

大韓民国のプライバシー権に関する

NGO 報告書(日本語仮訳)

2019 年 6 月

大韓民国へのプライバシー権に関する特別報告者の公式訪問に向けた韓国市民社会組織ネットワーク

ASUNARO: Action for Youth Rights of Korea, Center for Health and Social Change, HIV/AIDS Activists Network Korea, Korea National Council of Consumer Organizations, Korean Progressive Network Jinbonet, Rainbow Action Against Sexual-Minority Discrimination¹, MINBYUN-Lawyers for a Democratic Society, Open Net Korea, and People's Solidarity for Participatory Democracy

ここに訳出したのは『유엔 프라이버시 특보 방한을 위한 한국 시민사회 보고서』英語版: NGO Report on the Right to Privacy in the Republic of Koreaである。韓国語版と英語版との間には若干の異動があり、日本語に訳す際には英語版を基に、韓国語版も参照した。なお、このレポートの翻訳は、2020年2月29日、3月1日に、本レポートの参加団体でもある進歩ネットワークの代表、オ・ピョンイルさんを招いての講演会に間に合わせるために急遽作成された。そのために、訳文、固有名詞等で十分な推敲がされないまま仮訳として公表するものです。この点をご理解の上お読みください。プライバシー問題に関する網羅的な調査報告であり、ネット監視社会のなかで韓国の運動体がどのような課題に直面し、どのように闘っているのかについての具体的な報告として日本のプライバシー運動、反監視運動にとって貴重な資料でもあります。ぜひご活用ください。(JCA-NET 訳者: 小倉利丸)

1 GongGam Human Rights Law Foundation, Korean Lawyers for Public Interest and Human Rights(KLPH), Labor Party-Sexual Politics Committee, Minority Rights Committee of the Green Party, Daegu Queer Culture Festival, Daajeon LGBTQ Human Rights Group Solongos, QUV; Solidarity of University and Youth Queer Societies in Korea, Social and Labor Committee of Jogye Order of Korean Buddhism, the Korean lesbian community radio group, Lezpa, Rainbow Jesus, Rainbow Solidarity for LGBT Human Rights of Daegu, QIP Queer In Pusan, Busan Queer Festival, Gruteogi : 30+ Lesbian community grocommunity, Seoul Human Rights Film Festival, Seoul Queer Culture Festival Organizing Committee, Korean Anglican Church's Youngsan House of Sharing (Social Minority Life and Human Rights Center), Yeohaengja : Gender non-conforming people's community, PFLAG Korea, Advocacy for LGBTQ's rights to knowledge, Northwest, Collective for Sexual Minority Cultures PINKS, The Korean Society of Law and Policy on Sexual Orientation and Gender Identity, Sinnaneuncenter: LGBT Culture, Arts & Human Rights Center, Unninetnetwork, Lesbian Human Rights Group 'Byunnal' of Ewha Womans University, Open Door in JB, Sexual Minority Committee of the Justice Party, Network for Glocal Activism, LGBTQ Youth Crisis Support Center 'DdingDong', Korean Transgender Rights Organization JOGAKBO, Trans Liberation Front, Chingusai - Korean Gay Men's Human Rights Group, Lesbian Counseling Center in South Korea, Korean Sexual-Minority Culture and Rights Center(KSCRC), Youth PLHIV Community of Korea 'R', Solidarity for LGBT Human Rights of Korea, Solidarity for HIV/AIDS Human Rights Nanuri+

目次

| | |
|---|----|
| 1. 情報捜査機関とプライバシー | 3 |
| 1) 国家情報院 (NIS) | 3 |
| NIS による監視 | 3 |
| 国家情報院のサイバーセキュリティ権限 | 6 |
| 2) 防衛セキュリティ司令部 | 7 |
| 2-1) 防衛セキュリティ司令部によるセウォル号災害の犠牲者家族に対する違法な監視 | 7 |
| 2-2) 防衛セキュリティ司令部の不正な盗聴 | 8 |
| 3) 警察庁 | 9 |
| 3-1) 捜査情報システム | 9 |
| 3-2) 警察の手配車両検索システム | 10 |
| 3-3) CCTV 統合コントロールセンター | 11 |
| 3-4) 国内情報警察 | 17 |
| 2. コミュニケーションの秘密 | 19 |
| 1) パケット盗聴 | 19 |
| 2) 通信確認データ | 21 |
| 3) 通信データの提供 | 24 |
| 4) デジタル情報の搜索と押収 | 27 |
| 3. 住民登録システム | 29 |
| 1) 住民登録番号システム | 29 |
| 2) 強制指紋システム | 31 |
| 3) 本人確認機関システム | 31 |
| 4) 接続情報 (CI) | 32 |
| 4. コミュニケーションの匿名性 | 34 |
| 1) 携帯電話の実名システム | 34 |
| 2) インターネット実名制：公職選挙法、青少年保護法、ゲーム産業法 | 35 |
| 2-1) 公職選挙法上の実名制 | 35 |
| 2-2) 青少年保護法上の実名制 | 36 |
| 2-3) ゲーム産業法実名制 | 36 |
| 5. 個人情報の保護 | 37 |
| 1) ビッグデータと個人情報保護法制 | 37 |
| 2) 個人情報の監督機関 | 38 |
| 3) 消費者の個人情報 | 39 |
| 4) 健康情報とプライバシー権 | 40 |
| 4-1) 医療情報の目的外利用及び提供 | 40 |
| 4-2) 健康情報の保存 | 41 |
| 4-3) 医療機関による個人情報の保護に関する保障措置の義務不履行 | 41 |
| 4-4) 個人の健康情報のオープンデータ化 | 41 |
| 4-5) 健康情報の研究目的利用 | 42 |
| 5) 公共機関の個人情報の捜査機関への情報提供 | 42 |
| 6) 社会保障情報システム | 44 |
| 7) DNA データベース | 45 |
| 6. 労働監視 | 47 |
| 7. 社会的少数者のプライバシー権 | 48 |
| 1) 性少数者 LGBTIQI とプライバシー | 48 |
| 1-1) 軍隊内の合意による同性間の性的行為の犯罪化とプライバシー権 | 48 |
| 1-2) 住民登録番号 | 49 |
| 1-3) HIV/ AIDS とプライバシー権 | 49 |
| 1-4) トランスジェンダーの身体と自律性を確保する権利とプライバシー権 | 50 |
| 2) HIV/ AIDS とともに生きる人々 (PLHIV) とプライバシー | 50 |
| 2-1) 医療現場での PLHIV のプライバシーの侵害 | 50 |
| 2-2) 拘禁施設内 HIV 感染のプライバシー侵害 | 52 |
| 2-3) 青少年 PLHIV のプライバシー | 55 |
| 2-4) PLHIV の労働現場でのプライバシー | 55 |
| 2-5) HIV 感染の兵士と準軍人のプライバシー | 56 |
| 2-6) 国家による PLHIV の私的領域 (性行為) の制御と介入 | 56 |
| 3) 北朝鮮離脱住民のプライバシー権の侵害 | 56 |
| 4) 外国人被疑者のプライバシー権の侵害 | 59 |
| 5) 児童のプライバシー権の侵害 | 60 |
| 5-1) 生活記録簿と全国教育情報システム (NEIS) | 60 |
| 5-2) 学校の学生生活規定や慣習的に行われる個人情報の侵害 | 61 |

| | |
|---|----|
| 5-3) 保育園 CCTV..... | 61 |
| 5-4) 性に関するプライバシーの侵害..... | 62 |
| 5-5) 満 14 歳未満の個人情報の自己決定権..... | 62 |
| 5-6) 青少年のスマートフォン監視法のスマートフォン監視アプリ..... | 63 |
| 6) 性犯罪報道による被害者等のプライバシー権の侵害と被疑事実公表の問題..... | 64 |
| 7) 女性のプライバシー..... | 66 |
| 7-1) 男性インターネットユーザーによる女性のプライバシー権の侵害..... | 67 |
| 7-2) オンラインプラットフォームの女性人身取引..... | 70 |

1. 情報捜査機関とプライバシー

1) 国家情報院 (NIS)

NIS による監視²

A. 背景

1) 市民への捜査

現在の韓国国家情報院法³によると、NIS が処理できる国内情報の範囲は、セキュリティ情報、特に反共産主義、防諜、反テロリズムに関する諜報活動、および国際犯罪組織のリストを作成するためのデータの収集、執筆、および配布に限定されている。したがって、民間企業や市民団体の調査はその任務を超えており、違法である。

●NIS の任務には制限があるが、NIS は、政府に反対または批判する韓国国民を密かに監視している疑いがある。

○独裁政権の時代に、元々 NIS は韓国中央情報局 (KCIA) として設立され、その後再編成され、国家安全保障計画局 (ANSP) に名称が変更された。人権を抑圧し、政治的反対を抑圧するために、さまざまな監視と制御の戦術を採用した。1998 年、金大中大統領政権 (1998～2003 年) は KCIA の活動を縮小し、国内の情報収集に従事することを禁止し、NIS と改名した。

○しかし、2002 年 9 月、第 16 代大統領選挙 (2002 年 12 月) に先立って、ハンナラ党の Lee Seong-hun は、当時大統領秘書室長だったパク・ジウォンがハンファグループによる韓国生命保険の買収に介入したのではないかと疑念が持ち上がった。

○2005 年 7 月、朝鮮日報 (保守派の大手新聞) は、金大中政権時代に ANSP の秘密部隊が市民への不法盗聴に関与していたことを明らかにした。盧武鉉政権下 (2003～2008 年) で、当時の NIS トップのキム・スングュは、ビジネスマン、政治家、ジャーナリスト間の会話を不法に傍受するために使用された秘密監視チーム Mirim チームの活動を調査するよう命じた。調査の結果、このチームは金大中政権とその後の金泳三政権 (1993～1998) で活動していたことが判明した。1997 年の大統領選挙のために賄賂を手配する政治家の会話の盗聴を含む政治スキャンダル X ファイルスキャンダルとして知られるようになった一に加えて、このチームはまた、市民社会グループ、宗教者および政府外のグループリーダーの会話も盗聴していた。

○2008 年 10 月、ある通信社が、NIS 職員が公企業および民間企業に対して市民団体への寄付に関するデータの提供を要求したことを報じた。この行動は、NIS の活動を逸脱したもので、権力の濫用に該当する。この報道の後、市民社会グループは、NIS によるこうした行き過ぎを強く非難した。

2 執筆、参加型民主主義のための民衆連帯 People's Solidarity for Participatory Democracy

3 韓国国家情報機関法第 3 条 (1) NIS は、以下の各サービスを実施するものとする。1 国外の情報と国内セキュリティ情報 [対共産主義、対政府転覆、防諜、テロ対策や国際犯罪組織] の収集・作成と配布。

○2009年6月、Hope Instituteのシニアディレクターであるパク・ウォンスンは、NISがHope InstituteとBeautiful Foundationのスポンサーにデータの引き渡しとスポンサーから降りるよう企業に要請していると主張した。当時弁護士であった、パク・ウォンスン、および彼の事務所に対するNISによる監視疑惑から、市民社会グループに対するさまざまな違法な監視活動が明らかになった。NISは以下のような行動をとった。ソウル市に圧力をかけて環境映画祭の財政支援を停止するよう要請した。大運河プロジェクトに反対する教授グループの調査の実施、四大河川再生プロジェクトの対抗委員会の集団行動を妨害すること、韓国の新首都（世宗市）関連法に関する合意を確保するために地方当局者を交代させること、光州市に圧力をかけて、四川復興プロジェクトを批判した芸術作品を撤去すること、曹溪寺で開催される市民社会イベントのキャンセルを要求するなどである。

○2010年5月、国連の表現の自由に関する特別報告者であるフランク・ラ・ルーはNSIに尾行され、ビデオを撮られる。彼は、こうした行動に抗議した。

○2011年3月、国家安全保障法に違反しているとして捜査中の個人が、何年もの間「パケット盗聴」と呼ばれるネットワーク盗聴の対象となっていたことが判明する。市民社会組織は、被害者とともに、憲法裁判所に申し立てを提出した⁴。NISはGmail (@ gmail.com)でのパケット盗聴を認め、これを継続すると主張した。これは、サーバーが海外にあるからGmailを盗聴することは不可能だというNISの主張が嘘だということを明らかにした。

○2012年12月、NISの元職員は、李明博政権下で世論調査を組織し、世論操作したことを明らかにした。NISサイバーチームのメンバーは、民間の支援者とともに、市民社会組織を含む反対派を批判しながら、李政権を擁護するコメントを投稿した。オンラインで政治的表現を監視し操作しようとしたこのキャンペーンは、NISが国内政治に関与することを禁止している韓国国家情報局法⁵に違反している。

○2013年5月、国会の民主党議員ジン・ソンミは、NISが、授業料半額、福祉政策の拡大、解雇からの復職、および臨時雇用労働者の正社員への転換に関する政策についての情報収集を含む国内の情報収集に関与していると報告した。市民社会グループを含む111人の市民が韓国国家情報局法に違反したNISを告発した。

●NISは、以下の理由から、民間人に対する違法な監視に繰り返し関与しつづけている。

○NISは、国家安全保障法で指定された犯罪を捜査、逮捕、および拘束する権限を持っている。これらの権限は、他の捜査当局から切り離されたままである。

○NISの法的権限の範囲はあいまいであり、法律ではなく大統領令または規則に基づいて権限を行使している。

○NISが国内の監視活動などの人権侵害を犯した場合でも、捜査当局や国内人権団体によるNISから独立した公平な調査への期待は限定的なものでしかない。

○2015年6月、マスコミは、公務員候補者の身元調査を実施するメディアとしての役割を果たす過程で、NISが司法候補者の社会問題に関する思想信条を調査していると報道した。これは国家安全保障に関するものとはいえず、NISはその権限をいちじるしく逸脱して活動していた。

○大統領令「セキュリティ規制」第33条1項（身元調査）の下で、NISは国家安全保障に対する忠誠心、完全性、信頼性を調査するために、公務員候補について身元調査を実施するものとされている。

4 2011年憲法裁判所 HUNMA 165

5 韓国国家情報局法、第9条（政治への関与の禁止）

○他の組織でも公務員資格を評価できるにもかかわらず、33条(1)は引き続き有効とされて、NISはこうした調査を主導している。⁶

○2005年2月17日、韓国国家人権委員会は、NISの活動には法的根拠が欠けており、対処と改善を勧告した。

1) Remote-Control System (RCS) ハッキングプログラムの購入と使用

● 2015年7月、WikiLeaksは、ミラノに拠点を置くハッカーHackingTeamの顧客リストを公開した。この顧客の中には、NISもあり、コンピューター、スマートフォン、モニターに侵入するスパイウェアプログラムであるHackingTeamのRemote Control System (RCS)を購入して使用していた。

○HackingTeamのサイトから漏えいした情報によると、NISは次のことを試みた。モバイルメッセージングアプリケーションであるKakaoTalk、およびSamsung Galaxy 3スマートフォンの国内モデルへの侵入。国内のウイルス対策プログラム(V3 Mobile 2.0など)のバイパス。ソウル工科大学の卒業生リストや、Microsoft Wordファイルを用いた韓国海軍の船舶Cheonanhamに関するアンケートに悪意のあるコードを挿入。

○RCSを使用すると、NISは市民のコンピューターとスマートフォンを監視できる。これにより、プライバシー侵害だけでなく、ハッキングを禁止する情報通信ネットワークの利用と情報保護の促進に関する法律などの法律違反も明らかになった。不正な盗聴を禁止する通信秘密保護法、そして、韓国国家情報局法における権力濫用の規定にも違反している。

○2015年7月30日、合計2,786人と41の市民社会グループがNISをハッキング容疑で提訴し、この件は捜査中である。

●NISには、国内問題に介入する権限と捜査権限があるため、違法なハッキングと監視活動に従事し続けている。NISの捜査機関の権限と国内情報収集の権限を分離し、後者の権限を他の機関に移す対処をすべきである。

2) 市民と公共の安全の保護のためのテロ対策法(テロ対策法としても知られる)

●10年以上前の2001年から審議されてきた反テロ法案が2016年3月2日、第19回国会において可決された。

○2001年、NISは2002年のワールドカップに先立ち、反テロ法案を国会情報委員会に提出した。しかし、市民社会組織と国家人権委員会の反対により、これは失敗した。

○2003年、別の法案が提出され、NISからも支持を得た。これは、反韓国感情の高まりと、韓国によるイラクへの軍隊の追加配備に伴うテロの脅威の増大への懸念に動機付けられたものだ。しかし、この法案への反対運動が続き、法案は期限満了により最終的に断念された。

○2015年11月、パリのイスラム過激派グループによるテロ攻撃を受けて、朴槿恵政権(2013～2017年)は反テロ法の成立を求めた。2016年3月、多くの市民と市民社会グループの反対にもかかわらず、反テロ法案が国会本会議で可決された。

●反テロ対策法の主な内容は、NISが率いる「テロ対策センター」を設立することにあった。

●法律の実際的な内容には、テロリズムの包括的な概念の導入が含まれ、NISが人々の財務記録や通信に関する情報を収集することを許可している。したがって、この法律は、国家による監視の包括的な権限をNISに無制限に付与している。

●2016年3月2日にテロ対策法が可決された後、朴政権は法律の施行に動いた。2016年5月、セヌリ党のイ・チョウル議員がテロ対策法案を提案し、続いて2017年1月に国家サイバーセキュリティ法案

6 保安規則、第33条(1) 国家情報局長は国家安全保障に対する忠誠心と信頼性を調査することを指導する。

が提出された。国家サイバー安全保障法案の主な内容は、国家情報院のサイバーセキュリティ権限を法的に保障し、既存の国家情報通信網への国家情報院のサイバーセキュリティ権限をキャリア・ポータルなどの民間部門に拡大することである。これにより、NIS が個人情報の収集を含む、民間部門の情報および通信ネットワークに関する監視および情報収集に関与する可能性への懸念が生じることになる。

B 勧告

NIS が情報機関としての本来の役割を果たすために、NIS を国際的な情報収集機関に再編成すること。

- 他の政府部門に対する統制を実行するための基盤となっている NIS の計画および調整権限を廃止する。

- 国内の政治的介入の基礎を提供する NIS の国内情報収集サービスを廃止する。

- 刑事捜査権限を警察と検察に移す。

- 心理戦の機能と心理戦実行組織の廃止

- サイバーセキュリティ権限を他の機関に移管する。

- NIS への監督権限を持つ唯一の組織である国会情報委員会の役割を強化する。

- 反対テロ法の廃止。

C 責任官庁と機関

- 国家情報院(NIS)

国家情報院のサイバーセキュリティ権限⁷

A. 背景

- NIS は、情報通信ネットワーク上のサイバーセキュリティに対して計り知れない力を持っている。

- 国家のサイバーセキュリティの全体的な管理と調整

- 公共エリアの主要な情報および通信ネットワークインフラストラクチャのサイバーセキュリティの全体的な管理⁸

- サイバー危機の防止と主要な通信インフラストラクチャを含む公共情報および通信ネットワークの攻撃の検出⁹

- サイバー侵入の捜査と脅威に関する情報の分析¹⁰

⁷ 執筆 韓国の進歩的なネットワーク Jinbonet

⁸ 情報通信インフラの保護に関する法律に従って、NIS は「情報通信インフラの保護委員会」の下で「公共部門を担当する作業委員会」を握り、管理組織が重要な情報を保護する対策を実施しているかどうかを、公共部門の通信インフラストラクチャ（第 5-2 条（1））、保護対策の策定に関するガイドラインの確立（第 6-4 条）、技術サポートの提供（第 7-1 条）、脆弱性の分析と評価に関する基準の決定（第 9-4）、およびその他を確立してチェックしている。

⁹ 国家情報院法のホームページによると、常に主要な全国のコンピュータネットワークとシミュレーショントレーニングを実施している。

http://eng.nis.go.kr/EAF/1_7.do

¹⁰ サイバー侵入の捜査と脅威に関する情報の分析。ハッカーによる攻撃を含め、政府/公共組織に対するサイバー侵入が発生した場合、NIS はインシデントを捜査し、その原因を確認し、サイバー脅威に関する情報分析を実施する。NIS はまた、国内外の関連機関と協力関係を確立している。（http://eng.nis.go.kr/EAF/1_7.do）

○セキュリティ検証スキーム：国家および公的機関に導入された情報保護システムの安全性を検証するシステム¹¹

○韓国語暗号モジュール検証プログラム¹²

●ただし、法的根拠はなく、NIS が公開情報および通信ネットワークインフラストラクチャのサイバーセキュリティに関する権限を持っているのは、情報機関としては適切とはいえない。NIS の歴史的な観点から見ると、民間人の動静をかきまわることの特徴とする活動方法を権限の悪用による民間に対する査察など、サイバースペースを介した違法な情報収集と査察には大きなリスクがある。

●NIS のサイバーセキュリティの権限には法的根拠がない。国家情報院法には、こうした権限についての明白な規定がない。国家サイバーセキュリティに関する規制は、上位の法律に基かない大統領令にすぎない。

情報通信インフラストラクチャの保護に関する法律によれば、NIS は「情報通信インフラストラクチャ保護委員会」の下で「公共部門作業委員会」の一部を担っているが、公共部門の情報通信インフラストラクチャとサイバーセキュリティに関するタスクに限定されている。そうであるとしても、NIS が情報機関としてこれらのタスクを担当する必要はない。

●NIS は、情報公開および通信ネットワークのサイバーセキュリティを担当する一方で、収集された個人データの処理に関する規制はない。

●サイバー危機の防止や攻撃の検出など、NIS が日常のネットワーク監視タスクを担当するのは適切ではない。というのは、情報機関によるプライベートな監視をコントロールし情報収集に対するセーフガードがないからである。

●NIS は、サイバー侵入の捜査と脅威に関する情報分析という使命を遂行しているが、令状を要件として実施されていない。NIS が暗号化モジュールを検証するためには、企業はソースコードを提出する必要がある。これによって NIS は暗号化市場をコントロールすることができるが、コードの信頼性を損なう可能性がある。

B. 勧告

公共情報通信ネットワークのサイバーセキュリティは必要だが、NIS が情報機関として活動するのは不適切である。政府は、公共情報および通信ネットワークのサイバーセキュリティに関する権限を他の機関に移すべきである。

C. 担当省庁

●国家情報機関

●青瓦台、国家安全保障局

2) 防衛セキュリティ司令部

2-1) 防衛セキュリティ司令部によるセウォル号災害の犠牲者家族に対する違法な監視¹³

A. 背景

11 電子政府法第 56 条および公的機関によるアーカイブの管理の施行令第 5 条

12 国および公的情報やおよび通信ネットワークで使用する暗号モジュールを検証するシステム。電子政府法の施行令第 69 条および暗号モジュールのテストと検証のガイドライン。

13 執筆 MINBYUN-Lawyers for a Democratic Society

- 2014年4月16日、韓国のフェリー、セウォル号が韓国の南西海で沈没し、304人の乗客（主に学生）が死亡または行方不明になった（「セウォル号大事故」）
- セウォル号大事故の犠牲者の家族は政府にその真実を調査するよう要請したが、大事故の明確な原因は明らかにされておらず、大事故の責任者は処罰されていない。処罰されたのは1名の政府職員のみである。
- 朴槿恵政権は、特別調査委員会を強制的に解散させるなど、災害に関する調査と疑惑のある人物に対する処罰を組織的に妨害した。
- 現在の政権下の民間および軍の役人で構成された合同調査チームは、2014年4月17日、災害の翌日、国防保安部隊が部下に被害者家族の状況をスパイするよう命令したことを発見した。
- 防衛セキュリティ司令部は、生年月日、携帯電話番号、インターネットポータルアクティビティ、個人のブログアドレス、メールアドレス、インターネット経由で購入した商品のリスト、家族の身分証明書と預金通帳の写真などを違法に収集した。防衛セキュリティ司令部は、部下に命令して、ネット上で家族の一員になりすましてスパイすることなども行なった。
- 特に、防衛セキュリティ司令部は、家族を「親北朝鮮」に分類するなどの国家犯罪を行い、家族に関する虚偽の事実をメディアで広めた。
- 2018年の防衛省の特別調査チームの発表によると、公式に起訴された容疑者は5人で、残りの4人は起訴猶予とされた。

B. 勧告

- 防衛セキュリティ司令部による違法監視に関する徹底的な調査を実施し、監視の責任があるとされる人物を処罰すること。
- 独立した監督システムの確立など、違法な監視の再発を防ぐための具体的な計画を準備すること。
- 家族の真実、正義、および賠償の権利を確保する必要がある。

2-2) 防衛セキュリティ司令部の不正な盗聴¹⁴

A. 背景

- 防衛セキュリティ司令部は、国防省の情報機関であり、軍事情勢、軍事安全保障と防諜、そして犯罪捜査に関する情報収集を目的としている。しかし、朴槿恵政権時代の2014年のセウォル号沈没直後、この機関による行方不明者の家族への査察と、弾劾を求めるろうそく集会が行なわれていた2017年の戒厳令準備は、社会的な論争を巻き起こした。この論争により、この機関は2018年9月に解散し、防衛安全保障支援司令部に再編成された。
- 2019年4月8日、平和民主党の議員であるチョン・ジョンベが防衛セキュリティ司令部作成の<セウォル号 TF>の日報を公開し、この機関が一般市民を違法かつ無差別に電話盗聴していたことが明らかになった。
- 2014年6月10日から2014年7月22日まで、ソウル、ハナム、ソンナム、ヨンイン、アンソンの裁判所の承認なしに、独自のモバイル監視機器と科学・ICT・将来計画省（現在は科学・ICT省）の下にある電波管理局の電波管理所を使用して、私信の内容を違法に聞きとり、記録した。タクシー、病院、遊び場、映画館での個人的な会話が無差別に盗聴されたことが判明した。¹⁵

¹⁴ 執筆 Korean Progressive Network Jinbonet

¹⁵ JTBC、セウォルフェリー災害直後、民間人の違法監視...映画館、レストランなどでの無差別盗聴
2019.4.8

●当該機関のこのような活動は、セウォル号の所有者ユ・ビョンオンを捜査することを目的としていたが、当該機関の義務の範囲を逸脱しており、裁判所の承認なしの盗聴は通信秘密保護法に違反して違法である。

●電波管理所の使命は、「電波法第 49 条から第 51 条に従って混乱を取り除くことを含め、電波の秩序を維持するために電波を監視する」ことにある。当該機関は検察への無線管理サービスの支援を受けて盗聴することを示唆し、最高検察庁は実際にこの機関との協力を求める考えをもっており、これは、検察と当該の省の関与を意味しており、違法な活動とそれらを取り締まる義務を放棄した。

●2019 年 4 月 15 日、市民社会組織は、防衛セキュリティ司令部を含む違法な監視をした者を検察に告発した。

B. 勧告

●防衛セキュリティ司令部による不法盗聴の徹底的な調査を実施し、関連する職員を処罰すること。

●当該機関がその権限を超えて民間人を違法に捜査およびスパイすることを防ぐために、独立した監督システムを確立すること。

C. 担当省庁

●防衛安全保障支援司令部（旧防衛セキュリティ司令部）

●科学・ICT 省（前科学・ICT・未来計画省）

●電波管理所

3) 警察庁

3-1) 捜査情報システム¹⁶

A. 背景

●2017 年の政府機関の調査のデータによると、警察は 83 のデータベースシステムを通じて約 37 億件を保有している¹⁷。しかし、国会でさえ現状を正確に把握することはできていない。

●収集された証拠システムなど、警察のほとんどのデータベースシステムには、その設置と運用に関する特別の法的根拠がない。特別の法的根拠があるのは、刑事司法情報システムや DNA の識別情報システムなど、ごく少数のシステムだけである。

●これらの警察システムは法的な根拠なしに運用され、個人データは他の目的に使用されたり、異なるシステムに接続されることが可能であり、より一層自動識別の対象になりやすくなっている。

●その結果、大規模な警察の個人情報データベースシステムおよび個人データの処理を規制することはできていない。一般の人々は、警察システムによって何が収集されているのかも知らない。また、個人情報へのアクセス、修正、削除、停止の権利を行使することもできない。

●1999 年、社会組織の活動家は、法的根拠のない 17 歳以上のすべての市民からの 10 指の指紋データベースの設立と運用に反対して、憲法で定められた申し立てを提出した。しかし、2005 年に憲法裁判所は、警察法および警察官の職務遂行に関する法律に「治安情報の収集、作成、および配布」が義務の範囲として含まれていることを理由に、申し立てを棄却した。¹⁸

16 執筆 Korean Progressive Network Jinbonet

17 NEWSIS. (2017). 警察、37 億件の個人情報を確保... 犯罪情報システムで 27 億件を確保。

http://www.newsis.com/view/?id=NISX20170114_0000117579 [15 May 2019]

18 憲法裁判所, May 26, 2005, 99Hun-ma513, etc.

●その後、裁判所および憲法裁判所は、あらゆる種類の警察システムに対しても同様の立場を維持している。2010年社会団体の活動家が、具体的な法的根拠なしに警察がすべての被疑者、参考人はもちろん、被害者の情報を膨大に収集し、データベースシステム（CIMS：Crime Information Management system）を構築、運用することに対して損害賠償訴訟を提起した。しかし、裁判官は原告敗訴の判決を出した。¹⁹

●2018年、警察改革委員会は、根拠、手続き方法、および統制に関して警察情報システムを設置・運用する別個具体的な法的根拠を確立するよう勧告した。さらに、警察の内外に開かれていない情報システムの設置と運用を禁止することを勧告した。ただし、こうした改善は実施されていない。

B. 勧告

●警察が運営している個人情報のデータベースシステムにおいては、個人情報を処理する目的、手順、方法、および制御装置を具体的に規定された法律に基づいて規制を受けるべきであること。

●警察の個人情報データベースシステムに関する独立した第三者機関の監督を採用すること。

C. 担当省庁

●警察庁

3-2) 警察の手配車両検索システム²⁰

A. 背景

●車両検索システムは、2015年10月に出された警察独自の運用ガイドライン²¹に従ってのみ運営されている。このシステムは、犯罪を犯していない人々（1日あたり2,400万人以上）の運転ルート情報を収集し、30日間これらの記録を保存する。さらに、警察は宅配便会社 CJ Korea Express と覚書 MOU を締結しているため、CJ からブラックボックス映像を入手することができる。²²

●警察は人々の個人情報の大規模収集と蓄積を行っているが、こうしたデータは、一般的な規制（たとえば、警察の情報収集、作成、配布²³または法的根拠のない警察自身のガイドラインに従うだけで慣習的に処理されている。特に、指名手配者の緊急検索の場合、車両検索システムは「類似検索」が可能のように設計されており、ナンバープレートから2文字または数字を入力するだけで済む。求められている車両番号と類似のライセンス番号を持っている場合、このシステムがその人のルートを開示する可能性がある。2014年、304人の命（主に子供）を奪ったセウォル号の運航海運会社の会長である Yoe Byungeun を検索したとき、警察は、スマートフォンのナビゲーションアプリケーションを介して、特定の地名を検索した一般市民の個人情報までランダムにチェックした。2014年にも同様のことがあり、警察は手配車両検索システムを使用して鉄道労働組合のストライキのメンバーを追跡した。このなかには、ストライキに参加している人だけでなく、参加者の叔父や叔母など一家親戚の車まで三ヶ月間どの地域で運転されていたかを検索した。

19 最高裁判所, October 25, 2012, 2012Da12641

20 執筆、People's Solidarity for Participatory Democracy

21 [https://www.police.go.kr/cmm/fms/FileDown.do?](https://www.police.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000083492&fileSn=1&bbsId=B00000032)

[atchFileId=FILE_000000000083492&fileSn=1&bbsId=B00000032](https://www.police.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000083492&fileSn=1&bbsId=B00000032)

22 <http://news.donga.com/3/all/20160616/78695611/1>（訳注：ブラックボックスとは映像や草稿ルートなど運転時の状況を証拠能力のある形で記録できる装置。）

23 Police Act, Article 2(4) (Scope of Job) and the Act on the Performance of Duties by Police Officers, Article 2(4) (Scope of Job)

- このように、何の法的規制なしの手配車両検索システムは、「地引き網式」捜査や無作為の照会に悪用される可能性があり、国民の私生活を監視、制御する強力な監視手段になりうる。
- 個人情報の収集・作成および配布は、「法律の特別な規制」があるか職務遂行のために「やむおえない」場合にのみ許可されるべきである。²⁴しかし、警察の現在の手配車両検索システムは、比例性の原則に違反している。
- これに対して、市民社会は、シビリアンコントロール、情報システムの運用状況に関する報告書を作成し国会がチェックし、情報システムの閲覧、検索などのノード（ローカルエリアネットワーク）の手順の規制などの法的装置が必要であると主張している。

B. 勧告

- 警察による個人情報の収集には、開かれた議論と国会での立法による規制の策定が必要である。さらに、車両検索システムの法的根拠を確立する必要がある。これには、システムのシビリアンコントロール、システムの運用状況に関する年次報告書の作成、国会による報告書、および手続き管理規則が含まれる。

C. 担当省庁

- 行政安全部/警察庁

3-3) CCTV 統合コントロールセンター²⁵

A. 背景

- 地方自治体によって設置および運用されている CCTV 統合コントロールセンターは、すべての画像を 1 か所で確認できるように、さまざまな公的機関の CCTV を接続することが可能である。

<Installation Status of CCTV Integrated Control Center>

(Unit: the number of cities and towns)

| Category | Recent statistics | | | | | | | |
|---|-------------------|------|------|------|------|------|------|------|
| | ~2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
| Number of CCTV Integrated Control Centers | 26 | 34 | 27 | 33 | 29 | 22 | 19 | 18 |
| Total | 26 | 60 | 87 | 120 | 149 | 171 | 190 | 208 |

※2010 figures include up to the number before 2010

- 行政安全部によると、2017 年末現在、韓国の 226 の地方自治体の合計 208（92％）が統合コントロールセンターを設置し、運用している。行政安全部は将来、すべての地方自治体に統合管理センターを設立する支援を予定しており、このプロジェクトは束草、平昌、華川、陽陽、珍島を含む 5 つの都市で現在進行中である。

²⁴ プライバシー法 15 条(2)No2、No3。

²⁵ 執筆 People's Solidarity Participatory Democracy

- CCTV 統合コントロールセンターは、地方自治体によって設置された CCTV を接続して、映像を確認および保存する。警察官は、ほとんどの統合コントロールセンターで犯罪対応のために働いている。
- 警察庁の 2017 年のデータによると、警察と地方政府（CCTV 統合コントロールセンター）の間でビデオ情報共有システムが確立された。CCTV 統合制御センターからの映像は、警察署の危機管理室で見ることができる。

| Order | National Police Agency | Police Station | CCTV Integrated Control Center | Location | The number of systems accessible by PC |
|-------|----------------------------------|--------------------------------|-------------------------------------|-------------------------------|--|
| 1 | Seoul Metropolitan Police Agency | Seoul Yongsan Police Station | Yongsan Integrated Control Center | Police Station Situation Room | 1 |
| 2 | Seoul Metropolitan Police Agency | Seoul Seongbuk Police Station | Seongbuk Integrated Control Center | Police Station Situation Room | 1 |
| 3 | Seoul Metropolitan Police Agency | Seoul Seongdong Police Station | Seongdong Integrated Control Center | Police Station Situation Room | 1 |
| 4 | Seoul Metropolitan Police Agency | Seoul Gangbuk Police Station | Gangbuk Integrated Control Center | Police Station Situation Room | 1 |
| 5 | Seoul Metropolitan Police Agency | Seoul Geumcheon Police Station | Geumcheon Integrated Control Center | Police Station Situation Room | 3 |
| 6 | Seoul Metropolitan Police Agency | Seoul Jungnang Police Station | Jungnang Integrated Control Center | Police Station Situation Room | 1 |
| 7 | Seoul Metropolitan Police Agency | Seoul Gangdong Police Station | Gangdong Integrated Control Center | Police Station Situation Room | 2 |
| 8 | Seoul Metropolitan Police Agency | Seoul Jongam Police Station | Seongbuk Integrated Control Center | Police Station Situation Room | 1 |

| | | | | | |
|----|----------------------------------|--------------------------------|-------------------------------------|-------------------------------|---|
| 9 | Seoul Metropolitan Police Agency | Seoul Yangcheon Police Station | Yangcheon Integrated Control Center | Police Station Situation Room | 1 |
| 10 | Seoul Metropolitan Police Agency | Seoul Songpa Police Station | Songpa Integrated Control Center | Police Station Situation Room | 1 |
| 11 | Seoul Metropolitan Police Agency | Seoul Bangbae Police Station | Seocho Integrated Control Center | Police Station Situation Room | 1 |
| 12 | Seoul Metropolitan Police Agency | Seoul Dobong Police Station | Dobong Integrated Control Center | Police Station Situation Room | 1 |

| | | | | | |
|----|---|--------------------------------|---------------------------------------|-------------------------------|---|
| 20 | Incheon Metropolitan Police Agency | Incheon Gyeyang Police Station | Gyeyang -gu Integrated Control Center | Police Station Situation Room | 1 |
| 21 | Incheon Metropolitan Police Agency | Incheon Ganghwa Police Station | Ganghwa-gun Integrated Control Center | Police Station Situation Room | 2 |
| 22 | Incheon Metropolitan Police Agency | Incheon Yeonsu Police Station | Yeonsu-gu, Incheon Free Economic Zone | Police Station Situation Room | 2 |
| 23 | Gyeonggi Nambu Provincial Police Agency | Suwon Jungbu Police Station | Suwon-si Integrated Control Center | Police Station Situation Room | 2 |
| 24 | Gyeonggi Nambu Provincial Police Agency | Suwon Nambu Police Station | | Police Station Situation Room | 2 |
| 25 | Gyeonggi Nambu Provincial Police Agency | Suwon Seobu Police Station | | Police Station Situation Room | 2 |
| 26 | Gyeonggi Nambu Provincial Police Agency | Anyang Dongan Police Station | | Police Station Situation Room | 1 |
| 27 | Gyeonggi Nambu Provincial Police Agency | Anyang Dongan Police Station | Anyang-si Integrated Control Center | Police Station Situation Room | 1 |

| | | | | | |
|----|---|------------------------------|---|-------------------------------|---|
| 28 | Gyeonggi Nambu Provincial Police Agency | Anyang Manan Police Station | ontrol Center | Police Station Situation Room | 2 |
| 29 | Gyeonggi Nambu Provincial Police Agency | Gunpo Police Station | Gunpo-si Integrated Control Center | Police Station Situation Room | 1 |
| 30 | Gyeonggi Nambu Provincial Police Agency | Bucheonsosa Police Station | Bucheon-si Integrated Control Center | Police Station Situation Room | 1 |
| 31 | Gyeonggi Nambu Provincial Police Agency | Bucheonwonmi Police Station | | Police Station Situation Room | 1 |
| 32 | Gyeonggi Nambu Provincial Police Agency | Bucheonojeong Police Station | | Police Station Situation Room | 1 |
| 33 | Gyeonggi Nambu Provincial Police Agency | Gwang Myeong Police Station | Gwang Myeong-si Integrated Control Center | Police Station Situation Room | 1 |
| 34 | Gyeonggi Nambu Provincial Police Agency | Ansan Danwon Police Station | Ansan-si Integrated Control Center | Police Station Situation Room | 1 |
| 35 | Gyeonggi Nambu Provincial Police Agency | Ansan Sangnok Police Station | | Police Station Situation Room | 1 |

| | | | | | |
|----|---|-------------------------------|---------------------------------------|-------------------------------|---|
| 36 | Gyeonggi Nambo Provincial Police Agency | Siheung Police Station | Siheung-si Integrated Control Center | Police Station Situation Room | 1 |
| 37 | Gyeonggi Nambo Provincial Police Agency | Hwasung Dongbu Police Station | Osan-si Integrated Control Center | Police Station Situation Room | 1 |
| 38 | Gyeonggi Nambo Provincial Police Agency | Yongin Dongbu Police Station | Yongin-si Integrated Control Center | Police Station Situation Room | 1 |
| 39 | Gyeonggi Nambo Provincial Police Agency | Yongin Seobu Police Station | | Police Station Situation Room | 4 |
| 40 | Gyeonggi Nambo Provincial Police Agency | Gwangju Police Station | Gwangju-si Integrated Control Center | Police Station Situation Room | 1 |
| 41 | Gyeonggi Nambo Provincial Police Agency | Gwacheon Police Station | Gwacheon-si Integrated Control Center | Police Station Situation Room | 2 |
| 42 | Gyeonggi Nambo Provincial Police Agency | Hanam Police Station | Hanam-si Integrated Control Center | Police Station Situation Room | 1 |
| 43 | Gyeonggi Nambo Provincial Police Agency | Icheon Police Station | Icheon-si Integrated Control Center | Police Station Situation Room | 1 |

| | | | | | |
|----|---|-------------------------------|--|-------------------------------|---|
| 44 | Gyeonggi Nambu Provincial Police Agency | Kimpo Police Station | Kimpo-si Integrated Control Center | Police Station Situation Room | 1 |
| 45 | Gyeonggi Nambu Provincial Police Agency | Yeoju Police Station | Yeoju-si Integrated Control Center | Police Station Situation Room | 2 |
| 46 | Gyeonggi Bukbu Provincial Police Agency | Dongducheon Police Station | Dongducheon-si Integrated Control Center | Police Station Situation Room | 1 |
| 47 | Gangwon Provincial Police Agency | Wonju Police Station | Wonju city information center | Police Station Situation Room | 1 |
| 48 | Gangwon Provincial Police Agency | Jeongseon Police Station | Jeongseon-gun Integrated Control Center | Police Station Situation Room | 1 |
| 49 | Gangwon Provincial Police Agency | Hongcheon Police Station | Hongcheon-gun Integrated Control Center | Police Station Situation Room | 1 |
| 50 | Jeonbuk Provincial Police Agency | Jeonju Wansan Police Station | Jeonju-si Integrated Control Center | Police Station Situation Room | 2 |
| 51 | Jeonbuk Provincial Police Agency | Jeonju Deokjin Police Station | | | |
| 52 | Jeonbuk Provincial Police Agency | Wanju Police Station | Wanju-gun Integrated Control Center | Police Station Situation Room | 1 |
| 53 | Gyeongbuk Provincial Police Agency | Yecheon Police Station | Yecheon Integrated Control Center | Police Station Situation Room | 1 |

| | | | | | |
|----|-------------------------------|----------------------------|--------------------------------|-------------------------------|---|
| 54 | Jeju Provincial Police Agency | | Jeju Integrated Control Center | 112 General Situation Room | 1 |
| 55 | Jeju Provincial Police Agency | Jeju Dongbu Police Station | | Police Station Situation Room | 1 |
| 56 | Jeju Provincial Police Agency | Jeju Seobu Police Station | | | 1 |
| 57 | Jeju Provincial Police Agency | Jeju Seogwi Police Station | | | 1 |

●市民の個人情報のプライバシーを侵害する可能性があるにもかかわらず、すべての CCTV 映像を収集および保存する統合コントロールセンターは、個人情報保護法その他の法律に運用根拠がない。さらに、CCTV 画像は多くの場合、本来の意図以外の目的で使用され、犯罪捜査のために警察に提供される。2018 年 5 月 5 日、韓国国家人権委員会は、行政安全部大臣に「憲法の基準を遵守するための CCTV 統合管理センターの運用に関する法的基盤を確立し、法制定による個人のビデオ情報の使用についての詳細を規定すること」とした。²⁶

●現在の個人情報保護法の下では、CCTV Integrated Control Center の法的根拠はない。

●個人の画像情報を保護するために提案された法律の諸問題

○国家人権委員会は、行政安全部によって提案された個人の画像情報を保護する法律が統合管理センターに明示的に言及しておらず、人権侵害を最小限に抑えるための法律としても十分ではないと指摘した。

B. 勧告事項

●CCTV 統合制御センターの運用に関する目的、要件、手順、および他の機関とのリアルタイムでの映像の共有に関する規定を定め、そのような共有のための規制手順を確立するために、厳格な法的規定が必要である。

C. 担当省庁

行政安全部、警察庁

3-4) 国内情報警察²⁷

A. 背景

●韓国の警察庁は、警察法第 3 条（5）および警察官職務執行法第 2 条（4）の包括的な認可規則に基づく犯罪捜査とは無関係な情報を収集する部門を運用してきた。これは「公安に関する情報の収集、準

²⁶ 国家人権委員会常任委員会決定 2015.5.3.「CCTV 統合制御センターの設置と運用の改善のための勧告事項」

²⁷ 執筆 Korean Progressive Network Jinbonet

備、および配布」である。さらに、警察の国内情報機関は、政府を批判する人々を監視し、与党の支配のための政治的な報告を作成している。

●メディア報道²⁸によると、2018年の情報警察の活動の大部分は、大統領府に送信された「ポリシーデータ」の作成だった（22.5%）。これに外国の協力（20%）と議会工作（12.3%）が続き、本来の仕事である犯罪情報は1.3%にしかない。

●上記の数値は、「公共の安全に関する情報」としてのリスク防止や犯罪捜査に必要な情報の違法かつ広範な収集の証拠である。

●情報警察は、各市民から情報を収集して使用している。その過程で、個人のプライバシーに対する無謀な侵入があり、データ主体自身も監視対象になっているかどうかを認識する方法がない。

●情報警察による市民監視の証拠が次々と明るみに出ている。2019年5月14日「警察による人権侵害調査チーム」によると、サムスン電子サービスの労働者ヤム・ホースク²⁹は、労働組合に対する企業の弾圧に抗議するスト中に自殺した。彼の死後、情報警察は会社と共謀して労働者の家族と知人を監視した。³⁰さらに、安山のダンウォン高校からジンドのペンモク港までのウォーキングツアーで、セウオル号大事故の遺族を警察官が尾行しているのが発見された。³¹

●また、市民だけでなく州職員や議員への監視も実施されている。国内情報警察は、各議員の性格を分析し、政府と与党が対応すべき方向を提案することにより、政権にとって面倒な人物を監視・分析してきた。

●国内情報警察は、選挙に積極的に関与してきた。2011年、情報警察は、ソウル市長選挙で与党の候補者を当選させるために、他の候補者の動静をチェックし、関係する市民グループを調査し、選挙状況を分析し、選挙前後の国政を担う大統領府の計画を提案することにより、明らかに政治的な動きをした。³²朴槿恵政権下で、情報警察は、与党議員の性格を分析することにより、与党議員を警察寄りの立場に変える戦略を模索した。³³

●李明博政権の時代に、情報警察は自分たちを政府の「前衛」と呼び、政府の成功を願って政治指導者の見返りとして政府に彼らを利用するように求めた。さらに、彼らは文書のなかで感觸の地位を主張した。³⁴その文書では、「警察は、どの政府よりも李明博政権の成功を祈っている」と述べられている

28 KBS(2019), Criminal Information is only 1.3%.... "Cheong Wa Dae opposes the recommendation to abolish the intelligence policy",

<http://news.kbs.co.kr/news/view.do?ncd=4149872&ref=A> , [17, May, 2019]

29 The Kyunghyang Shinmun (2019), Police Acted as "Agent for Samsung" in the case of Yeom Ho-Seok,

http://english.khan.co.kr/khan_art_view.html?artid=201905151627557&code=710100 [21, May 2019]

30 Hankyoreh (2019). In the late Yeon Ho Suk case, the intelligence police acted as Samsung's hands from start to finish.

http://www.hani.co.kr/arti/society/society_general/893837.html [17, May, 2019]

31 Hankyoreh (2014). [Single] The plainclothes police are detected again while following the families of the Sewol victims.

https://www.hani.co.kr/arti/society/society_general/646775.html [2019.5.17]

32 Hankyoreh (2019), [Single] Domestic Intelligence Police, Na Kyoung-won's self-appointed campaign during the Seoul mayoral race,

http://www.hani.co.kr/arti/society/society_general/892328.html [17 May 2019]

33 Hankyoreh (2019), The Domestic Intelligence Police, Make 'Party Management Card' and inspect personal connections,

http://www.hani.co.kr/arti/society/society_general/881576.html [17 May 2019]]

34 The Kyoungyang Shinmun (2019), Police under the Lee administration, claiming to be

る。さらに、この文書では、「警察の高官の大多数が李明博の選挙運動で活動し、現場の警察官にも影響を与えた」ことが明かになっている。

B. 勧告

- 犯罪捜査とは関係のない「国内情報警察」を廃止し、国内情報警察が実施した市民の監視と選挙の干渉について徹底的な事実調査を実施し、責任者を処罰すること。

- 犯罪捜査のための警察の情報活動の場合、独立機関による管理と監督を強化する必要がある。

C. 担当省庁

- 警察庁

2. コミュニケーションの秘密

1) パケット盗聴³⁵

A. 背景

- パケット盗聴には、特定のインターネット回線を介して交換されるネットワークトラフィックの傍受と監視が含まれる。

- 現在のパケット盗聴技術では、ターゲット情報（犯罪に関連する情報など）を他の種類の一般情報と区別することはできない。これは、通信秘密保護法の要件を満たす上での課題だ。このような技術的な制約があるにもかかわらず、裁判所は捜査機関の盗聴を許可しており、裁判所の許可を得て、調査機関は情報収集の手段としてパケット盗聴を採用する場合がある。

- パケット盗聴の全容は不明のままである。2018年には、NISは盗聴の99.4%³⁶を担当していたと推測されることから、パケット盗聴もNISが利用している監視手法であると想定できる。

- 憲法裁判所 2018. 8. 30. 2016 HUNMA 263「犯罪の疑いのない者を含む大多数の者が1つのインターネット回線を共有しているため、パケット盗聴は裁判所が許可する範囲を逸脱している。容疑者のデータだけでなく、犯罪の疑いのない人のデータも収集される。したがって、捜査機関が取得した個人通信データの量を、インターネット盗聴による監視などの他の通信制限措置と比較することはできなかった。インターネット盗聴に関しては、第三者の情報または犯罪捜査に関係のない情報が調査機関によって収集または保存されているかどうか、また捜査機関が当初許可された目的に従ってその範囲内でデータを使用および処理しているかどうかを監視または監督する法的措置が強く求められる。」

以上のように判示し、インターネット回線の盗聴に制御装置が設けられていない状態で、これを許可することは、個人の通信と私生活の秘密と自由を侵害するもので違憲という趣旨で、憲法に反するとの決定を下した。

●事例

○2008年9月27日、南北共同宣言実践連帯政策委員メンバーである Kwak Dong-gi は、国家保安法違反の容疑で逮捕され拘留された。彼は、2008年6月12日から2008年8月11日まで、国家情報

“Frontier Guard’ and pledging loyalty.

http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201905130600015 [17 May 2019]

35 執筆 People’s Solidarity for Participatory Democracy

36 Ministry of Science and ICT 2019. 5. 10. Press Release <Announcement of status report on communication data and communication confirmation in the second half of 2018>

院(NIS)によって自宅とオフィスでアクセスしたすべての IP アドレスと接続履歴をリアルタイムでパケット盗聴されていたことが裁判で明らかになった。

○2011 年 2 月、NIS は、過去に国家保安法違反の罪で無罪となったキムという名前の個人を、再捜査する過程で、パケット盗聴を実施した。2011 年 3 月 29 日、キムは憲法裁判所に申し立てを提出した。しかし、2016 年 2 月 25 日、裁判所は被害者の死亡を理由に申し立ての処理終了とした。2016 年 3 月 29 日に、市民社会組織はパケット盗聴の被害者に関して憲法上の申し立てを提出した。これにより、最終的に裁判所は、パケット盗聴の使用は違憲であるとの判断を下した。

○2014 年 10 月 1 日、労働党副議長のチョン・ジヌは、捜査中に警察が 3,000 人との会話を含むカカオトークのチャット記録を盗聴したと述べた。これにより、当局がカカオトークのパケット盗聴に関与していることが懸念され、多くのユーザーが外国のサービスに移行することになった。

○警察庁のサイバーセキュリティ捜査責任者である Min-Soo Kwon がパケット盗聴と同様の監視活動に「クライアントコンピューティングシステム」(B.F.S Matrix SW)を使用していたことが判明した。軍サイバーセキュリティ司令部の「レッドペン」資料(政府・政策など非難のコメント投稿者 ID、ニックネームなど)を渡され、捜査に活用し、この過程で傍受プログラムを利用して令状なしの不法盗聴したものだが、どのようにして多くの市民のパケット盗聴を行なったのか、その規模と期間はまだ明らかにされていない。

○2019 年、韓国通信委員会は、禁止サイトへのアクセスをブロックするために「HTTPS SNI フィールドブロック」を導入した。ただし、自動システムを使用して SNI ブロッキングすることと盗聴を行うことの技術的な境界はあいまいであり、ブロッキングシステムはパケット盗聴にも利用できる懸念がある。

●盗聴許可取得要件を定めた通信秘密保護法第 5 条(1)は、パケット盗聴を許可する根拠とすべきではない。

○第 20 回国会では、盗聴の許可要件を厳密に遵守させるように、通信秘密保護法に関する多くの改正が発議された。ただし、パケット盗聴は標的を絞った監視方法ではなく、大量監視の形式であるため、通信秘密保護法の下で傍受令状によって執行されることになると、個別事案ではなく包括的な令状を可能にするものであり、憲法上容認できない。

○憲法裁判所は、パケット盗聴は過剰な権力行使であると判断し、2020 年 3 月 31 日までに修正を求めた。標的となる個人への大規模な情報収集と盗聴の利用は、執行段階から法によるコントロールと実施後の通知を行う必要があるとされた。³⁷

●パケット盗聴で取得された情報が、実際に犯罪の証拠として提出されたことは、ほとんどない。

○パケット盗聴は、プライバシーの侵害の範囲や程度が他の盗聴と比較できないほど深刻であるという点を考慮すると、パケット盗聴を利用した捜査は、その必要は厳密性が要求されるべきである。つまり、犯罪捜査のために不可欠であることが、まず証明されるべきである。

○実際のパケット盗聴のほとんどが情報機関、国家情報院で行われており、国家情報院が 6 年にわたって回線盗聴をしたことが知られている、祖国統一汎民族連合国家保安法違反事件でも、検察は盗聴で確保した資料を証拠として提出しておらず、上記の憲法裁判所審理の過程でも、国家情報院は 7 年の間、インターネット回線盗聴をしたが、その過程で獲得した情報のうち、実際の裁判で証拠として提出した資料はないことが明らかになっている。

○過去のパケット盗聴事例から、パケット盗聴が、実際の刑事司法手続きで利用できる「証拠」の収集方法として果たして必要だったのかについて、強い疑問が提起されてきた。証拠として使

37 憲法裁判所 2016 HUNMA 263

わない幅広い情報収集がなぜ必要なのかについて、国家情報院など実際にパケット盗聴を実施していた機関は、適切に答えられないでいる。

○果たしてパケット盗聴が犯罪捜査のために行われたかどうか疑問な状況では、今後パケット傍受のための厳格な審査が必要であり、犯罪捜査への期待だけでこれを許してはならず、これまで実行されたパケット盗聴が「証拠」獲得の手段としてみた場合、個人のプライバシーの侵害を避けられない異例の手段の利用が本当に必要なのか、根本的な見直しが必要である。

●情報捜査機関のパケット傍受執行のための法的制度的統制制度の不備

○国家機関の盗聴装置は、科学技術情報通信部が管理しているが、情報機関はここから除外される。盗聴の執行の圧倒的多数を行なっている国家情報院は、情報機関の特性上、無令状盗聴で行われており、どのような盗聴設備を持っているかなどの盗聴の実態が事実上秘密に包まれている。

○裁判所の盗聴許可を受けているが、その実行過程は、取得した情報の管理や廃棄など、盗聴の執行で取得した膨大なデータをどのように処理しているのかについて、事前、事後の規制の手続きが全く存在しない。

B. 推奨事項

●現在のパケット盗聴技術では、対象データと一般データを区別することはできない。したがって、パケット盗聴の厳密な規制の手続きを確立する必要がある。

C. 担当省庁

法務省/科学 ICT 省

2) 通信確認データ³⁸

A. 背景

●通信秘密保護法第 13 条により、法執行機関は、犯罪捜査やその遂行に必要な場合、通信の事実を確認できるデータ（通信確認データ）へのアクセスまたは当該データの送信を電気通信事業者に要求することができる。

●捜査機関は、通信確認データを要求するために裁判所から許可を取得することが明確に規定されているが、管轄地の裁判所または支部裁判所から許可を取得しえない緊急の理由が存在する場合、その許可を通信確認データを要求した後に取得することができる。³⁹ 捜査機関は令状ではなく裁判所の許可によって簡単にこのようなデータにアクセスできるため、規制が脆弱ななかで通信確認データの無謀な要求がなされている。

●2014 年、韓国国家人権委員会（「NHRC」）は、「電気通信事業法および通信秘密保護法の下での通信確認データ提供の改善に関する勧告」によって、通信確認データを要請するための許可要件があいまいであり、捜査機関の悪用を防ぐことができず、プライバシー保護には不十分である」と指摘した。

●上記の勧告では、NHRC は「リアルタイムの位置追跡」を通信確認データから削除し、通信確認データの提供の条件を「関係する事件に関連して容疑者が犯罪を犯したという疑いに合理的な根拠があ

38 執筆 Korean Progressive Network Jinbonet

39 通信秘密保護法第 13 条の 2 第 1 項の規定による通信事実確認データ提供を要請する場合には、要求の理由としてその加入者との関連性と必要なデータの範囲を記録した書面で管轄地方裁判所（通常軍事裁判所を含む。以下同じ。）又は支部裁判所の許可を受けなければならない。ただし、管轄地方裁判所または支部裁判所の許可を受けることができない緊急事由があるときは、通信事実確認データ提供を要求した後、遅滞なく、その許可を受けて、電気通信事業者に送付しなければならない。

る」という事実に限定することを勧告した。また、要件の強化に加えて、犯罪捜査のための「リアルタイム位置追跡」の場合、補充性の要件を満たす場合に限定することが勧告された。

●通信方法による通信確認データに対する要求の数⁴⁰

(Unit: Number of documents)

| Year | Telephone | Mobile Phone | Internet and PC communication |
|------|-----------|--------------|-------------------------------|
| 2014 | 48,890 | 177,361 | 32,933 |
| 2015 | 57,838 | 207,004 | 36,100 |
| 2016 | 58,755 | 213,813 | 30,753 |
| 2017 | 59,590 | 204,524 | 37,207 |

●通信確認データは、コンテンツを含まないメタデータだが、さまざまな種類の情報を組み合わせて分析することにより、データ主体に関する情報を推測できる機密データである。⁴¹

●捜査機関が要求する通信確認データには、電話番号、通信の時間と期間、インターネットのログの記録、IP アドレス、通信の発信元の基地局の場所が含まれる。⁴²

●捜査機関は「基地局捜査」を幅広く活用しており、これには、特定の対象者を指定せずに特定の時間にその場所にある基地局に接続したすべての人々の通信記録を要求する。また対象者の将来位置をリアルタイムで追跡する「リアルタイム位置追跡」を広く活用している。

40 科学技術情報通信部、通信データおよび通信事実確認資料提供などの現状（2014～2017 年）

41 憲法裁判所，2018 年 6 月 28 日，2012Hun-ma538

42 通信秘密保護法第 2 条の定義規定で「通信事実確認データ」とは、次の各号のいずれか一つに該当する電気通信の事実に関するデータを含むと定義している。

- (a) 加入者による通信の日付。
- (b) 電気通信開始および終了時間。
- (c) 発着信の通信番号など、および相手方の加入者番号。
- (d) 使用頻度。
- (e) コンピューター通信またはインターネットのユーザーが電気通信サービスを使用したという事実に関連するコンピューター通信またはインターネットログ記録。
- (f) 情報通信ネットワークに接続する情報通信装置の位置を追跡するデータ。
- (g) 情報通信ネットワークに接続するためにコンピューター通信またはインターネットのユーザーが使用する情報通信装置の位置を確認できるコネクタケーブルの位置をトレースするデータ。

●2015年、UNHRCは、捜査機関が捜査目的を理由に令状なしで電気通信事業者に利用者情報を要求することに懸念を表し、集会参加者を特定するための「基地局捜査」の執行及びこれに対する不十分な規制にも懸念を示した。⁴³

●捜査機関の「基地局捜査」は、通信の秘密とプライバシー権の不可侵性に直接違反する。さらに、疑いのない者に対する場合には、通信の秘密性と位置データの秘密に違反する。

●どのような犯罪であれば通信確認データを要求できるかについての規定がないため、いかなる犯罪も要求対象となる。裁判所からの令状なしで、個人の通信の詳細や位置データなどの機密データを捜査機関に提供されてしまう。

●2012年、選挙運動中の贈収賄容疑の捜査中に、捜査機関は特定の時間、地域の基地局を利用した659人の通信確認データの提供を受けた。これに対して、同年、憲法裁判所に申し立てがなされた。2018年、憲法裁判所は、「基地局捜査」条項は、情報の自己決定とコミュニケーションの自由の権利を侵害するという理由で違憲の裁定を下した。⁴⁴

●携帯電話の「リアルタイム位置追跡」は、通話中だけでなく待ち受けモードでも10～30分ごとに携帯電話の位置を自動的に確認し、特定の基地局の位置データが捜査員の携帯電話に送信される。

●現在の通信秘密保護法では、誰が通信確認データの提供の対象となるかが明確ではなく、容疑者だけでなく、その家族や関係のない知人も通信確認データの対象になる。

●2011年6月から10月まで釜山の造船所で解雇された労働者を支援するために「希望バス集会」を開催したことを理由に活動家が「集会およびデモに関する法律」違反で起訴された。その後、捜査機関は、2011年12月から2012年4月までの通信確認データを取得した。このため、活動家グループが憲法裁判所に憲法違反の申し立てを行った。憲法裁判所は、この条項が比例原則に違反し、情報の自己決定およびコミュニケーションの自由の権利を侵害しているという理由により、違憲の裁定を下した。

⁴⁵

●捜査機関は、2013年12月9日から12月30日まで、韓国鉄道の民営化に反対していた議長を含む15人の鉄道労働者組合員と21人のその家族の通信確認データを取得した。捜査機関は、携帯電話とインターネットサイトの位置データを追跡していたことも明らかになっている⁴⁶。この事件に関与した人々は2014年に憲法裁判所に憲法違反の申し立てを行った。憲法裁判所は、この条項が比例原則に違反し、情報の自己決定とコミュニケーションの自由に対する権利を侵害したという理由で違憲の裁定を下した。⁴⁷

●憲法裁判所は、通信確認データは特定できないコンテンツを含むメタデータだが、さまざまな種類の情報を組み合わせて分析することでデータ主体を推測できるため、機密データであると述べた。さらに、位置データは機密データであり、徹底して保護する必要があるとみなした。憲法裁判所は、通信確認データの提供の要求に対して、より厳しい要件を設けることを勧告した。

●政府は、「通信制限措置の延長」、「位置追跡データ」、「基地局捜査」などの違憲要素を排除する改正を発表したが、修正には人権侵害を最小限に抑えるための十分な手段が講じられていない。こ

⁴³ CCPR/C/KOR/CO/4. para42~43.

⁴⁴ 憲法裁判所, 2018年6月28日、2012Hun-ma538

⁴⁵ 憲法裁判所, 2018年6月28日、2012Hun-ma538 および 550、2014Hun-ma357。

⁴⁶ 当時、警察は、通信事実確認資料を通じて当事者の携帯電話の位置、インターネット接続位置をリアルタイムで追跡したのはもちろん、令状もなく、健康保険公団など公共機関が保有している鉄道労組執行部と家族の個人情報も提供されたという事実が明らかになった。

⁴⁷ 憲法裁判所, 2018年6月28日、2012Hun-ma538 および 550、2014Hun-ma357。

の改正は、捜査の利便性と法執行機関の効率を何よりも優先しており、情報社会における人権侵害の可能性が残されている。

B. 勧告

- 調査機関による情報化社会における人権侵害および権限を有する当局による権力濫用を最小限に抑えるために、通信秘密保護法を改正すること。
- 通信事実確認データの提供に令状主義を導入して、裁判所の規制を受けるようにしなければならず、送受信が完了した電気通信の押収、捜索、検証の要件を強化し、相当な理由と補充性の要件を規定して、当事者の参加権を明示しなければならない。
- 「基地局捜査」のために、特別の規定と要件の強化が必要である。
- 位置追跡データ、特に「リアルタイム位置追跡」には、リアルタイムの盗聴効果がある。したがって、対象となる犯罪を限定して要件を厳格化する必要がある。

C. 担当省庁

- 法務省

3) 通信データの提供⁴⁸

A. 背景

電気通信事業法の第 83 条 (3) は、捜査機関が、加入者の特定が必要な場合に、裁判所の許可なしに、名前、ID、住民登録番号、住所、電話番号 (通信データ) などの加入者情報を電気通信事業者から取得できると規定している。主に初動捜査の段階で捜査対象者の個人情報の把握が目的というが、その要件が広すぎ、また不明確である。

●憲法裁判所は、捜査機関による通信データの要求は、強制調査に当たらないと判断した。⁴⁹2010 年 3 月、インターネットポータル Naver が捜査機関に加入者情報を渡した Naver 事件に関する損害賠償裁判で最高裁判所は、⁵⁰ 通信事業者が手続き要件を満たしている場合、調査機関の要求に応じて通信プロバイダーは顧客のデータを提供しなければならないとして情報提供を支持した。第 83 条 (3) は、司法の命令がないとしても、捜査機関が必要とみなした場合には、捜査機関による要求に電気通信サービスプロバイダーは従わなければならない、というように実際には運用されている。

●さらに、通信事業者 (または代理店) は、通信データの提供の前または後に、そのような提供を顧客に通知する必要がない。したがって、捜査対象者は、通信データの収集が必要性和適切性を備えた正当な法執行プロセスであるかどうかを確認できる基本情報にアクセスできない。

●韓国では、「住民登録番号」と呼ばれる国民 ID システムによって状況は悪化している。このシステムでは、大量の重要な個人情報が組み合わされている。したがって、住民登録番号は、個人情報の主要な情報源として機能している。捜査機関は、独自の裁量で特定の個人の住民登録番号を取得できる。これは、基本的な市民的権利の侵害が他の国よりも韓国では悪化していることを意味している。

●2013 年から 2017 年にかけて、平均 1,034,036 件の (9,539,337 アカウトに関連する) 通信データが毎年捜査機関に提供されている。2016 年以降、電気通信全体とインターネット両方からの通信データの提供が漸減する傾向にある。

48 執筆 People's Solidarity for Participatory Democracy

49 憲法裁判所 2010 HONMA 439

50 最高裁判所 2012 DA 105482

| Communication data provision | In 2013 | | In 2014 | | In 2015 | | In 2016 | | In 2017 | |
|------------------------------------|---------------------|--------------------|---------------------|--------------------|---------------------|--------------------|---------------------|--------------------|---------------------|--------------------|
| | Number of documents | Number of accounts | Number of documents | Number of accounts | Number of documents | Number of accounts | Number of documents | Number of accounts | Number of documents | Number of accounts |
| All communications | 944,927 | 9,574,659 | 1,001,013 | 12,967,456 | 1,124,874 | 10,577,079 | 1,109,614 | 8,272,504 | 989,751 | 6,304,985 |
| The Internet ¹⁷⁵ | 115,194 | 392,511 | 114,260 | 489,916 | 100,643 | 423,533 | 84,302 | 312,056 | 65,151 | 635,795 |
| Two major companies ¹⁷⁶ | 1 | 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

(訳注：表左欄の The Internet および Two major companies については下記脚注 50 及び 51 を参照^{51 52)})

○インターネット経由の通信データの提供はドキュメント数の点で減少しているが、2017 年では、アカウント数は前年の 2 倍以上になっている。

○毎年、捜査員は、950 万のアカウントに関する情報を令状なしで取得している（総人口の 18.4%）。

51 「インターネット全体」は、科学技術情報通信部プレスリリースの通信手段のうち「インターネットなど」に相当し、有線・携帯電話を除いた残りの通信事業者（ポータルなどの付加通信事業者とインターネット網事業者など）が報告した数値の合計ある。

52 「2つの大手企業」とは、透明性レポートを提供した韓国の2つのオンラインサービスプロバイダー、Naver と Kakao を指す。犯罪の疑いが不明な加入者の身元情報を捜査機関に提供したポータルサイトに損害を賠償するよう下級審判決（ソウル高等法院 201210.18.宣告、2011 や 19012 判決）が 2012 年に出て以降、主要ポータルサイトは 2013 年からの通信データの提供を停止している。2016 年 3 月、最高裁（最高裁判所 2016 年 310.宣告、2012 105482 判決）で本判決は破棄されたが、両事業者は、その後も通信データ提供要求に応じていない。主要ポータルサービス事業者が通信資料提供を中止したので、現在のインターネット利用者の通信データの提供は、主にインターネットサービスプロバイダーによって行われているものと見ることができる。

● 国家人権委員会は、通信データ提供制度に関する次の意見を憲法裁判所（憲法裁判所 2016 Hunma388）に提出した：「個人情報収集の目的と対象の範囲が広すぎる。事前または事後の司法による統制がなく、通知の手続きが存在しないため、情報の自己決定権の侵害につながる可能性がある。」

● 事例

○ 2010 年 3 月、オンラインネイバーカフェ Naver cafe の掲示板に、ネチズンが、当時の世界的なスターでもあったスケーターのキム・ヨナの動画を投稿した。文化スポーツ・観光省の長官ユ・インチョンが彼女を抱きしめようとしたとき、キム・ヨナが、接触を避けているように見えるものだった。警察は、キム・ヨナへの名誉毀損の疑いでネチズンを捜査した。捜査中に、このネチズンは、ネイバーが彼に通知せずに捜査機関に彼の個人情報を提供したことを知った。このため、彼はネイバーに対して訴訟を起こし、第一審では却下されたが、控訴審⁵³では、ネイバーが情報の自己決定と匿名性に対する原告の権利を侵害し、ユーザーの個人情報の保護を怠ったとして 50 万ウォンの損害を認めた。2012 年 10 月の判決以来、大手インターネット企業（Naver、DAUM、SK Telecom、Kakao など）は、裁判所の命令なしに調査データを提供していない。

○ 2013 年 4 月、捜査機関への通信データの提供と、その提供に関連する情報開示の要求に応じなかったことを理由に、3 つの通信会社に対する訴訟が、ユーザーによって起された。ユーザーは、関連情報の開示と損害賠償を要求した。第一審では、裁判所は電気通信事業者への損害賠償請求は退けながらも情報を開示するよう命じた。損害賠償は控訴審では認められたが、その決定は遅すぎた。⁵⁴控訴審は、捜査業務に支障が発生することがあるという漠然とした事情だけで憲法と法律が保証する情報主体の個人情報の自己決定権を制限することができないと判決した。

● さらに、電気通信会社が長期間にわたって原告の開示要求を拒否することは、情報の自己決定権を侵害する違法行為であるとした。電気通信会社は判決に対して上告したが、最高裁判所は 2018 年 7 月 20 日に上告を棄却し、控訴審判決が確定した。

○ 2016 年 3 月、捜査員が、議員や労働組合員など、テロ対策法の制定に反対した多くの人々の通信データを収集していたことが判明した。市民社会グループは、キャンペーンを展開し、市民に通信データが収集されているかどうかを確認するよう促した。この結果、最終的に 500 人以上の市民のデータが収集されていたことが確認され、83 条（3）に基づく憲法上の申し立てを提出した。現在、この申し立ては手続きが継続中である。

B. 勧告

● 捜査機関が裁判所の命令なしに無制限に個人情報を収集できないように、電気通信事業法を改正する。

● 捜査機関が令状なしで通信ユーザーの情報を収集できる通信データ提供システムを完全に廃止する。

● 捜査機関の活動の利便性を優先する現実を修正し、情報の自己決定の権利を改善する措置を実施する。

C. 担当省庁

法務省、韓国通信委員会、科学情報通信省

53 ソウル高等裁判所 2011 Na 19012

54 ソウル高等裁判所 2014 NA 2020811

4) デジタル情報の搜索と押収⁵⁵

A. 背景

●個人間の通信は、私的領域の重要な部分を占めており、通信内容の秘密の保障は個人のプライバシーの保護において最も基本的かつ重要なものである。しかし、送受信が完了したメールは、現行の刑事訴訟法上では「物品」とされ、一般的な搜索手順に従う。送受信が完了した一定期間のメールを搜索押収するために、コンピュータサーバやノートパソコンなどが見られることになると、それまでなされた通信内容と通信相手が無防備な状態でさらされていることになる。捜査機関は、搜索押収で得た私的な電子メールの情報まで有罪の証拠として提示することもあり、批判されてきた。

●したがって送受信が完了したといっても、一定期間にわたって送受信したメールは、広範な情報収集に基づくプライバシー侵害の危険性にさらされる可能性があり、一般的な搜索押収とは別の方法による手順と基準を適用しなければならないという主張が有力である。テレビ番組 PD Notebook の場合、スタッフの電子メール記録が搜索押収されたため、次のような問題が生じた。

○2008 年 4 月 29 日、李明博政権による米国産牛肉輸入の増加に対して大規模なろうそく抗議運動が開始されたとき、PD Notebook は「緊急報告：米国産牛。狂牛病は安全か？」を放送した。李明博政権は、PD Notebook が大規模な抗議の背後で操っているものであると主張し、そのプロデューサーを政府への名誉毀損（食品、農林水産省）として告訴した。この事件で、検察は事前通知なしに電子メールを搜索しただけでなく、捜査結果を個人の電子メールとともに公開し、これを犯罪の証拠だと主張した。検察は、刑事告発の範囲を超えて個人的な電子メールを閲覧したことが報告されている。

●2010 年 8 月、韓国人權委員会（NHRCK）は、刑事訴訟法の改正について国会議長に次のように助言した。「通信事業者に保存された電子メールの押収の根拠と手続きを立法化することが望ましい。押収目的で搜索する場合、その範囲は刑事告発に関連したものとして特定する必要がある。」⁵⁶

●インターネット通信網をベースに流通されている電子通信の形態は多様で、搜索押収が刑事訴訟法の一般的な搜索押収規定に基づいて行われているのは問題である。コンピュータのハードディスクに保存されているデジタル情報の場合は、単に物を搜索押収するのとは異なり、技術的に犯罪容疑と関連した情報のみを別に抽出することが容易ではないみなされて、これまで包括的な押収方法がとられてきた。これにより、膨大なデジタル情報の収集が可能となり、犯罪容疑とは無関係なプライバシーの侵害、通信の秘密の侵害が著しく大きいと指摘されてきた。捜査機関が搜索と押収によって収集した情報に基づいて新たな捜査を開始した韓国の教職員労働組合（KTU）やセウォル号大事故に関する事案が議論を呼んだ。

○2009 年 6 月、KTU は、メディア立法の審議中止と大運河プロジェクトを非難する声明を発表した。検察は、KTU オフィスにおける機材の押収令状を発行し、令状を執行するなかで、ソウルの KTU 本部で 3 台のデスクトップコンピューターと 10 台のサーバーコンピューターを押収した。この時点では、検察は押収されたコンピューターから得た情報に基づいて、民主労働党への党費月 5,000～20,000 ウォンを支払ったりカンパした教師に捜査範囲を拡大した。その後、KTU の教師は、政党法および政治基金法の違反で告発された。

○KTU は、検察の押収手続きが令状に規定されている手続きを逸脱していると反論した。最高裁判所は、電子情報の押収は、申し立てと押収の場所に関連する令状に具体的に印刷されているものに限って実行されるべきであること、さらに、現場からデータストレージデバイスを取り外すことは、令状で特定されている例外的な場合にのみ許されるを明確にした。

55 執筆 People's Solidarity for Participatory Democracy

56 韓国人權委員会 2010 年 8 月 18 日

○2011年7月以降、刑事訴訟法は情報記憶媒体に関する新しい規定を含むように改正され、特にデータ記憶装置の押収は原則としてコピーによって実行されるべきであると定められた。⁵⁷

○2014年7月、警察は、セウォル号災害に関連する宣言作成を主導した疑惑で、KTUの76人のメンバーを捜査した。警察は、ソウル瑞草洞にあるKTUのサーバーを緊急捜索した。令状は「ホームページサーバーデータ」と「サーバーに保存されたKTU電子メールアカウントの記録」に限定されていたが、警察の捜索中、個人的な会話を含む電子メールとネイバーバンド Naver Band の会話の押収が行なわれたことが知られている。捜査官が行った電子メールとバンドの記録の捜索と押収には、犯罪申し立ての範囲外の会話記録やコンテンツが含まれていた。警察は、捜査対象ではない人々の会話を検証したりでき、プライバシー権の深刻な侵害行使であるとの批判が出た。

●2015年7月16日、最高裁判所⁵⁸は、捜査中に、以前に明らかにされていない犯罪が行われたことが判明した場合、捜査官はそれらの犯罪に関する令状を取得する必要があると判決し、電子情報押収の原則を確認した。

●その他の事案

○2008年、ソウル教育長官候補であり、建国大学の教授であるチュ・ギョンボクの選挙法違反容疑を検察が捜査中に、事前に通知することなく彼の7年間の電子メールが捜索され、その内容が押収された。裁判ではじめて、このことが明かにされた。

○2009年、the Justice for Yongsan Evictees の共同議長であるパク・レグンは、弁護士との弁護についての会話に関連するメール記録を押収された。

○2009年、警察は、業務妨害容疑で捜査中の20人のYTN組合員から9か月分の会社の電子メール記録を押収した。これには、メディア労働組合の会議文書や申し立てとは無関係の会計記録が含まれていた。メンバーには通知されなかったため、捜索が行なわれてから3か月以上経過するまで捜索に気づかなかった。

○Naver Band または KakaoTalk チャットルームの記録の押収は、リアルタイム盗聴などの監視技術によって行われる場合があるにもかかわらず、刑事訴訟法における押収の規定に従って行われている。これらの押収は、一般的な種類の押収よりもはるかに侵害の程度が大きいものである。

B. 勧告事項

57 第106条(差押)(1)必要に応じて、裁判所は、証拠として使用されるか没収の責任があると思われる物品を、そのような物品が被告事件に関連するとみなされる場合に限り、差し押さえることができる：行為に別段の定めがある場合。 <2011年7月18日法律第10864号により改正>(2)裁判所は、そのような物品の制作にかかわった所有者、占有者、または保管者に、差し押さえるべき物品を指定し、命じることができる。(3)差し押さえられる物品がコンピューターディスクまたはそれに類するその他のデータ記憶媒体(以下、この段落では「データ記憶媒体など」と呼ぶ)である場合、裁判所は、その中のデータが指定された範囲のデータを印刷またはコピーする場合。附則：指定された範囲のデータを印刷またはコピーすることが実質的に不可能であるか、または押収の目的を達成することができないとみなされる場合、押収することができる。 <2011年7月18日法律第10864号により新たに挿入>

58 最高裁判所、2015年7月16日。2011MO 1839年判決。「原則として、調査機関による電子情報の捜索は、捜査機関が所持する記憶媒体にファイルをコピーするか、令状が発付された刑事申し立てに関連する部分のみの印刷物を収集することによって行われるべきである。記憶媒体自体をエクスポートしたり、記憶媒体をサイトから取り外して記憶媒体に含まれるすべての電子ファイルを取得することは、例外的な場合にのみ許可される。関連情報の取得に長期間を要する場合、または範囲を設定して印刷またはコピーすることが不可能な場合、または捜索の目的を達成することが極めて困難であると認識されている場合は、その場合のみ例外として許可される。」

●刑事訴訟法に基づく一般令状による電子情報の搜索と押収は、比例の原則に反しており、プライバシーとコミュニケーションの侵害の程度が深刻である。これらの点を考慮し、関連する規制を改善する必要がある。

C. 担当省庁

●法務省

3. 住民登録システム

1) 住民登録番号システム⁵⁹

A. 背景

●すべての韓国国民は、出生時から住民登録番号（「RRN」）と呼ばれる固有の国民識別番号が付与される。RRNは13桁で構成され、最初の数桁は生年月日、最後の7桁は性別、出生地、出生日の出生登録順序、およびエラー検証番号を含むもので構成されている。原則として、RRNは一度付与されると一生変更することはできない。

●RRNは、さまざまな公共および私的領域での個人識別のために収集されている。したがって、RRNは、異なるデータベースからの情報を接続するための鍵になる可能性がある。こうした状況下では、RRNを含む大量の個人情報漏洩が重大な損害を引き起こす。たとえば、RRNは次の企業から漏洩した。

○2008年にオークション1800万件が流出

○2011年に、SK Coms Nate, Cyworldから3500万件が流出

○2011年にNexon 'Maple Story'から1300万件が流出

○2014年にロッテカード、NHカード、KBカードから1億1,400万件が流出

○2016年には、インターパークから1,030万件が流出。

●第1回UPR（2008）は、公共の利益に必要とされる目的でのみRRNの使用を制限するよう勧告した。

60

●RRNの過剰な収集を制限するため、「情報通信ネットワークの利用と情報保護等の促進に関する法律」の改正により、2012年8月以降、オンラインでRRNを収集することは禁止される。2014年8月7日から「個人情報保護法」において、許可なくRRNを収集することは禁止される。

●2014年8月8日、韓国人権委員会（NHRC）は、国会議長と首相がRRNシステムの抜本的な改革を行うこと、RRNは、住民登録に関する管理業務等に限定して使用することを勧告した。⁶¹他の分野では、その分野に固有の番号を使用し、RRNを変更できるようにし、個人情報が含まれていない任意の一連番号に変更することを勧告した。

●憲法裁判所は、RRN自体の変更を許可しないことは情報の自己決定権に違反すると判決し、2015年12月23日の現行住民登録法を違憲とした。同時に、憲法裁判所は住民登録法を2017年12月31日までに改訂するよう勧告した。⁶²

●RRNシステムには3つの問題がある。まず、RRNはプライベートおよびパブリックエリア全体から過度に収集されるため、さまざまな個人情報を統合し、個人を追跡またはプロファイリングするための

59 執筆 Korean Progressive Network Jinbonet

60 A/HRC/8/40, para 64.13

61 韓国人権委員会、RRNシステム改善勧告 2014年5月8日。

62 憲法裁判所 2015年12月31日、2014Hun-ma449 および 2013Hun-ma68。

基盤となる。第二に、RRNは原則的に変更することができず、その結果、RRNの漏洩による潜在的な損害を引き起こす可能性がある。最後に、生年月日、性別、生年月日などを含むRRNにより、データ主体がそれを望まない場合でも個人情報公開され、差別の根拠として使用される可能性がある。

●個人情報の収集を制限するため、2014年8月からRRNを収集することは法律で許されていないが、それでも多くの法律がRRNの収集を可能にしている。2014年1月に安全保障省（現在、内務省）が発表したデータによると、866の法令によりRRNの収集が許可されており、民間の金融および通信部門でもRRNが収集されている。さらに、場合によっては、RRNは、法律や施行規則ではなく、書式に基づいて収集されている。

●2015年12月、憲法裁判所の憲法違反の判決を受けて、国会は2016年5月19日に住民登録法改正案を可決し、住民登録番号の変更を認めた。⁶³漏えいによる生命、身体、財産、性的暴力などの損害を被ったり、被る可能性が高い人のみ変更が認められる。実際には、RRNの漏洩によって引き起こされる直接的な被害を証明することは困難である。さらに、13桁のRRNのうち後ろ6桁のみが変更でき、新しいRRNには生年月日と性別に関する情報が含まれており、ここからRRN全体を類推することができる。これに対して、NHRCは、限定された変更に遺憾の意を表明し、客観的な番号と乱数の導入を要求する声明を発表した。⁶⁴

●個人情報は、生年月日、性別、および出生地に関する情報を含み、RRNで意図せずに公開されるため、年齢、性別、および地域による差別を助長する可能性がある。さらに、RRNは個人情報からも追跡できる。

○2014年のソウル国立科学技術大学の調査によると、Facebookの個人情報を使用することで、RRNの45%、115,615件が取得できた。⁶⁵

○2015年のハーバード大学の調査：米国のIMS Healthに売却された韓国のRRNは、RRNシステムのあるモデルを利用して23,163件を特定することに成功した。「出生、性別、地域、確認番号のデータのためにこれは容易であった。」⁶⁶

○2009年の認知度調査によると、住民の77.2%は、住民登録番号によって性別や出生データに関する情報がさらされることについて、「望まないのに、私の情報が公開されて気になる」と回答。⁶⁷

○RRNの性別は男性と女性のみに分けられ、男性の数字は1（2000年以降に生まれた人は3）、女性の数字は2（2000年以降に生まれた人は4）。これは男性優位の認識であり、性的マイノリティを差別する要因になっている。

●2014年にNHRCが勧告したにもかかわらず、担当の内務省は、RRNシステムを乱数システムに変更することを望んでいない。

63 第19回国会で通過した住民登録法に関する社会組織の共同声明（2016年）-不完全に終わったRRNを改善し、第20回国会で変更せよ！

<http://act.jinbo.net/wp/9538/> [14 May 2019]

64 韓国人権委員会（2016）。〈住民登録法〉の一部を改正する法案の承認に関する委員長声明

<https://www.humanrights.go.kr/site/program/board/basicboard/view?>

[&boardtypeid=24¤tpage=55&menuid=001004002001&pagesize=10&boardid=611785](https://www.humanrights.go.kr/site/program/board/basicboard/view?&boardtypeid=24¤tpage=55&menuid=001004002001&pagesize=10&boardid=611785) [14 May 2019]

65 チャンネルA（2014）。[シングル] Facebookで住所を入力すると、住民登録番号が表示される。

http://www.ichannela.com/news/main/news_detailPage.do?publishId=61503088-1 [14 May 2019]

66 ハンキョレ。（2019）。[シングル]福祉部門のビッグデータのリスク...個人情報が暗号化されていても解読できる。http://www.hani.co.kr/arti/society/society_general/762609.html [14 May 2019].

67 Kim, Min Ho et al. 2009. A Study on the Improvement of the resident registration number system. National Competitiveness Council.

B. 勧告事項

- 住民登録番号の収集と利用は、書式ではなく法律に基づいて行う必要がある。
- 住民登録番号の利用は、行政および司法の目的のために厳密に制限する必要があり、公共部門以外の領域では、その目的に固有の別個の識別番号（税番号など）が使用されるべきである。
- さまざまな分野の識別番号が、法律に基づかずに RRN にリンクされることを防ぐこと。
- RRN を、個人情報を含まない乱数システムに変更すること。
- RRN は、関連する要件が満たされさえすれば変更可とすること。

C. 担当省庁

- 内務省安全省居住局
- 首相

2) 強制指紋システム⁶⁸

A. 背景

- 指紋は誰にとっても固有の生体認証情報であり、機密情報として保護する必要があり、特別な保護が必要である。
- 指紋認証システムは、1968 年に韓国で住民登録証の発行にともなって導入され、17 歳以上の韓国人はすべて指の指紋認証を受けている。現在、すべての市民の指紋は電子的に管理され、自動指紋識別システム（AFIS）を通じて捜査目的で警察庁によって利用されている。内務省には指紋情報を保有し、識別のために使用されている。
- 17 歳以上のすべての韓国人の指紋を強制的に採取し、犯罪捜査の目的で使用することは、国民全体を潜在的な犯罪者として扱うことである。
- 1999 年、社会組織の活動家は、17 歳以上の市民の指紋に関する警察の情報収集、およびデータベースシステムの確立と運用に対して憲法裁判所に憲法違反の申し立てを行った。2004 年、17 歳に達した 3 人の 10 代の若者が、国の指紋認証システムが違憲であるとして告発した。しかし、憲法裁判所は、警察法および警察官の職務執行に関する法律に「公安に関する情報の収集、準備、および配布（第 2 条、4 条）」が義務の 1 つとして含まれているという理由で、2005 年にこれを退けた。⁶⁹ 2011 年、異議申立人は再び憲法裁判所に申し立てたが、同じ理由で憲法裁判所はこれを退けた。

B. 勧告事項

強制的な指紋認証システムの廃止を勧告する。

C. 担当省庁

内務省居住局

3) 本人確認機関システム⁷⁰

A. 背景

68 執筆 Korean Progressive Network Jinbonet

69 憲法裁判所 2005 年 52699 헌마 513 など

70 執筆 Open Net Korea

●政府は、大規模なデータ侵害事件が繰り返し発生したことに対応して、2012年以降、情報通信ネットワークを通じたデータ侵害の主な標的である住民登録番号（RRN）の収集を禁止した。情報通信ネットワーク Act⁷¹に基づく本人確認機関には、引き続き RRN を収集する権限がある。

●本人確認を必要とする多くの法律は、本人確認機関が提供する本人確認方法を使用することを規定している。したがって、少年保護法、公職選挙法、ゲーム産業振興法などの法律で身分証明義務のあるインターネット企業は、情報通信ネットワーク法の下で身元確認を使用する必要がある。さらに、施行令で規定されている識別方法は極めて限定されているため、インターネット企業は唯一の一般的な識別方法である通信会社が提供する本人確認サービスに依存する必要がある。

○識別サービス市場は、SMS 識別サービスを提供する通信会社によって独占されている。韓国通信委員会から得たチェ・ミョンギル議員のデータによると、3つの主要な電気通信の識別サービスからの収益は、2015年の1年間だけで258億ウォンであった。

●本人確認機関システムを採用する目的は、RRN システムに代わる識別方法の開発を機関に奨励することにあった。ただし、携帯電話加入者の RRN を収集する主要な3つの通信会社はすべて、本人確認機関として指定されている。したがって、通信の識別サービスは、携帯電話番号を携帯電話ユーザーの RRN に正確に一致させることができるため、モバイル RRN システムに基づく識別と実質的に同じである。

●2014年3月、主要な3つの通信の1つ KT（Korea Telecom）がハッキングされ、1200万人のユーザーの RRN その他の個人情報が盗まれた。このような大規模な漏洩は、KT が本人確認機関として RRN を収集できるように発生した。

●さらに、通信事業者は、ユーザーのオンラインでの識別処理を記録する必要がある。これは、プライバシー情報に属するユーザーによる年齢制限のあるサイトへのアクセスなどの Web サイトのログがあることを意味している。通信会社がこれらの個人データを蓄積し続けることが許されている場合、ユーザーの好みをプロファイルすることが可能であり、ビッグブラザーとなる可能性がある。

●2014年6月にオープンネットワークは、憲法裁判所に本人確認機関の指定制度が国民の個人情報の自己決定権を侵害するという理由で申し立てを行なう。

B. 勧告事項

特定の企業に加入者の住民登録番号と機密情報の収集を義務付ける情報通信ネットワーク法に基づく身元確認機関システムを廃止すること。

C. 担当省庁

●韓国通信委員会

4) 接続情報（CI）⁷²

A. 背景

●接続情報（以下「CI」）とは、88バイトで暗号化された情報を意味し、サービスリンケージのために Web サイトの共通識別子 co-identifier として使用される。オンライン識別サービス機関は、住民登録番号（以下「RRN」）に基づいて CI を生成し、Web サイト間で提携サービスを提供するときに顧客の識別に使用される。

71 第23条の2（住民登録番号の使用の制限）（1）情報通信サービスプロバイダーは、次のサブパラグラフのいずれかに該当しない限り、ユーザーの住民登録番号を収集または使用してはならない。1. 第23-3条に従って本人確認機関として指定されている場合

72 執筆 Korean Progressive Network Jinbonet

- CI は仮名での RRN 情報である。CI は 1 対 1 照合できるため、「オンライン住民登録番号」のように、オンラインのどこからでも人物を認識させることができる。
- すべての行政サービスと民間企業が RRN によって識別されているため、RRN の収集と利用に関する問題が常に発生する。問題の指摘が繰り返された結果、RRN の収集と利用を制限する場合にのみ認められるように法律が改正され、RRN の代わりにオンラインで ID を検証する手段として CI が導入された。
- 韓国の大手インターネット企業は、ユーザーに必要以上の本人確認を要求するだけでなく、CI は RRN のような保護がなされていないため、法律の抜け穴を利用して、使用規約を介して包括的な同意を得て CI を使用している。また、捜査機関は CI を利用して、特定のユーザーのオンライン活動を追跡している。
- 結局のところ、RRN にリンクされた CI を通じて、個人のオンラインおよびオフラインの活動が、追跡できる状態になるだけでなく、匿名に基づくオンラインにおける表現の自由を侵害している。
- CI を使用した識別システムは、インターネットの実名システムに直接リンクしている。言い換えると、匿名に基づいてオンライン環境で自分自身を認証しなくても各ユーザー相互を識別し、犯罪などの問題が発生した場合にブロックして処罰する方法があるにもかかわらず、実名認証と本人確認により、当該利用者の表現の自由を制約する萎縮効果を生み出している。
- 2012 年 8 月 23 日、憲法裁判所⁷³は、個人の身分証明手続きを経なければ掲示板のユーザーとして許可されないとすることは、ユーザーの表現の自由、個人情報の自己決定の権利、および掲示板を運営している通信サービスプロバイダーのメディアの自由を侵害すると判断した。
- 実際の CI は暗号化されており、CI だけでは識別できないが、電話番号、名前、携帯電話番号の組み合わせにより、RRN などの個人を識別できる。
- 2019 年 2 月 14 日、科学技術情報通信部は、「情報通信振興と融合促進などに関する特別法」を根拠に、最初の ICT 規制サンドボックス事業についてカカオペイと KT が申請した「メッセージング・文字ベースによる行政・公共機関のモバイル電子通知サービス」に暫定的な認可を下した。この措置を通じて、行政・公共機関のモバイル電子通知のために住民登録番号を CI に一括変換して使用することができるようにした。
- 公共機関が住民登録番号を処理するためには、「法令上具体的に住民登録番号の処理を要求または許可する根拠がある事務」である必要がある。⁷⁴しかし、現在の文字、電子メールなど同意の通知を実行する行政機関は、当事者の携帯電話番号、電子メールアドレスなどがよく変わるために、どこにいても追跡して知らせられるようにするためには CI ベースの「アラートトークサービス」が必要だという立場である。しかし、政府が活用しようとする「アラートトークサービス」は、住民識別番号が民間部門と公共エリアで一般的に収集、活用されている韓国でのみ可能な異常なサービスである。
- 機密の個人情報である RRN を特定の企業のサービスに利用することに政府が積極的に関与することは、情報の自己決定権に対する明確な違反である。

B. 勧告

- 情報通信ネットワーク法上の本人確認機関の指定制度を廃止する必要がある、したがって、オンライン社会保障番号である CI も廃止する必要がある。
- オンラインでの不要な本人確認は、個人情報の自己決定権の侵害であり、したがって、個人情報監督機構は、不必要な本人確認が行われないように啓蒙する必要がある。

⁷³ 憲法裁判所 2012 年 8 月 23 日、2012、 2010Hun-ma47 及び 252。

⁷⁴ 個人情報保護法 第 24 条。

C. 担当省庁や機関

- 科学 ICT 部
- 放送通信委員会
- 個人情報保護委員会

4. コミュニケーションの匿名性⁷⁵

1) 携帯電話の実名システム

A 背景

●2014 年 10 月に新設された電気通信事業法第 32 条の 4⁷⁶は、電気通信事業者が電気通信サービスの提供に関する契約を締結する過程で不正登録防止システムなどを利用して、契約相手方の本人かどうかを確認しなければならない「携帯電話実名制」を規定している。すなわち、移動通信会社は、携帯電話の契約締結時の契約相手方の本人かどうかを確認する必要があり、本人ではない場合や、本人かどうかの確認を拒否した場合には、契約の締結を拒否することができる。

●携帯電話実名制は、利用者の匿名通信の自由、プライバシーの秘密と自由、個人情報の自己決定権を侵害し、これに対してオープンネットは 2017 年 11 月憲法裁判所に申し立てを行ない、現在の審理中である。

○匿名通信の自由の侵害：表現の自由について、憲法裁判所は、匿名表現の自由が含まれることを明らかにした事があり、同様に、通信の秘密の保護対象には通信の内容だけでなく、通信の当事者（受信者と送信者）、宛先と送信元、送信回数などの通信に関連する一切が含まれ、これには、相手との第 3 者に身元を明らかにせず匿名で通信する自由、「匿名通信の自由」が当然含まれることを確認した。ところが、携帯電話実名制は、匿名通信を全面的に不可能にするので、匿名通信の自由を明らかに侵害する。

○プライバシー侵害：今日、オンラインで行われるすべての通信と表現行為は記録が残されるために、国家による監視と追跡が極めて容易である。携帯電話実名制は、すべての通信機器を利用者の実際の身元と強制的に連携させることで、政府だけでなく、企業や個人によるプライバシー侵害の危険を増すことになる。

75 執筆 Open Net Korea

76 第 32 条の 4（移動通信機器不正利用防止等）

1 省略

2 電気通信役務の種類、事業規模、利用者保護等を考慮して、大統領令で定める電気通信事業者は、電気通信役務提供に関する契約を締結した場合、（電気通信事業者を代理したり、委託を受けて、電気通信役務の提供を契約する代理店と荷受人を通じた契約を含む）契約相手方の同意を得て、第 32 条の 5 第 1 項の規定による不正登録防止システムなどを利用して本人かどうかを確認しなければならない、本人ではないか、本人かどうか確認を拒否した場合、契約の締結を拒否することができる。電気通信役務提供の譲渡、その他の利用者の地位承継等により、利用者本人の変更がある場合は、その変更に応じて、電気通信役務を提供する受けよう者に対してもまた同じである。

3 第 2 項の規定により本人確認をする場合、電気通信事業者は、契約相手方に住民登録証、運転免許証など本人であることを確認できる証明書と書類の提示を求めることができる。

4 第 2 項の規定による本人確認方法、第 3 項の規定による本人であることを確認することができる証明書と書類の種類等に必要事項は、大統領令で定める。

○個人情報の自己決定権の侵害：携帯電話実名制は、電気通信事業者が情報主体の名前、住民登録番号、住所などの本人確認情報を調査し、収集・保管することを義務づけているが、本人確認情報は、個人の同一性を識別することができる情報として個人情報に該当し、当然、利用者の個人情報の自己決定権を侵害する。

●携帯電話実名制は、個人情報の過剰な集積によってハッキングなどを通じた流出の危険性を高め、実際、毎年大規模な情報流出事故が継続的に発生している現実がある。特に携帯電話会社は何度か個人情報流出事故の元凶になったにもかかわらず、携帯電話実名制は携帯電話会社による個人情報収集を制限するどころか、さらに多くの収集権限を認めている。

B. 勧告

●匿名通信の自由、プライバシーの権利および個人情報の自己決定権を侵害する、携帯電話実名制を廃止すること。

C. 担当省庁・機関

●科学 ICT 部

2) インターネット実名制：公職選挙法、青少年保護法、ゲーム産業法

2-1) 公職選挙法上の実名制

A. 背景

●公職選挙法第 82 条の 6⁷⁷は、インターネット報道機関が選挙運動期間中、自社のホームページの掲示板・チャットルームなどの政党・候補者への書き込みを投稿する場合は、実名を確認しなければならないとしており、その方法として情報通信網法第 44 条の 5 による本人確認措置を列挙している。

●インターネット報道機関には、ネイバーなどポータルサイトもその対象となる。また、法は、本人確認の措置義務の対象として「政党・候補者への支持・反対の文を一般の利用者が投稿できるようにする場合」として支持、反対のメッセージが投稿される「可能性」があれば、規制対象とされるので、事実上一般の利用者がメッセージを投稿できるようにしている掲示板、コメントなどのサービスを提供している場合は、すべて規制対象となる。

●公職選挙法上実名制は、匿名表現の自由を侵害するだけでなく、匿名通信の自由を侵害する。

B. 勧告

●匿名通信の自由を侵害する公職選挙法の実名制を廃止すること。

C. 担当省庁や機関

●中央選挙管理委員会

⁷⁷ 第 82 条の 6 (インターネットの掲示板・チャットルーム等の実名確認) 1 インターネット報道機関は、選挙運動期間中に、当該インターネットのホームページの掲示板・チャットルームなどの政党・候補者への支持・反対の文字・音声・画像や動画などの情報 (以下この条文において「情報等」という。) を発することができるようにする場合には、行政安全部長官又は「信用情報の利用及び保護に関する法律」第 2 条第 4 号の規定による信用情報業者 (以下「信用情報業者」という) が提供する実名認証方法によって実名を確認する技術的措置を講じなければならない。ただし、インターネット報道機関が「情報通信網利用促進及び情報保護等に関する法律」第 44 条の 5 による本人確認措置をした場合には、実名確認の技術的措置をしたものとみなす。

2-2) 青少年保護法上の実名制

A. 背景

2012年9月16日から施行されている青少年保護法第16条⁷⁸では、青少年有害媒体物を提供しようとする者に「年齢確認」のほか、「本人確認」の義務を課している。

●青少年有害媒体物にアクセスしようとする人の年齢確認にとどまらず、若者や成人を含むすべての人々の本人確認義務化は、匿名通信の自由、個人情報の自己決定権、匿名表現の自由、知る権利を侵害する。

●特に青少年保護法上の本人確認のためには、本人確認機関が利用者の個人情報を常に確保している必要がある。事業者の本人確認要求に応じて発生する本人確認情報が本人確認機関に集積されると、必然的に、個人情報の流出の危険が増すことになる。

●オープンネットは、2013年5月、この条項について憲法裁判所に申し立てを行なった。

B. 勧告

●匿名通信の自由と個人情報の自己決定権を侵害する青少年保護法上の実名制を廃止すること。

C. 担当省庁や機関

●女性家族部

2-3) ゲーム産業法実名制

A. 背景

●2012年9月16日から施行されているゲーム産業法第12条の3⁷⁹はゲームへの没頭と中毒予防のために、オンラインゲーム関連事業者には会員登録時に加入者の本人確認することとしており、18歳未満の青少年の場合親権者など法定代理人の同意を得ることを義務づけている。

●オンラインゲーム会員登録時に、青少年と成人を含むすべての人々に対して、本人確認をすることは、匿名通信の自由、個人情報の自己決定権、匿名表現の自由を侵害する。

○特に本人確認のためには、本人確認機関が利用者の個人情報を常に確保している必要があり、このように事業者の本人確認要求に応じて発生する本人確認情報が本人確認機関に集積されると、必然的に、個人情報漏洩の危険が増す。

●オープンネットは、2013年7月、この条項について憲法裁判所に申し立てを行なった。

78 第16条（販売禁止など）1 青少年有害媒体物として大統領令で定める媒体物を販売・レンタル・配布したり、視聴・観覧・使用するために提供しようとする者は、その相手方の年齢と本人を確認しなければならない。青少年に販売・レンタル・配布したり、視聴・観覧・使用させてはならない。

79 第12条の3（ゲームへの没頭・中毒予防措置など）1 ゲーム関連事業者[「情報通信網利用促進及び情報保護等に関する法律」第2条第1項第1号の情報通信網（以下「情報通信網」という。）を通じて公衆にゲーム利用サービスを提供する者に限る。以下この条において同じ。]は、ゲーム利用者のゲームへの没頭・中毒を予防するために、次の各号の内容を含む、過剰なゲーム物利用防止措置（以下「予防措置」という。）をとらなければならない。

1. ゲーム利用者の会員登録時に実名・年齢確認と本人認証
2. 青少年の会員登録時に親権者など法定代理人の同意を得ること
- 3.-7. 省略

B. 勧告

- 匿名通信の自由と個人情報の自己決定権を侵害するゲーム産業法上の実名制を廃止すること。

C. 担当省庁や機関

- 文化体育観光部

5. 個人情報の保護

1) ビッグデータと個人情報保護法制⁸⁰

A. 背景

- 政府は、ビッグデータ産業の活性化を理由に、情報主体の同意を得ない個人情報の活用を可能にすることにより、情報主体の個人情報の自己決定権を侵害している。

- 2016年6月に、朴槿恵政権は関係省庁（国務調整室、行政自治部、放送通信委員会、金融委員会、未来創造科学部、保健福祉部）は合同で<個人情報の非識別措置ガイドライン>を発表する。これによると、個人情報をガイドラインに沿って非識別措置された場合は、「個人情報ではないものと推定」して、情報主体の同意なしに収集目的外利用ができるようにする。また、韓国インターネット振興院（KISA）などの公共機関を専門機関に指定して、さまざまな企業で非識別処理された個人情報の結合をサポートし、結合された(非識別)個人情報を元データを保有する企業に提供する。

- 2017年の国政監査で明らかになったところによると、非識別措置のガイドラインに基づいて2016年8月から2017年9月までに26回にわたって約3億4千万件の民間企業のデータが結合された。情報主体は、自分の個人情報が結合のために活用されたことについて通知受け取っておらず、その企業に閲覧を要求しても回答得られていない。

- 市民団体は、2017年11月9日、4つの非識別専門機関と20の企業を、個人情報保護法違反などの疑いで告発したが、検察は2019年3月25日、この告発を不起訴処分とした。

- 文在寅政権は2018年11月15日、個人情報保護法改正案（印在謹議員代表発議）を提出したが、これによると、統計の作成、科学研究目的のために仮名情報を情報主体の同意なしに、当初の収集目的外で利用したり、第三者に提供できるとしている。（第28条の2）。ところが、ここでいう科学研究には、データに基づいて、新しい技術・製品・サービスの開発など、企業内部のR&Dが含まれている。また、<個人情報の非識別措置ガイドライン>同様、指定された専門機関を介して相互に他の企業の個人情報を結合し、結合された個人情報を仮名や匿名処理して、元データ保持企業、あるいは第3者企業に提供できる。（第28条の3）仮名情報については閲覧権、保管期間の制限、流出通知などの情報主体の権利も制限されている。

- 市民社会は、政府の個人情報保護法の改正案は、企業が仮名処理された個人情報を情報主体の同意なしに販売、共有、結合できるようにすることで、消費者（利用者）の個人情報の権利を侵害していると批判している。

- 政府が2018年11月15日発議した信用情報法改正案（キム・ビョンウク議員代表発議）は、上記の個人情報保護法改正案のように、個人の信用情報を仮名処理をすれば、企業の営利的な研究目的のために、情報主体の同意なしに活用できるようにしているだけでなく、SNSの情報を情報主体の同意なしに信用評価を目的として活用できるようにしている。公開されたSNSの情報とはいえ、情報主体の意

80 執筆 Korean Progressive Network Jinbonet

思とは無関係に自由に活用できるわけではなく、SNSの情報を信用評価に活用することは、利用者のSNSを通じた表現の自由を侵害するおそれがある。

B. 勧告

●仮名処理された個人情報の同意なしでの活用は社会の学術的基盤を強化する学術研究に制限されるべきであり、単に企業の内部的な研究のために、企業間販売、共有、結合してはならない。学術研究目的のために個人情報を提供するばあいであっても、可能な匿名処理をするなど、十分な安全対策が設けられなければならない、当該目的の達成を阻害しない限り、情報主体の権利を保障しなければならない。

●ビッグデータの経済的活用を優先する政府の個人情報保護法改正案と信用情報法改正案は、廃案とすべきであり、少なくとも欧州 GDPR レベルの個人情報保護制度を準備すべきである。

C. 担当省庁や機関

- 行政安全部
- 放送通信委員会
- 金融委員会
- 個人情報保護委員会

2) 個人情報の監督機関⁸¹

A. 背景

●国連の<コンピュータ化された個人データファイルの規制に関するガイドライン>(1990)は、すべての国は、列挙された原則の遵守を監視する独立した機関を設置するように求めている。また、欧州評議会の<監督当局および国境を越えたデータフローに関する個人データの自動処理に関する個人保護条約の追加議定書>(2001年)は、調査権、命令権、意見提示権、司法訴追権などの個人情報監督機関の具体的な権限を明示している。

●韓国の場合、個人情報保護法、情報通信網法、信用情報法などに分散しており、個人情報監督機構も行政安全部、放送通信委員会、金融委員会、個人情報保護委員会などに分散されている。行政安全部は、政府省庁としての独立性がなく、放送通信委員会と金融委員会は、ビッグデータの産業育成を口実に個人情報保護の緩和政策を推進している。個人情報保護委員会は、人事や予算の独立性がなく、調査権、是正措置権などの監督機関として執行権限を持っていない。また、監督機関が分散されており、統一された個人情報保護方針の推進と効率的な監督が阻害されている。

●政府は2018年11月15日に個人情報保護法の改正を提案し、内務省と韓国通信委員会の監督当局を個人情報保護委員会に統合しました。これは歓迎すべき動きである。ただし、金融サービス委員会の監督当局は依然存在し、この改正が個人情報保護委員会の一部の権限のみを指揮監督するように首相の権限を排除していることや首相が個人情報保護に関連する法律の改善、データ保護に関するポリシーと計画の確立と実施など、委員会の重要な機能を監督することを前提すると、個人情報保護委員会の独立性は制限されている。

B. 勧告

●個人情報監督機構を、個人情報保護委員会に一元化して、完全な独立性を確保すること。

81 執筆 Korean Progressive Network Jinbonet

C. 担当省庁や機関

- 行政安全部
- 放送通信委員会
- 金融委員会
- 個人情報保護委員会

3) 消費者の個人情報⁸²

A. 背景

- ホームプラスは、保険会社に有償販売する目的で個人情報約 712 万件を収集しながら、この販売の事実を告知しなかった。消費者が読めないように個人情報の同意事項を 1mm のサイズの大きさの文字で記載した。また誕生日、子供の数など、不要な項目についても同意せざるをえないようにさせた。
- 一方、ホームプラスは、第三者への提供の同意なしに、保険会社に個人情報を渡した。保険会社はフィルタリングを行ない、保険契約を締結する可能性がある人だけを抽出した。こうして抽出された人々の同意を得てホームプラスは、再び保険会社にデータを渡した。
- 韓国消費者団体協議会が、消費者 683 人を原告とし、被告ホームプラス、ライナ生命保険、新韓生命保険に対して起した損害賠償請求訴訟で、控訴審は、ホームプラスがお客様感謝イベントの一環として、景品を支給するような欺罔的な広告行為をしたこと、個人情報の収集・利用目的等の事項を約 1mm のサイズの読みにくい小さな文字で記載した点、抽選の事実を知らせるのに必要な個人情報と関連のない私生活の秘密に関する情報と固有の識別情報まで収集したことにより、目的外の情報収集などを指摘し、個人情報保護法、表示広告法などに違反したとした。そして、このようなホームプラスの不法行為で被害者らが精神的苦痛を受けたことが認められるとして、ホームプラスに慰謝料 20 万ウォンを支給するように判示した。また、ホームプラスが第三者である保険会社に個人情報を提供した行為は、個人情報保護法に違反したものとした。ファミリーカード会員としては、自分の個人情報を第三者が知る不安や、これを営業に活用することで、自分たちが営利行為の対象として扱われているという不快感を感じているとして、ホームプラスと保険会社は、共同して、精神的損害に対する賠償各 50,000 ウォンを支払わなければならないと判示した。
- 一方裁判所は、個人情報保険会社に提供された事実の立証責任は消費者にあるとした。違法行為の被害者であることを消費者側が立証できていないと判断して、刑事訴訟においては、個人情報提供が明確に立証されていないファミリーカード会員 222 人の請求をすべて棄却した。現在の原告 222 人の上告審手続が進行中である。
- 集団訴訟、消費者の被害について、民事訴訟法上の損害賠償請求だけが提起できている。しかし、多数の侵害があったとしても、共同訴訟に参加した消費者のみが救済される。また、企業がすべての証拠を握っている状況で、消費者に立証責任があるために、訴訟にかかる長い時間と高いコストに耐える必要がある。たとえこれに耐えることができても賠償金額は被害額に比べて著しく低い。したがって、消費者の被害を補償するうえで明らかに限界がある。

B. 勧告

- ホームプラスは、個人情報約 600 万件を販売し、約 119 億ウォンという莫大な収益を得たにもかかわらず、被害救済額は 1% にも満たないほど少ないことは、集団訴訟制が存在しないことによる消費者被害救済の限界である。したがって集団訴訟制の迅速な導入が必要である。

82 執筆 Korea National Council of Consumer Organizations

●少額、多数の被害を救済することができる最も効率的な方法は、「消費者集団訴訟制」の導入である。消費者被害の特性に合った手順と立証責任の軽減、証拠開示制度、懲罰的損害賠償などの法の実効性を高めることができる「消費者集団訴訟制」の導入が必要である。

●裁判所はファミリーカード会員の個人情報保険会社に提供された可能性が少なくないし、証拠の偏在などにより、被告が証明する上で容易な立場にあることを認めながらも、法解釈の原則だけを固守し、消費者に立証責任を負わせた。消費者が企業の不法行為の事実を立証することは事実上不可能に近く、立証責任の転換が必要である。

C. 担当省庁や機関

●労働安全部

●個人情報保護委員会（個人情報保護法所管省庁）

4) 健康情報とプライバシー権⁸³

4-1) 医療情報の目的外利用及び提供

A. 背景

●診療の過程で医療機関から収集された情報は、原則として医療機関が個人の医療目的達成のためにだけ収集、利用する。

●しかし、現代の医療はますますデジタル化され、様々な医療情報の処理主体が介入することにより（電子処方箋メーカー、電子カルテのメンテナンス会社、医療情報ストレージ会社、医療機器会社、薬局など）、これらのそれぞれが、患者の明示的な同意と法的根拠なしに医療機関で収集された患者の医療情報を処理している状況が生じている。

●関連する状況

○2010年SKテレコムが電子処方箋の形式で提供された医療機関の患者情報を患者の同意なしに、独自のサーバーに保存して処理し、ここから利益を得た：現在刑事裁判進行中である。

○2010年薬学情報センターが医療機関が処方で薬局に提供した医療情報を加工して、患者の同意なしにIMS Healthに提供して利益を得た：現在刑事裁判進行中

○医療機関がクラウドサービスを提供するIT企業と提携して、患者の医療情報を関連するIT企業のクラウドに集積し、これを患者の同意なしに、さまざまな用途で活用しようとする試みを見せている

○アサン医療センター（現代グループに属する主要病院）、現代重工業（コングロマリット）、カカオコーポレーション（大手IT企業）が合併会社を設立することに関するニュース報道：「カカオAは医療ビッグデータ産業に進出」

○ソウル大学ブندگان病院（最高ランクの病院の1つ）、デウン製薬（韓国最大の製薬会社の1つ）、NAVER（別の大手IT企業）が合併会社を設立したことに関するニュース報道：「IT企業、医療業界に手を伸ばす」

○政府は、モバイルアプリケーションを介して、個人の医療情報を保険会社に簡単に提供することができる方法を推進：「政府は保険会社から個人の健康情報を保護する障壁を取り除く」

○健康保険審査評価サービス（HIRA）は、提供されたデータが特定されないかたちで、52回（サンプル総数は6420万人）にわたり民間保険会社にサンプル研究DBを提供。

83 執筆 Center for Health and Social Change

B. 勧告

- 情報主体の同意なしに医療情報の目的外利用、提供を厳しく規制し、極めて例外的な場合に限るとし、法制度を明確にして、規制に関連するグレーゾーンをなくす。

C. 担当省庁や機関

- 保健福祉部

4-2) 健康情報の保存

A. 背景

- 健康関連の個人情報は、目的達成の必要性がなくなった後は廃棄することが原則である
- しかし健康保険公団、健康保険審査評価院、個別医療機関等は、研究目的の使用などの理由で明確な法的根拠なしに関連情報を半永久的に保持しているのが実情である。
- (デジタル権利研究所、データセットの接続と結合を強化するシステム開発に関する研究、原題 데이터 연계·결합 지원제도 도입방안 연구, 2017)2017年。

B. 勧告

- 健康情報を扱う医療機関および公的機関が健康情報を保持および使用できる期間を定義する法的および管理上のガイドラインをより具体的に定義する必要がある。

4-3) 医療機関による個人情報の保護に関する保障措置の義務不履行

A. 背景

- 健康情報は、個人情報の中でも特に重要な個人情報であるため、個人情報保護法で定めるセキュリティ関連の基準以上に、より徹底してセキュリティ対策が必要な情報である。
- それにもかかわらず、韓国の医療機関は、個人の医療情報のセキュリティレベルが低下し、医療情報の流出や個人情報保護法違反事例が頻繁に発生している。
- 行政安全部が2015年~2016年までの分野別に行政処分した結果を見ると、全体の違反件数(30機関)は73件であり、このうち、医療分野違反件数は22件(6つの機関)であった。(2015年1つの機関4件、2016年5機関18件)

B. 勧告

- 医療機関の個人情報保護義務の履行のために指導、監督を強化

4-4) 個人の健康情報のオープンデータ化

A. 背景

- 健康情報は、センシティブ情報であるため、それ自体はもちろんのこと、仮名処理されたデータも公開は不可である。
- しかし健康保険公団は2017年以前には、仮名処理したという理由で標本データセットを誰でもダウンロードして利用できるようにし、現在も研究者に一定の手続きを経て、標本のデータセットをダウンロードして利用できるようにしている(健康保険公団のホームページ https://nhiss.nhis.or.kr/bd/ab/bdaba000eng.do;jsessionid=khxrsio04MpXAmdiwCaTsdSnb25XGhnGp95JFbHr1BYVCTI9UHBjeXLjrNkSje6p.primrose22_servlet_engine1 を参照)

B. 勧告

●健康情報は仮名化されたとしても、オープンデータの形式では提供しないように関連制度を明文化することを勧告する。

4-5) 健康情報の研究目的利用

A. 背景

●健康情報は、個人の同意なしに研究目的のために利用されることがあるが、その目的は、本来の収集目的に沿うものでなければならず、最大限の安全対策をとった状態で利用する必要がある。

●しかし韓国の場合、法的制度的な規定が不備の状態でありながら、個々の医療機関や公共機関（健康保険公団など）が保有している個人の医療情報を仮名処理し、一定の手続きを満たしたという条件下で研究者が利用できるようにしている。

●個人情報の主体に個人情報の利用を通知し opt-out する権利を与えなければならないにもかかわらず、これらの手順が守られていない。（健康保険公団のホームページを参照

https://nhiss.nhis.or.kr/bd/ab/bdaba000eng.do;jsessionid=WZzEkwUgzPcCQ9o2asY0Z1KmssRBDsa0pBV7LGvbTNWhzjrdUYlzAD01u70Xrtdr.primrose22_servlet_engine1）

B. 勧告

●個人の同意なしに行うことができる科学研究の範囲は、手続き、セキュリティ対策などについて法制度の明文化を勧告する。

5) 公共機関の個人情報の捜査機関への情報提供⁸⁴

A. 背景

●現行の個人情報保護法（PIPA）によると、「犯罪捜査と公訴の提起及び維持のために必要な場合」、個人情報を目的以外の用途に利用したり、これを第三者に提供することがある（第 18 条第 2 項第 7 号）。「情報主体または第三者の利益を不当に侵害するおそれがあるときを除き」とあるが、具体的な要件が与えられていない。

●現行の個人情報保護法によると、「国家安全保障に関連する情報分析目的で収集または提供要求された個人情報」には、個人情報保護法の主な規制が適用されない（第 58 条第 1 項第 2 号）。

●特に公共機関が保有している個人情報が情報機関や捜査機関に広く提供されていることをめぐって大きな議論がある。捜査機関の場合には、公共機関が保有している個人情報を大量に提供されて容疑者ではない人々を対象に、地引き網式（dragnet）に捜査することが増加しており、健康情報などセンシティブ情報でさえ無令状で提供されている。

●2013 年、警察は、ストライキ中の鉄道労組員の療養給与内訳を国民健康保険公団から無令状で提供を受ける。当時、無令状で警察に提供された鉄道組合員の情報は、国民健康保険公団だけではなく、国民年金管理公団、教育庁などいくつかの公共機関も含まれる。鉄道労組の組合員は違法ストライキの疑いで、2014 年 3 月 11 日に起訴されたが後に無罪判決を受ける。組合員は療養給与内訳の提供について憲法申し立てを提起し、2018 年憲法裁判所で違憲の決定が出される。⁸⁵

84 執筆 Korean Progressive Network Jinbonet

85 憲法裁判所 2018 年 8 月 30 日 2014Hun-ma368

- 2014年、警察は建物に「朴槿恵政権退陣」「国家情報院の不法な選挙介入」などの政府を批判した落書きをした者を捕えることを口実に地方自治体から無令状で3000人の基礎生活受給者の情報を提供を受ける。⁸⁶
- 2016年、警察は、障害者の介助者600人の個人情報と地方自治体から無令状で提供を受け、過去の携帯電話の発信位置情報などを追跡する方法で障害者の受給不正の一斉捜査を実施。障害者の介助者を対象とした地引き網式捜査手法は、多くの地域の警察で利用されている。介助者が憲法申し立てを提起したが、2018年棄却された。
- 2014年国会の国政監査によると、特に健康情報の場合、検察と警察が年平均96万7千件、1日平均2649件の健康保険医療情報を閲覧している。
- 2013年、政府の反対にもかかわらず、国家情報院長を公職選挙法違反で起訴した検察総長に対して、大統領府と国家情報院が、その私生活について査察した。この過程では、地方事務所の保有する家族関係情報、警察コンピュータネットワーク、健康保険システム(NHIS)、学校情報システム(NEIS)、行政システムなどの電子政府システムが不法に照会され、関係者が現在裁判中である。
- しかし憲法裁判所の違憲決定をはじめ、議論が続いているにもかかわらず、情報機関や捜査機関の個人情報の収集を規制・監視する制度改善が行われていない。
- 韓国の憲法裁判所は、公共機関が保有している個人情報を捜査機関に提供することは令状が不要な任意捜査と判断した。ただし、鉄道労働者の申し立てに関しては、病気の名前を含む繊細な医療給付の2年から3年の情報の提供を理由として違憲であるとだけ判決した。しかし、障害者の介助者の憲法訴訟については、受給不正犯罪の公益性が極めて大きいため、地方自治団体の大規模な個人情報の提供は行き過ぎではないという趣旨で棄却した。
- 調査機関による個人情報の収集に関しては、欧州評議会の警察勧告の制定以降、2016年に欧州が「警察指令」⁸⁷と呼ぶものを制定するまで、プライバシーの原則を順守するために、捜査機関にも同様の要求する国際的な基準が強化されてきた。
- 情報機関の個人情報の収集(data collection)については、エドワード・スノーデン事件の後、国連総会のデジタルプライバシー決議(A/RES/68/167)など、国際的に適切な規制と監督の要求が続いている。⁸⁸

B. 勧告

- 警察などの捜査機関の個人情報の収集について個人情報保護原則を遵守するよう規制し、独立した第三者機関からの監督を受けることができるよう制度を改善すること。非容疑者を含む大規模な個人情報収集には、その要件と手続きを具体的に規定するなど、法律に基づく規制を受けるようにすること。特に健康情報など敏感な情報の収集時に令状などの裁判所の規制を受けるようにすること。
- 情報機関の個人情報の収集について必須で衡平性を確保するために、独立した第三者機関からの監督を受けることができるよう制度を改善すること。情報機関が個人情報を収集するためには、その要件と手続きを具体的に規定するなど、法律に基づく規制を受けるようにすること。

86 HUFFPOST KOREA. (2014). The Government Critic Graffiti, Finding Among One of the Basic Feeders? https://www.huffingtonpost.kr/2014/10/15/story_n_5987854.html [15 May2019].

87 IRECTIVE (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

88 A/RES/68/167

C. 担当省庁や機関

- 行政安全部/個人情報保護委員会（個人情報保護法所管省庁）
- 警察庁/国家情報院

6) 社会保障情報システム⁸⁹

A. 背景

- 2010年保健福祉部は、複数の福祉給与事業を1つの電子情報システムで管理する社会保障情報システムの構築（2013年一度拡充し、現在22省庁の360以上の事業管理）
- 社会保障情報システムは、社会保障給付やサービスを受けるすべての者を個人、世帯別に登録し、資格と履歴の管理システムで、2015年12月に、登録された福祉対象者は、17,140,887人（重複を含む）
- 社会保障情報システムの重要な機能の一つは、申請者と受給者の財産と所得の調査のための資料収集と管理である。
- 財産および収入調査のために福祉給与やサービス申請者から一括同意を受けて納税情報など24の公共機関が保有している77の情報（2017年12月基準）と140以上の金融機関から金融取引情報を収集。収集された情報のうちには、出入国記録もある。このうち相当数のデータは年2回の所得・財産変動の確認調査が実施されて自動的に更新されてきた。
- 2014年経済的困難を理由とした60代母と30代の二人の娘の自殺が社会的に大きな反響を起し、政府は支援が必要な人を積極的に掘り起こすと宣言して、「社会保障給付の利用・提供と受給権者の掘り起こしに関する法律」（社会保障給与法）を制定し、停電・断水・健康保険料の滞納などの情報を当事者の同意なしに収集することができるようにしている。ビッグデータを活用した危機家庭の「発掘」により社会保障の死角地帯を解消するというのが目的である。
- こうして発掘された対象者について収集された情報の一部について、地方自治団体に本人の同意なしに提供され、本人同意あれば、民間の慈善団体にも提供されることがある。
- 2017年社会保障給与法を改正し、貸付金、クレジットカード、代金延滞などの個人信用情報を社会保障情報システムによって収集できるようにした。
- しかし、社会保障以外の受給貧困層の根本的な原因は、社会保障制度、特に公共扶助制度を支配する残余主義(福祉などの扶助を主として家族などに委ね、それが無理な場合だけ公的扶助を与えるという考え方：訳注)にある。たとえば、社会保障情報システムに登録された扶養義務者の所得・財産が一定レベルを超えると、公共扶助から排除する方式である。このように、厳格な受給要件により、公共扶助が必要だが給付を受けられない人口は、2015年基準で93万人に達する（政府の推定値）。一方、多くの受信者は、SSISの柔軟性のなさが原因で、受給資格を失ない、自殺につながるケースがあった。
- 政府資料によると、2018年1～11月の間、ビッグデータを活用して、「発掘」した243647人のうち33.4%である81354人だけが支援や連携を取得し、その中で28932人だけが公共サービスを連携を受け、残りは民間の慈善事業に委ねられた。つまり「発掘」された脆弱階層のうち、12%未満が、公共サービスの連携にむすびつけられたにすぎない。
- 2019年4月、保健福祉部は、3,560億ウォンをかけて「次世代社会保障情報システム」を構築すると発表。「次世代社会保障情報システム」として実装する機能の一つは、全国民を対象とする「福祉メンバーシップ」制度である。このシステムは、定期的にシステムに登録された者が適格であると思われる社会保障給付またはサービスに関する評価を行い、特典やサービスの「パーソナライズされたリスト」を提供する。これは、登録された者が同意した家計、収入、財産に関する情報をもとにする。

89 執筆 MINBYUN-Lawyer for a Democratic Society

●つまり、社会保障情報システムに「メンバー」として登録された人について、現在、実際に社会保障給付やサービスを受けていなくても、家計、財産、所得に関する情報を収集し、定期的に変動を反映させるというものである。全国民を対象としており、公共機関、金融機関等数百の機関が収集する膨大な情報を考慮すると、本人の同意を前提としていても、個人情報の保護とプライバシー権の潜在的な脅威が存在する。

●このように、社会保障給付やサービスの潜在的な提供を掲げて、個人のプライバシーに属する膨大な情報を収集し、社会保障システムを電算システムに置き換えるという発想は、情報の集中を通じた統制力強化を目指すものである。

●潜在的な社会補償サービスやその利益の潜在的な提供を口実に、膨大な個人情報を収集しようという考え方、そして、社会サービスの給付システムハ中央集権化されたコンピュータシステムによって補完されうるという考え方は、互いに補いあうことのないセグメント化された利益とサービスのシステムと、これによって立証責任を当事者に負わせ、肝心の脆弱階層は、適切な支援にアクセスすることが困難になるという排除的な構造をそのまま放置するものであって、情報の集中と中央集権化を介した支配をしようとするものである。

B. 勧告

●社会サービスや福利厚生を必要とする人を「発掘する」という口実の下で、脆弱な人々の同意なしに情報収集を中止すること。予算を増額し対象範囲を拡大することにより、社会保障システムの「死角」をなくすこと。

●社会保障情報システムへの過剰な情報集中をもたらす「福祉メンバーシップ」計画を廃棄して、申請者のニーズに合った給与が保証されるように改革し、福祉給付とサービスへのアクセスを向上させること。

C. 担当省庁や機関

●保健福祉部

7) DNA データベース⁹⁰

A. 背景

●住宅取り壊しに反対する住民、労働組合員、露店活動家などがDNA採取対象となり国のDNA身元確認情報データベース(DNA identification database)にDNAの身元確認情報(DNA identification informationの「プロファイル」)として保管されている。

●2011年竜山の住宅解体と双竜労働者が提起した憲法申し立てについて、2014年却下が決定された。DNA被採取者の場合、DNAの身元確認情報が、他の個人情報や指紋などの生体情報とは異なり、家族と共有する遺伝情報が含まれており、国のデータベースへの収集による人権侵害は、子供など家族にまで拡張されることを訴えた。

●2016年KEC労働組合の組合員が憲法申し立てを提起する。2010年の工場占拠ストライキの座り込み中に、「多数の威力により、他人の建造物に侵入した罪」で有罪判決宣告後、令状が発付され、2015年から2016年の間にDNAの鑑識試料(DNA sample)が採取された。2017年の民主露天商全国連合の活動家が憲法申し立てを提起する。2013年アウトレット商店街占拠集会のなかで「多数の威力により、店頭に侵入した罪」で有罪判決が出、れたが、この過程で令状が発付されて、DNAの鑑識試料が採取さ

90 執筆 MINBYUN-Lawyers for a Democratic Society

れた。2018年8月30日、上記二つの事件を併合して、違憲判決が出される。⁹¹令状によるDNA採取理由には、対象者の意見、不服申し立ての権利、および救済が欠けているのがその理由。

●しかし憲法裁判所の違憲判決をはじめ、議論が続いているにもかかわらず、政府は制度の改善のための法改正案を提出しておらず、被害者のDNA情報の削除請求を拒否している。

●2010年に制定されたDNAの身元確認情報の利用及び保護に関する法律の場合に、個別に再犯の可能性について検討することなく少年犯を含む被疑者に対してすべてDNAを採取する。そのDNAの身元確認情報（「プロファイル」と呼ばれる）をデータベースに保管して捜査に利用している。

○このDNA法は、DNAの鑑定試料の採取条件に再犯の危険性を明示しておらず令状手続規則でも令状の要件を明示しておらず、採取対象犯罪に該当する場合、画一的に採取しているという問題がある。

○これによりDNAの身元確認情報データベースのなかで、刑の確定者は23%に過ぎない。⁹²

○また採取対象に住居解体反対で占拠や座り込みを行った住民、労働組合員、露店活動家などが、「集団による威力」行使とみなされてDNA採取対象に含まれる。

●DNA法は、次の場合に限り、データベースから身元確認情報を削除することができる。つまり、無罪など特別な事由である。対象者が死亡した場合、職権又は本人の申請がある場合にのみ身元確認情報を削除することができる。

○対象者が再犯せずにかかなりの時間が経過している場合でもDNAの身元確認情報の保存期間が極めて長いという点で問題は深刻である。

○特に少年犯の場合、非常に過酷である。

○憲法裁判所は、DNA削除規定についての判決における反対意見と補足意見のなかで、国民の基本権の制限を最小限に抑えるため、一定期間再犯しない適切な範囲の対象者の場合には、DNAの身元確認情報を削除できるように改善する必要があると繰り返し指摘している。

第13条（DNA身元確認情報の削除）（1）DNAの身元確認情報担当者は、再審で無罪、免訴、公訴棄却の判決または公訴棄却の決定が確定した場合には、職権又は本人の申請により、第5条の規定により採取され、データベースに収録されたDNAの身元確認情報を削除しなければならない。

（2）DNAの身元確認情報担当者は、拘束被疑者等が次の各号のいずれかに該当する場合には、職権又は本人の申請により、第6条の規定により採取され、データベースに収録されたDNAの身元確認情報を削除しなければならない。

1. 捜査で疑いがないとされ、不起訴処分となるか、第5条第1項各号の犯罪にある被疑者の罪名が捜査又は裁判中同項各号以外の罪名に変更された場合。ただし、不起訴だが、「治療監護法」第7条第1号に基づいて治療監護の独立請求を行なう場合は除く。

2. 裁判所の無罪、免訴、公訴棄却の判決または公訴棄却の決定が確定した場合。ただし、無罪判決であるが治療監護を宣告する場合は除く。

3. 裁判所の「治療監護法」第7条第1号の規定による治療監護の独立請求の請求棄却判決が確定した場合。

91 憲法裁判所 2018.8.30.2016Hun-ma344・2017Hun-ma630。上記法律条項は2019.12.31.を時限的に立法者が改正されるまで適用される。

92 DNA識別データベースの2017年の年次報告書によると、データベースに登録されている合計137,519人のうち、罰金、執行の一時停止、保護観察の一時停止などの刑を宣告されて投獄されている37,636人、および投獄されていない99,883人である。

3 DNAの身元確認情報担当者は、拘束被疑者等が死亡した場合には、第5条又は第6条の規定により採取され、データベースに収録されたDNAの身元確認情報を職権または親族の申請により削除しなければならない。

B. 勧告

●国はDNA身元確認情報データベース収録対象にあり、個々の対象者の再犯危険性について慎重に判断することができるように司法審査手続きを補完し、対象者が意見を陳述したり不服申し立てをすることができるように救済手続きを置くこと。

●対象者が再犯せずにかかりの時間を経過するなど、データベースの目的が達成された場合には、収録された者の身元確認情報の削除権を保証すること。

C. 担当省庁や機関

- 法務部（法律所管省庁）
- 大検察庁（型確定者データベース操作事務）
- 警察庁（拘束被疑者、犯罪現場のデータベース操作事務）

6. 労働監視⁹³

A. 背景

●最近、監視カメラ（以下、「CCTV」）や携帯電話のアプリケーションなどの電子機器を利用して、労働者を監視することが社会的に大きな問題となっている。

●大企業KTは労働者に、特定のアプリケーションのインストールを指示したが、そのアプリケーションをインストールした場合、会社の管理者が個人の携帯電話の連絡先、テキストメッセージはもちろん、現在の位置、カレンダースケジュール、アカウントと写真情報などにアクセスすることができる。会社は、労働者がインストールを拒否すると、その労働者に1ヶ月の懲戒処分を下すなど、実質的にアプリケーションのインストールを強制した。CCTV映像資料を労働者の懲戒に使用した事例は、民間企業だけでなく、教師、警察官など公務員まで、さまざまな業種での問題となっており、いくつかの民間企業は、労働組合の設立後、200人余りが勤務する工場の従業員休憩室などにCCTVの200台設置して、問題になった。

●個人情報保護法⁹⁴は、1)法令で具体的にインストールを許可した場合、2)犯罪の予防及び捜査のために必要な場合、3)施設の安全性と火災予防のために必要な場合、4)交通取締りのために必要な場合、5)交通情報の収集・分析及び提供のために必要な場合以外に公共の場所に映像情報処理機器を設置・運営してはならないと定めている。したがって、労働者を監視する目的でCCTVを設置することは法律で定められた目的から外れ、法的根拠がない。

一方、労働者の参加と協力推進に関する法律第20条第1項第14号は、「事業所内の労働者の監視設備の設置」を労使協議会協議事項に定めており、労働者と協議した場合、労働者の監視の余地を残しているが、個人の携帯電話の内部情報を任意に取得することができるアプリケーションのインストールを強制することは、どのような法律にもその根拠はない。

●国家人権委員会は、CCTVを用いた労働監視を中止し、雇用労働部に事業所が電子監視から労働者の個人情報保護を強化する対策を準備するように勧告したが、現場ではまだ様々な電子機器を利用した

93 執筆 MINBYUN-Lawyers for a Democratic Society

94 個人情報保護法第25条（映像情報処理機器の設置、運営制限）

監視が蔓延しており、新しいメディアを利用した労働監視について対策がなされていないのが実情である。

B. 勧告

●「電子機器を利用した労働監視」を防ぐために、政府省庁レベルでどのような努力がなされているのかを明らかにすべきである。

●2013 年人権委が実施した「情報通信機器による労働人権侵害実態調査」によると、事業所の電子監視のために自分の個人情報侵害されても、これに対して正式に異議申し立てするとの回答は、回答者の 28.4%に過ぎず、個人情報保護法に基づく個人情報侵害申告センターが運営されているという事実を知っている場合も 29.4%にとどまった。こうした認識を改善する方策を提示すべきである。

C. 担当省庁や機関

- 雇用労働部
- 個人情報保護委員会

7. 社会的少数者のプライバシー権

1) 性少数者 LGBTQI とプライバシー⁹⁵

1-1) 軍隊内の合意による同性間の性的行為の犯罪化とプライバシー権

A. 背景

●軍刑法第 92 条の 6 は軍内部の男性間での合意された同性性行為を処罰しており、国内で唯一の合意同性性行為を刑事処罰する条項である。多くの国連機関が上記の条項の廃止を勧告している。憲法裁

95 執筆 Rainbow Action Against Sexual-Minority Discrimination (GongGam Human Rights Law Foundation, Korean Lawyers for Public Interest and Human Rights(KLPH), Labor Party-Sexual Politics Committee, Minority Rights Committee of the Green Party, Daegu Queer Culture Festival, Daegu LGBTQ Human Rights Group Solongos, QUV; Solidarity of University and Youth Queer Societies in Korea, Social and Labor Committee of Jogye Order of Korean Buddhism the Korean lesbian community radio group, Lezpa, Rainbow Jesus, Rainbow Solidarity for LGBT Human Rights of Daegu, QIP Queer In Pusan, Busan Queer Festival, Gruteogi : 30+ Lesbian community grocommunity, Seoul Human Rights Film Festival, Seoul Queer Culture Festival Organizing Committee, Korean Anglican Church's Youngsan House of Sharing (Social Minority Life and Human Rights Center), Yeohaengja : Gender non-conforming people's community, PFLAG Korea, Advocacy for LGBTQ's rights to knowledge, Northwest, Collective for Sexual Minority Cultures PINKS, The Korean Society of Law and Policy on Sexual Orientation and Gender Identity, Sinnaneuncenter: LGBT Culture, Arts & Human Rights Center, Unninetnetwork, Lesbian Human Rights Group 'Byunnal' of Ewha Womans University, Open Door in JB, Sexual Minority Committee of the Justice Party, Network for Glocal Activism, LGBTQ Youth Crisis Support Center 'DdingDong', Korean Transgender Rights Organization JOGAKBO, Trans Liberation Front, Chingusai - Korean Gay Men's Human Rights Group, Lesbian Counseling Center in South Korea, Korean Sexual-Minority Culture and Rights Center(KSCRC), Youth PLHIV Community of Korea 'R', Solidarity for LGBT Human Rights of Korea, Solidarity for HIV/AIDS Human Rights Nanuri+)

判所では、上記の規定の違憲審査が過去 14 年間行われたが、憲法裁判所は 2016 年 7 月の違憲審査で旧軍刑法第 92 条の 5 を合憲とした。政府は憲法裁判で、上記の条件が性的指向に対する処罰ではなく、軍隊内の規律を確立するためのものだ回答した。2017 年メディアは、軍隊内の軍刑法違反の疑いで同性愛者の兵士の捜査を報じ、軍の捜査官は、ゲイの出会い系アプリやソーシャルメディアを利用して、ゲイの兵士を追跡した。軍捜査官は、被疑者の携帯電話に保存されたリアルタイム通信とメッセージなどの個人情報を悪用し、同性愛者と疑われる他の者の身元を把握する連鎖捜査を行なった。大尉 A として知られた軍将校は、起訴され、懲役 6 ヶ月執行猶予 1 年を宣告された。

B. 勧告

- 合意による性的行為を犯罪化する軍刑法第 92 条の 6 を廃止すること
- 軍刑法第 92 条の 6 に基づく捜査の中止を宣言すること

C. 担当省庁や機関

- 国防総省

1-2) 住民登録番号

A. 背景

- 韓国人は出生届をするとき、13 桁の数字で構成された住民登録番号(RRN)を付与される。この数字には、生年月日と性別などの情報が含まれている。1900 年代に生まれた男性の場合、最後が 1 で始まり、女性の場合、2 で始まる。2000 年以降に生まれた人の場合、男性は 3、女性は 4 で始まる。
- 住民登録番号は万能の識別番号として活用されているので、韓国人の場合、不動産取引から投票までのすべての業務で身分証明書と住民登録番号の開示が要求される。このように、多目的に使用される住民登録番号は、厳密かつ侵害の要件により、法的に性別を変えなかったトランスジェンダーは大きな困難をかかえている。身分証明書の提示が難しいのでさまざまな状況で就職、携帯電話の契約、投票などを断念することになる。

B. 勧告

- 住民登録番号を個人の情報を担持しないランダム乱数方式で変更されるべきである。

C. 担当省庁や機関

- 行政安全部

1-3) HIV/ AIDS とプライバシー権

A. 背景

- エイズ予防法が医療関係者による HIV プライバシー権の侵害を防止するための法律の規定を定めているが、医療分野や刑務所で、PLHIV のプライバシー権が侵害されている場合が多い。
- 一般的に会社は、労働者の健康診断の結果が労働者に直接通知されるので、その結果を知ることができない。しかし、企業が特定の医療機関を医療診断先に指定した場合、医療関係者が、労働者の HIV 感染を企業に漏洩することがある。一部の企業では従業員に健康診断結果を直接提出するよう要求している。
- 3 人の PLHIV が国家人権委員会に陳情を提出した。3 人は 2018 年頃、大邱刑務所収監中に看守たちによるプライバシー権侵害があったことを主張した。

●陳情者たちは「特別な患者」と表示され部屋に分離収容された。警備員は、陳情者たちを「特別な患者」または時には「エイズ」と大きな声で呼び、他の収容者と一緒に運動させなかった。時折看守は運動場に線を引き、陳情者たちに制限を加えた。

●エイズ予防法第 19 条は、HIV キャリアを「AIDS 蔓延」に足るウィルスが検出されていなくてもいまだに犯罪者扱いしている。

B. 勧告

●HIV / AIDS とともに生きる者のプライバシー権の侵害を防ぐために必要な措置をとること

●エイズ予防法第 19 条の規定による調査、起訴、処罰をやめること

C. 担当省庁や機関

●保健福祉部

●疾病管理本部

1-4) トランスジェンダーの身体と自律性を確保する権利とプライバシー権

A. 背景

●2006 年最高裁判決⁹⁶以降、裁判所のガイドラインでは、トランスジェンダーの法的認定手続きについての調査事項を示している、⁹⁷「調査事項」という言葉は、裁量権を内包しているが、裁判所は、これを事実上の条件として受け入れている。上記の手続きによると、トランスジェンダーの申請者は 19 歳以上、不妊手術や性転換手術をしており、未婚で、未成年の子供がいないこととされている。申請人は成人であるが、親の同意を必要とする慣行がある。一部の裁判所は、2013 年以降、外部生殖器の手術を必要としないとしているが、他の裁判所では、外部生殖器の手術を含む性転換手術を必要としている。

B. 勧告

●性別変更のために性器の除去、再建手術などの外科的手術を強制することを禁止すること

C. 担当省庁、機関

●最高裁判所

2) HIV/ AIDS とともに生きる人々(PLHIV)とプライバシー⁹⁸

2-1) 医療現場での PLHIV のプライバシーの侵害

A. 背景

●韓国はエイズ予防法⁹⁹にプライバシー侵害を防ぐ条項が存在する。

96 最高裁判決 2006.6.22.2004Su2

97 性転換の性別訂正許可申請事件など事務処理の手順（出典：性転換の性別訂正許可申請事件謄写無処理の手順（改訂 20151.8.[家族関係登録例規第 435 号、施行 20152.1.]）。SOGI 法政策研究会が翻訳したガイドラインの英訳は http://annual.sogilaw.org/review/law_list_en

98 執筆 HIV/AIDS Activists Network Korea

99 エイズ予防法第 7 条（秘密漏洩の禁止）次の各号のいずれかに該当する者は、この法律又はこの法律に基づく命令や他の法令で定めている場合、または、本人の同意がある場合を除いては、在職中もちろん退職

●しかし法の規定の有無にかかわらず、医療現場で PLHIV のプライバシーが侵害される状況が頻繁に発生している。

●以下のような状況・行為が発生している。

○病院が PLHIV の同意なしに他の病院に照会を送信する行為

○病院が PLHIV の同意なしに照会や証明書などの書類に HIV 感染の事実を記載する行為

○病院が PLHIV の同意なしに家族に HIV 感染の事実を知らせる行為

○病院で PLHIV に何の告知なしに HIV 検査を実施する行為

○病院の HIV 検査結果の不注意な通報行為

○病院で医療スタッフが PLHIV が利用する物品に標識をつけて分離して、他人が知りうるようになる状況

[参考]2016 国家人権委員会 HIV 感染医療差別の実態調査

| | Mostly / Usually Yes | | | |
|--|--------------------------------|-------------|-------------|-------------|
| | Period living with HIV (Years) | | | |
| | <5 | 5~9 | 10+ | Total |
| Examination/Surgical operation delay | 6 9.7% | 15 23.8% | 28 35.4% | 49 24.0% |
| Discrimination during medical treatment in other medical divisions | 10 16.4% | 13 20.6% | 31 38.8% | 54 26.5% |
| Discrimination by nurses | 7 11.3% | 9 14.3% | 17 21.5% | 33 16.2% |

後も感染に対して業務上知り得た秘密を漏らしてはならない。

1. 国又は地方自治団体にエイズの予防・管理と感染の保護・支援に関する事務に従事する者
2. 感染の診断・検眼・診療と看護に参加した人
3. 感染に関する記録を維持・管理者

| | | | | |
|---|-------------|-------------|-------------|--------------|
| Discrimination by radiation or laboratory personnel | 3 4.8% | 4 6.3% | 10 12.7% | 17 8.3% |
| Discrimination by administrative staff | 3 4.8% | 6 9.5% | 11 14.1% | 20 9.9% |
| Gossiping about PLHIV by hospital staff | 6 9.7% | 13 20.6% | 21 26.9% | 40 19.7% |
| Marking of HIV into medical chart | 8 13.1% | 19 30.2% | 29 37.2% | 56 27.7% |
| Difficulty faced when disclosing HIV status while visiting a hospital for other illnesses | 43 69.4% | 51 82.3% | 60 76.9% | 154 76.2% |
| Wishing to move to a larger city due to inconvenience while visiting a hospital for medical treatment | 18 29.0% | 18 28.6% | 37 46.8% | 73 35.8% |
| Stating HIV status on prescriptions against the patient's will | 11 17.7% | 14 22.2% | 29 36.7% | 54 26.5% |

B. 勧告

- 後天性免疫予防法の第7条（秘密漏洩の禁止）が実質的効力を発揮できるように措置
- 医療関係者のために必須の教育

C. 担当省庁や機関

- 保健福祉部

2-2) 拘禁施設内 HIV 感染のプライバシー侵害¹⁰⁰

A. 背景

¹⁰⁰ 本内容は、被害当事者2人と人権団体2団体が国家人権委員会に陳述したものに基いている。

●エイズ予防法¹⁰¹に秘密漏洩禁止条項があるにもかかわらず、拘禁施設内でPLHIVの感染の事実が同意なし他人に知られる状況が頻繁に起きている。また、刑務所収監中の活動でHIV感染を理由に分離、排除、差別行為をするのは、「憲法」第10条の人間の尊厳と価値、幸福追求権と「憲法」第11条の平等権を侵害し、「国家人権委員会法」と「刑の執行と収容者の処遇に関する法律」で禁止している病歴を理由にした明白な差別行為である。

●拘禁施設内HIV感染が起居する部屋に特異患者という標識を表示して感染事実が公開されざるをえない状況（例えば、ドアに特異患者と大きく表記して、感染事実が露呈される）

●運動時間を別々に割り当てて、一緒に運動する場合にも、運動場に線を引いて分離・排除する行為

●一切の娯楽活動、更生プログラム参加から排除する行為

●PLHIVの受刑者を他の既知のPLHIVの受刑者と同居するように割り当て、隔離する行為

●呼名するとき大声で特異患者と呼称する行為

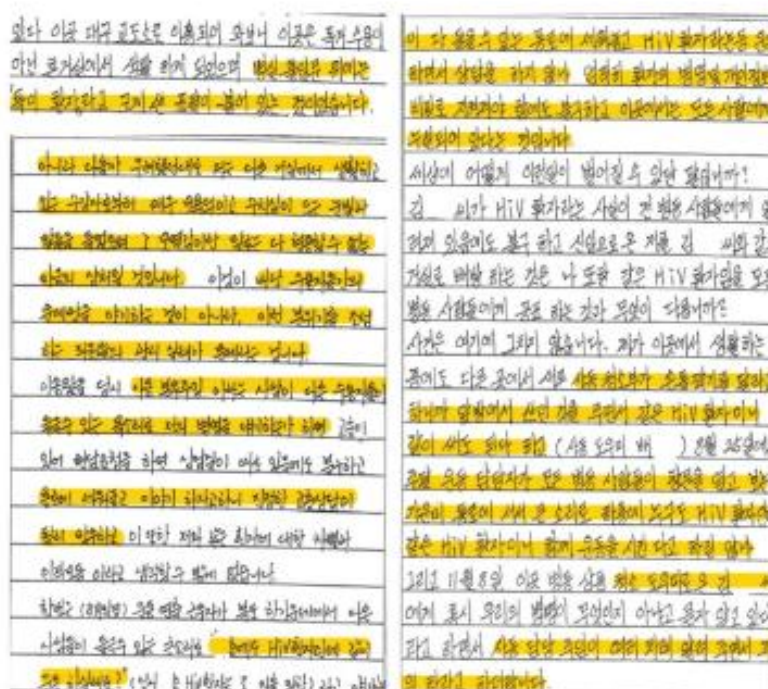
●他の収容者が知りうる状況でHIV病名を記載して感染事実が知られうる状況（例：受刑者が廊下にいる時に病名について話す/保安検査中、警備員が互いに「エイズの部屋に入らないように」と言う/警備員が仲間の囚人の前で「HIV」とマークされた箱から爪切りを取り出してPLHIVに渡す）

●HIV感染収容者との接触の場合にのみマスクなどを使用すること

●矯正行政システムを通じてHIV感染の事実が広く露出した状態

●司法省と校正本部が苦情対応の回答文書に実名で感染と明記して、感染の事実を公開した行為

[参考]大邱刑務所収監中のPLHIVの被害事実が入れられた手紙



101 第7条（秘密漏洩の禁止）次の各号のいずれかに該当する者は、この法律又はこの法律に基づく命令や他の法令で定めている場合、または、本人の同意がある場合を除いては、在職中はもちろん、退職後にも感染に対して業務上知り得た秘密を漏らしてはならない。

1. 国又は地方自治団体でエイズの予防・管理と感染の保護・支援に関する事務に従事する者
2. 感染の診断・検眼・診療と看護に参加した人
3. 感染に関する記録を維持・管理者



[参考]2019.02.15 法務部の方針ブリーフィング（人権侵害の事実を否定する内容で、これ当事者調査一度なく大邱刑務所の回答だけを根拠に発表したものである）

A. 勧告

●入所・収容生活の中で同意されていない HIV 強制検査を停止

○収容医療管理指針第 3 条（入会者の健康診断の実施）5 項は、「すべての新入収容の迅速管轄保健所または検査専門機関に依頼して、梅毒とエイズ検査を行う」ように規定している。この過程で、収容者に HIV 検診事実すら告知されていない状況。本人の同意なしに採血をしたり、検査をすること自体が人権侵害であるため、このような行為を試みてはいけない。

●不十分秘密保障規定（医療情報システム & ボーラムシステム）の改善

○刑務所行政システムの患者情報の保持・記録・管理するための具体的なガイドラインと手順上の秘密漏洩の禁止規定の不在。医療情報システムは、キャリアレーション情報システム（ボーラムシステム）と連動しており、他の拘禁施設でも、収容者の病歴情報を照会することができ、広く PLHIV 収容の情報が公開されている。

●PLHIV の健康権の制限

○収容医療管理指針第 20 条（移送対象の血液透析患者）は、エイズ感染など感染症に罹患していない者だけが、血液透析を受けられるようにして PLHIV の医療アクセスを制限している。しかし、血液透析が必要な PLHIV のための医療アクセス制限措置は、医学的に根拠がなく、疾病管理本部と院内感染管理協会が発行した「透析室での感染管理標準指針」（2010）では「血液媒介感染検査において透析患者が HIV 検査を定期的に行う必要がなく、HIV の予防と管理のために HIV に感染した患者を他

の患者から隔離したり、透析機械を取り外したり担当医療関係者を区別する必要はない。また、透析装置を再利用してもよい。」と規定している。

●人権侵害の再発を防止するために、PLHIVの要求を集約するシステムの導入

○処遇改善要求に調査もせずに対応をする大邱刑務所はもちろん、矯正本部と大邱矯正庁は受刑者の声を聞こうともしておらず、次のように精神的苦痛を訴えている。「彼らは囚人の苦しみを無視し、1回の現地調査もせず大邱刑務所職員からの虚偽の報告を真に受けていることを嘆かざるをえません」

●PLHIVへの人権侵害の再発防止のため、刑務官への教育を導入すること

●法務部所属の全国矯正局に収監されているPLHIVの人権侵害状況の全数調査

●拘禁施設内PLHIV収容者の健康と人権/プライバシー確保のための指針の策定

B. 担当省庁や機関

●法務部

2-3) 青少年 PLHIV のプライバシー

A. 背景

●青少年 PLHIV の数が増えていることに比べて、青年 HIV 感染の心理的安定、人権などを確保するための法制度的装置がない状況である。

●青少年の HIV 感染の事実が当事者の同意なしに法律により家族等の法定代理人に通知することができる状況

B. 勧告

●HIV/AIDS に関する正しい正確な情報と PLHIV の人権についての包括的な性教育の実施

●青少年の HIV 感染の事実を当事者の同意なしに法定代理人に通知させる法条項の廃止

●青少年 PLHIV の実質的な人権保障のための国家的支援システム作り

C. 担当省庁や機関

●保健福祉部

●女性家族部

2-4) PLHIV の労働現場でのプライバシー

A. 背景

●エイズ予防法第 8 条の 2 の 3 項の内容とは異なり、労働現場で HIV 感染の事実を知ることができる状況が頻繁に起きている。

●就職時採用検診に HIV 検査が強制的に含まれている状況

●就職後の定期的な職場内の健康診断の項目に HIV 検診が強制的に含まれている状況

B. 勧告

●労働権の侵害を防ぐために法（第 8 条の 2 の 3 項）が正常に効果を発揮できるように措置すること

●採用検診と職場内の健康検診で HIV 検査を強制的にしないように制度を整備すること

C. 担当省庁や機関

- 雇用労働部
- 保健福祉部

2-5) HIV 感染の兵士と準軍人のプライバシー

A. 背景

- 兵士および準軍人など軍関係者が PLHIV である場合には、機関の長に通報される。また、軍内で HIV 感染の事実が同意なしに他人に知られる状況が発生している。PLHIV は軍事義務から免除されているため、ほとんどの場合、軍入隊後に HIV 感染について知ったときに生じる。
- 軍において HIV 感染の事実が同意なしに他人に知られている状況
- HIV/AIDS を恐れるような雰囲気醸成し排除する雰囲気の形成（例えば、消毒の命令など）

B. 勧告

- 疾病管理本部が推進しているように、共同生活で感染する恐れはないので、通知条項を廃止すること
- 正しく正確な HIV/AIDS の情報と PLHIV の人権について関係者の教育を実施するとお

C. 担当省庁や機関

- 国防総省
- 兵務庁
- 警察庁

2-6) 国家による PLHIV の私的領域（性行為）の制御と介入

A. 背景

●U = U キャンペーンによって、抗レトロウイルス治療を受けている PLHIV が HIV を感染させる可能性は 0% であることが証明されている。それにもかかわらず、HIV/AIDS 防止法の第 19 条（HIV/AIDS の伝播および拡散の禁止）により、「コンドームのなしの性行為」で PLHIV は罰せられる可能性がある。エイズ予防法上 19 条の行為の禁止条項は、PLHIV の「コンドームのない性行為」を処罰している。これは、関係する相手が PLHIV が HIV の状態を事前に通知していて、その後 PLHIV との性行為にすすんで同意した場合でも同様である。さらに、これは、性的行為の結果として HIV の感染が生じなかった場合にも当てはまる。法律は、国による PLHIV のプライバシー権の明らかな違反である。

B. 勧告

- エイズ予防法上 19 条の保持・拡散行為の禁止条項を廃止。

C. 担当省庁や機関

- 法務部

3) 北朝鮮離脱住民のプライバシー権の侵害¹⁰²

A. 背景

102 執筆 民主社会のための弁護士の会

●2016年4月12日、中国の北朝鮮系の食堂で働いていた従業員12人と支配人1人が集団入国し、入国直後、統一部の緊急ブリーフィングで入国の事実が公開された。

●北朝鮮離脱住民が大韓民国に入国する場合、国家情報院が捜査を進め、当事者の身元、入国の事実と入国経緯については公開せずに保護及び定着支援を決定した場合、統一部は、保護と支援内容の詳細を決定する。

●しかし2016年4に入国した従業員については、入国直後に入国事実が明らかにされ、当事者が北朝鮮離脱住民の保護センターに入る様子を撮影した写真がマスコミを通じて公開された。撮影者の身元はわからないが、当時従業員を撮影した写真がマスコミに報道され、現在も関連記事に引用されている。



●その従業員たちは、写真がメディアに公開されるとは全く思わなかったし、保護センターに入る写真が報道されるとも考えていなかった。その従業員を知っている人であれば、写真を使用して身元を割り出すことができ、実際に当該従業員が関連する質問を受けたりしている。

●北朝鮮離脱住民の保護センターは国家情報院が運営、管理しているが、情報院は、関係法令上、北朝鮮離脱住民に対する捜査の権限があるのみであって、原則的に北朝鮮離脱住民の保護及び定着支援業務は、統一部の所管である。それにもかかわらず、北朝鮮離脱住民の身元確認及び調査に関する権限を国家情報院が幅広く保有し、恣意的に北朝鮮離脱住民に関する情報を公開するかどうかやその内容を決定している（添付2関連法令）。

●北朝鮮離脱住民を保護し、定着支援する法制度の目的とは異なり、北朝鮮離脱住民の保護センターを運営、管理する国家情報院は、北朝鮮離脱住民の個人情報収集し活用するプロセスを制御することが困難になっている。また、国家情報院長が保護するかどうかを決定する「国家安全保障に著しい影響を与えるおそれがある者」の判断基準が曖昧で、誰が国家情報院の管理対象となるのか予測しにくく、また国家情報院の判断に委ねられている。上記従業員の場合は、中国の北朝鮮系食堂で働いていたという履歴が「国家安全保障に著しい影響を与えるおそれがある場合」とみなすのは困難であるにもかかわらず、国家情報院は、従業員を北朝鮮離脱住民の保護センターで継続して管理している。

B. 勧告

●国家情報院が北朝鮮離脱住民の保護センターを運営、管理しつつ、具体的な基準なしに北朝鮮離脱住民の捜査を実施して関連情報を収集し、管理することは適切ではない。北朝鮮離脱住民の個人情報を含む関連情報の一律的な管理システムを設け、これを北朝鮮離脱住民の保護及び定着支援業務の所管省庁である統一部の担当にする必要がある。

C. 担当省庁や機関

- 国家情報院
- 統一省

北朝鮮離脱住民の保護及び定着支援に関する法律

第10条（定着支援施設の設置）

1 統一部長官は、保護対象者の保護及び定着支援のため定着支援施設を設置・運営する。ただし、第8条第1項ただし書の規定により国家情報院長が保護することに決定した人のためには、国家情報院長が、別の定着支援施設を設置・運営することができる。

第8条（保護決定など）

1 統一部長官は、第7条第3項の規定による通知を受信すると、協議会の審議を経て、保護するかどうかを決定する。ただし、国家安全保障に著しい影響を与えるおそれがある者に対しては、国家情報院長が、その保護するかどうかを決定し、その結果を遅滞なく統一部長官と保護申請者に通知したり、通知しなければならない。

第7条（保護の申請など）1 北朝鮮離脱住民としてこの法律による保護を受けようとする者は、在外公館やその他の行政機関の長（各級部隊の章を含む。以下「在外公館長等」という。）に保護を直接申請しなければならない。ただし、保護を直接申請していないことがある、大統領令で定める事由がある場合には、この限りでない。

2 第1項本文による保護の申請を受けた在外公館長等は、遅滞なく、その事実を所属中央行政機関の長を経て、統一部長官と国家情報院長に通知しなければならない。

3 第2項の規定により通知を受けた国家情報院長は一時保護やその他の必要な措置をした後、遅滞なく、その結果を統一部長官に通報しなければならない。

北朝鮮離脱住民の保護及び定着支援に関する法律施行令

第12条（臨時保護などの内容）1 法第7条第3項の規定による一時保護やその他の必要な措置は、保護の申請後、保護申請者の一時的な身辺安全措置と保護するかどうか決定などのための必要な調査とする。

2 国内に入国した保護申請者の第1項の規定による一時的な身辺の安全対策と調査の期間は、その保護申請者が国内に入国した日から90日を超えることはできない。ただし、入国者の増加などやむを得ない事由がある場合には、協議会の審議を経て、その期間を1回に限定して30日の範囲で延長することができる。

3 第1項の規定による一時保護やその他の必要な措置の内容・方法と必要な措置のための施設の設置・運営等については、国家情報院長が定める。

4) 外国人被疑者のプライバシー権の侵害¹⁰³

A. 背景

●2018年10月7日、京畿道高陽市ファジヨンダンのパイプライン会社の支社の屋外ガソリントank 14基中1基が爆発する火災事故が発生した（以下、「高揚貯油所火災」という）。高揚貯油所の火災は、非常に大きな火災であり、ガソリン火災だったので、消火が難航した。警察は火災数時間前に外国人労働者のランプの火を高揚貯油所火災の原因と指摘し、2018年10月8日、外国人労働者Aを緊急逮捕した。警察は直ちにメディアにAの実名、国籍、年齢、職業、収入、逮捕場所などを伝えた。

●高揚貯油所の火災は、メディアの大きな関心を集めた事件だったために、メディアで多くの報道がなされた。メディアは、関連記事では、Aの国籍に関心を寄せて「0000(国名)の」という表現が継続的に使用された。いくつかのメディアは、Aの年齢と職場、居住地などの個人情報の詳細報道しており、さらにAの顔を公開したメディアもあった。警察はその後メディアにAの陳述と捜査内容を公開し、これがリアルタイムで報道された。

●警察の問題

○「人権保護のための捜査公報準則（法務部訓令第761号）」によると、捜査事件を公報するに当たっては、目的の達成に必要な最小限のものを正確に公開しなければし、事件関係人の名誉など人権を侵害したり、捜査に支障を与えないように注意しなければならない（第13条）。したがって公訴提起前の捜査事件の容疑事実と捜査状況など捜査関連の内容一切を、原則として公開せず、（第9条）、やむを得ず事件関係人を公開する場合、匿名の使用を原則とし、事件関係人の人格と私生活、犯罪電力、文の内容、証拠関係など、特別な事情がない限り公開を禁止している（第19条）。また、合理的な理由なく性別、宗教、年齢、障害、社会的身分、出身地域、民族、国籍、政治的意見などを理由にした差別を禁止している（第6条）。

○警察は捜査事件の内容を公開することができる例外事由に該当しないにもかかわらず、高揚貯油所の火災事件の捜査内容を公開しており、Aの実名、国籍、年齢、職業、収入、逮捕場所などを公開した。警察の公開行為は、人権保護のための捜査公報準則違反であり、Aの個人情報の自己決定権を侵害する行為である。

○特に警察はAの国籍と外国人労働者という身分を強調し、メディアもこれを強調して報道した。これは出身地域、人種、国籍、社会的身分を理由にした差別である。

○国家人権委員会は、2019年5月17日、警察がAのプライバシーを侵害したことを認める決定を下した。

●メディアの問題点

○メディアは、警察が公開したAの個人情報をむやみに報道してAの個人情報の自己決定権を侵害した。

○国家人権委員会と韓国記者協会が共同で作成した人権報道準則によれば、メディアは固定観念や社会的偏見などによる人権侵害を防止するために用語の選択と表現に注意を払う必要がある（人権擁護のための報道準則6条）。また、メディアは移民の根拠薄弱で不正確な推測による否定的なイメージを助長したり、差別してはならない（人権のための報道準則分野別要綱第5条）。しかし、マスコミはAの国籍と外国人労働者という身分に集中して報道した。端的な例として、Aが放った風ランプは、前日B小学校の行事で使用された風ランプだったが、B小学校の名前はほとんど報道されなかった。Aは、少なくとも1000回以上報道された。結局メディアは高揚貯油所の火災と無関係なAの国籍と外国人労働者という身分を集中的に報道することによって、移民への否定的なイメージを助長した。

103 執筆 MINBYUN-Lawyers for a Democratic Society

B. 勧告

- 警察は、人権保護のための捜査公報準則を遵守しなければならない。また、捜査公報準則に違反した公報の制止ができるような実効性のある方法を模索する必要がある。
- メディアが人権報道準則を厳密に遵守するように強制する方法を模索する必要がある。

C. 担当省庁や機関

- 警察、言論仲裁委員会

5) 児童のプライバシー権の侵害

5-1) 生活記録簿と全国教育情報システム (NEIS) ¹⁰⁴

A. 背景

- 学生に対して作成が義務づけられている学生生活記録簿に追加されている内容が多すぎ、学生の細かい個人情報まで収集され記録されている

1. 個人情報 - 本人の氏名、性別、社会保障番号、住所/家族の氏名、生年月日/特記事項
2. 学校事項 - いつどの学校を卒業し、いつでも学校に入学したのか
3. 出欠状況 - 授業日数、欠席日数、遅刻、早退、結果 (病気/不正/その他)
4. 受賞歴
5. 資格と認定取得状況 - 資格と認証取得状況、National Competency Standard の修了
6. 進路希望
7. 創造的体験活動状況 - 自律活動、ボランティア活動、サークル活動、進路活動、自治活動、特別活動など
8. 教科学習状況 - 内申評価 (成績) / 科目別の詳細能力特記事項
9. 読書活動状況 (2016 年までは本のタイトルと簡単な感想を、2017 年からは本のタイトルのみ減少)
10. 行動特性と総合意見 (各学年担任の意見)

- これらの学生生活記録簿の追加内容は、個々の学生への同意手続きなしに収集され記録さ入力過程に学生が関与できる制度は存在しない

- こうして作られた学生生活記録簿は NEIS というオンライン教育情報システムに保存されるが、その結果、政府は、すべての学生の個人情報を同意手続きなし一括して収集することができる。また、NEIS に収録されたデータについては、学生の意思に反しても、親または管理者などが閲覧可能。

- NEIS に保存された学生生活記録簿は、半永久的に保存される。同意手続きを経ずに収集した生徒の個人情報を廃棄期限を定めないまま国が保管している。

B. 勧告

- 生活記録簿の作成のために収集する情報の範囲を縮小する必要がある
- 生活記録簿の内容に対する異議申請、対処手順などを用意するなど、生活記録の作成プロセスについて、学生が制度的に参加できる方案が用意する必要がある。
- 学生の意思に反する NEIS 個人情報の収集と保護者などの第 3 者の閲覧を制限することができる手順が用意する必要がある
- 学生の意思に基づいて NEIS に収集された個人情報が廃棄されることができる手順が用意する必要がある

104 執筆 ASUNARO: Action for Youth Rights of Korea

C. 担当省庁や機関

●文部科学省

5-2) 学校の学生生活規定や慣習的に行われる個人情報の侵害

A. 背景

●学校内の生活規則、慣行などで名札付、持ち物検査、日記帳の検査が行われている

●多くの学校では、学校生活の規定に制服に名札を付け、学校に通学するときは制服を着るように義務づけられ、これにより、在学中の学校、学年、名前という情報が望まなくても、登下校で不特定多数に公開されることとなる。2010年人権委で人権侵害との指摘を受け、しばらく減少したが、最近再び学校レベルで名札をつけるように誘導し再び増加傾向にある。

●2016年人権委で実施した「学校生活における学生の人権保障の実態調査」によると、調査に参加した学生の17.6%が事前の同意なしに持ち物検査を受けたと答え、学生人権条例が制定されているところではこれは禁止されているが、制定されていないところでは、学生生活の規則や慣行に基づいて行われる場合が多い

●強制的に日記を書くと、日記帳の検査を実施する慣行が小学校では強く残っている。2008年から人権委はこれを人権侵害との結論を出したが、十分改善されていない

B. 勧告

●持ち物検査禁止、日記帳検査禁止、名札禁止など児童のプライバシー権を保護するための内容が実効性のある基本的な法律で規定される必要がある

●学生の生活のために規則を改定する際に学生が参加できる手続的権利が保障されるべきであり、参加が排除された場合、異議を申し立てることができる手続きも準備する必要がある

C. 担当省庁や機関

●文部科学省

5-3) 保育園 CCTV¹⁰⁵

A. 背景

●2015年4月、保育園 CCTV 義務化を含む乳幼児保育法が国会を通過した

●児童と保育所の従業員のすべての行動が撮影されることにより、児童と教師の日常生活全般が記録されて子供のプライバシーを侵害する結果になっている

●児童虐待に関するメディアの報道で CCTV 映像が目的外利用される場合に、児童のプライバシー侵害が広範囲に発生するおそれがある

●CCTV 設置義務化措置にもかかわらず、保育園児虐待件数と全児童虐待事件における保育園児虐待事件の割合は増加しているので(保健福祉部全国児童虐待の現状レポート)、こうした対策は疑問である

●加えて、親と教師の同意の下に CCTV を設置をしていない場合でも、親の保育所への参加権を促進などを通じて、児童のプライバシーを侵害しない方法での子供の安全を確保することができている

B. 勧告

105 執筆 ASUNARO: Action for Youth Rights of Korea

- 保育園 CCTV 設置義務を廃止する必要がある
- 保育教師の処遇の改善、児童当事者の意思に合致して、プライバシー権が確保されることができる
保育環境の改善対策を講ずる必要がある

C. 担当省庁や機関

- 行政安全部
- 文部科学省

5-4) 性に関するプライバシーの侵害¹⁰⁶

A. 背景

- アスナロで、2010 年 9～11 月に行われた「愛しあうことは 19 歳以下でも禁止されない - 若者の恋愛弾圧調査」によると、ソウル冠岳区の中学校、高等学校の 81.3%、京畿道華城市中学校、高校のうち 86.7%の学校が学則に「不健全な異性交際」、「男女間の破廉恥な行為」、異性間あるいは同性間の連絡、関心の表現、出会い、異性間あるいは同性間の身体的な接触、同室滞在、セックス自体を処罰する規定を設けていた。このように、学生のプライバシーを侵害する恋愛弾圧の規定は、まだ多くの中、高校に存在している。
- さらに学校において性少数者を探し出す試みが報告されている。

B. 勧告

- 学生の性的な行為や LGBT 差別に学校が干渉することを禁ずる学生の人権基本法制定が必要である。
- 学生生活のための規定の制定や改訂が、学生の同意を受けて、学生が実質的に参加できる手順を用意する必要がある。

C. 担当省庁や機関

- 文部科学省

5-5) 満 14 歳未満の個人情報の自己決定権¹⁰⁷

A. 背景

- 個人情報保護法第 22 条第 6 項は、個人情報の処理が満 14 歳未満の児童の個人情報を法定代理人の同意を得て処理することができるとしている。
- 上記の法施行令第 17 条第 4 項は、法定代理人の同意を得ずに、児童から法定代理人の氏名・連絡先に関する情報を収集することができるようにしている。
- これらの法により、満 14 歳未満の児童は、自分の意思とは関係なく、自分の情報の処理が決定されている。
- 例えば朝鮮大学が 2017 年頃、政府予算の支援を受けた青少年犯罪や遺伝子関連の研究では、国内の中学校の学生 800 人の口腔上皮細胞などの生体、遺伝情報を収集し、5 年間、その生徒の発達過程を追跡するなど、対象学生のプライバシー権を著しく侵害するおそれが存在した。それにもかかわらず、朝鮮大学は、学生の意思とは関係なく法定代理人の同意だけで研究を進めた。市民団体は、国家人権委員会に、上記の研究は、児童のプライバシー権などを侵害するという内容の陳情を提出した。

¹⁰⁶ 執筆 ASUNARO: Action for Youth Rights of Korea

¹⁰⁷ 執筆 ASUNARO: Action for Youth Rights of Korea

B. 勧告

●満 14 歳未満の児童の個人情報の自己決定権を確保するために法定代理人の同意を得て、児童の意思を確認することができる手順を用意しなければならない。個人情報の処理に関する説明と意思確認の方法は、子供の年齢や発達の様子が考慮されるべきでない。

●児童の意思を確認することができない場合は、法定代理人の同意権行使が子供の意思がに沿うものかどうかを、子供にとっての最善の利益の原則に基づいて判断する手順が必要である。

C. 担当部署/機関

●行政安全部

5-6) 青少年のスマートフォン監視法のスマートフォン監視アプリ¹⁰⁸

A. 背景

●2015 年 4 月 16 日から電気通信事業法(TAB)とその施行令が実施され、法第 32 条の 7¹⁰⁹は、移動通信事業者が、青少年と電気通信サービス提供に関する契約を締結する場合は、青少年有害情報のブロック手段を提供しなければならないとし、同法施行令第 32 条の 8¹¹⁰は通信キャリアが契約締結時にブロック手段の種類と内容等を告知し、ブロック手段を設けることを強制し、契約締結後には、ブロック手段が削除されたり遮断手段が 15 日以上動作しない場合には、法定代理人に通知するとしている。

●ブロック手段とは、スマートフォンのアプリケーションを指すが、現在市販されているブロックアプリは、有害情報遮断以上に、スマートフォン利用状況の監視、位置照会など青少年のプライバシーを過度に侵害し、個人情報を収集する機能を備えている。

○このように監視ないし監視機能を備えたアプリは、セキュリティが脆弱な場合が多く、ハッカーの標的にされ、青少年を、個人情報の流出、ハッキングなどのセキュリティリスクにさらす。特に、政府が開発、販売した「スマート保安官」は、なんと 26 件のセキュリティ脆弱性を有していることがトロント大学 the Citizen Lab at Munk School of Global Affairs のレポート¹¹¹によって明らかにされ、大きな波紋を呼んだ。また、3 大移動通信会社のうちの二つ KT と LGU+によって提供されているブロック手段もセキュリティ上非常に脆弱であることが明らかになっている。¹¹²

●青少年スマートフォン監視法は、移動通信事業者が、青少年のスマートフォンに遮断手段を義務的に設け、青少年がどのような情報を検索し、アクセスするのかを常時監視することで、スマートフォ

108 執筆 Open Net Korea

109 第 32 条の 7 (青少年有害媒体物等のブロック) 1 「電波法」に基づいて割り当てられた周波数を使用する電気通信事業者は、「青少年保護法」による青少年の電気通信サービス提供に関する契約を締結している場合は、「青少年保護法」第 2 条第 3 号の規定による青少年有害媒体物と「情報通信網利用促進及び情報保護等に関する法律」第 44 条の 7 第 1 項第 1 号の規定によるエッチ情報のブロック手段を提供しなければならない。

110 第 37 条の 8 (青少年有害媒体物等のブロック手段を提供すると手順) 1 法第 32 条の 7 第 1 項の規定により、「青少年保護法」による青少年の電気通信サービス提供に関する契約を締結する電気通信事業者は、青少年が電気通信サービスを介して「青少年保護法」第 2 条第 3 号の規定による青少年有害媒体物と違法エッチ情報(以下「青少年有害媒体物等」という。)に接続することを遮断するためには、青少年の移動通信端末装置に青少年有害媒体物等を遮断するためのソフトウェアなどのブロック手段を提供しなければならない。

2 第 1 項の規定により遮断手段を提供する場合には、次の各号の手順に従う。

1. 契約締結時に青少年と法定代理人にブロック手段の種類と内容等の告知

ブロック手段の設置状況をチェック

2. 契約締結後：ブロック手段が削除されたり遮断手段が 15 日以上に動作しない場合、毎月、法定代理人のその事実を通知

111 <https://citizenlab.ca/2015/09/press-release-security-privacy-issues-in-smart-sheriff-south-korea/>

112 <https://citizenlab.ca/2017/11/still-safer-without-kt-olleh-kidsafe-clean-mobile-plus/>

ンを使用している若者の私生活の秘密と自由を侵害し、青少年と法定代理人の個人情報を収集、保管、利用するために、個人情報の自己決定権も侵害している。また、ブロック手段によって有害情報だけでなく、合法的かつ教育的な情報も遮断されて青少年の知る権利を侵害し、ブロック手段を設けるかどうかについて、青少年と法定代理人の選択を認めておらず親の子供への教育権を侵害している。

●オープンネットは、青少年及び青少年の法定代理人（親）を代理して、2016年8月に青少年スマートフォン監視法について憲法申し立てを起し、現在の審理中である。

●青少年スマートフォン監視法は、有害情報から青少年を保護しようという趣旨で導入されたが、移動通信会社は、若者や親の意思とは関係なくブロック手段を義務的にインストールする必要がある、ブロック手段の削除または無効化を親に通知しなければならない。このような監視アプリを強制設置の法は、全世界的に類例がなく、極めて国家による後見主義的な制度である

●特に保護が必要な児童と青少年が無条件に使用するアプリには、さらに厳格なセキュリティ基準が適用されるなければならないにもかかわらず、政府はこうした考慮は一切せず、むしろセキュリティ脆弱アプリを勧めており、これは、より多くの若者をセキュリティリスクに晒す結果を招く。

B. 勧告

●青少年のプライバシーを過度に侵害する青少年のスマートフォン監視法を廃止する。

●青少年をセキュリティリスクに晒すスマートフォン監視アプリ（管理アプリ）のセキュリティ審査基準を設け、現在提供されているアプリの安全性審査を推進する。

C. 担当省庁や機関

●放送通信委員会

●韓国インターネット振興院

6) 性犯罪報道による被害者等のプライバシー権の侵害と被疑事実公表の問題¹¹³

A. 背景

●現在、私たちの社会の性犯罪報道によるプライバシー権の侵害状況

○最近私たちの社会各界各層で性犯罪報道と関連して多くの問題が発生している。メディアは報道の過程で被疑者、被害者とその家族などの個人情報を公開したり、事件と関連のない私的領域を扇情的に報道している。

○一般人でも有名人でも実名で「○○○事件」と報道し、社会的烙印を押す場合が存在する。

○事実関係が歪曲されている場合があり、インターネットやソーシャルメディアを介しこれが迅速に流布されている。

○この場合被疑者、被害者又はその家族等周りの人たちに発生するプライバシー権の侵害は非常に深刻である。

●被害者の民事訴訟を通じた救済

○性犯罪報道によるプライバシー侵害当事者が直接報道機関を相手に民事訴訟（損害賠償、記事の削除など）を提起することも可能であるが、被害者がタイムリーに救済されることは難しい。プライバシー権の侵害はまた、ほとんどの場合、私的な情報が広く流布された状態となるため、被害者の回復が困難である。

113 執筆 MINBYUN-Lawyers for a Democratic Society

○2012年羅州市で小学生を相手に発生した強姦事件があった。上の事件で報道の対象となった被害者と被害者の家族は、報道機関を相手に裁判所に民事訴訟を提起して損害賠償や記事の内容の一部削除が認められる。

○裁判例では、裁判所が、当該報道機関が次のような内容を同意なしに報道して、被害者のプライバシーを過度に侵害したことを認めた。

- 1 衛星写真、家の外部、ドアの窓越しに家の中の乱れた様子などを撮影して放送、
- 2 被害者の子供の傷ついた顔、加害者による歯形のような暴力の痕跡などを放送、
- 3 事件と無関係な被害者の映像日記、読書記録、ノートに描かれた絵などを、被害者の両親の同意なしに撮影して放送

○しかし、第1審 2014年判決、第2審 2015年判決、裁判所の最終的な判決に多くの時間がかかった。

●制裁措置と是正勧告などを利用した規制

○放送法及び放送審議に関する規定に基づく放送通信審議委員会の放送審議、言論仲裁及び被害救済等に関する法律に基づく言論仲裁委員会の是正勧告がある

○こうした措置は、被害者が直接裁判所に提起する民事訴訟に比べて迅速な制裁と勧告がなされるが、事後的であることによる限界があり、被害者の権利回復には失敗している。

○YouTubeなどを利用する個人メディアに対して民事、刑事上の手続以外の規制手段がない。

○国外事業者とプラットフォーム事業者がプライバシー権侵害を引き起こす場合の規制策にも配慮する必要がある。

●メディアの自主規制と捜査機関の被疑事実公表

○メディアの報道自体を事前に法律で規制して制限することは表現の自由を侵害するおそれがあるので、報道機関の自主規制を期待しなければならない

○各報道機関は、自主規制のための個別の取材準則、放送綱領、倫理規範などを設けているが、自主規制の特性上、守られない場合がある

○一方、捜査機関の起訴前被疑事実公表は、法律ではなく、行政規則等で行われており、これにより、被疑事実の公表が広く行われ、性犯罪の被疑者を含む被疑者全般の人格権などの侵害が発生している。

○刑法は被疑事実公表罪を規定しているが、法務部が国会に提出した資料によると、2013年から2018年8月までに受理された約200件の被疑事実公表で起訴になったケースはない。

B. 勧告

●法律が事前にメディアの放送または報道を規制および制限すると、表現の自由を侵害する可能性が懸念される。したがって、メディアの自主規制を優先する必要がある。自主規制が失敗した場合にプライバシー権侵害を防ぐ具体的な計画を策定する必要がある。

●個人メディアによるプライバシー権侵害の問題を解決する具体的な計画を提示すること。

●国外事業者とプラットフォーム事業者によるプライバシー権の侵害を防止するための具体的な計画についての情報を提供すること。

●捜査機関の不当な被疑事実公表による被疑者の人格権などの侵害を防止する具体的な計画を提供すること。

C. 担当省庁や機関

●放送通信委員会

●言論仲裁委員会

- 文化体育観光部
- 法務部

7) 女性のプライバシー

オンライン空間のジェンダー暴力とプライバシー

プライバシー権に関してジェンダー的視点を適用すること。誰かが女性のプライバシーを侵害した場合、その「誰」かが、政府、企業、個人に関係なく、重大な基本的人権侵害とされなければならない。プライバシー権保護の原則を女性の経験に適用すること。しかし、韓国でこれまで行われたプライバシー権保護の議論では、個人のプライバシーから「女性」が除外されてきた側面がある。

韓国サイバー性暴力対応センターは主に「サイバー性暴力」を扱う。サイバー性暴力は、オンライン空間で発生するジェンダー暴力であり、プライバシーの権利を含む多くの人権を侵害している。オンライン空間では、女性のプライバシー権が悪影響を受けている。以下に示すサイバー性暴力事件は、サイバー性暴力自体がプライバシー権の重大な侵害であることを示している。

女性のプライバシー権の侵害状態は直ちに救済されるどころか、非常に長期にわたって「男性の権利」、「どうしようもないこと」とであると認識されてきた。2019年の今でも、サイバー性暴力対応活動の中で、女性のプライバシー権の侵害状況を解決しようとする試みが「表現の自由の侵害」、「男性プライバシー権の侵害」とみなされてしまう場合がある。

たとえば、大規模なプライバシー侵害行為が明らかに発生している不法な画像配布プラットフォームにアクセスすることができないように接続遮断措置がなされたとき、「表現の自由の侵害」、「プライバシー侵害」という反発が起きた。接続遮断措置は、そのサイトにアクセスする一主に男性であるインターネットユーザのプライバシーを侵害する可能性があるので、絶対に許すべきではないというものである。「侵害される可能性」の段階から、絶対に保証すべきプライバシー保護の原則が、男性には適用されているのに対し、すでにそのサイトに私的な画像がアップされて深刻なプライバシー権の侵害を経験している女性には適用されない。

また、女性に対するプライバシー権の侵害行為は、性差別的な社会文化構造の中で経済的利益を創出する行為である。韓国社会では、女性の私生活を同意なしに撮影し、同意なしにアップした映像を問題視せずのひとつのポルノジャンルとして認識してきた歴史がある。そのような映像を商品とする産業構造まで作ってきた。2018年には、女性のプライバシー権を侵害することにより、金を稼ぐビジネスの癒着構造が露呈し、「ウェブハードカルテル」という呼ばれるようになった。

今韓国で起きている女性のプライバシー権侵害と脅威をさらに可視化し、女性を含むプライバシー権概念を再確立する必要がある。韓国は、「性別、およびプライバシーと人権の包括的な原則に従って、プライバシー権に対する特定の利益、経験、脅威を認識する横断的アプローチを採用しなければならない」。¹¹⁴

オンライン空間の女性に対する暴力の問題においては、個人対個人、個人企業のプライバシー権の侵害に介入することができる公権力の役割が重要である。巨大企業と国家権力を中心に扱われてきた従来のプライバシー権の侵害を強姦文化に拡張することが必要である。女性にとって、強姦文化はビッグブラザーの別名である。企業と国家権力が傍観したり、容認する場合には、女性たち一人ひとは、自分のプライバシーを守るために戦うべき相手は、企業、国、インターネットユーザー一人一人にさらに拡張されるほかはない。

¹¹⁴ 2019年2月27日、Joseph Cannatacithé、プライバシー権に関する特別報告者[プライバシー権：ジェンダーの視点-プライバシー権利に関する特別報告者の報告]

単純な一時的措置では、この問題を解決することができない。国は、オンライン空間に対して、この領域が治外法権ではなく、プライバシー侵害を経験しない権利があるという視点を明かにし確立する必要がある。オンライン空間の理解に基き、この空間自体の国レベルのビジョンを策定し、オンライン空間で行われる女性に対する暴力と憎悪を終わらせるための体系的、包括的な対策を講じなければならない。

7-1) 男性インターネットユーザーによる女性のプライバシー権の侵害

A. 背景

●性的撮影物を利用したプライバシー権侵害

●最高検察庁の統計によると、カメラ等を利用した撮影罪の性犯罪発生件数は、過去10年間で性犯罪のなかで最も急増している。2008年性暴力犯罪全体に占める割合が4.6%だったが継続的に増加し、2015年には24.9%になった。2016年には17.9%に縮小したが、2017年には20.2%に増加した。カメラ等利用の撮影罪の統計は、不法撮影と流布が統合されて集計されたものである。違法撮影にはトイレ、公共交通機関などの日常的空間で撮影するタイプと性交などの性的シーンを撮影するタイプがある。

○2018年4月30日から12月31日までの女性家族部傘下の韓国女性人権振興院のデジタル性犯罪被害者支援センターの被害支援統計によると、被害件数5,687件。その中でオンラインスペースに不法撮影物流布が2,267件。違法撮影物投稿のなかで合意なしの投稿で削除された件数が2万8879件である。

○2万8879件の削除の分析をもとに2018年デジタル性犯罪被害者支援レポートが作成される。流布された5件のうち1件以上の割合で被害者を特定できる個人情報が含まれていた。センターは、削除された違法撮影物における個人情報流出被害が確認できたのは6700件で全体の23.2%となった。全個人情報流出被害の47.8%が被害者の名前の流出で最も多い。続いて、仮名流出(23.7%)アドレス(9.3%)の順である。被害者が所属している集団と電話番号と一緒に流布されている場合は、それぞれ8%、3.1%に達する。

○センターの支援を受けた被害者の半分以上が違法撮影、流布、拡散脅迫、サイバーいじめなどの被害を重複して経験している。特に、被害者を支配する目的で性的撮影分を活用する流布脅迫の場合、全体の14.1%に相当する803件の被害がみられた。家宅搜索令状、逮捕令状がなく加害者が証拠を隠滅したり、撮影物を流布してしまう場合も生じている。

○流布脅迫を経験した被害者は、どのような対策をとっても流布の不安を感じている。加害者が撮影物を所持しているという理由から、加害者の脅迫を無効化することが難しい。被害者は、他人が所持している自分の性的撮影をコントロールすることができるような法的権限がなく、加害者に削除を強制することもできない。

○児童・青少年の場合、ランダムチャットアプリなどを介して簡単にオンラインの性的グルーミング(下心を隠して相手を信頼させ、いかがわしい行為をしようとすること—訳注)被害にさらされ、自分で自分の身体や性的なシーンを撮影して、加害者に渡している。児童・青少年が被害支援機関に連絡したときにはすでに、200以上の身体の撮影やオナニー映像などを加害者に渡したというケースもある。オンライングルーミングを介しての撮影データを得た加害者は追加ノ撮影を得るための脅迫手段としてコレヲ活用するか、または海外サーバーのサイトを介して撮影データを販売したりする。このような場合は、加害者が画像を配信する、または実際に配信すると脅迫するなど、追加の被害が発生した場合に法的に対処できる。

○女性家族部傘下の「デジタル性犯罪被害者支援センター」は、法的代理人の同意を受けていない未成年者に削除のサポートを提供しない。つまり、オンライングルーミングなどを通じて性的撮影物が流布されると、未成年者は流布された撮影データを削除するために、両親に被害事実を告知しなければならない。したがって、法定後見人への通知が困難な未成年の被害者にとって、正義は通用しない。

○国が加害者を明確に特定できないため、サイバー犯罪が容認される。捜査機関で「被害者自ら加害者を特定しなければ検挙することができない」と被害者に捜査の責任を転嫁する場合がある。このように、被害者の申告を受理せず立件自体をしない場合があり、2018年1～8月の間集計された不法撮影物流布の被害届164件のうち、検挙件数は52件（検挙人員66人）である。

事例1 成人男性がランダムチャットアプリケーションで15歳の女性にアクセスして交際をする。最初は名前と年齢、学校名を尋ね顔が出ているセクシーな写真を撮って送ってくれと要求し、ますます要求する写真が激しいものになる。男性は15歳の女性に性器の写真を送ってくれと要求する。女性がこれを拒絶し性器の写真を送らないと、以前に送信した胸の写真を流布すると脅迫する。男性は「君が写真を送って始まったことなので訴えることもできない」と恐怖心を与え、女性は仕方なく、加害者に性器写真を送らざるをえなかった。

事例2 女性が元ボーイフレンドとのセックス映像を撮り、別れる時には消去すると約束した。しかし、しばらくして知人から女性の性的関係映像が流布されていることを伝え聞かされる。すでにいくつかのサイトに流布されヒットが何万回に達していた。被害者を嘲笑したり、侮辱するコメントも数百あり、絶えず映像が流れていた。女性は自分のセックス映像を削除するために努力したが、いくら消してもまた流布されることを経験し、無力感と絶望感を感じ、自分の被害が収束しないことで精神的な打撃を受けた。

●性的合成と編集後の拡散を通じたプライバシー権の侵害

○女性がSNSやメッセージアプリプロフィールなどの日常の写真を当事者の同意なしに収集して性的なイメージに加工する。このような虐待の形態には、被害者の顔を別の女性の裸の体と結合すること、顔の画像に精液をグラフィカルに追加すること、または性行為を示唆するために表情を編集することが含まれる。通常、知人男性が加害者であるため、「知人間のレイプ」と呼ぶ。合成された画像を流布する場合、被害女性の個人情報と一緒に公開して性的に侮辱したり、虚偽の事実を流布する場合も多く、サイバー上のいじめの性格を帯び、こうした記事がアップロードされると、コメントと共有を介して不特定多数による性的侮辱が更に行われる。

○2018年4月30日から12月31日の間に、デジタル性犯罪被害者支援センターの支援の現状によれば、5,687件の被害件数のうち、写真合成は2.7%に相当する153件、サイバー上の嫌がらせは、4.4%に相当する251件の被害であった。

○主に男性同士で共有されるオープンチャットルームへのリンクなど、女性のアクセスが困難な空間での拡散が行われるため、被害者は、自分の私生活情報がどこにどのように流布されたことを把握することも難しい状況にある。プライバシー権の侵害が最初から被害者の認知範囲外に起こるので、性的合成や編集後の拡散が2.7%しか起こらないのではなく、認知できる部分が2.7%であることが見てとれる。

○画像を合成したり、編集することは性暴力処罰法には該当しない。事例に基づいて、サイバー名誉毀損や侮辱罪を適用することができる。したがって、性暴力処罰法に該当する場合に保証さ

れる権利が認められない。犠牲者は、元の画像が犠牲者によって撮影されたという理由で些細なもの
と見なされてしまう。

事例1：「知人間レイプ」テレグラムのチャットアプリでは、300人程度の人々が知人の写真を
撮影し、性的に合成、編集して、被害者を「レイプ」していた。1人の男性ユーザーが画像を
アップロードし、他のユーザーがダウンロードして、画像に性器または精液を追加した画像を再
アップロードする。この場合、1人のユーザーが被害者の学校に侵入し、被害者の体操服に射精
し、グループチャットに写真をアップロードした。ユーザーは、お互いの知人の写真を操作した
り、そのような画像を売買したりするのに利用した。

●サイバーストーカーを通じたプライバシー権侵害

○オンライン空間でのストーカーは、被害者の個人情報や撮影物が被害者の同意なしに収集さ
れ、無断で利用される。ストーカーはインターネットの掲示板、チャットルーム、電子メールなどの
情報通信網を介して相手が望まない接触を継続的にしようとしたり、悪口、脅迫内容を含むメール送
信を続けるだけでなく、被害者の個人情報を盗んだり、詐称する場合もある。

○サイバー犯罪捜査のために捜査機関の努力と専門不足で匿名の加害者を特定することが難し
い。撮影物を盗み、個人を詐称する行為に対する処罰法も不在である。

事例1：匿名の加害者がSNSメッセージャーを利用して、被害者に継続的に性的イメージやメッ
セージを送信する。加害者は、被害者の日常を隠し撮りした動画を投稿した。加害者は、こうし
た行為が通告されると取り下げては別のアカウントから被害者へのハラスメントを続けた。それ
だけではなく、加害者は被害者の画像を使用して被害者になりすまし、被害者の個人情報をイン
ターネット売春ウェブサイトアップロードした。被害者には、メッセージや個人データ、画像
をオンラインで継続的に配信したりすることを阻止するための効果的なアクセス手段がなかった。

B. 勧告

- サイバー犯罪捜査の専門性を高めるための大々的な資源投入と捜査力の強化対策が必要である。
- 所持罪の新設、削除サポート保証など、被害者が自分のイメージを制御する権利を保障するための
対策を講じなければならない。
- 法定後見人から同意を得られない、または法定後見人に通知したくない未成年者にサポートを提供
するシステムを構築する。
- 性的合成写真や編集された写真の拡散、拡散の脅迫を性暴行処罰法で処罰できるように性暴行処罰
法の改正・新設が必要である。
- 被害者の知りえる範囲を超えて起こるプライバシー権侵害を防止する措置が必要である。

C. 担当省庁や機関

- 警察庁
- 法務部
- 女性家族部
- 科学技術情報通信部
- 放送通信委員会

7-2) オンラインプラットフォームの女性人身取引

A, 背景

●韓国は性器や肛門が露出する「ポルノ」の制作及び流通が禁止された国である。しかし、「家庭内ポルノ」も存在する。実際の恋人の間のセックスを当事者、特に女性の同意なしに撮影し、広範に流布させて視聴することが一つの「ポルノ」のジャンルとして韓国社会で確立されている。韓国の男性は同意なしに流布された女性の私生活の撮影を「家庭内ポルノ」と呼んでいる。

●2000年代以降、「家庭内ポルノ」の流通と消費は、巨大な産業構造となっている。タブレット、スマートフォンなど、さまざまなデジタル機器の普及と韓国的高速インターネット技術の発展は、「家庭内ポルノ」の産業化を加速させた。

●同意のない性的イメージの流布は、生産・流通・消費に関わる全ての者たちによる集団的な犯罪であり、男性は「レクリエーション」として理解され、男性は「家庭内ポルノ」消費を権利として認識するようになる。「家庭内ポルノ」が、産業になり男性が「家庭内ポルノ」を合法的に購入できるのはまさにこうした社会的背景によるということに留意する必要がある。

●韓国のこのような状況をよく表している事例として、以下の例が挙げられる。ポータルサイト、P2Pプログラム、ウェブハード、SNSなどの事業者であるオンラインサービスプロバイダ（OSP）に「家庭内ポルノ」の検索を制限するフィルタリングシステムの構築を義務付け、その流通を放置した場合事業者を処罰できるようにした電気通信事業法の改正案が2014年国会を通過し、2015年に施行されたが、男性中心のオンラインコミュニティは、男性ユーザーが支配するWebサイトは、この法案を「オナニー規制法」と呼んで修正を攻撃した。

●これらのユーザーは、インターネットの台頭により非合意の親密な画像へのアクセスが「民主化」されたとし、規制は、男性の性的快楽に対する基本的権利を侵害し、性的素材にアクセスする際の経済的不平等をもたらすから、こうした規制は時代に逆行していると主張した。これはかつてゲイル・ルービン（Gayle Rubin、2011/2015）が「女性の人身取引引き」（the traffic in Women）と呼び、男性間の関係と連帯の維持のために、女性が交換の対象として利用される姿とも似ている。流通プラットフォームを介して増幅されたイメージを利用したサイバー性暴行は、画像を利用して、女性のセクシュアリティを特定のイメージに固定し、男性が交換する女性の範囲を大幅に拡大することによって、このような「女性の人身取引引き」を近代化するものだ。

●ウェブハード Web-Hard

○国内ファイル共有プラットフォームである「ウェブハード」は、被害者が存在するのイメージを流通し、収益を得る構造を作った。ドラマや映画のように、著作権のあるコンテンツは、収入の70%を著作権者に与え、残りの30%を、コンテンツのアップローダと配分するが、著作権がなく、被害者が存在する「国産ポルノ」は、収入の70%をウェブハードが取り30%をアップローダが取るので、大きな利益を得ることができる「商品」であった。

○これに加えて、ほぼすべてのウェブハードが従業員を介してコンテンツを集め、直接アップロードしたり、違法なコンテンツを集めてアップロードするヘビーアップローダーを採用する方式を採用している。ウェブハードは、同意のない親密な画像の配布から生じる利益全てを獲得することができた。

○KCSVRCは、2017年に、ウェブハードへのモニタリング調査を通じて、ひとつのウェブハードサイトで多くて10万以上の「家庭内ポルノ」が流通し、各ウェブハードあたりの平均は数万個単位で「家庭内ポルノ」が流通したことを確認した。流通量において上位を占めた某ウェブハード業者は、国に申告した収入だけでの年に300億を超え、上位ウェブハード企業の場合、年間収益が千億を超える場合もあった。

○ウェブハード業者は、同意なしに流布された女性の性的イメージの削除要求を拒否したり、そのイメージの再流通防止の技術的措置が可能であってもそうした措置をせず、要求されたデータのみを削除している。2017年5月に韓国サイバー性暴行対応センターが無料の削除サポートを開始するまで、被害女性は、民間オンライン管理会社に月に200～300万ウォン程度を長期間支払い、侵害された自分のプライバシー権を自力で救済しなければならなかった。

○2018年には、アップローダ、プラットフォーム、プラットフォームの不法情報流通を規制するための技術的措置を提供する業者、民間削除メーカーはすべて一人の所有であり、癒着構造によって異常な高収益を得てきたという事実は、「ウェブハードカルテル」という名前で呼ばれるようになっていく。

●海外違法ポルノサイト

○海外にサーバーを置いて、国内法と韓国の捜査機関を避けて運営する違法サイトで、国内事業者よりもさらに大胆に不法イメージが流通されている。「家庭内ポルノ」、「素人ポルノ」、「流出ポルノ」、「未成年ポルノ」のようなキーワードカテゴリーを作成し、違法イメージを大量に流通させている。最も代表的なサイトは、「ソラネット」である。利用者が100万人を超える大規模なサイトでは、男性が自分の女性の家族と知人をこっそり撮ってアップして共有する掲示板が盛んである。2016年に国民の閉鎖要求で捜査が進められ閉鎖されたが、同様の違法ポルノサイトはまだ多く残っている。2017年韓国サイバー性暴行対応センターが支援した206人の犠牲者の映像が流布されたサイトのうち、海外の違法ポルノサイトだけで300以上にのぼる。

○ビットコイン、売春、アダルトグッズやギャンブルの広告を介して広告収入を得ること。ソラネットの場合、1日1億ウォンの広告収入を稼いでいた時期がある。

B. 勧告

●オンライン事業者は「人権と企業に関する国連指針」を履行して、事業者の活動のジェンダーに固有の影響を効果的に考慮して、自分のビジネス慣行で影響を受けるすべての人の人権を侵害することを避ける必要がある。

●プラットフォーム事業者向け処罰法強化：現行法は、不法な情報流通の事実を知らず意図的に対処しなかった事業者に2000万ウォン以下の罰金を課すだけなので、当該事業者に大きな打撃にはなっていない。違法なオンラインプラットフォーム事業者を実効性ある規制のための法改正が必要である。

●プラットフォーム事業者の社会的責務：犯罪化されていない女性への暴力と女性嫌悪の領域においても、オンライン事業者の責任が継続的に強化されること。

●被害救済のために違法な情報を流通させる海外のインターネットサイトのブロック強化に加え、サイト運営者を検挙し、サイトを閉鎖することができるような根本的な対策を用意する必要がある。

C. 担当省庁や機関

- 法務部
- 科学技術情報通信部
- 放送通信委員会
- 放送通信審議委員会
- 警察庁