급격히 감소하고 있는 것으로 알려졌다.[923] 2019년 9월 2일 경찰청 발표에 따르면 폴리스캠 활용 건수는 2017년 2만 2,046건이던 것이 2018년에는 1만 729건으로 감소하였고, 2019년의 경우 5월 기준으로 1,786건에 불과한 것으로 집계되었다고 한다.[924] 폴리스캠이 외면 받는 주된 이유로는 화질이나 배터리 용량 등 성능이 떨어지고 장착이 불편하다는 점이 거론된다. 특히 녹화된 영상이 실시간으로 전송되지 않기 때문에 현장경찰이 출동업무를 종료한 후에 사무실에 복귀해서 일일이 수동으로 녹화된 현장영상을 전송 및 등록해야 하는 번거로움이 크다고 한다.[925] 이에 네트워크로 연결되어 자동으로 전송되는 시스템이 구축될 필요가 있는데, 공권력 남용의 방지나 사건 현장의 증거 확보라는 장치 도입의 주된 취지가 구현되기 위해서는[926] 변경이

---

921) 2018년 11월 24일 서울 강남에 있는 클럽 버닝썬에서 손님 김씨가 폭행을 당했지만 경찰은 오히려 김씨를 가해자로 체포하고 폭행까지 하였다. 김씨는 경찰이 클럽 측을 옹호하였다고 폭로하고, 이를 계기로 클럽 버닝썬과 관련된 여러 의혹에 대해 언론 등에 제보가 이뤄지면서 사회적 파장을 불러일으켰다. 사건 당시 경찰의 과잉진압논란이 있었던바 경찰은 바디캠으로 현장을 촬영한 영상을 공개하였다.

922) 2019년 1월 13일 오후 7시경 암사역 3번 출구 부근에서 친구인 두 사람이 다툼을 벌이다 흉기인 커터칼을 꺼내 휘둘렀고 피해자가 허벅지를 찔려 쓰려진 후에도 계속된 난동에 출동한 경찰이 대치를 벌이다 테이저건을 발사했지만 제대로 맞지 않고 가해자는 흉기를 든 채 도주하였는바, 이 당시 경찰의 모습이 담긴 영상이 유튜브 공개되었는데 커터칼을 든 피의자를 상대로 머뭇거리며 대응하는 모습에 비난 여론이 있었지만 경찰이 몸에 부착한 개인 촬영장비를 통해 긴박한 검거 장면이 공개되면서 여론은 바뀌게 되었다.

923) 최미경/최정민, "경찰청 웨어러블 폴리스 캠의 운영 실태 및 개선과제", 이슈와 논점 제1590호, 국회입법조사처, 2019.6.13., http://nars.go.kr/brdView.do?brd_Seq=25291&currtPg=1&cmsCd=CM0018&category=a4&src=&srcTemp=&pageSize=10 (2019년 10월 23일 최종접속).

924) "필요해서 사놓고… 지구대 캐비닛서 잠자는 '폴리스 캠'", 서울신문 2019년 9월 3일자, https://www.seoul.co.kr/news/newsView.php?id=20190903012015&wlog_tag3=naver#csidxcc3da0e98fa019a88db90634b9955d6 (2019년 10월 23일 최종접속).

925) "경찰 97% 찬성한 '폴리스캠'… 1주일간 영상등록 2건뿐", 동아일보 2015년 11월 9일자, http://www.donga.com/news/article/all/20151109/74665899/1 (2019년 10월 23일 최종접속).

926) 미국에서는 2014년 8월 9일에 미주리 주 퍼거슨에서 비무장 상태의 18세 아프리카계 미국인 남성 마이클 브라운(Michael Brown)이 길을 걷던 중 그를 편의점 강도 용의자로 오인한 경찰로부터 총격을 당해 사망한 사건이 발생하였다. 사건 직후 경찰은 거친 몸싸움 도중 총격이 있었다고 설명했으나 이는 두 손을 머리 위로 올리고 항복한 브라운을 경찰이 저격했다는 목

불가능한 클라우드 데이터베이스로 영상 자료가 전송되어야 한다.

한편 폴리스캠의 이용 활성화를 위해서는 관련 법률을 정비할 필요가 있다. 경찰청은 경찰관의 공권력 남용 등을 방지하는 한편 경찰에 대해 가해지는 공무집행 방해 등을 막기 위해서 웨어러블 폴리스 캠을 시범·운영하였고, 그 사용 절차는 운영 등에 관한 필요한 사항을 규정하기 위해 경찰청 내부훈령인 「웨어러블 폴리스캠 시스템 운영 규칙」을 제정하여 폴리스캠의 사용 절차 및 운영 등에 필요한 사항을 규정하였다.[927] 그러나 폴리스캠의 경우 근접 촬영으로 인한 사생활 침해나 촬영된 영상의 외부 유출 등이 문제되고 있는바, 그 우려를 해소할 수 있도록 운영에 대한 근거 법률이 마련되어야 한다. 이에 2017년 12월 22일 「개인 영상정보의 보호에 관한 법률안」이 정부 발의로 제출되었으나[928] 동 법안은 소관위원회의 검토를 거친 후 아직 국회에 계류 중이다. 요컨대 사물인터넷 디바이스 및 시스템의 형사사법적 활용을 활성화시키기 위해서는 형사정책적 기능과 그 사용절차 및 사이버보안 기술에 대한 검토가 이루어져야 하고, 동 기술 적용으로 인한 인권침해를 방지하기 위한 연구도 지속적으로 진행되어야 한다.[929]

격자들의 진술과 배치되었다. 이 사건을 계기로 대규모 시위가 발생했고, 경찰의 카메라 착용을 의무화하는 이른바, '마이클 브라운법(Michael Brown Law)' 제정을 요구하는 백악관 탄원서에 14만 8,000여명이 서명하였다. "Petition for 'Michael Brown law' passes threshold for consideration", The Washington Times 2014.8.27., https://www.washingtontimes.com/news/2014/aug/27/petition-michael-brown-law-passes-threshold-consid/ (2019년 10월 23일 최종접속).

927) 경찰청 훈령 제778호, 웨어러블 폴리스캠 시스템 운영 규칙, https://www.police.go.kr/portal/bbs/list.do?menuNo=200629&bbsId=B0000032 (2019년 10월 23일 최종접속).

928) 「개인 영상정보의 보호에 관한 법률안」의 제안이유는 「영상정보 처리 기술이 고도화됨에 따라 영상정보처리기기의 설치·운영이 크게 증가하면서 개인영상정보의 오용·남용 및 사생활 침해 등에 대한 우려도 증가하고 있는바, 영상정보처리기기를 고정형 영상촬영기기 및 이동형 영상촬영기기 등으로 구분하여 해당 기기를 설치하거나 개인영상정보를 촬영할 수 있는 구체적 근거를 마련하고, 개인영상정보의 안전한 관리, 영상정보주체의 열람·삭제 요구 등 개인영상정보의 안전한 처리 및 보호에 관한 사항을 규정함으로써 국민의 개인영상정보에 대한 권리와 이익을 보장하려는 것」이다. 의안번호 10980. 국회 의안정보시스템 웹페이지, http://likms.assembly.go.kr/bill/billDetail.do?billId=ARC_K1B7H1B2X2V2C1G6A0B4D3W1Q9P8D2 (2019년 10월 23일 최종접속).

929) John S. Hollywood/Dulani Woods/Richard Silberglitt/Brian A. Jackson, Ibid., p.26.

나. 기타 고려 사항

1) 정보보호영향평가

미국이나 유럽의 사이버보안법에는 정보보호영향평가에 대한 규정이 마련되어 있는데, 사물인터넷에 대해서도 정보보호영향평가가 이루어질 필요가 있다. 한국에서도 개인정보보호법의 발효에 따라 개인정보영향평가가 행해지고 있다. 즉, 개인정보를 취급하는 신규 시스템을 구축하거나 기존 시스템을 변경하는 경우 개인정보영향평가를 받게 된다(개인정보 보호법 제33조). 그 평가 대상은 동법 시행령에 규정되어 있는데, "1. 구축·운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일, 2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일, 3. 구축·운용 또는 변경하려는 개인정보파일로서 100만 명 이상의 정보주체에 관한 개인정보파일, 4. 법 제33조 제1항에 따른 개인정보 영향평가(이하 "영향평가"라 함)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일로서 이때 영향평가 대상은 변경된 부분으로 한정한다."라고 명시되어 있다(동 시행령 제35조). 이는 유럽의 사이버보안법에서 개인정보침해 여부를 판단하는 시스템에 비하면 그 범위가 너무 넓다. 유럽은 마치 기업의 준법감시인과 같이 사이버보안으로 인해 프라이버시가 침해되는지 여부를 수시로 판단할 수 있도록 하고 있다. 프라이버시 담당관이 지속적으로 사이버보안으로 인한 프라이버시 침해 여부를 모니터링 하게 되는 것이다. 그에 비하면 한국의 개인정보영향평가 제도는 다분히 형식적인 측면이 있다. 인공지능 등 새로운 기술의 등장과 네트워크의 확장으로 인하여 개인정보가 사용될 가능성은 보다 높아졌는바, 개인정보영향평가에 대한 모니터링이 상시적으로 이루어질 필요가 있다. 또한 개별 기술의 특징이 제대로 반영된 영향평가가 이루어질 수 있도록 그 평가요소를 보다 구체적으로 설정하는 방안도 논의될 수 있을 것이다.

2) 수사 및 재판의 효율성·전문성 제고

수사기관은 법원에게 사이버보안과 관련된 기술적인 문제를 설명하여 법원을 설득시켜야 하는데 그것이 쉽지 않다. 이에 교육이 필요한데 독일의 연방형사청(BKA)이 실시하는 사이버범죄 수사 전문가 교육은 컴퓨터 관련 전공 이수자 또는 물리학, 수학 등 기술·과학 관련 학위를 받은 자 중 선발을 거쳐 향후 20개월[930] 동안 기본 경찰 교육 및 사이버범죄 관련 전문 교육을 이수한 후 현장에 투입되도록 한다.[931] 또한 교육 내용은 해킹공격 대응, 인터넷 및 컴퓨터 응용 사기범죄 대응, 디지털 증거 포렌식 방법, 조직범죄 및 테러 대응 수사, 정보의 수집 및 분석 등이다.[932] 우리나라도 사이버범죄 전문수사관, 디지털포렌식 전문수사관, 사이버수사 지휘관, 사이버특채경찰관 등을 대상으로 여러 교육 기관별로 사이버범죄 이론 및 실무교육을 실시하고 있다.[933] 그러나 우리나라의 사이버범죄 수사 교육은 주로 실무적인 내용에 치우쳐 있어서 이론적이고 체계적인 분석이 부족한 상황이다.[934] 나아가 사이버수사관 특채 경찰관의 경우에는 중앙경찰학교를 졸업한 후 곧바로 일선에 투입되고 있는데, 이는 범죄수사나 디지털 포렌식 전문 지식을 획득하기에는 턱없이 부족한 교육시간 및

930) 연방정부는 "사이버범죄수사관"이 되기 위한 교육기간을 20개월로 단축하기로 결정하였다. 사이버범죄수사관과 동일한 직무 단계에 이르기 위해 기존에는 일반적으로 36개월 정도가 걸려야 했던 반면, 교육기관을 단축함으로써, 유능한 인력이 BKA에 지원하도록 하는 한편, 전문교육을 통해 사이버범죄 대응 능력을 높이고자 한 것이다. "'Cyberkriminalisten': Kabinett beschließt verkürzte Polizei-Ausbildunghttps", heise online 2019.10.3., https://www.heise.de/newsticker/meldung/Cyberkriminalisten-Kabinett-beschliesst-verkuerzte-Polizei-Ausbildung-4545165.html (2019년 10월 23일 최종접속).

931) BKA 웹페이지, https://www.bka.de/DE/KarriereBeruf/EinstiegBeimBKA/Berufserfahrene/Cyberkriminalist/cyberkriminalist_node.html (2019년 10월 23일 최종접속).

932) BKA 웹페이지, https://www.bka.de/DE/KarriereBeruf/EinstiegBeimBKA/Berufserfahrene/Cyberkriminalist/cyberkriminalist_node.html (2019년 10월 23일 최종접속).

933) 우선, 경찰대학은 사이버법, 사이버범죄수사론, 경정·경감기본교육과정 및 치안정책과정 등 사이버범죄 특성, 디지털 포렌식 관련 교육을 실시하고 있다. 다음으로 경찰수사연수원은 사이버범죄수사과정, 사이버테러수사과정, 디지털포렌식 전문 및 고급과정, 해킹범죄수사과정, 수사지휘과정, 추적수사전문과정, 등 실무 교육을 하고 있다. 경찰 교육센터는 사이버수사 네트워크 과정을 개설하고 있으며, 경찰 사이버 교육포털에서는 전 경찰관의 직무 능력 향상을 위한 온라인 강의가 제공되고 있다. 또한 수강의 용이함을 위해 사이버교육 포탈서비스 앱을 설치하여 모바일 기기에서 활용할 수 있도록 하였다. 이와 별도로 사이버수사관의 IT 전문지식의 제고를 위해 매년 민간전문 교육기관에 해킹, 악성코드, 데이터복구, 운영체제 등 첨단기술 분야를 위탁교육을 시행하고 있으며, 고려대 정보보호대학원, 연세대 정보대학원에 디지털 포렌식 맞춤형 석사과정을 개설하여 위탁교육을 진행하고 있다. 자세한 내용은 박노섭, 경찰청 사이버범죄 대응능력 향상을 위한 교육훈련 체계 개발, 경찰청, 2015.12., 143-162면; 경찰청, 2018 경찰백서, 2018, 224면 참조.

934) 박노섭, 앞의 보고서, 186면.

프로그램이라고 파악되므로 이에 대한 보완이 필요하다.[935] 또한 경찰청은 해킹, 악성코드, 암호 등 첨단기술 분야에 대한 석·박사급의 고급인력을 충원하고 디지털 증거분석에 대한 역량을 제고하고자 민간 IT 전문가를 채용하는 「경찰관·연구직 공무원 특별채용제도」를 운영 중이며, 사이버 경력채용은 2017년 12월 기준 464명, 연구직 특별채용은 디지털포렌식센터에서 13명이 근무하고 있는데,[936] 그 업무량에 비해 인력이 부족한 상황이다.

사이버범죄가 발생한 경우 법원의 입장에서는 판단이 용이하지 않은 사항들이 많을 것이다. 그런데 기술적인 부분의 이해가 좀 더 필요한 사이버보안과 관련된 문제는 죄의 유무를 판단해야 하는 법원의 입장에서 상당한 부담이 될 수 있는바, 법관에 대한 전문성 제고 교육이 필요하다.[937] 사이버보안과 관련된 기술적 부분의 판단과정을 지원하는 '(가칭)법원 사이버 담당관'을 두는 방안도 고려해볼 수 있는데, 기술적인 문제에 대해서는 법관의 지휘에 따라 법원 사이버 담당관이 대응하도록 함으로써 법관은 법률적인 해석의 문제에 좀 더 집중할 수 있을 것이다. 나아가 사이버보안과 관련된 민감한 사안을 다루는 전담재판부 제도의 도입도 논의될 수 있다. 영국의 경우 '사이버범죄·사기·경제범죄를 전담하는 법원(Court to Exclusively Tackle Cyber-Crime, Fraud, and Economic Crime)'의 설립을 결정하였는데, 2025년경 런던시에 설치될 것으로 예상되고 있다.[938] 우리나라도 사이버보안을 비롯해서 국익을 위해 보안 유지가 필요한 사안을 다루는 전담재판부의 도입이 필요한지 다각적으로 검토되어야 한다.

3) 가이드라인 마련

현재 비트코인 등 암호화폐와 관련해서는 형사법적으로 다양한 의문이 제기되고 있는데, 특히 수사 및 재판 등 형사절차상 이를 어떻게 처리할지가 문제된다. 이에 법적 근거를 마련할 필요가 있으나, 암호화폐의 법적 성격을 규명하고 그 특징을 반영

935) 박노섭, 앞의 보고서, 183면.
936) 경찰청, 2018 경찰백서, 2018, 223-224면.
937) 법원에서도 이미 어느 정도의 일반적인 교육은 온라인과 오프라인을 통해서 수행하고 있다.
938) "World-class fraud and cybercrime court approved for London's Fleetbank House site", GOV.UK 2018.7.4., https://www.gov.uk/government/news/worldclass-fraud-and-cybercrime-court-approved-for-londons-fleetbank-house-site (2019년 10월 23일 최종접속).

하여 입법화에 이르기까지는 어느 정도의 시간이 소요될 것이다. 그러나 암호화폐와 관련된 범죄가 늘고 있는 상황에서 법률의 불비로 인해 초래될 혼란을 막아야 할 것인 바, 수사 실무 담당자들이 참조할 수 있는 가이드라인이 신속하게 제공되어야 한다.

미국에는 이미 비트코인 수사 분야의 가이드라인이 존재한다.[939] 이는 크게 4단계로 나뉘어 규정되고 있는데, 우선 제1단계에서는 증거물의 압수와 같은 모든 절차를 문서화해야 한다.[940] 제2단계에서는 기관 명의의 비트코인 지갑(Department's Bitcoin Wallet)에 접근할 수 있는 권한을 확인해야 한다.[941] 제3단계에서는 수사기관이 피의자의 비트코인 지갑에 접근할 수 있는 경우와 없는 경우로 나뉘어 그 지침이 제시되고 있는데, 우선 전자의 경우에 피의자의 비트코인 지갑에서 기관의 지갑으로 비트코인을 전송하려면 지갑 내에 있는 개인키(Private Key)에 접근할 수 있어야 한다. 피의자가 개인키를 자발적으로 제출하도록 하는 것이 가장 이상적이지만, 임의제출을 거부하는 경우에는 피의자가 지갑을 해제하도록 하는 명령을 청구해야 한다. 반면 후자의 경우에는 암호화된 지갑이 저장되어 있는 장치를 압수한 후 신속하게 IT 전문 요원의 지원을 받아야 한다. 마지막 제4단계는 모바일 지갑과 소프트웨어 지갑 및 하드웨어 지갑 등 비트코인의 지갑 유형에 따라서 후속절차를 제언하고 있다.[942] 나아가 압류된 비트코인은 경매 절차를 통해서 매각하도록 한다.[943]

독일에도 비트코인의 압수 및 처분을 규정한 가이드라인이 존재한다. 이에 의할

---

939) ROCIC, Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide, 2018, pp.10-16.

940) 비트코인 지갑이 발견될 당시에 암호화를 통해 보호되고 있는 경우가 있다. 우선 피의자의 컴퓨터 또는 모바일 장치가 잠금 해제 상태인 경우, 현 상태를 유지하여 잠김이 일어나지 않도록 주의한다. ROCIC, Ibid., pp.12-13 참조.

941) 기관 명의의 비트코인 지갑에 접근하려면 자격 증명이 있어야 한다. 기관 명의의 비트코인 지갑이 없는 경우에는 절대로 개인 명의의 지갑을 사용하지 않아야 한다. 비트코인 지갑이 없으면 이후의 프로세스를 진행될 수 없다. ROCIC, Ibid., pp.12-13 참조.

942) 첫째, 모바일 지갑을 피의자가 사용하는 경우, 피의자의 지갑에서 전송 탭을 눌러 전송하기를 선택하면 된다. 이 때 기관 명의의 지갑 주소를 직접 입력하거나 QR 코드를 스캔하여 이전하는데, 지갑에 담긴 전체 금액을 기관 명의의 지갑으로 전송한다. 둘째, 소프트웨어 지갑의 경우에는 일반적으로 모바일 지갑과 동일한 방법으로 비트코인을 전송한다. 한편, 피의자의 개인키에 접근할 수 있는 경우 그 개인키와 연결되어 있는 계정에 무기한으로 접근할 수 있다. 수사관이 이러한 개인키에 접근 시도를 하지 않는 것이 권고되며, 해당 장치를 암호화된 장치로 취급하는 것이 중요하다. 셋째, 하드웨어 지갑은 개인키를 포함하는 외부 USB 메모리 또는 종이로 프린트된 QR 코드로 존재하는데, 이 경우에는 하드웨어 지갑을 확보하고 가능한 빨리 전문가에게 의뢰해야 한다. ROCIC, Ibid., pp.12-13 참조.

943) usmarshals.gov 웹페이지, https://www.usmarshals.gov/assets/2018/bitcoinauction/ (2019년 10월 23일 최종접속).

때 비트코인의 몰수와 관련해서는 통상적인 몰수 관련 조항인 독일 형법 제74조 이하 규정 및 독일 형사소송법 제111조b 이하에 따라 이루어진다.[944] 특히 형사소송법 111조c 제2항의 "그 밖의 재산권"[945]에 비트코인을 비롯한 암호화폐가 포함될 수 있다.[946] 다음으로 비트코인에 대한 압수는 비트코인 지갑이 저장되어 있는 하드웨어를 압수하는 방법도 있으나 주로 소유자가 비트코인에 접근할 수 있도록 하는 개인키(Private Key)를 압류하는 방식으로 수행된다.[947] 개인키를 압류하지 못한 경우에는 비트코인에 접근할 수 없는바, 수사관들은 비트코인 처리를 위해 지갑과 개인키를 동시에 확보하려고 해야 한다.[948] 개인키가 확보되면 이를 이용해서 비트코인을 수사관이 개설한 지갑으로 전송한다.[949] 압수된 비트코인의 매각은 일반적으로 독일 형사소송법 제459조g[950]에 따른 '압수명령의 집행(Vollstreckung einer Einziehungsentscheidung)에 관한 법원 판결'에 의해서 이루어진다.[951] 나아가 형사소송법 제111조p에 따른 '긴급매도(Notveräußerung)'도 가능한데, 동법 제111조c에 따른 압수물 또는 제111조f에 따라 압류된 물건이 부패하거나 보관·관리를 하면서 그 가치가 현저하게 떨어질 가능성이 있는 경우, 또는 관리비가 많이 소요되는 경우에는 긴급매도를 할 수 있다(제111조p 제1항).[952] 이 때 긴급매도의 명령권자는 검찰(동조 제2항)이며, 그 실행도

---

944) Landtag Nordrhein-Westfallen, Dr. 17/1717, S.2, https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMD17-1717.pdf (2019년 10월 30일 최종접속); Christian Rückert, "Vermögensabschöpfung und Sicherstellung bei Bitcoins", MMR 5/2016, 2016, S.295.

945) 제111조c 압수의 실행 (2) 채권 압수 또는 부동산 강제집행에 관한 규정이 적용되지 않는 그 밖의 재산권의 압수는 압류로써 실행한다. 채권과 그 밖의 재산권에 대한 강제집행에 관한 민사소송법의 규정을 그 한도에서 준용한다.

946) Jutith Sikora, "Bitte ein Bitcoin – staatlicher Millionengewinn aus beschlagnahmten Bitcoins?", 2018.2.15., https://www.juwiss.de/13-2018/ (2019년 10월 23일 최종접속).

947) Christian Rückert, a.a.O.("Vermögensabschöpfung und Sicherstellung bei Bitcoins"), S.295.

948) Jutith Sikora, "Bitte ein Bitcoin – staatlicher Millionengewinn aus beschlagnahmten Bitcoins?", 2018.2.15., https://www.juwiss.de/13-2018/ (2019년 10월 23일 최종접속).

949) Jutith Sikora, "Bitte ein Bitcoin – staatlicher Millionengewinn aus beschlagnahmten Bitcoins?", 2018.2.15., https://www.juwiss.de/13-2018/ (2019년 10월 23일 최종접속). 이에 따르면 헤센주 검찰은 이른바 "경찰 지갑"의 설립을 계획하고 있다고 한다.

950) 제459조g 부수형의 집행 (1) 물건의 몰수 또는 사용불능화 명령은 그 명령의 대상이 되는 사람에게서 그 물건을 빼앗는 방법으로 집행한다.

951) Dr. 17/1717, S.2.

952) Dr. 17/1717, S.2; Christian Rückert, a.a.O.("Vermögensabschöpfung und Sicherstellung bei Bitcoins"), S.299(해당 논문에서는 제111조l로 표시하고 있으나 2017년 독일 형사소송법 개정 이후 긴급매도 조항은 제111조p로 바뀌었다).

검찰에 의해 이루어진다(동조 제4항).

스위스의 경우에도 암호화폐 처리 절차에 대한 가이드라인이 언급되고 있다. 스위스 형사소송법 제266조 제2항[953]에 의하면 제263조 제1항[954]에 따라 압수한 물건 또는 자산을 안전하게 유지·보존하기 위한 방법을 강구해야 한다. 요컨대 압류된 암호화폐를 안전하게 유지·보존하기 위해서는 별도의 '주정부 지갑(staatliche Wallet)'이 개설되어야 한다.[955] 또한 압류된 자산의 조기 처분을 위해서는 국가가 암호화폐 거래소에 지속적으로 접근할 수 있어야 하는바, 스위스에 주소지를 둔 거래소가 선호된다.[956] 불법적으로 획득한 암호화폐의 판매 또는 교환을 막기 위한 대안으로 소위 "거래 블랙리스트" 도입이 논의될 수 있으나, 이러한 접근 방식은 현재 법적인 근거가 없고, 블랙리스트 등록 암호화폐의 거래 금지를 위해서는 국제적 협력이 요구되기 때문에 아직까지는 별도의 주정부 지갑이 필요하다.[957] 한편 암호화폐의 압수에 대해서는 일반적인 압수에 대한 규정인 스위스 형사소송법 제263조 이하가 적용된다.[958]

---

953) 수사기관은 압류된 물건이나 자산의 목록을 작성하고, 해당 물건이나 자산을 그 성격에 맞도록 적절하게 보관해야 한다.

954) 피의자 또는 제3자의 물건이나 자산은 다음과 같은 경우 압수될 수 있다.

955) Monika Simmler/Sine Selman/Daniel Burgermeister, "Beschlagnahme von Kryptowährungen im Strafverfahren", AJP/PJA 8/2018, 2018, S.976.

956) Monika Simmler/Sine Selman/Daniel Burgermeister, a.a.O., S.976.

957) "거래 블랙리스트"란 블랙리스트에 등록된 경우 서비스제공업체가 이를 합법적인 지불수단으로 사용할 수 없도록 함으로써 해당 암호화폐를 통한 거래가 유인성을 잃도록 하는 방안이다. Monika Simmler/Sine Selman/Daniel Burgermeister, a.a.O., S.977.

958) Monika Simmler/Sine Selman/Daniel Burgermeister, a.a.O., S.978.

결 론

윤 지 영

제6장

결 론

오늘날 우리는 또 한 번의 네트워크 혁신 시대를 맞이하고 있다. 사람이 아닌 사물도 인터넷으로 연결되어 정보를 수집·전달·공유하는가 하면, 네트워크 및 정보처리 과정에 암호화라는 기술이 접목되기 시작하였는바, 사물인터넷과 블록체인 기술은 연결망의 확대와 암호화라는 측면에서 제4차 산업혁명의 기반이 되는 네트워크 혁신을 선도하고 있다. 이러한 기술의 발전은 제조업 등 생산 방식에만 영향을 미치는 것이 아니라 범죄의 발생 양상이나 형사사법 시스템 전반에 영향을 미칠 수 있다. 이에 본 연구는 사물인터넷과 블록체인의 기술적 이해를 바탕으로 해당 기술들을 활용하는 과정에서 문제될 수 있는 형사법적 쟁점들을 도출하고, 그 대응 방안을 모색하였다.

우선 형사실체법적인 측면에서 현행법상 정보통신망 침해에 대한 규제는 정보통신망 자체의 안정성을 확보하기 위한 행정형법적인 성격이 강하고, 실제로 사생활의 침해를 당하는 피해자를 직접적으로 보호하지 않으므로 기술적 수단을 이용한 사생활에 대한 침해를 처벌할 수 있는 형법상 근거 규정을 신설할 것을 제안하였다. 그리고 사물인터넷을 조작해서 과열로 인해 화재를 일으킨 경우도 현행법상 방화죄로 처벌될 수 있는지가 문제되는데, 이에 '불을 놓아'를 '불을 내어'라는 용어로 변경하거나 전자기기나 통신기기 등을 조작·통제하거나 이를 통하여 불을 낸 경우를 처벌하는 별도의 구성요건을 마련하는 방안도 제시하였다. 한편 암호화폐는 형법상 재물에 해당되지 않지만 민법상 채권의 목적물이 될 수 있고 현실적으로 거래소에서 시세에 따른 환금성을 가질 수 있으므로 형법상 이득죄의 객체가 될 수 있다. 또한 암호화폐 자체에 대한 전자적 방식의 탈취행위는 컴퓨터등을 이용한 권한 없는 자금의 이체 등과 같은 구조로 보아 절도죄가 아닌 형법상 컴퓨터등 사용사기죄로 의율할 수 있다. 다만, 미공개정보를 이용한 암호화폐 거래나 거래소에 대한 시세조종행위 등을 현행 형법의

범죄구성요건으로 포섭하기에는 난점이 있는바, 이러한 시장교란행위 등을 금지 및 처벌하는 규정을 마련할 것이 요청된다.

다음으로 형사절차법적인 측면에서 네트워크와 사이버 공간을 직접 대상으로 한 수사가 이루어질 수 있도록 온라인 수색 내지는 네트워크 수사기법(NIT)을 도입할 것을 제안하였다. 다크넷에 대한 수사활동을 위해서는 일정한 신분을 가공해서 증명할 것이 요구되기도 하므로 형사소송법상 비밀수사관 제도의 도입 방안도 논의될 필요가 있다. 아울러 현행 형사소송법은 종이 형태의 물리적 영장제도를 전제하고 있는데, 향후 전자적 방식으로도 영장의 발부와 제시가 이루어질 수 있도록 형사소송법을 정비해야 한다. 한편 암호화폐에 대한 압수 절차 및 방법에 대한 규정도 정비되어야 할 것인바, 법원이나 수사기관은 그 명의의 암호화폐 계정을 만들어 이에 대한 관리 절차를 두어야 하고, 이체의 과정에서 발생하는 수수료 등에 대한 처리 규정과 함께 이체의 과정을 공식적으로 기록해서 문서화한 후 일정기간 동안 보유하도록 하는 내용의 절차 규정이 마련되어야 한다. 또한 암호화폐를 압수하기 위해 필요한 계정정보 등은 피의자나 피고인이 임의제출을 하지 않는 이상 그 확보가 어려우므로 압수수색영장의 효력범위에 피의자나 피고인의 개인기록을 포함하도록 하여 거기서 얻어진 정보들을 이용해서 법원이나 수사기관이 암호화폐의 거래에 필요한 정보를 찾아낼 수 있는 방안이 모색되어야 한다.

형사정책적인 측면에서는 사물인터넷의 사이버보안 기준을 재정립하는 등 사이버보안을 강화할 수 있는 법제 정비가 요청된다. 아울러 사물인터넷이나 블록체인을 형사사법 분야에서 활용하는 방안도 논의될 필요가 있는데, 사물인터넷의 경우 이미 도입된 폴리스캠 등의 사용이 활성화될 수 있도록 이들 디바이스를 네트워크상에 연결시키고 자동으로 데이터가 전송될 수 있는 시스템을 구현하는 한편, 시스템 운영 등을 규율하는 근거 법률을 마련해야 한다. 나아가 사이버범죄와 관련된 수사 및 재판의 효율성과 전문성을 제고시키기 위한 교육 프로그램을 정비하고 전담재판부를 도입하는 방안도 고려될 수 있다. 그 외에도 사물인터넷에 대해서는 정보보호영향평가가 이루어져야 하고, 암호화폐와 관련해서는 법률의 불비로 인한 수사 실무상 혼란이 초래되지 않도록 담당자들이 참조할 수 있는 가이드라인이 신속하게 제공될 것이 요청된다.

최근 구글이 양자컴퓨터[959] 개발에 성공했다는 언론보도가 나오면서 암호 자체가 무력화될 수 있다는 우려로 인하여 비트코인 등 암호화폐의 가격이 폭락하였다.[960] 물론 이에 대해서는 회의적인 입장을 취하는 전문가도 있지만, 향후 양자컴퓨터가 구현되면 현재 우리가 논하고 있는 사물의 연결성이나 암호화의 수준은 컴퓨터 개발 초창기에 집채 만했던 '에니악'을 떠올리는 것처럼 평가될 지도 모른다. 1939년 세계 최초의 전자식 컴퓨터가 공개된 지 80여년 만에, 1969년 최초의 인터넷망인 '아르파넷'이 구축되고, 1973년 미국 모토로라의 마틴 쿠퍼 박사팀에 의해 셀룰러 시스템을 활용한 휴대전화가 개발된 지 50여년 만에, 그리고 2007년 애플의 '아이폰'이 등장한 지 불과 10여년 만에 세상이 바뀌었다. 더불어 그러한 기술적 진보는 범죄의 발생 양상을 변화시키면서 형사사법적 대응을 요청하고 있다. 사물인터넷과 블록체인은 이제 더 이상 미래의 기술이 아니다. 빛의 속도로 빨라질 것만 같은 기술의 발전으로 인해서 어느 순간에 또 다른 첨단기술들이 그 자리를 대체할지 모를 일이지만, 두 기술을 중심에 두고 논의를 전개한 이 보고서가 보다 신속하게 형사사법 분야의 제도를 개선하고 국가형사정책을 수립하는 데에 조금이라도 기여하기를 기대해 본다.

---

959) 기존 컴퓨터는 '비트' 단위를 쓴다. 0과 1 두 숫자의 조합으로 모든 것을 표현하고 처리했기 때문에 용량을 늘리는 데 한계가 있었다. 동전으로 치면 앞면 아니면 뒷면, 이런 식으로 계속 이어졌던 셈이다. 이러한 한계를 극복하기 위하여 등장한 양자컴퓨터는 양자역학 원리를 이용하여 0과 1이라는 2개의 상태를 동시에 가질 수 있다. 동전이 계속 회전하고 있는 상태와 비슷하다고 보면 된다. 양자정보의 기본 단위는 '큐비트(qubit)' 또는 '양자비트'라고 한다. 동전이 회전하는 것처럼 중첩과 얽힘 현상이 발생하기 때문에 0과 1이라는 2개의 상태를 동시에 가질 수 있다. "알파고 넘는 '양자컴퓨터' 온다", 매일경제신문 2019년 5월 15일자, https://www.mk.co.kr/news/it/view/2019/05/320104/ (2019년 10월 23일 최종접속).

960) "구글 '양자컴퓨터 개발' 발표에 암호화폐 급락 이유는", TV 조선 2019년 10월 25일자, http://news.tvchosun.com/site/data/html_dir/2019/10/25/2019102590037.html (2019년 10월 23일 최종접속).

참고문헌

1. 국내문헌

[단행본]

4차산업혁명위원회/관계부처 합동, 스마트공장 확산 및 고도화 전략, 2018.3.8.

KCERN(창조경제연구회), 4차 산업혁명 국가 로드맵 작성을 위한 정책연구,「창조경제연구회 제46차 공개포럼」보고서, 창조경제연구회, 2018.

강석구/이원상, 사이버범죄 관련 법령 정비방안, 한국형사정책연구원, 2014.

경찰청, 2018 경찰백서, 2018.

경찰청, 2018 사이버위협 분석 보고서, 2019.

경찰청, 2019년 상반기 사이버위협 분석 보고서, 2019.

과학기술정보통신부, 신뢰할 수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전전략, 2018.6.

관계부처 합동, K-ICT 사물인터넷 확산 전략, 2015.12.7.

관계부처 합동, 초연결 디지털 혁명의 선도국가 실현을 위한 사물인터넷 기본계획, 2014.5.8.

국회도서관, 현안관련 외국입법례, 제51호, 2018.

국회 법제실, 4차 산업혁명 입법과제, 2017.12.

권오상/남승용/조대근/김유석/이수연, 인터넷전용회선 및 IDC 요금에 대한 사후규제 방안 연구, 방송통신위원회, 2018.

금융위원회, 관계기관 합동 가상통화(Virtual currency) 현황 및 대응방안, 2017.9.

김대근/임석순/강상욱/김기범, 신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구 – 기술적 수단을 사용한 사이버 금융사기를 중심으로, 한국형사정책연구원, 2016.

김성도, 호모 모빌리쿠스: 모바일 미디어의 문화생태학, 삼성경제연구소, 2008.

김성돈, 형법각론 제4판, 성균관대학교출판부, 2016.

김성준/박주석/박지웅/전은정/김나라/강혜정/정혜인/신세미/김정은/민경은/최홍선/안호정/김우리, IoT 제품·서비스 책임강화 방안연구, 한국인터넷진흥원, 2015.11.

김일수/서보학, 새로쓴 형법총론 제6판, 박영사, 2005.

김혜정, 전자감독제도의 장기 발전전략 수립을 위한 부착명령 대상범죄 및 부착기간 등의 적정성에 관한 연구, 법무부 정책연구보고서, 2015.

나채준/이준호/김현희/양태건/라정일/정재도, 스마트시티 조성확산을 위한 제도개선 연구, 한국법제연구원, 2018.

넥스텔리전스, 2018 글로벌 정보보호 산업시장 동향조사, 한국인터넷진흥원, 2018.

노명우/윤명희, 탈근대사회에서의 개인과 공동체 관계의 변화, 정보통신정책연구원, 2008.

대통령직속 4차산업혁명위원회, 4차 산업혁명 대정부 권고안, 2019.10.

대통령직속 4차산업혁명위원회/관계부처 합동, 도시혁신 및 미래성장동력 창출을 위한 스마트시티 추진전략, 2018.

미래창조과학부, 제5차 국가정보화 기본계획(2013-2017), 2013.

미래창조과학부/법무부, 전자문서법 해설서-전자문서 효력의 일반적 인정과 예외 및 전자문서 활용-, 2017.

박노섭, 경찰청 사이버범죄 대응능력 향상을 위한 교육훈련 체계 개발, 2015.12.

박철순/김성훈, 한국 이동통신 서비스 및 단말기 산업의 변천과 발전방향, 서울대학교 출판부, 2007.

백광훈, 인터넷범죄의 규제법규에 관한 연구, 한국형사정책연구원, 2000.

성낙일/이명호/김도환/성극제/손상영/강인수, 한국정보통신 20세기사: 정책/산업부문 조사, 집필 -제5편 도약 발전시기(1980년-2000년)-, 정보통신정책연구원, 2001.

손동권, 형법각론 제3개정판, 율곡출판사, 2010.

송성수, 발명과 혁신으로 읽는 하루 10분 세계사: 종이에서 로봇까지, 생각의힘, 2018.

안정배, 한국인터넷의 역사 - 되돌아보는 20세기, 블로터앤미디어, 2014.

연성진/전현욱/김기범/신지호/최선희, 암호화폐(Cryptocurrency)관련 범죄 및 형사정책 연구, 한국형사정책연구원, 2017.

오영근, 형법각론 제4판, 박영사, 2017.

우동진/이동철/백광천, 우리나라 전기통신기술 발달사에 관한 연구, 한국전기통신연구소, 1989.

윌리엄 스탈링스(강지양/남기혁 역), 현대 네트워크 기초이론: SDN, NFV, QoE, IoT, 클라우드, 에이콘출판사, 2016.

윤지영/임정호/이민화/김성돈, 제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(I): 자율주행자동차와 드론, 한국형사정책연구원, 2018.

이민화/주강진/김애선/김예지/윤예지/장아침/손문영/이명호/차원용/정현호, 4차 산업혁명 국가 로드맵 작성을 위한 정책연구, 국회 4차 산업혁명 특별위원회, 2018.5.

이병욱, 블록체인 해설서, 에이콘출판사, 2019.

이영란, 형법학-각론강의-제3판, 형설출판사, 2013.

이원상, 프라이버시와 범죄통제의 균형을 위한 통신수사 법체계 마련, 대검찰청, 2015.

이원상/채희정, 사이버범죄의 새로운 유형과 형사정책적 대안연구, 한국형사정책연구원, 2010.

이재상/장영민/강동범, 형법각론 제11판, 박영사, 2019.

이재상/조균석, 형사소송법 제12판, 박영사, 2019.

이재현, 멀티미디어, 커뮤니케이션북스, 2013.

이재현, 모바일 미디어, 커뮤니케이션북스, 2013.

이재현, 인터넷, 커뮤니케이션북스, 2013.

이재현, 인터넷과 사이버사회, 커뮤니케이션북스, 2001.

이천현/도중진/권수진/신동일/김현우, 형법각칙 개정연구[9] -우리나라 및 주요 국가의 형법개정 동향-, 한국형사정책연구원, 2007.

이 철, 컴퓨터범죄와 소프트웨어보호, 박영사, 1995.

장영민/조영관, 컴퓨터범죄에 관한 연구, 한국형사정책연구원, 1991.

정선종/박세경, UHF대역 셀룰러 이동 무선전화 시스템을 위한 채널 최적 할당방식에 관한 연구, 한국전기통신연구소, 1987.

정성근/박광민, 형법총론 전정판, 성균관대학교출판부, 2013.

정성근/박광민, 형법각론 전정판, 성균관대학교출판부, 2012.

정지훈, 거의 모든 인터넷의 역사 : 우리가 지금껏 알지 못했던 인터넷 혁명의 순간들, 메디치미디어, 2014.

한국무역협회 베이징지부, 중국 블록체인 규정 해설, 2019.3.
한국무역협회 북경지부, 중국 사이버보안법 관련 법규 해설, 2017.6.
한국인터넷진흥원, 워너크라이 분석 스페셜리포트, 2017.10.
한국인터넷진흥원, 2016년 Mirai 악성코드 동향, 2016.12.
한국전산원, 정보화 역기능 현황 및 분석, 1994.12.
행정안전부/한국정보화진흥원, 정부사물인터넷 도입 가이드라인, 2019.7.
홍승필/민경식/김혜리, 블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구, 선거연수원, 2017.

[논문]
강동범, "사이버범죄와 형사법적 대책", 형사정책연구 제11권 제2호(통권 제42호), 한국형사정책연구원, 2000.
강동범, "컴퓨터범죄에 대한 입법론적 대책", 형사정책 제3호, 한국형사정책학회, 1998.
곽진교, "스마트사이니지포럼", TTA 저널 제170호, 한국정보통신기술협회, 2017.
국경완, "블록체인 기술 및 산업 분야별 적용 사례", 주간기술동향 1900호, 정보통신기획평가원, 2019.6.12.
김경호, "헤드업 디스플레이(Head-Up Display)", KISTI market report 2015년 9월호(통권 55호), 한국과학기술정보연구원, 2015.
김병연, "ICO의 법적 개념 및 각국의 규제동향에 관한 연구", 일감법학 제43호, 건국대학교 법학연구소, 2019.
김상겸, "스팸규제에 관한 헌법적 연구", 공법학연구 제5권 제3호, 한국비교공법학회, 2004.
김종호, "비공식 자금이체 방식인 이른바 환치기 거래의 정산방법 분석과 그 거래규모의 측정을 통한 정책적 함의의 탐색", 한양법학 제34호, 한양법학회, 2011.
김종호, "디지털 포렌식의 원리와 소송에서의 증거평가 방식", 경희법학 제52권 제1호, 경희대 법학연구소, 2017.
김준영/김계정/문준호, "ICO(Initial Coin Offering)에 대한 주요 이슈 및 시사점", 증권법연구 제19권 제2호, 한국증권법학회, 2018.
김태석, "컴퓨터 바이러스의 제작유포행위에 대한 형사법적 규제", 중앙법학 제4집 제3호, 중앙법학회, 2002.

김형석/전용태, “컴퓨터 바이러스 등 유해 프로그램의 법적 규제 검토 - 미국의 제정법과 판례를 중심으로 -”, 법이론실무연구 제7권 제2호, 한국법이론실무학회, 2019.

김혜정/조상희, “피해자없는 범죄의 규제에 관한 소고”, 피해자학연구 제23권 제1호, 한국피해자학회, 2015.

나유진, “딥웹으로 퍼져나가는 네덜란드 대마초”, Barun ICT newsletter, 연세대학교 바른ICT연구소, 2019.11.

도중진, “범죄수사에 있어서 잠입수사관제도의 도입여부”, 중앙법학 제13집 제3호, 중앙법학회, 2013.

문인철, “사이버공간의 특성과 안보화 문제”, 국가안보와 전략 제17권 4호(통권 68호), 국가안보전략연구원, 2017.

민영성/강수경, “독일의 인터넷 비밀수사에 관한 논의와 그 시사점”, 법학논총 제31권 제2호, 국민대학교 법학연구소, 2018.

박상기, “개정형법의 내용과 문제점”, 형사정책연구 제7권 제1호(통권 제25호), 한국형사정책연구원, 1996.

박선종, “가상화폐의 법적 개념과 지위”, 일감법학 제42호, 건국대학교 법학연구소, 2019.

박웅신/이경렬, “다크넷의 범죄현상과 형사법적 대응방안”, 형사법의 신동향 제58호, 대검찰청, 2018.

박현제, “한국 인터넷 역사와 표준”, TTA Journal 제143호, 한국정보통신기술협회, 2012.

박희영, “예방 및 수사목적의 온라인 비밀 수색의 허용과 한계”, 원광법학 제28권 제3호, 원광대학교 법학연구소, 2012.

방태웅, “4차산업혁명의 기반기술, 블록체인”, Weekly TIP Vol. 108, 융합연구정책센터, 2018.2.

배상균, “일본 사이버 보안 정책에 관한 검토-사이버 시큐리티 기본법의 성립과 개정을 중심으로-”, 외법논집 제42권 제2호, 한국외국어대학교 법학연구소, 2018.

백대열/송희권, “형법상 재물과 재산상의 이익 간 구분 기준으로서의 관리가능성”, 서울대 법학평론 제9권, 서울대학교 법학평론 편집위원회, 2019.

성희활, “가상화폐의 공모(ICO)와 상장에 대한 적정 규제방안”, 상사법연구 제37권 제1호, 한국상사법학회, 2018.

송란희, “한국의 스토킹 피해 실태 및 특징”, 한일 심포지엄「스토킹 피해 실태 및

법적 대응」 자료집, 한국여성정책연구원/남인순 국회 여성가족위원장실/교토여자대학교, 2016.8.25.

송민정, "IoT 기반 스마트 사이니지 현황 및 발전 방향", TTA 저널 제170호, 한국정보통신기술협회, 2017.

송은지/강원영, "미국 오바마 정부 2기의 사이버보안 강화정책", INTERNET & SECURITY FOCUS 2014년 9월, 한국인터넷진흥원, 2014.

신 원, "안티포렌식 기법 분석을 통한 안티포렌식 대응 방안", 보안공학연구논문지 Vol.11 No.6, 보안공학연구지원센터, 2014.

심우민, "정보통신법제의 최근 입법동향: 정부의 규제 개선 방안과 제19대 국회 전반기 법률안 중심으로", 언론과 법 제13권 제1호, 한국언론법학회, 2014.

양근원, "디지털 포렌식과 법적 문제 고찰", 형사정책연구 제17권 제2호(통권 제66호), 한국형사정책연구원, 2006.

양성은, "사이버범죄의 동향과 이에 대한 형사법적 책임", Internet & Security Focus 2013년 9월호, 한국인터넷진흥원, 2013.

양종모, "랜섬웨어 공격에 대한 형사법적 고찰", 홍익법학 제20권 제1호, 홍익대학교 법학연구소, 2019.

양천수/지유미, "미국 사이버보안법의 최근 동향 - '사이버보안 정보공유법'을 중심으로 하여'", 법제연구 제54호, 한국법제연구원, 2018.

오기두, "정보통신망 모니터링에 의한 범죄통제의 적합성", 형사정책연구 제27권 제4호(통권 제108호), 한국형사정책연구원, 2016.

오병철, "IoT환경에서의 프라이버시 보호에 관한 연구", NAVER Privacy White Paper, 네이버, 2016.

오영근, "인터넷범죄에 관한 연구", 형사정책연구 제14권 제2호(통권 제54호), 한국형사정책연구원, 2003.

유주선/강현구, "가상통화에 대한 입법적 방안과 법적 쟁점 연구", 금융법연구 제15권 제1호, 한국금융법학회, 2018.

윤동호, "수사협조범죄자 기소면제 및 형벌감면 법제화 비판", 비교형사법연구 제13권 제2호, 한국비교형사법학회, 2011.

윤배경, "가상화폐의 법적 성질과 민·형사상 강제집행", 인권과 정의 474호, 대한변호사협회, 2018.6.

윤창술, “스팸메일(Spam Mail)에 대한 규제방안”, 기업법연구 제12집, 한국기업법학회, 2003.

이규호, “4차 산업혁명의 효과와 형사정책적 과제”, 법학연구 제75권, 한국법학회, 2019.

이상복, “디지털 포렌식 업무의 법·제도적인 개선방향”, 서강법학 제10권 제2호, 서강대학교 법학연구소, 2008.

이상학, “테러방지 수권규정과 기본권침해의 한계 - 독일연방수사청법의 테러방지권한에 대한 연방헌법재판소의 판결(2016.4.20.) 검토를 중심으로”, 공법학연구 제17권 제3호, 한국비교공법학회, 2016.

이연수/이수연/윤석구/전재성, “주요국의 사이버안전 법·조직체계 비교 및 발전방안 연구”, 국가정보연구 제1권 제2호, 한국국가정보학회, 2008.

이용수, “세계의 이동통신현황과 경쟁도입”, 통신정책연구 1991년 여름호, 정보통신정책연구원, 1991.7.

이원삼, “가상화폐의 의미와 법적 지위 – 비트코인을 중심으로 -”, 상사판례연구 제31집 제2권, 한국상사판례학회, 2018.

이원상, “스토킹 처벌규정 도입에 대한 고찰”, 형사정책연구 제24권 제2호(통권 제94호), 한국형사정책연구원, 2013.

이정훈, “블록체인과 가상화폐의 형사법적 문제와 전망 -대법원 2018. 5. 30. 선고 2018도3619 판결을 중심으로-”, 홍익법학 제20권 제1호, 홍익대학교 법학연구소, 2019.

이지언/이보미, “ICO 현황과 규제방안 – 자본시장법 중심으로 -”, KIF VIP 리포트 2018-07, 한국금융연구원, 2018.

이효은/홍승표, “한국 IT 산업의 발자취”, 주간기술동향 제1500호 특집, 정보통신산업진흥원, 2011.6.17.

임종률, “컴퓨터범죄와 형법적 대응”, 법학논총 제5집, 숭실대학교 법학연구소, 1989.

장여경/김지성, “한국의 이동통신 도감청과 통신비밀보호법”, 계간 정보운동 액트온(Act On) 2009년 제1호(통권 제5호), 진보네트워크센터, 2009.

장영민, “개정형법의 컴퓨터범죄”, 고시계 1996년 2월호(통권 제468호), 고시계사, 1996.

장용석, “ARPA, DARPA, ARPA-E : 창의적 연구개발 모형”, 과학기술정책 제21권 제3호(통권 제184호), 과학기술정책연구원, 2011.

장준원, “실시간 디지털증거 수집기법을 이용한 사이버 순찰 체계 구축 및 활용사례”, 디지털포렌식연구 제8권 제2호, 한국디지털포렌식학회, 2014.

전길남, “초기 한국 인터넷 역사(1982년-2004년), The e-Bridge 제12호, 한국정보처리학회, 2011.

전지연, “인터넷 피싱의 형사법적 책임”, 형사정책연구 제20권 제4호(통권 제80호), 한국형사정책연구원, 2009.

전지연, “컴퓨터범죄에 대한 형법적 대응방안”, 한림법학 FORUM 제5권 제1호, 한림대학교 법학연구소, 1996.

정대용/김기범/권헌영/이상진, “디지털 증거의 역외 압수수색에 관한 쟁점과 입법론-계정 접속을 통한 해외서버의 원격 압수수색을 중심으로-”, 법조 제65권9호, 법조협회, 2016.12.

정상조, “위치기반서비스 규제에 관한 연구”, 2015 NAVER privacy White Paper, 네이버, 2016.

정승화, “블록체인 기술기반의 분산원장 도입을 위한 법적과제”, 금융법연구 제13권 제2호, 한국금융법학회, 2016.

정연덕, “악성프로그램의 정의와 해석에 관한 법적 문제”, 동아법학 제53호, 동아대학교 법학연구소, 2011.

정 완, “사이버범죄의 주요 쟁점과 대응책에 관한 소고”, 홍익법학 제17권 제3호, 홍익대학교 법학연구소, 2016.

정익래/홍도원/정교일, “디지털 포렌식 기술 및 동향”, 전자통신동향분석 제22권 제1호, 한국전자통신연구원, 2007.

정태진/이광민, “다크웹 범죄활동 동향: 국제공조 및 대응전략”, 한국경찰연구 제17권 제1호, 한국경찰연구학회, 2018.

정해상, “가상화폐발행(ICO)의 특성과 규제의 쟁점”, 법학논총 제43권 제1호, 단국대학교 법학연구소, 2019.

조규정, “컴퓨터조작범죄: 유형과 처벌을 중심으로”, 형사정책연구 제1권 제2호(통권 제2호), 한국형사정책연구원, 1990.

조진삼, “경찰미래비전 2045”, See Futures 제10호, KAIST 문술미래전략대학원 미래전략연구센터, 2016.

채송화, “디지털 사이니지(Digital Signage) 기반 콘텐츠산업의 현황과 전망”, 코카포커스 2012-06호(통권 54호), 한국콘텐츠진흥원, 2012.

최미경/최정민, “경찰청 웨어러블 폴리스 캠의 운영 실태 및 개선과제”, 이슈와 논점 제1590호, 국회입법조사처, 2019.6.13.

최병각, “조직범죄수사의 협조자에 대한 양형과 형사면책”, 비교형사법연구 제5권 제2호, 한국비교형사법학회, 2003.

최준혁, “효과없는 악성코드 제거프로그램 배포에 관한 형법의 쟁점”, 법학연구 제42집, 전북대학교 법학연구소, 2014.

최호진, “비트코인에 대한 몰수 가능성 - 대상판결 : 대법원 2018.5.30. 선고 2018도3619 판결 -”, 비교형사법연구 제20권 제3호, 한국비교형사법학회, 2018.

한국인터넷진흥원, “미국 국토안보부, 국가 중요 인프라에 대한 사이버보안 전략 보고서 발표”, 인터넷 법제동향 제144호, 한국인터넷진흥원, 2019.9.

한국인터넷진흥원, “일본 총무성, IoT·5G 보안 종합 대책 발표”, 인터넷 법제동향 제144호, 한국인터넷진흥원, 2019.9.

한국인터넷진흥원, “일본 경제산업성, 사이버·물리보안 대책 프레임워크 개정안 발표”, 인터넷 법제동향 제133호, 한국인터넷진흥원, 2018.10.

한동진/김현희, “마이크로 디스플레이를 이용한 소형 헤드업 디스플레이 광학계 설계”, 한국산학기술학회 논문지 제16권 제9호, 한국산학기술학회, 2015.

한서희, “가상자산 관련 범죄에 대한 연구 – 실제 사례를 중심으로”, 한국형사정책연구원/블록체인법학회 공동학술대회 발표자료집, 2019.10.7.

한성훈, “가상화폐 관련 형사법적 문제에 관한 소고”, 경상대학교 법학연구 제27권 제2호, 경상대학교 법학연구소, 2019.

허 황, “최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신 감청에 관한 연구”, 형사법의 신동향 제58호, 대검찰청, 2018.

황만성, “형법상 사기죄 관련규정의 제·개정방안”, 형사정책연구 제20권 제1호(통권 제77호), 한국형사정책연구원, 2009.

[보도자료]
경찰청 보도자료, “미국 법무부, 아동음란물 다크웹사이트 국제공조사건 수사결과 발표”, 2019.10.16.
경찰청 보도자료, “경찰청, 가상화폐 다단계유사수신 사기 뿌리 뽑는다”, 2017.7.12.
경찰청 보도자료, “경찰청, ‘경찰 미래비전 2045’발표 - ‘선진 국민 경찰’을 지향하는 과학 경찰, 정예 경찰, 시민 경찰을 제시-”, 2016.1.14.
과학기술정보통신부 보도자료, “제5회 과학치안 아이디어 공모전 시상식 개최”, 2019.10.22.
과학기술정보통신부 보도자료, “2018년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 발표”, 2019.5.10.
과학기술정보통신부 보도자료, “민간의 혁신 아이디어, 블록체인 기술로 실현한다”, 2019.2.28.
과학기술정보통신부 보도자료, “블록체인 공공 시범사업 2배로 확대하고 민간 프로젝트도 함께 추진한다”, 2018.12.21.
과학기술정보통신부 보도자료, “와이파이·사물인터넷 등 신산업 육성을 위한 규제 개선 시행”, 2018.12.5.
과학기술정보통신부 보도자료, “2018년 상반기 통신자료 및 통신사실확인자료 제공 등 현황 발표”, 2018.11.9.
과학기술정보통신부 보도자료, “블록체인 글로벌 기술경쟁력 확보, 선도사업 본격 추진”, 2018.6.21.
과학기술정보통신부 보도자료, “2017년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 발표”, 2018.5.18.
국토교통부 보도자료, “강력범죄 수배차량 CCTV로 실시간 추적…도시 안전망 강화”, 2019.9.24.
국토교통부 보도자료, “서울·제주 등 12개 지자체 스마트시티 통합 플랫폼 사업지 선정”, 2018.2.28.
금융감독원 보도자료, “2018년 유사수신 혐의업체 특징 및 소비자 유의사항”, 2019.4.25.
금융위원회 보도자료, “제30기 제3차 국제자금세탁방지기구(FATF) 총회 참석”, 2019.6.24.

금융위원회 보도자료, “국제자금세탁방지기구(FATF) 총회 참석 결과”, 2018.10.22.
금융위원회 보도자료, “제29기 제3차 자금세탁방지기구(FATF) 총회 결과”, 2018.7.3.
금융위원회 보도자료, “「가상통화 관련 자금세탁방지 가이드라인」 개정”, 2018.6.27.
금융위원회 보도자료, “가상통화 투기근절을 위한 특별대책(`17.12.28) 중 금융부문 대책 시행”, 2018.1.23.
금융위원회, 보도자료 “「가상통화 관계기관 합동 TF」 개최 - 가상통화 현황 및 대응방향”, 2017.9.4.
대통령직속 4차산업혁명위원회 보도자료, “4차위, 4차 산업혁명 대정부 권고안 발표”, 2019.10.25.
미래창조과학부 보도자료, “미래부, 사물인터넷(IoT) 실증사업 본격 추진”, 2015.6.24.
미래창조과학부 보도자료, “초연결 디지털 혁명의 선도국가 실현을 비전으로 사물인터넷 국가전략 수립”, 2014.5.8.
법무부 보도자료, “법무부, 가상통화 관련 범죄에 대해 지속적 엄정 대응 방침”, 2019.7.19.
법무부 보도자료, “전자감독제도 10년! 재범 억제 능력을 입증하고, 수용시설 과밀화 대안으로 주목받다”, 2018.9.5.
서울시 보도자료, “서울시, ‘안심이 앱’ 11만 명 돌파…CGV와 안전캠페인”, 2019.9.23.
서울시 보도자료, “서울시, ‘안심이 앱’ 신고로 성범죄자 현행범 검거”, 2019.6.12.
서울시 보도자료, “서울시, 밤길 ‘안심이’ 전 자치구 확대…시민 대표 호신앱으로”, 2018.10.26.
서울시 보도자료, “서울시, “밤길 두려운 여성은 ‘안심이 앱’을 켜세요””, 2016.3.8.
서울시 보도자료, “길거리 공중전화 부스, 안심부스로 새 단장”, 2015.11.9.
중앙선거관리위원회 보도자료, “중앙선관위, “블록체인을 적용한 온라인투표 서비스 첫 개시””, 2018.11.28.
행정안전부 보도자료, “공공 사물인터넷, 품질은 높이고 도입은 더 쉽게 – 행안부, “정부 사물인터넷 도입 가이드라인”마련”, 2019.7.17.
한국인터넷진흥원 보도자료, “KISA, 스마트홈 가전 분야 보안취약점 대응 나선다 -침해사고 예방위해 9월까지 신규 보안취약점 집중 신고기간 운영 -건별 최고 500만원 신고 포상금 지급, 제조사에는 보안패치 요청”, 2017.8.1.

2. 외국 문헌

가. 영미문헌

[단행본]

Adrian McEwen/Hakim Cassimally, Designing the Internet of Things, Wiley Publishing, 2013.

Andrew Murray, Information Technology Law: The Law and Society, Oxford University Press, 2019.

Anna DiStefano/Kjell Erik Rudestam/Robert Silverman, Encyclopedia of Distributed Learning, SAGE Publications, 2004.

B. Jack Copeland, Turing: Pioneer of the Information Age, Oxford University Press, 2012.

Barry M. Leiner/Vinton G. Cerf/David D. Clark/Robert E. Kahn/Leonard Kleinrock/Daniel C. Lynch/Jon Postel/Larry G. Roberts/Stephen Wolff, A Brief History of the Internet, Internet Socity, 1997.

Bernard A. Galler, Software and Intellectual Property Protection: Copyright and Patent Issues for Computer and Legal Professionals, Quorum Books, 1995.

Cath Senker, Cybercrime & the Dark Net: Revealing the Hidden Underworld of the Internet, SIRIUS, 2017.

Charles P. Pfleedger/Shari Lawrence Pfleeger/Jonathan Margulies, Security in Computing, 5th Edition, Prentical Hall, 2015.

David E. Lundstrom, A Few Good Men From Univac, MIT Press, 1987.

Department of Defense, Quadrennial Defense Review Report, 2010.2.

ETSI, CYBER; Cyber Security for Consumer Internet of Things, ETSI TS 103 645, V1.1.1, 2019.2.

European Commission, COMMISSION RECOMMENDATION of 26.3.2019 - Cybersecurity of 5G network, 2019.

Edith Law/Luis von Ahn, Human Computation(Synthesis Lectures on Artificial Intelligence and Machine Learning), Morgan & Claypool Publishers, 2011.

Financial Action Task Force, The FATF Recommendations, 2019.6.

Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019.6.

Geoffrey W. A. Dummer, Electronic Inventions and Discoveries: Electronics from its earliest beginnings to the present day, Fourth Edition, Institute of Physics Publishing, 1997.

Gerard O'Regan, World of Computing: A Primer Companion for the Digital Age, Springer, 2018.

I. Bernard Cohen, Howard Aiken: Portrait of a Computer Pioneer(History of Computing), MIT Press, 2000.

IJIS Institute, Correction Tech 2020. Technological Trends in Custodial & Community Corrections, 2017.3.

Imar De Vries, Tantalisingly Close: An Archaeology of Communication Desires in Discourses of Mobile Wireless Media, Amsterdam University Press, 2012.

ITU-T Y.2060, Overview of the Internet of Things, 2012.6.

Janet Abbate, Inventing the Internet, MIT Press, 1999.

Jeffrey A. Hart/Robert R. Reed/Francois Bar, The Building of the Internet: Implications for the Future of Broadband Networks, Berkeley Roundtable on the International Economy, UC Berkeley, 1992.

Jennifer Bachner, Predictive Policing: Preventing Crime with Data and Analytics, IBM Center for The Business of Government, 2013.

John S. Hollywood/Dulani Woods/Richard Silberglitt/Brian A. Jackson, Using Future Internet Technologies to Strengthen Criminal Justice, RAND Corporation, 2015.

John V. Atanasoff, "Computing Machines for the Solution of Large Systems of Linear Algebraic equations", Iowa State University, 1982.

K. G. Coffman/A. M. Odlyzko, Growth of the Internet, AT&T Labs - Research, 2001.

Marc Goodman, Future crimes: inside the digital underground and the battle for our connected world, Anchor Books, 2016.

Marjie T. Britz, Computer Forensics and Cyber Crime, Pearson Education, 2013.

Mingtao Shi, Technology Base of Mobile Cellular Operators in Germany and China: A Comparative Study from the Perspective of the Resource-based View, Univerlagtuberlin, 2007.

Mitch Waldrop, DARPA and the Internet Revolution, 50 Years of Bridging the Gap, DARPA, 2015.

National Research Council, Funding a Revolution: Government Support for Computing Research, The National Academies Press, 1999.

Neil Gershenfeld, When things start to think, Henry Holt and Company Inc., 1999.

NISC, Cybersecurity Strategy, 2018.7.27.

NISC, Japanese Government's Efforts to AddressInformation Security Issues, 2007.

NYPD Domain Awareness System(DAS), Public Security Privacy Guidelines, 2009.4.2.

Paul Baran, On Distributed Communications, RM-3420-PR, RAND Corporation, 1964.

Robert Curley, Breakthroughs in Telephone Technology: From Bell to Smartphones, Britannica Educational Publishing, 2012.

ROCIC, Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide, 2018.

Ronald A. Asherson/Ricard Cervera/Jean-Charles Piette/Yehuda Shoenfeld, The Antiphospholipid Syndrome II: Autoimmune Thrombosis, Elsevier Science, 2002.

Thomas Haigh/Mark Priestley/Crispin Rope, ENIAC in Action: Making and Remaking the Modern Computer, MIT Press, 2016.

Tim Berners-Lee/Mark Fischetti, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor, Harper Collins Publishers, 1999.

[논문]

Alan M. Turing, “On Computable Numbers, with an Application to the Entscheidungsproblem”, Proceedings of the London Mathematical Society, Volume s2-42, 1937.

Andrew Guthrie Ferguson, “Big Data and Predictive Reasonable Suspicion”, University of Pennsylvania Law Review Volume 163, University of Pennsylvania Law School, 2015.

Andrew D. Selbst, “Disparate Impact in Big Data Policing”, Georgia Law Review Volume 52, Number 1, University of Georgia School of Law, 2017.

B. Jack Copeland, “Colossus: Its Origins and Originators”, IEEE Annals of the History of Computing Volume 26, Issue 4, IEEE, 2004.

Barry M. Leiner/Vinton G. Cerf/David D. Clark/Robert E. Kahn/Leonard Kleinrock/Daniel C. Lynch/Jon Postel/Larry G. Roberts/Stephen Wolff, “A Brief History of the Internet”, Computer Communication Review, Volume 39, Number 5, ACM SIGCOMM, 2009.

Carla Hustedt, “A Public Value Perspective on Predictive Policing in the US”, Research Paper, 2016.11.

Clary Blair Jr., “Passing of a Great Mind: John von Neumann, a Brilliant, Jovial Mathematician, was a Prodigious Servant of Science and his Country”, Life Magazine, Volume 42, Number 8, Time Inc., 1957.2.25.

David Chaum, “Blind signature for untraceable payments”, Advances in Cryptology, Springer, 1983.

David Chaum, “Security without identification: Transaction systems to make big brother obsolete”, Communications of the ACM, Vol. 28 No. 10, Association for Computing Machinery, 1985.10.

David Malakoff, “The Real Father of the Internet”, Science Volume 285, Issue 5433, American Association for the Advancement of Science(AAAS), 1999.9.3.

E. S. Levine/Jessica Tisch/Anthony Tasso/Michael Joy, “The New York City Police Department's Domain Awareness System”, Journal Interfaces, Volume 47

Issue 1, INFORMS Institute for Operations Research and the Management Sciences(INFORMS), 2017.

Emily Thomas, "Why Oakland Police Turned Down Predictive Policing", Motherboard, 2016.12.28.

Forrest M. Mims III, "The Tenth Anniversary of the ALTAIR 8800", Computers & Electronics 1985.1.

H. F. Dylla/Steven T. Corneliussen, "John Ambrose Fleming and the Beginning of Electronics", Journal of Vacuum Science & Technology, Volume 23, Issue 4, A Vacuum Surfaces and Films, 2005.

Hari Mukundhan, "Anatomy of an IoT DDoS Attack and Potential Policy Responses", ISACA Journal Volume 5, ISACA, 2017.

Harold C Deutsch, "The Historical Impact of Revealing The Ultra Secret", The U.S. Army War College Quarterly Parameters, Volume 7, Number 3, U.S. Army War College Publications, 1977.

Jack M. Balkin, "The Constitution in the National Surveillance State", Minnesota Law Review, Vol.93 No.1, University of Minnesota Law School, 2008.11.

Jim Costello/Paul Dyer/David L Jeanes, "Packet switching", Fraidoon Mazda(ed.), Telecommunications Engineer's Reference Book, Butterworth-Heinemann, 1993.

Joel A. Snow, "ENIAC or ABC?", Physics Today Volume 54, Issue 6, American Institute of Physics, 2001.

John V. Atanasoff, "Computing Machines for the Solution of Large Systems of Linear Algebraic equations", Iowa State University, 1982.

John Ludwig von Neumann, "First draft of a report on the EDVAC", IEEE Annals of the History of Computing, Volume 15, Issue 4, IEEE, 1993.

John Naughton, "The evolution of the Internet: from military experiment to General Purpose Technology", Journal of Cyber Policy, Volume 1, Number 1, Chatham House, 2016.

Jonathan Peter Bowen, "Alan Turing: The Founder of Computer Science", A History of Computing in Three Parts, 2013 Gresham College/British

Society of the History of Mathematics conference, 2013.10.31.

Joseph C. R. Licklider, "Man-Computer Symbiosis", IRE(now IEEE) Transactions on Human Factors in Electronics, HFE-1, 1960.3.

Joseph C. R. Licklider/Robert W. Taylor, "The Computer as a Communication Device", Science and Technology, Volume 76, 1968.

Joseph C. R. Licklider/Robert W. Taylor, "On-Line Man Computer Communication", G. A. Barnard(ed.), AFIPS(American Federation of Information Processing Societies): Proceedings 1962 Spring Joint Computer Conference, San Francisco, California, May 1-3, Volume 21, National Press, 1962.

Kiril Lubenov Boyanov, "John Vincent Atanasoff: the inventor of the first electronic digital computing", CompSysTech '03 Proceedings of the 4th international conference on Computer systems and technologies: e-Learning, 2003.6.19-20.

Kristian Lum/William Isaac, "To predict and serve?", Significance Volume 13, Issue 5, The Royal Statistical Society, 2016.

Lawrence G. Roberts, "The Evolution of Packet Switching", Proceedings of the IEEE, Volume 66, Issue 11, IEEE, 1978.

M. M. Irvine, "Early Digital Computers at Bell Telephone Laboratories", IEEE Annals of the History of Computing, Volume 23, Issue 3, IEEE, 2001.

Marc A. Shampo/Robert A. Kyle/David P. Steensma, "William Shockley and the Transistor", Mayo Clinic Proceedings, Volume 87, Issue 6, Mayo Foundation for Medical Education and Research, 2012.

Martin Campbell-Kelly, "Origin of computing", Scientific American, Volume 301, Number 3, Springer Nature, 2009.9.

Michael D. Godfrey/D. F. Hendry, "The Computer as von Neumann Planned It", IEEE Annals of the History of Computing, Volume 15, Issue 1, IEEE, 1993.

Robert Koch, "Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?", 2019 11th International Conference on Cyber Conflict (CyCon), IEEE(Institute of Electrical and Electronics Engineers), 2019.5.28.-31.

Roger Dingledine/Nick Mathewson/Paul Syverson, "Tor: The Second-generation

Onion Router", Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13, 2004.

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009.3.

Simon Kemp, "The Global State of Digital in October 2019", We Are Social, 2019.10.23.

Tim Bergin, "Keynote Address: A Short History of Computing or How Did We Get to Aberdeen?", Thomas J. Bergin(ed.), 50 Years of Army Computing From ENIAC to MSRC, the Army Research Laboratory and the U.S. Army Ordnance Center & School, 2000.

나. 독일문헌

[단행본]

Günes Önel, Verfassungsmäßigkeit und Effektivität der „elektronischen Fußfessel", Jahrbuch des Kriminalwissenschaftlichen Instituts der Leibniz Universität Hannover Band 1, Leibniz Universität Hannover, 2012.

Markus Mayer, Modellprojekts elektronischen Fußfessel: Wissenschaftliche Befunde zur Modellphase des hessischen Projekts, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2004.

[논문]

Christian Rückert, "Erlanger Cybercrime Tag 2018: Darknet und Underground Economy", KriPoZ 4/2018, 2018.

Christian Rückert, "Vermögensabschöpfung und Sicherstellung bei Bitcoins", MMR 5/2016, 2016.

Monika Simmler/Sine Selman/Daniel Burgermeister, "Beschlagnahme von Kryptowährungen im Strafverfahren", AJP/PJA 8/2018, 2018.

Abstract

The Criminal Justice Response and Development Strategy in the age of the Fourth Industrial Revolution (II) : The Internet of Things(IoT) and Blockchain

Yun, Jee-young · Chun, Hyun-wook · Kim Jin-mook ·
Ryu, Bu-gon · Lee, Byung-uk · Lee, Won-sang

The Fourth Industrial Revolution optimizes human lifestyles through the convergence of reality and virtuality. It is anticipated that it would be realized through 'Smart Transform' which combines reality-datarizing digital transform and data-realizing analogue transform. The Smart Transform has a virtuous cycle structure in 4 stages: ① Datarization, ② Informatization, ③ Intelligence, ④ Smartization.

In crime prevention, stage I is 'datarization'. The related information is collected through diverse IoT devices such as CCTV and drone as well as 112·119 calls. Stage II is 'informatization' in which tax delinquency information and financial transaction information as well as criminal history including sex offenders' personal information are collected, generating big data. Stage III('Intelligence') is a process to analyze the data collected through artificial intelligence(AI). During this stage, it is able to integrate and analyze crime scene, time and skill-related information and derive the areas and time of high crime probability. Based on these analysis results, Stage IV('Smartization') is performed. In other words, the efficiency of police duties can be enhanced by optimizing crime prevention strategies such as concentration of police force in areas and time of high crime probability. It can also increase a perceived safety index which

represents how much citizens feel safe from crime. The big data generated throughout these processes are used to enhance crime investigation efficiency, enabling optimum investigation. In fact, the digital transform for crime prevention and investigation has already begun, using 'predictive policing(PredPol)' and 'domain awareness system(DAS)'.

During the digital transform of crime prevention and investigation, the IoT enables data collection and information sharing through the networked devices. While conventional CCTV cameras or license plate readers would be installed for the purpose of data collection only, the new technology has made it possible to share data through individual networked devices. It is also possible to extend the purposes or scope of the use of data collected through such digital devices. For example, conventional security CCTV cameras have been used in integrating and managing data on various urban situations such as traffic, disasters and environment. The Smart City Integrated Platform Distribution Project launched by the Ministry of Land, Infrastructure and Transport(MOLIT) targets to build infrastructure needed to realize 'Smart City' through such linkage services.

Meanwhile, blockchain technology has been recognized as one of the promising next-generation engines for growth. However, the utilization of such new technology is still under a review of its possibility as a public sector-led pilot project. In other words, it is too early to say that blockchain technology is widely used in the Republic of Korea and around the world. From a technical perspective, even though blockchain technology is not definitely linked with cryptocurrency, it is cryptocurrency which has led its growth and development. In fact, blockchain has been hardly used in areas other than cryptocurrency. Therefore, most blockchain-related legal policy studies handle cryptocurrency-related issues.

The IoT and blockchain technologies lead network innovation which is the basis of the Fourth Industrial Revolution in terms of network expansion and encryption. Therefore, there is a necessity to search for a criminal justice

response plan. First of all, regarding the IoT, it is required to improve criminal laws in consideration of technological development. Under current laws, the privacy of a resident who experiences an information communications network intrusion is not properly protected in terms of legal benefits. In the past, people's privacy was protected spontaneously when they closed the door and went into their house. However, today's technology development has diversified ways to penetrate into other people's personal spaces. As a result, there has been a strong request for legislative policies for privacy protection. Because an information and communications network intrusion is punished under current laws, there might be some objections against a necessity of criminal policies for the benefits and protection of laws regarding privacy. However, regulations on such information and communications network intrusion have character of administrative criminal law to secure stability of the network. In fact, the victims of privacy invasion are not directly targeted for protection. Therefore, they are not enough as criminal legislation which protects privacy and freedom. Therefore, 'privacy protection from a technical means' should be considered directly in terms of the benefits and protection of the criminal law.

Furthermore, under current crime of arson-related laws, 'setting the fire' is interpreted as 'an act to burn a target object'. However, there is an issue of if such crime of arson can be punished under current laws when a fire occurs due to overheating during the IoT operation. If it is subsumed, such interpretation could be against 'void for vagueness' under the principle of 'nullum crimen, nulla poena sine lege'. Considering the absence of punishment due to the unavailability of laws on new issues which took place as computer became popular, it is not easy to conclude that such crime of arson using the IoT can be punished with teleological interpretation. In awareness of this kind of problem, there have been suggestions that 'setting the fire' should be rephrased into 'setting the fire directly, using a tool or via communication'. In this case, however, as a means such as

a tool and communication is specified, there is a possibility that diverse types of arson acts may not be subsumed. Therefore, rephrasing 'setting the fire' into 'starting a fire' can be an option. Furthermore, arson using the IoT can be committed in the distance with a criminal's safety secured and cause huge damage using the expansible means (the Internet) so that the enactment of separate clauses can also be considered.

Then, the meaning of the criminal use of cryptocurrency from the perspective of criminal law should be analyzed. A court has denied the monetary aspect of cryptocurrency such as Bitcoin. Since cryptocurrency exists in a digital format, it doesn't belong to an object in the civil law or property in the criminal law. Even so, it has property values and is traded in reality so that it can be appraised as property right/benefit or value under criminal and civil laws. Under the civil law, cryptocurrency can be an object of bonds and tradable in exchanges. Therefore, it can be assessed with certain property values or profits under the criminal law as well. Hence, cryptocurrency can be an object of 'enrichment crime' under the criminal law.

Meanwhile, cryptocurrency robbing in an electronic manner is understood as a transfer of funds in an electronic fashion, using computer. Therefore, it can be viewed as fraud by use of computer under the criminal law, not theft. However, there are difficulties in subsuming market manipulation by exchanges as an element of crime under the criminal law. Considering the characteristics of cryptocurrency transactions and exchanges, however, relatively small-scale collusion can cause a big chaos on the market. Therefore, it is required to set provisions on the prohibition and punishment of market abuse such as manipulation and use of material nonpublic information. Furthermore, using multiple users' accounts during market manipulation through collusion can be controlled and punished in accordance with the Act on Promotion of Information and Communication Network Utilization and Information Protection. To further

clarify the illegality of such wrongdoing, however, the related rules should be added to the laws on the issuance and transaction of cryptocurrency.

In May 2018, the Supreme Court ruled that Bitcoin could be confiscated from criminals who obtained the cryptocurrency as a consideration of any criminal act. However, it is hard to conclude that the Supreme Court's decision that Bitcoin can be confiscated under current circumstances that very diverse types of cryptocurrencies are being developed is the complete acceptance of the issuance and transaction of cryptocurrency. However, such ruling can be understood as a sign that there should be legal regulations on the issuance and transaction of cryptocurrency in that its existence and property values have been accepted. In terms of the code of criminal procedure, furthermore, concerning practical cryptocurrency confiscation procedures & methods and confiscated cryptocurrency disposition procedures & rules, legislative assignments are given to researchers and legislators.

Therefore, this study proposes cryptocurrency confiscation and disposition procedures as follows: In terms of confiscation procedures and methods for general objects, they are confiscated in accordance with the Criminal Procedure Act. In other words, the cryptocurrencies confiscated with seizure warrant or voluntary evidence submission and kept by an criminal investigation agency are converted into confiscated articles according to the court's ruling. Unless confiscated yet, they are confiscated by the court's decision. Therefore, cryptocurrency confiscation procedures refer to a discussion on the procedures and methods to confiscate cryptocurrencies. To confiscate cryptocurrencies in a way of account creation and transfer, it is needed to create an account under the name of a court of justice or criminal investigation agency and establish the management procedures. The court's or criminal investigation agency's account and wallet should be kept secure and safe from hacking or a cryptocurrency exchange's insolvency. The transfer process and transfer

fee-handling regulations shall be recorded and documented, and the maintenance procedures should be developed. Even though a cryptocurrency account is created by a court or criminal investigation agency, and the related management procedures are ready, there is no proper means to confiscate cryptocurrencies by force unless they are submitted by the suspect or the accused voluntarily. In this case, an indirect method based on the effects of a search and seizure warrant is the only option. The effect extent of the search and seizure warrant should include the suspect's or the accused's personal records(e.g., PC, mobile phone, memo, etc.). Based on the acquired information, then, the court or criminal investigation agency needs to find the information needed for cryptocurrency transactions.

Regarding the disposition of confiscated cryptocurrencies as well, no clear procedures are available yet. In case cryptocurrency is viewed as a 'marketable object', the confiscated cryptocurrency should be converted into fiat currency through public sales and reverted to the national treasury. If the confiscated cryptocurrencies are recognized as 'marketable securities', on the contrary, they would be reverted to the national treasury. With active consideration of legal policies which do not accept the issuance and transaction of cryptocurrencies, they might be just destroyed. However, because blockchain cannot be altered or destroyed once created, whether or not it is possible to destroy cryptocurrency is uncertain. Since it's been legally accepted that cryptocurrency is an object of confiscation and actually confiscated and disposed of, it is valid to admit it as a marketable object and revert it to the national treasury through public sales. For this, institutional improvement should follow.

In an era of network innovation, the Criminal Proceedings Act should be improved according to the cyber and Internet environments. Most crimes take place in cyber spaces such as darknet. The clue or evidence of crime is also found in a networked cyber space or electronic & telecommunication devices.

Therefore, it is needed to investigate such network and cyber spaces in person. For this, online search or network investigative technique(NIT) should be adopted. Furthermore, it is essential to verify the qualification for access to such cyber spaces and investigation on the darknet. If it requires an act to process and prove certain identity in addition to nondisclosure of an investigator's identity, a part of entrapment or illegal secret investigation, not generally allowed voluntary investigation, could be assessed. Therefore, there should be legal grounds on this issue, and it is needed to introduce a secret investigator system according to the code of criminal procedure. In addition, the fact that the current Criminal Procedure Act is based on a paper-type physical warrant system, and its issuance and presentation regulations are strictly interpreted has been a problem. There should be a measure to keep the lawful and accurate execution of warrants 'legitimacy of proceedings' undamaged and improvement of the Criminal Procedure Act which ensures warrant issuance and presentation in a digital fashion.

From criminal policy aspects, cyber security criteria should be reestablished in advance. It is also required to search for a way to utilize the IoT or blockchain criminal policies. In the IoT, for example, there is a necessity to implement a system which connects devices on a network and makes data transmitted automatically to promote the use of police cam and others. Furthermore, the basis laws which regulate the system operation should be improved. In addition, data protection impact assessment(DPIA) on the IoT should be requested. It is also needed to improve educational programs and introduce a specialized court to enhance the efficiency and expertise of investigation and court decision. At present, regarding cryptocurrency such as Bitcoin, various questions have been raised concerning the criminal laws. In fact, there has been a problem of how to handle criminal proceedings such as investigation and trial. Therefore, it is required to establish legal grounds, investigate the legal definitions of

cryptocurrency and reflect its characteristics and wait until they are legislated. Recently, however, cryptocurrency-related crimes have occurred more frequently. Under these circumstances, it is needed to prevent chaos resulting from the absence of the related laws. For this, a useful guide should be provided to law enforcement officers.

Recently, the news on Google's quantum computer made cryptocurrencies such as Bitcoin collapse because it could disable encryption itself. Even if some experts don't agree with this article, once quantum computer is realized, current object connectivity or encryption could be like 'ENIAC', the world's first electronic computer which was as large as a house. It was released in 1939, and the first Internet network 'ARPANET' was constructed in 1969. In 1973, a cellular system-based mobile phone was developed by Dr. Martin Cooper's Team from MOTOROLA in the U.S. Then, Apple's iPhone was first introduced to the world in 2007, and in nearly 10 years, the world has changed. Furthermore, such technological advances have changed crime patterns and asked for criminal justice responses. The IoT and blockchain are not future technologies anymore. No one knows what other cutting-edge technologies could come through technology development. However, it is anticipated that this report which discussed the two different technologies would make a contribution to the improvement of criminal justice systems and develop national criminal policies more quickly.

연구총서 19-CB-03

제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(II)
: 사물인터넷(IoT)과 블록체인

발 행 | 2019년 12월
발 행 처 | 한국형사정책연구원
발 행 인 | 한 인 섭
등 록 | 1990. 3. 20. 제21-143호
주 소 | 서울특별시 서초구 태봉로 114
전 화 | (02)575-5282
홈페이지 | www.kic.re.kr
정 가 | 10,000원
인 쇄 | (주)케이에스센세이션 02-761-0031
I S B N | 979-11-89908-47-8 93330

• 사전 승인없이 보고서 내용의 무단 전제 및 복제를 금함.