

디지털 환경에서 아동·청소년 프라이버시 권리를 위한 교육방안과 제도개선 연구

책임연구 이선민(시청자미디어재단 선임연구원)
공동연구 장여경(정보인권연구소 상임이사)
김법연(고려대 정보보호대학원 연구교수)
오병일(진보네트워크센터 대표)
김상현(캐나다 BC주 수도권청 정보공개·개인정보 담당관)

이 보고서는 2021년도 방송통신위원회 방송통신발전기금 시청자권익증진사업의 연구결과로
보고서 내용은 연구자의 견해이며, 시청자미디어재단의 공식입장과 다를 수 있습니다.

목 차

요약문	ix
제 1 장 서 론	3
1. 연구 배경과 목적	3
2. 연구서 구성	8
제 2 장 아동·청소년 권리와 미디어 리터러시 관점에서 프라이버시	11
1. 데이터 시대 프라이버시	11
2. 미디어 리터러시로서 프라이버시	14
3. 아동·청소년 프라이버시의 개념적 이해	17
4. 아동·청소년의 프라이버시 의미와 현황	21
제 3 장 디지털 환경에서 아동·청소년 개인정보 및 프라이버시 침해 위협	29
제 1 절 디지털 환경에서 아동·청소년 개인정보 침해가능성 확대	29
1. 디지털 신기술 현황과 개인정보 위협	29
2. 아동·청소년 디지털 활용 특성과 개인정보 침해 우려	32
제 2 절 아동·청소년 개인정보 침해 사례 검토	35
1. 틱톡 사건	35
2. 이루다 사건	36
3. 부모의 개인정보 침해	38
4. 온라인 그루밍	40
5. 불법도박사이트 인증 및 매매	43
제 3 절 디지털 플랫폼별 개인정보 침해 위험요소 분석	46
1. 트위터	46
2. 페이스북	50
3. 인스타그램	55

4. 유튜브	58
5. 틱톡	62
6. 인공지능 스피커	66
제 4 절 아동·청소년에 대한 보호와 감시의 딜레마	70
1. 아동·청소년의 스마트폰 감시	71
2. 아동·청소년의 생체정보 수집	81
제 4 장 아동·청소년 개인정보와 프라이버시 교육 현황	99
제 1 절 해외 교육 사례	99
1. 프라이버시에 대한 접근	99
2. 미국의 프라이버시 교육	101
3. 캐나다의 프라이버시 교육	120
4. 영국의 프라이버시 교육	127
5. 호주의 프라이버시 교육	133
6. 시사점	137
제 2 절 국내 아동·청소년 개인정보 교육	141
1. 학교 교과 교육의 현황과 내용	141
2. 개인정보보호위원회 등의 교육 현황과 내용	144
3. 국내 개인정보 보호 교육에 대한 평가	150
제 5 장 아동·청소년의 개인정보와 프라이버시 보호 규범 현황	157
제 1 절 아동·청소년과 개인정보와 프라이버시 보호 규범	157
1. 아동·청소년의 프라이버시 보호 관련 국제 규범	158
2. 유럽의 아동·청소년 프라이버시 보호 규범	163
3. 영국의 아동·청소년 프라이버시 보호 규범	176
4. 미국의 아동·청소년 프라이버시 보호 규범	181
5. 국내 아동·청소년 프라이버시 법제와 침해 구제	182
제 2 절 인공지능 관련 규범과 아동·청소년	203
1. 국제규범과 인공지능	204

2. 국내 법제와 인공지능	213
제 3 절 소결	218
제 6 장 아동·청소년의 개인정보와 프라이버시에 대한 인식	223
1. 아동·청소년 인터뷰 개요	223
2. 인터뷰 진행방식 및 주요 내용	225
3. 인터뷰 결과	227
4. 소결	258
제 7 장 아동·청소년 개인정보 교육과 제도에 관한 전문가 평가 및 의견	263
1. 전문가 인터뷰 개요 및 방법	263
2. 인터뷰 결과(법제도 분야)	265
3. 인터뷰 결과(교육 분야)	280
4. 소결	293
제 8 장 결론	299
제 1 절 아동·청소년 프라이버시 교육방안	299
1. 교육의 필요성	299
2. 교육 목표	300
3. 교육 방향	302
4. 교육 방안	306
제 2 절 디지털 환경에서 아동·청소년의 프라이버시 권리 보장 방안	311
1. 법제도 개선	311
2. 부모 세대의 교육과 인식 전환	311
3. 교사와 학교당국의 태도 개선	312
4. 아동·청소년 프라이버시 권리를 존중하는 환경 조성	312
참고문헌	313

표 목차

〈표 2-1〉 유니세프의 아동의 온라인 프라이버시와 표현의 자유에 관한 일반원칙	20
〈표 3-1〉 인공지능 스피커별 음성정보 수집·이용 현황	68
〈표 3-2〉 학교 CCTV 설치현황	89
〈표 4-1〉 학교급별 정보 교육 상황	141
〈표 4-2〉 2015년 개정 교과 중학교 정보교과 내용체계	142
〈표 4-3〉 연령별 개인정보 교육 내용	145
〈표 4-4〉 연령별 개인정보 세부 교육 내용	148
〈표 5-1〉 영국 연령적합설계 실행규칙의 기준과 요구 사항	179
〈표 5-2〉 각급 학교 학생 프라이버시권 관련 진정 처리 사례	183
〈표 5-3〉 국가인권위원회 아동·청소년·학생 프라이버시 및 개인정보보호 관련 의견	186
〈표 5-4〉 만 14세 미만 아동의 개인정보침해 신고 및 상담 접수 현황	190
〈표 5-5〉 만 14세 미만 아동의 개인정보 분쟁조정 현황	190
〈표 5-6〉 만 14세 미만 아동 관련 개인정보 침해요인 평가	191
〈표 5-7〉 만 14세 미만 아동 관련 정보통신망 개인정보 침해 처분	192
〈표 5-8〉 아동·청소년과 학생 권리 관련 자치법규	196
〈표 5-9〉 경기도교육청 사생활 권리 관련 학생인권 상담·조사·구제 건수	198
〈표 5-10〉 교내 사생활 권리 보장 관련 경기도 학생 응답	199
〈표 5-11〉 학교에서 휴대전화 지도와 관리 방식에 대한 경기도 학생 응답	200
〈표 5-12〉 온라인 이미지 및 개인정보 노출 경험에 대한 경기도 학생 응답	202
〈표 6-1〉 연구참여자 특성	223
〈표 6-2〉 인터뷰 질문과 진행순서	226
〈표 6-3〉 개인 데이터 수집·저장에 대한 인식	246
〈표 7-1〉 인터뷰 대상 전문가 프로필	263

〈표 7-2〉 전문가 인터뷰 질문 264
 〈표 8-1〉 유럽평의회 디지털 시민성 영역 301
 〈표 8-2〉 아동·청소년 프라이버시 교육안 310

그림 목차

[그림 2-1] 프라이버시 차원과 데이터 유형 18
 [그림 3-1] 동의 목적 외 개인정보를 활용한 트위터의 맞춤형 광고 시스템 49
 [그림 3-2] 페이스북의 개인정보 제공 구조 52
 [그림 3-3] 인스타그램의 생년월일 정보 수집 화면 58
 [그림 3-4] 유튜브에서 맞춤형광고가 금지된 항목 61
 [그림 3-5] 청소년 유해물 차단앱 현황 77
 [그림 4-1] 아동용 프라이버시 계몽서 아이몽거(The Eyemonger) 116
 [그림 4-2] 캐나다 온타리오주 OPIC의 아동·청소년 프라이버시 프로그램 124
 [그림 4-3] 호주 온라인 안전위원회 134
 [그림 4-4] 초등학생 대상 개인정보보호 교육콘텐츠 147
 [그림 4-5] 중학생 대상 개인정보보호 교육콘텐츠 147
 [그림 4-6] 고등학생 대상 개인정보보호 교육콘텐츠 148
 [그림 4-7] 영국 ICO 초중고생 개인정보보호 기초교육 자료 중 일부 152
 [그림 5-1] 서울특별시교육청 인공지능 등급 평가 매트릭스 217
 [그림 6-1] 프라이버시에 관한 답변을 모은 워드클라우드 228
 [그림 8-1] 유럽평의회 프라이버시와 보안의 핵심역량 302

요 약 문

1. 제 목

디지털 환경에서 아동·청소년 프라이버시 권리를 위한 교육방안과 제도개선 연구

2. 연구 목적 및 필요성

행동 타겟팅, 자동화된 정보 처리, 프로파일링, 의무적 신원 확인, 정보 필터링, 대중 감시와 같은 행위가 일상화된 사회에서 아동·청소년 프라이버시가 위협·침해될 수 있고, 이는 장기적으로 아동·청소년의 삶에 부정적 영향을 미칠 수 있다. 프라이버시 이슈는 개인에게 가장 직접적이고 부정적인 영향을 미칠 가능성이 높은 영역임에도 지금까지 미디어 리터러시에서 부차적으로 다루졌다. 국내 예서는 아동·청소년에 대한 프라이버시 침해와 위협 현황과 개인정보와 프라이버시 관련 교육 등에 대한 분석이 거의 이뤄지지 않았다.

미디어 리터러시 논의 또한 주로 교육에 초점이 맞춰져, 제도 변화 등 미디어 환경 개선 이슈에 상대적으로 소홀했다. 이 연구는 개인정보자기결정권으로서 디지털 환경에서 프라이버시 권리에 주목해 프라이버시 권리 취약층인 아동·청소년을 중심으로 그들의 생활 영역인 가정·학교·미디어 세 영역에서 프라이버시 침해와 위협 사항을 분석하고, 아동·청소년 프라이버시와 관련한 국내 교육과 법제도를 진단해 아동·청소년의 프라이버시를 증진시킬 수 있는 구체적인 교육과 제도 개선 방안을 도출하려 한다.

3. 연구의 구성 및 범위

연구서는 다음과 같은 내용으로 구성됐다.

첫째, 문헌연구를 바탕으로 데이터 시대 프라이버시의 중요성, 미디어 리터러시와 프라이버시의 관련성을 논하고, 디지털 네이티브인 아동·청소년에게 프라이버시가 중요한 이유와 아동·청소년의 프라이버시와 개인정보에 대한 인식과 실천 현황을 다뤘다.

둘째, 미디어, 학교, 가정 등 아동·청소년의 생활영역에서 프라이버시 위협·침해 요인을 아동·청소년 FGI, 전문가 인터뷰, 정보공개청구, 문헌연구를 통해 발굴·분석했다. 아동·청소년 관련 개인정보보호법 위반 사례와 가정(스마트폰 감시앱), 학교 공간(온라인 수업환경, 아동 영상정보와 생체정보 처리 등), 미디어 서비스(인스타그램, 페이스북, 틱톡, AI스피커 등)의 프라이버시 위협·침해 요인과 양상을 다뤘다.

셋째, 국내외 개인정보와 프라이버시 교육 사례를 소개·분석했다. 미국, 캐나다, 영국, 호주의 프라이버시 교육 사례와 국내 개인정보 교육 사례(중학교 정보 교과, 개인정보보호위원회 교육)를 분석했다.

넷째, 아동·청소년 프라이버시 보호 목적의 국제 규범과 해외 법제도를 분석해 시사점을 도출하고, 국내 개인정보보호법과 프라이버시 관련 제도 현황을 진단했다. 인공지능의 프라이버시 침해 위협에 대한 국내외 규범 제정 움직임도 함께 다뤘다.

다섯째, 아동·청소년 FGI, 전문가 인터뷰, 국내외 개인정보와 프라이버시 교육 프로그램과 법제도 분석을 종합해, 아동·청소년 프라이버시 권리 증진을 위한 교육방안과 제도개선 방안을 제시했다.

4. 연구 내용 및 결과

1) 디지털 환경에서 아동·청소년 개인정보와 프라이버시 침해 위험

(1) 가정·학교·미디어의 아동·청소년 프라이버시 침해 및 위협 사례

디지털 네이티브인 아동·청소년은 온라인 활동에 능숙하지만 프라이버시나 개인정보의 중요성에 대한 인식, 새로운 기술이나 서비스에 내포된 위험요소에 대한 충분한 인지역량을 지니지 못해, 성인과 달리 추가적 보호 조치가 필요하다. 타겟 광고, 생체인식 데이터 처리, 디지털 추적·감시, 자동화된 의사결정, 프로파일링 등이 아동·청소년에게 미치는 영향에 대한 대책은 부족하다.

미디어의 아동·청소년 개인정보 침해(만 14세 미만 아동 개인정보 수집시 법정대리인의 동의 위반)사례로, 틱톡은 만 14세 미만 아동에게 서비스를 제공하지 않는다고 고지하면서 회원가입 단계에서 이를 차단하는 절차를 마련하지 않고, 만 14세 미만 아동의 개인정보를 보호자 동의 없이 최소 6,000건 이상 수집했고, AI 챗봇 ‘이루다’ 개발사는 14세 미만 아동 20여만 명의 개인정보를 보호자 동의 없이 수집했다.

아동·청소년이 주로 이용하는 페이스북, 인스타그램, 틱톡, 인공지능 스피커 등은 개인정보와 프라이버시에 위협을 가하고 있는 것으로 나타났다. 페이스북은 경력, 학력, 거주지, 연락처, 가족 및 결혼/연애 상태, 정치적 관심사 등 민감한 내용을 입력하도록 안내하거나 페이스북 내부 앱을 통해 제3자에게 개인선호도와 민감정보가 포함된 개인정보를 당사자 동의없이 제공하는 경우가 많은 것으로 나타났다. 또, 페이스북은 타사 데이터를 확보하기 위한 소셜로그인 연동 기능으로 이용자 동의 절차를 지나치게 간소화해 정보주체가 본인의 정보를 제3자에게 과도하게 넘기도록 유도하고 있었다. 인스타그램의 위치정보 설정 기능은 범죄 위험이 높고, 위치태그가 포함된 사진은 대상자가 최근 방문한 장소를 기반으로 정교한 피싱용 정보를 만들어낼 수 있다는 점에서 위험하다. 인스타그램의 활동 추적의 범위는 인스타그램이 소유하지 않은

웹사이트와 서버까지 확장되며 이렇게 분석된 정보는 제3자에게 전송된다. 틱톡은 ‘이미지 내 얼굴과 신체의 특징 및 속성의 존재와 위치를 수집할 수 있다’고 밝히고 있는데, 생체정보의 범위와 이용 목적을 설명하지 않아 해당 정보가 일반적 생체정보인지, 생체인식정보인지 파악하기 힘들며 그에 따른 권장조치 이행 여부도 확인하기 힘들다. 음성정보는 생체정보이며, 생체정보 중 더욱 강력한 보호조치가 요구되는 생체인식정보임에도 AI 스피커 서비스 기업은 아동·청소년의 목소리뿐 아니라 선호 콘텐츠, 스피커 사용기록과 같은 민감한 데이터의 수집·관리방법을 밝히지 않아, 개인에 관한 정보가 얼마나 저장되는지 인지하지 못하는 경우가 많다.

가정과 학교 영역에서 시행되는 아동·청소년 스마트폰 감시앱과 생체정보 수집 등은 보호를 명분으로 도입됐지만, 아동·청소년의 프라이버시를 침해하고 있다. 전기통신사업법에 근거한 ‘스마트폰 감시앱’은 부모에게 아동의 온라인 활동에 대한 모니터링 기능을 제공해 아동의 프라이버시를 침해하는 것으로 나타났다. 감시앱은 법에 명시된 청소년 유해매체물 차단 이외, 문자메시지·메신저 대화·인터넷 접속내역 모니터링, 앱이나 기기의 사용시간 제한·설정, 위치정보 확인, 설정 지역(학교, 학원)이나 위험지역 진입·이탈시 알람, 스마트폰 사용 중지, 카메라, 와이파이, 블루투스 등 스마트폰 기능 원격통제, 특정 번호 수신·발신 제한 등 다양한 감시 기능을 제공하고, 인터넷 접속내역, 위치정보 등 민감한 개인정보를 수집해, 아동·청소년의 사생활의 비밀과 자유, 개인정보 자기결정권을 제한하고 있는 것으로 나타났다.

공공 영역에서 아동·청소년의 생체정보 수집과 관련해, 학교 CCTV 영상 정보, 공공 목적의 유전정보 수집, 지문 등 아동 생체인식정보 처리 등이 파악됐다. 사회적 약자 보호를 명분으로 도입된 CCTV는 대상자를 지속적으로 촬영해 일거수일투족을 파악할 수 있게 해 프라이버시 침해 위험이 있다. 학교 내 CCTV는 개인정보보호법과 초·중등교육법을 근거로 하지만, 구체적인 안전조치 규정이 없고, 학교 CCTV의 약 10%가 법적 근거가 없는 통합관제 센터와 연계하는 등 제대로 관리되지 않아 프라이버시 침해 소지가 있는 것으로

나타났다. 지문 등 아동 생체인식정보 처리와 관련, 학생식당·출결시스템·건물 출입시스템 등의 지문인식과 기숙사 정맥인식기 도입 시도 등은 매우 제한적으로 수집되어야할 유전정보가 행정편의를 위해 수집될 수 있는 현실을 보여 준다.

2) 국내외 아동·청소년 개인정보 및 프라이버시 교육과 제도 분석

해외에서는 프라이버시 취약층인 아동·청소년의 프라이버시 침해를 막고 권리를 확장 하기 위해 다양한 교육과 제도를 시행하고 있다. 영국, 미국, 호주, 캐나다는 프라이버시에 초점을 맞춰, 국내는 개인정보를 중심으로 교육을 하고 있다. 해외 주요국은 단순히 개인정보 유출사례 소개와 방지법을 제시하는 교육이 아니라 연령별 주로 이용하는 플랫폼에서 어떤 프라이버시 위협이 발생하는지, 작동 원리와 작동 방식이 어떻게 악용되는지 등을 연구해 아동·청소년이 관련 사항에 대해 개인정보자기결정권을 행사할 수 있는 역량을 키울 수 교육방식을 채택하고 있었다. 반면 한국은 개인정보 침해로 인한 피해사례 소개와 예방법을 교육하고 있었다.

세계 각국은 개인정보보호 법체계 하에서 아동·청소년의 개인정보를 보호하고 있다. UN과 유럽연합 등은 보호의 객체이자 권리의 주체로서 아동·청소년의 프라이버시 보호를 위한 다양한 규범을 마련해왔다. 국제인권규범인 유엔 아동권리협약(1989)은 아동의 프라이버시권을 보호하고 있고, 유엔 아동권리위원회는 2021년 ‘일반논평 25호’ 디지털 환경에서 아동의 권리 보장을 발표하며 디지털 환경에서 아동의 프라이버시권과 개인정보 권리 침해에 대해 우려를 표했다. 유럽연합 GDPR도 국제규범에 따른 18세 미만 모든 아동을 ‘취약한’ 정보주체로 특별히 보호하며 아동의 개인정보를 수집·처리하는 자에게 추가 보호조치를 요구하고 있다. 아동이 이해할 수 있는 쉽고 명확한 언어로 개인정보 처리를 설명해야 하며(설명기반 동의), 마케팅 목적이거나 프로파일링 처리에서 아동의 이익에 대한 특별한 보호 등이 필요하다고 봤다. 영국 개인정보보호 감독기관 ICO는 ‘아동 최선의 이익 원칙(Best Interests of the Child)’하에

아동 대상 서비스에서 높은 개인정보보호 기준을 기본 설정으로 하는 ‘연령적합 설계 실행규칙’을 2021년 9월부터 시행하고 있다. 기업에게 권리 행사 보장을 요구하고, 아동의 개인정보는 최소한 수집하고 설득력 있는 이유가 없는 한 공유가 원칙적으로 금지되며, 위치정보와 프로파일링 기능은 기본설정에서 해제해 두게 하고, 아동에게 해로운 방식이나 나쁜 선택을 유도하는 설계는 금지된다. 미국은 개인정보보호에 대한 일반법이 없음에도 아동의 온라인 개인정보를 보호하기 위해 2000년부터 ‘아동 온라인 프라이버시 보호법(COPPA)’을 특별법으로 시행하고 있다.

국내의 경우 아동·청소년의 개인정보와 프라이버시 보호와 관련, 개인정보 보호법의 만 14세 미만 아동의 개인정보에 대한 법정대리인의 동의를 받게 한 것이 유일하다. 만 14세 이상 만 18세 미만 아동의 개인정보는 별다른 보호 규범 없이 성인과 동일하게 처리되고 있다. 만 14세 미만은 물론 성년에 도달하지 않은 아동에 대해 취약한 정보주체로서 성인과 구분해 취급하고, 아동의 개인정보 처리에 기반한 마케팅, 프로파일링 및 자동화된 의사결정에 대해 금지 방안을 마련할 필요가 있다. 일회성으로 끝나는 법정대리인의 동의는 이후 지속적으로 이용되는 아동의 개인정보에 대한 충분한 보호조치로 보기 어려우므로 아동의 개인정보 처리 주기 전반에 대해 정교한 규범을 수립할 필요가 있다. 아동의 개인정보 유출 등 보안성 보장은 아동의 생애에 걸쳐 영향을 미칠 가능성이 높으므로 엄격한 기준이 필요하다. 이와 관련해 개인정보보호 위원회는 보호 대상 확대와 연령대별 특성에 맞는 보호조치 마련 방안을 검토 중이다.

인공지능 기술은 장난감, 챗봇, 학습 소프트웨어 등 다양한 형태로 아동에게 서비스되고 있고, 아동이 자동화된 의사결정 시스템을 통해 영향을 받는 상황에서 인공지능과 프라이버시·안전·보안에 대한 위험이 제기되고 있다. 유럽집행 위원회는 2021년 ‘인공지능법안’을 발의해 학교 등 교육과 직업훈련에 사용되는 인공지능을 고위험으로 분류하고 엄격한 요구사항을 따르도록 했고, 개인정보 보호위원회는 2021년 5월 ‘인공지능 자율점검표’를 발표해, 인공지능 개발·

운영에 참여하는 사람의 개인정보보호 인식 제고와 개인정보보호법 준수를 요구했다. 서울시교육청도 인공지능 도입 시 영향 평가 기준과 체크리스트를 담은 ‘인공지능(AI) 공공성 확보를 위한 현장 가이드라인’을 보급하며 공교육에서 인공지능 도입여부 평가 기준으로 ‘개인정보 보호’를 제시하는 등 인공지능 관련 아동·청소년의 개인정보를 보호하려는 움직임이 나타나고 있다.

3) 아동·청소년의 프라이버시에 대한 당사자와 전문가의 인식

아동·청소년의 개인정보 및 프라이버시 현황을 알아보기 위해 아동·청소년 37명을 FGI한 결과, 프라이버시에 대한 인식은 낮았고, 개인정보를 ‘침해’와 ‘보호’ 차원으로 인식하는 것으로 나타났다. 아동·청소년들은 다양한 형태의 개인정보 유출 위협에 노출됐으나, 보호와 금지, 윤리 중심의 학교의 개인정보 교육은 별 도움이 되지 않은 것으로 나타났다.

아동·청소년들은 가정·학교·미디어 환경 등에서 프라이버시에 대한 위협을 받는 것으로 나타났다. △가정의 스마트폰 감시앱에 대해 사생활 침해, 감시, 통제라고 생각했고, 자신의 행동을 ‘자기검열’하게 된다는 반응을 보였다. 스마트폰 감시앱은 감시를 내재화하게 만들 뿐만 아니라 프라이버시와 미디어 리터러시에 대한 감수성의 발달을 방해할 가능성이 높으며, 부모 자녀의 신뢰 형성에도 부정적 영향을 미칠 수 있는 것으로 보인다. △학교에서는 온라인 수업으로 인해 얼굴 노출, 과제와 활동 공개 등 다양한 프라이버시 침해 상황이 발견됐다. 교사와 동료 학생뿐만 아니라 학부모 등 제3자에 의한 프라이버시 침해 가능성도 존재했다. △미디어와 관련해, 서비스 약관 동의와 가입 과정에서 정보의 비대칭성으로 인해 불평등한 조건에서 개인정보를 제공해야 했고, 이 과정에서 무력감을 겪는 것으로 나타났다. 약관 내용이 너무 어려워 읽지 못했고, 소셜미디어의 데이터 수집과 상업적 이용에 대해 인식하지 못하는 것으로 나타났다. 일부는 온라인의 행동데이터의 정보 수집·저장·이용에 대해 비판적이었으나 일부는 알고리즘과 AI에 막연한 기대와 신뢰를 품고 있었다. 아동·청소년들은 자신의 프라이버시 권리를 지킬 수 있는 방안으로 청소년 프라이버시

존중, 아동이 쉽게 이해할 수 있게 서비스 약관 제공, 정보의 제한적 수집, 정보 처리 단계별 동의 절차, 개인정보 판매 최소화를 강조했다.

프라이버시 정책 전문가와 미디어 리터러시 교육 전문가 15인을 인터뷰한 결과, 미디어 이용, 학교, 가정 영역에서 아동·청소년이 프라이버시나 개인정보를 위협받고 있다고 우려했다. △미디어 기업의 과도한 정보 수집과 개인정보와 프라이버시 침해 행위 파악의 어려움이 있고, △학교 공간과 관련, 학생인권과 프라이버시에 둔감한 교육행정과 학교환경이 개인정보와 프라이버시 침해가 쉽게 발행할 수 있는 온라인 수업 환경과 결합해 아동·청소년의 프라이버시가 광범위하게 위협받고 있고, 온라인 학습시스템 시스템을 통해 다양한 학생 데이터가 기업으로 대규모 유입되고 있으나 관리·감독되지 않고, 근본적으로 프라이버시나 교육에 미칠 영향에 대한 검토 없이 기술시스템을 도입·활용하는 것으로 나타났다.

전문가들은 국내 개인정보 교육이 기업, 국가에 대한 논의를 배제한 채, 피해와 예방, 보호주의 관점에서 개인정보 문제를 개인의 책임과 윤리 문제로 다루고 있다고 지적했다. 국내 개인정보 관련법과 제도가 아동·청소년에 대해 관심을 두지 않아, 아동·청소년 보호 차원에서 금지해야 할 부분이 방치되고, 개인정보에 대한 동의가 형식화된 점 등 국내 법제도의 미비를 지적했다.

4) 제언

첫째, 법적 의미의 ‘개인정보’가 아닌 자신에 관한 정보를 스스로 통제할 수 있는 권리인 ‘프라이버시’로 확장해 교육할 필요가 있다. 기술중심주의와 피해예방과 보호담론에서 벗어나 미디어 환경에 대한 이해와 정보주체로서 개인을 인식하게 하는 미디어 리터러시 관점의 프라이버시 교육이 필요하다.

둘째, 아동·청소년의 미디어 이용을 반영하고, 권리와 책임의 균형을 익힐 수 있는 프라이버시 교육이 필요하다. 정보공개에 따른 평판 형성과 평판에 근거한 의사결정, 서비스 이용과 편의를 대가로 한 개인정보 제공과 기업의 데이터 축적·활용 양상 등 개인정보 공개·제공에 따른 다양한 사안에 대한

판단을 돕는 교육이 필요하다.

셋째, 아동·청소년의 최선의 이익을 반영할 수 있도록 법 개정이 필요가 있다. 대표적으로 개인정보보호법은 아동 관련, 만 14세 미만 아동의 개인정보는 보호자의 동의를 받는다는 조항이 유일하다. 만 14세-18세 이하에 대한 보호와 개인정보에 대한 프로파일링 등 자동화된 의사결정 금지, 동의 없는 가명처리와 아동의 개인정보의 영리목적 활용금지 등과 같은 아동·청소년에 특화된 특별조항 개설과 교묘한 방식으로 개인정보를 부당하게 수집하는 행위 금지(다크패턴 규제), 정보삭제권 등 개인정보 처리과정 전반에서 아동친화적 절차 도입 등이 필요하다.

넷째, 개인정보 관련법 개정뿐만 아니라 학생인권조례 의무화 등 학교나 가정에서 아동·청소년의 프라이버시 권리를 구체적으로 보장할 필요가 있다. 자녀 스마트폰 감시앱 이용에 대한 검토, 학교 내 CCTV 관련 규정 확보 등 아동·청소년의 프라이버시 침해 우려가 있는 제도를 검토할 필요가 있고, 온라인 환경에서 프라이버시 침해 없이 안전하게 수업을 받을 수 있는 권리 등 디지털 환경 변화를 고려한 대응이 필요하다.

다섯째, 학부모와 교사의 인식개선과 교육이 필요하다. 교육당국, 교사, 학부모가 아동·청소년을 보호나 통제대상이 아닌 판단과 결정을 할 수 있는 권리 주체로 보고, 프라이버시 등 아동·청소년의 권리를 존중하는 자세가 필요하고, 인식전환을 위한 교육이 필요하다.

5. 정책적 활용 내용

이 연구는 디지털 환경에서 아동·청소년의 권리 확보를 위한 프라이버시 교육안 구성과 개인정보와 프라이버시 제도개선을 위한 구체적 방안을 제시하고 있다.

첫째, 가정·학교·미디어에서 아동·청소년의 프라이버시 침해사례와 위협요인을 당사자와 전문가 인터뷰, 정보공개청구를 통해 발굴·분석해, 아동·청소년의

프라이버시 권리 현황을 구체적으로 제시하고 있다.

둘째, 해외 아동 프라이버시 관련 규범과 주요 국가의 개인정보와 프라이버시 법제도와 정책을 아동·청소년 권리의 관점에서 분석하고, 현재 국내 아동·청소년 개인정보와 프라이버시 관련 기관의 프라이버시 권리 구제 현황에 대한 분석, 법제를 평가해, 제도개선 사항을 제안했다.

셋째, 해외 주요 국가의 프라이버시 교육 사례의 소개·분석과 국내 개인정보 교육 프로그램의 분석·평가를 통해 국내 교육의 한계점과 지향점을, 당사자인 아동·청소년과 전문가 관점에서 개인정보와 프라이버시 교육의 개선방향을 제시했다. 가정·학교 등의 프라이버시 교육에 활용할 수 있을 것이라고 본다.

6. 기대효과

국내에 부재했던 아동·청소년의 프라이버시 권리 이슈를 의제화해 아동·청소년의 디지털 권리로서 프라이버시 권리에 대한 인식을 제고하고, 아동·청소년의 프라이버시 교육과 함께 아동·청소년의 디지털 미디어 환경 개선점을 다룸으로써 교육에 초점이 맞춰진 미디어 리터러시 담론에서 제도와 플랫폼 개선 관련 논의를 촉발시켰고, 정부와 관계기관, 기업의 책임에 대한 사회적 환기에 기여할 것으로 보인다.

무엇보다 이 연구는 프라이버시 교육과 제도 개선의 필요성을 입증하고, 교육과 정책의 방향성을 제시해 아동·청소년의 프라이버시 권리 향상에 도움이 될 것이다. 국내외 교육사례 분석과 아동·청소년과 전문가 자문 등을 바탕으로 프라이버시 교육방안을 제시하고, 법제도 관련 아동·청소년 프라이버시 특수성, 해외 아동 프라이버시 규범, 미디어와 플랫폼 문제 등 종합적으로 제시해 법제도 개선에 기여할 것이다.

제 1 장

서 론

1. 연구 배경과 목적

디지털 환경이 지속적으로 확장하고 진화하면서 우리의 일상에서 온라인과 오프라인의 경계가 희미해지고 있다. 디지털 도구와 공간을 넘어서 디지털화된 사회를 살아가는 경험에 더해, 최근 메타버스로 통칭되는 가상세계에서의 다양한 사회·경제 활동을 목격하고, 코로나19 이후 스마트폰 없이 이동이 제한되는 온라인 네트워크가 지배하는 세상을 경험하고 있다. 인터넷과 모바일 기술, 디지털 네트워크, 콘텐츠, 서비스와 애플리케이션, 가상현실, 증강현실, 기계학습을 포함한 인공지능, 자동화된 시스템과 정보 분석, 생체인식 등을 아우르는 디지털 환경의 특징 중 하나는 과거 휘발되었던 개인의 행동이 데이터화된(datafication)는 점이다. 검색, 쇼핑, 이동 등 온오프라인에서 개인의 미시적인 행위와 경험은 기록되고, 대용량 데이터세트(dataset)를 형성하고, 데이터세트를 온라인 이용자에 대한 세분화된 개인정보 서류로 컴파일하는 게 가능해졌다(Selwyn & Pangrazio, 2018). 기업과 정부 등이 데이터의 가치를 발견하고 광범위하게 개인 데이터를 수집·추적·저장·이용하면서 개인의 프라이버시는 위협을 받게 됐다. 개인의 생활 반경은 온라인으로 확장되면서 경계가 사라지고 있지만 프라이버시는 축소되는 현상이 나타나고 있다(Livingstone, Stoilova, & Nandagiri, 2019).

데이터화된 사회에서 기업과 정부가 개인 데이터의 수집·분석·추적 과정을 통해 개인의 의사결정과 행동을 유도하거나 개인에 대해 판단·결정하는 문제와 함께 개인들이 자신의 데이터 수집과 이후 상황을 인지하지 못하거나 무시하는 상황이 벌어지고 있다. 개인이 자신의 데이터 수집 등을 무시하게 만드는

상황은 개인의 행동데이터가 어디에서나 만들어질 수 있게 하고, 무언가를 결정할 사안이 있다는 것을 알기도 전에 개인의 의사결정권을 사라지게 하고, 개인은 자신의 권리가 축소되는 것의 결과를 알 수도 예측할 수도 없게 한다. 이런 과정은 개인에게 무력감과 체념을 안긴다(Zuboff, 2019/2021, 144쪽). 게다가 개인정보 유출 사건이 빈번하게 일어나고, 프라이버시 개념이 희박한 한국 사회에서는 위협과 체념 모두 강하게 나타나고 있다.

디지털 환경에서 프라이버시의 위협과 침해는 아동·청소년 등 젊은 세대에게 더 특수하다¹⁾. 아동·청소년의 정체성은 자신의 의지와 무관하게 건강, 교육, 사회 복지 관련 공공 플랫폼과 가족에 의해(예. 부모의 SNS 사진 게재 등) 데이터화 된다(Selwyn & Pangrazio, 2018). 또, 프라이버시는 인간의 기본 권리임에도 아동·청소년을 독립된 주체로 인정하지 않는 분위기에서 아동·청소년의 프라이버시는 부정되고, 양육과정에 보호 논리가 작동하면서 아동·청소년의 권리 일체는 ‘보호자’에게 위임된다. 미디어 이용과 관련해, 아동·청소년이 개인정보가 가장 많이 생성·노출되는 소셜미디어의 주이용층이고, 페이스북의 아동용 인스타그램 개발 시도가 시사하듯 빅테크 기업이 아동·청소년을 타깃으로 한다는 점은 아동·청소년의 프라이버시에 더 짙은 그늘을 남긴다. 개인의 관심사, 관계, 위치뿐만 아니라 결제정보, 기기 운영체제, 배터리와 신호 강도 수집 등 페이스북, 구글 등 빅테크 기업의 광범위한 데이터 수집 관행에 대한 문제제기에 더해, 유니세프(2020)는 ‘Data governance for young people in the commercialized digital environment’ 보고서에서 AI와 머신러닝을 결합한 다양한 광고기법이나 게임플랫폼의 ‘playable ads’ 등의 광고기술을 사용해 성장한 틱톡, 구글, 페이스북 등 플랫폼 기업을 ‘키드 테크(Kidtech)’로 언급하면서 이들이 아동·청소년의 프라이버시를 위협하고 있다고 지적했다. 이러한 우려에도 디지털 환경에서 태어나 그곳에서 많은

1) 아동과 청소년은 사회적·법률적(예. 청소년기본법, 청소년보호법, 도로교통법 등)으로 다양하게 정의되나 이 연구서의 아동·청소년은 만 19세 미만인 사람을 의미한다. 참고로 UN 아동권리협약이나 아동복지법은 18세 미만을 아동으로 명명한다.

시간을 보내며 성장하는 아동·청소년에게 온라인은 기회와 위험이 공존하는, 떠날 수 없는 현실의 생활공간이다(UNICEF, 2018). 미디어뿐만 아니라 학교, 가정 등 전통적인 영역 또한 디지털화되고, 디지털 공간의 프라이버시 위협에 대한 자각이 크지 않은 점은 아동·청소년의 프라이버시 위협과 침해 폭이 예상보다 넓을 수 있음을 말해준다.

디지털 환경의 변화와 아동·청소년의 프라이버시, 디지털 권리와 관련해 해외에서는 적극적인 문제제기와 대안이 제시되고 있다. 2021년 UN 아동권리 위원회는 28개국의 만 9-22세 아동·청소년 700여명으로부터 디지털 기술과 아동 권리에 관한 의견을 들어, 일반논평 25호 ‘디지털 환경에서 아동권리(Children’s rights in relation to the digital environment)’를 발표했다. 일반논평 25호는 디지털 환경에서 아동의 권리가 존중받아야 한다는 일반론과 함께 ‘프라이버시권’ 등을 명시해 아동의 프라이버시 보호를 강조하고 있다. 자동 정보 처리, 프로파일링, 행동 타겟팅, 의무적 신원 확인, 정보 필터링, 대중 감시와 같은 디지털 행위가 더욱 일상화된 상황에서 자의적, 불법적으로 아동의 프라이버시권을 침해할 수 있고 장기적으로 아동의 삶에 부정적 영향을 미칠 수 있음을 언급하며 국가와 특히 기업의 적극적 조치와 주의를 당부하고 있다. OECD도 변화된 디지털 환경을 고려해 ‘온라인 아동보호 권고안’(2012)을 개정한 ‘디지털 환경에서의 아동에 관한 권고안(Recommendation on Children in the Digital Environment, 2021)’을 발표했다. 2020년 1월 영국 개인정보 감독기구(Information Commissioner's Office, ICO)는 온라인에서 아동의 개인정보보호를 위해 인터넷 서비스에 적용해야 하는 사항들을 담아 ‘연령적합 설계규약(Age Appropriate Design Code)’을 발표했다. 규약은 18세 미만 아동이 온라인에서 처한 위험을 분류하고, 아동이 이해하기 쉽게 간결하고 명확한 정보를 제공하기 위한 여러 조치를 담고 있다. 미디어 리터러시 관점에서 제도 개선과 함께 교육방안을 제시하고 있다.

디지털 환경 변화와 관련해 제기된 프라이버시 등 아동 권리 이슈는 미디어 리터러시 관련 기존 관행에 질문을 던진다. 지금까지 미디어 리터러시의 주요

흐름은 교육을 통한 개인 차원의 이해와 역량(competence) 강화에 주로 관심을 기울여왔다. 미디어 환경 개선이 미디어 리터러시의 중요한 영역이었음에도 주요하게 다루이지 않았다. 유럽시청자권익협회(EAVI, 2011)는 유럽 27개국의 미디어 리터러시 수준을 개인적 역량과 환경적 요소로 구분해 비교하면서, 개인의 미디어 리터러시 역량을 수월하게 하는 맥락적 요인으로서 미디어 교육 여부, 미디어 리터러시 정책, 미디어 산업, 시민사회 등의 환경적 요소를 언급했다. 개인이 미디어에 접근해, 이용하거나 참여하는 것도 중요하지만 안전하고 참여적인 미디어 환경의 조성도 필요하다는 것이다. 아동의 권리를 침해·위협하는 미디어 구조 속에서 교육을 통한 개인의 역량 증진은 한계가 있다. 이는 미디어 이용에 대한 책임을 개인에게 돌릴 가능성이 있다. 기업과 정부 차원의 미디어 환경 진단과 제도 및 환경 개선과 함께 교육을 통한 디지털 시민성(또는 역량) 증진이 필요한 이유다. 미디어 리터러시가 실천적 함의를 지니기 위해서는 개인 차원의 역량 강화뿐만 아니라 환경과 제도에 대한 비판적 인식을 바탕으로 자신의 권리를 자각하고 미디어 환경의 변화 즉, 미디어 기업과 정부 역할을 요구하는 것이 필요하다. 이는 정책 개선 등과 함께 미디어 환경을 변화시키는데 중요한 부분이다. 호주 미디어 리터러시 전문가 마이클 데주아니(Michael Dezuanni)도 최근 “미디어 문제를 해결하는데 미디어 리터러시와 함께 ‘규제’와 ‘정책’도 공존해야 한다. 성공적 미디어 환경을 위해 정부와 민간, 시민의 파트너십이 이뤄져야 한다. 미디어 기업이 규제를 받지 않는다면 교육의 성공 가능성은 낮다”고 지적한 것도 같은 맥락이다²⁾. OECD가 디지털 환경에서 아동에 관한 권고안에서 디지털 리터러시 증진과 함께 미디어 기업에 대한 가이드라인을 발표한 것, 영국 정부 등이 다양한 프라이버시 교육 프로그램과 함께 기업을 대상으로 ‘연령적합설계규약’을 발표한 것도 미디어 리터러시 관점에서 제도 개선과 교육이 함께 가야한다는 것을 보여주고 있다.

하지만 프라이버시 이슈는 개인에게 가장 직접적이고 부정적인 영향을 미칠

2) 금준경(2021.11.3.)미디어 교육 권위자의 조언, “팩트체크 그 이상이 필요”. 미디어오늘
<http://www.mediatoday.co.kr/news/articleView.html?idxno=300421>

가능성이 높은 영역임에도 지금까지 미디어 리터러시 교육에서 부차적으로 다뤄졌다(Culver & Grizzle, 2017). 특히 어린이 프라이버시 문제는 위협과 보호, 안전과 기술의 프레임에서 소극적으로 다뤄졌다. 국내에서는 법적 개념에 기초해 정형화된 정보로서 개인정보를 중심으로, 침해와 예방의 관점에서 개인이 스스로 보호해야할 영역으로 교육돼왔다. 앞서 언급한 미디어 환경을 고려할 때, 법적 개념에 머물지 않고 권리로서 프라이버시를 인식하고, 아동의 프라이버시와 표현의 자유에 대한 권리가 어떻게 인식되는지를 고려하는 것이 중요하다(UNICEF, 2018). 컬버와 그리즐(2017)은 프라이버시에 대한 무관심을 기업이 활용한 사례를³⁾ 언급하며 미디어 리터러시가 프라이버시에 대한 시민들의 잠재적 무관심을 정보, 미디어와 기술에 대한 참여로 바꾸는 데 도움을 줄 수 있다고 말한다. 시민들이 프라이버시를 개인적 침해 차원만으로 이해하는 것이 아니라 인권, 표현의 자유, 인터넷 자유, 경제와 사회 개발 등과의 관련성을 이해할 경우, 프라이버시에 더 적극적이고 비판적으로 관여할 수 있다는 것이다.

이상의 맥락을 종합해 이 연구는 인권과 표현의 자유 권리, 개인정보자기 결정권으로서 디지털 환경에서 프라이버시 권리에 주목해⁴⁾, 데이터화된 사회에서 프라이버시 권리 취약층인 아동·청소년을 중심으로, 그들의 생활 영역인 미디어 플랫폼, 학교, 가정 세 영역에서 프라이버시 위협과 침해 상황 등을 진단하고자 한다. 동시에 미디어 리터러시 관점을 확장해 미디어 제도와 교육 두 차원에서 아동·청소년의 프라이버시 권리를 증진시킬 수 있는 방안을 도출해보고자 한다.

3) 2012년 페이스북은 검색에서 페이스북 프로필을 숨길 수 없게 한 것과 관련해 반대의견이 상당수였음에도 투표 정족수 기준 미달을 이유로 이를 무효화했다.

4) 이 보고서에서 프라이버시는 디지털 프라이버시권의 개념으로 한정해 사용한다. 사생활은 사생활로, 권리로서(디지털) 사생활에 대한 권리일 경우 프라이버시나 프라이버시 권리로 사용한다.

2. 연구서 구성

연구서의 구성은 다음과 같다. 1장은 디지털 환경 변화에 따른 프라이버시 이슈와 교육의 필요성을 다루고 있고, 2장은 문헌연구를 바탕으로 데이터 시대 프라이버시 의미와 미디어 리터러시와 프라이버시 관련성, 아동·청소년 관점에서 프라이버시 중요성과 관련 현황을 담고 있다. 3장에서는 아동·청소년의 생활 영역인 미디어, 학교, 가정에서의 프라이버시 위협과 침해요인을 분석했다. 새로운 미디어 기술 등장에 따른 프라이버시 침해 위협과 개인정보 침해 사례, 주요 미디어 서비스(페이스북, 인스타그램, 틱톡 등)를 중심으로 프라이버시 위협 요인에 대해 분석했다. 가정의 프라이버시 위협·침해 사례와 17개 시도 교육청에 정보공개를 청구해 학교 공간(영상정보, 생체정보 처리 등)의 프라이버시 위협 사례를 제시했다.

4장은 미국, 캐나다, 영국, 호주 등의 해외의 프라이버시 교육 사례와 국내 개인정보 교육 사례(중학교 정보교과와 개인정보보호위원회 교육)를 분석했다. 5장은 UN아동권리 협약, EU GDPR, 영국 DPA, 미국 COPPA 등 아동·청소년 프라이버시 보호관련 국제규범을 분석해 시사점을 도출하고, 정보공개청구를 통해 14세 미만 아동과 학생의 개인정보와 프라이버시 침해·처분 사례를 제시하고, 관련 법제도를 분석했다. 6장은 아동·청소년 37명의 포커스그룹 인터뷰(FGI)를 기반으로 가정·학교·미디어의 프라이버시 침해와 프라이버시 교육과 제도개선 방안을 다뤘고, 7장은 전문가를 인터뷰해 국내외 개인정보 교육과 법제도 현황을 진단하고 프라이버시 교육 방안과 관련 법제도 개선안에 대한 의견을 들었다. 8장은 결론으로 프라이버시 교육방안과 제도개선 방안 등 아동·청소년 프라이버시 권리 증진 방안을 제시했다.

제2장

아동·청소년 권리와 미디어 리터러시 관점에서 프라이버시

제 2 장

아동·청소년 권리와 미디어 리터러시 관점에서
프라이버시

1. 데이터 시대 프라이버시

프라이버시는 사생활, 남에게 침해받지 않을 자유 등으로 해석되다가 19세기 이후 ‘혼자 있을 권리(right to be let alone)’로 개념화된 이래 디지털 기술의 발전과 확산에 따라 개념과 범위가 변해왔다. 프라이버시 권리에 대한 다양한 해석이 있지만, 일반적으로 자신의 정보에 대해 관리하고 통제할 수 있는 권리(일명 개인정보 자기결정권)로 이해된다. 국내에서도 정보·통신 등의 발달로 스스로 공개한 개인정보나 사생활에 대해 통제할 필요성이 생기면서 ‘자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관해 스스로 결정할 권리’로서 프라이버시 권리를 국민의 기본권으로 인정하고 있다⁵⁾. 다만 한국은 집단주의적 문화와 권력의 검열과 감시로 인해 프라이버시 개념 전반에 이해가 부족하고, 프라이버시를 ‘개인정보보호법’에 명시된 이름, 주민번호 같은 ‘개인정보’ 수준으로 좁게 이해하는 경향이 있어왔다.

그러나 ‘데이터가 집약되고, 과잉연결되고, 상업화된’ 디지털 환경에서 개인에 관한 정보를 대규모로 수집할 수 있고, 대용량 데이터세트로 컴파일할 수 있게 되면서 개인의 프라이버시는 심각한 위협을 받게 됐다(van der Hof, 2016; Selwyn & Pangrazio, 2018). PC, 스마트폰, AI 스피커 같은 디지털 미디어 기기와 SNS 등 플랫폼뿐만 아니라 스마트가전이나 홈시스템 등 네트워크화된 시스템과 자동화된 시스템 등 디지털 미디어가 다양한 환경에 내장(embedded)되거나 구현(embodied)되어(Hine, 2015), 개인의 행동, 개인에 관한 정보가

5) 현재 2005.5.26. 99헌마513 결정

데이터로 수집·추적되고, 정부의 인구조사부터 마트의 적립카드까지 인구사회적 요소와 심리 정보와 소셜플러그인, 쿠키, 데이터브로커가 오프라인에서 수집한 정보에서도 개인 데이터가 나오고(Bodle, 2016), 이런 데이터 안팎으로 감정 표현이나 정서 교류같은 구조화되지 않은 미세한 정보뿐만 아니라 메타데이터가 담겨있다(Peacock, 2014). SNS에서 개인 프로필, 플랫폼과 상호작용, 글·사진·비디오 콘텐츠, 기술적인 미세한 부분과 연결된 것까지 모든 것이 수집되고, 알고리즘은 수집한 개인 데이터를 바탕으로 이용자를 분류·제안·추천하고(Chun, 2016), 동시에 마케팅, 관리, 위협평가 목적으로 축적된 데이터 세트로부터 훈련받은 알고리즘이 다시 개인의 행위를 예측·유도하고 그에 관한 의사결정을 하는 등 프로파일링⁶⁾이 이뤄지면서 프라이버시에 대한 폭넓은 시각과 적극적인 접근이 필요해졌다.

개인이 의식하지 못하는 사이에 다양한 정보가 수집·추적·집적·이용·프로파일링되면서 프라이버시를 정보의 흐름에 대한 이해와 결정권 차원으로 보는 시각은 더욱 중요해지고 있다. 데이터 사회를 감시자본주의로 분석한 주보프(Zuboff, 2019/2021)는 “프라이버시란 자신이 믿거나 생각하거나 소유하고 있는 것을 공개나 노출할 개인의 선택권을 포함한다”는 미국 대법관 윌리엄 더글러스(William Douglas, 1967)의 말을 인용해, 테크 기업의 행동 추적과 관련, 프라이버시는 ‘사생활’ 침해에 국한된 것이 아니라 어떤 개인정보를 어떻게 공개할지에 대한 ‘의사 결정권’에 대한 침해라고 보았다(138쪽). 웨스틴(Westin, 1967)은 프라이버시를 ‘개인, 집단이나 기관이 자신에 대한 정보가 언제, 어떻게, 그리고 어느 정도까지 다른 사람들에게 전달되는지 스스로 판단하기 위한 주장’으로 정의했다(Livingstone et al., 2019). 유사하게 프라이버시 전문가 니센바움도 프라이버시를 ‘비밀권도 통제권도 아닌, 개인정보의 흐름을 적용할 권리’로 보았다(Nissenbaum, 2010). 이와 관련해 리빙스틴 등

6) 프로파일링은 개인의 선호 알아내기(특정 사람 타깃팅하기 위한 상품 광고), 행위예측(고용주가 특정 업무를 누가 잘 할 수 있을지 예측), 결정하기(은행에서 대출 심사 결정하기) 등 주로 세 가지 방식으로 활용된다(Children's Commissioner, 2018).

(Livingstone et al., 2019)은 프라이버시가 관계적이고 맥락적인 개념(어떤 사회적 맥락의 특정하고 중요한 부분이 되는 관계)을 포함하고, ‘전유’(누가 판단하고, 어떻게 협상하는가)와 ‘흐름’(누구에게서 누구로 또는 무엇으로) 즉, 개인이 독점적으로 소유하는 통제권이 아닌 참여자간의 협상 문제로 파악하며 데이터 시대의 관계·맥락·권력과 정보의 불균형 속에서 프라이버시를 종합적으로 사고할 필요가 있다고 봤다.

개인의 정보가 데이터화되는 경향에 맞춰 온라인 프라이버시를 재개념화하는 시도도 나타나고 있다. 대표적으로 반더호프(van der Hof, 2016)는 프라이버시를 법적 개념으로서 ‘개인 데이터(personal data)’, ‘식별되거나 식별가능한 개인과 관련된 정보(information that relates to an identified or identifiable individual)’와 다른 차원으로 △주어진 데이터(Data given), △추적 데이터(Data traces), △추론 데이터(Inferred data) 세 가지로 구분했다. ‘주어진 데이터’는 개인이 온라인에서 활동하는 동안 의도와 무관하게 잘 알고 기여하는 (자신이나 타인에 관한) 데이터를 의미한다(예. 소셜미디어 프로필 개인정보보란에 출생일 기재). ‘추적 데이터’는 개인이 모르는 새 기록된 데이터로 참여과정이나 데이터 추적기술을 통해 캡처된 쿠키, 웹 비컨이나 기기/브라우저의 흔적, 위치 데이터와 기타 메타데이터를 말한다(특정 앱 사용이나 포스트할 때 위치, 특정 플랫폼 사용시간 등). ‘추론 데이터’는 ‘주어진 데이터’와 ‘추적 데이터’ 분석에서 도출된 데이터로, 알고리즘(일명 프로파일링)에 의해 다른 데이터 소스와 결합하는 데이터(예. 나이, 성별, 페이스북 좋아요 등으로 개인이 살 만한 물건을 예측)를 말한다. 온라인 프라이버시 관련, 일반적으로 개인의 프라이버시와 당사자나 지인(아동의 경우 보호자)이 직접 입력한 데이터를 가장 먼저 떠올리지만, 추적 데이터나 추론 데이터가 프로파일링 등을 통해 아동의 삶에 장기간 영향을 미칠 수 있다(Children’s Commissioner, 2018)

데이터 수집을 위한 추적과 감시, 프로파일링이 일상화되면서 인간의 기본권이자 민주주의 사회에서 표현의 자유를 뒷받침하는 프라이버시의 본질을 재조명하는 목소리도 재조명되고 있다. 유엔 인권이사회(UN Human Rights

Council, 2017)는 프라이버시 권리를 “인격의 자유로운 발달을 가능하게 하는 권리”로 파악하고, “프라이버시 권리 침해가 표현의 자유 권리, 집회와 결사의 자유 권리를 포함한 다른 인권에 영향을 미칠 수 있다”고 보았다. 유네스코(2017)는 미디어리터러시에서 프라이버시의 초점은 “사회에서 정보의 흐름을 결정하는 프라이버시의 기능과 역할에 관한 것, 사회의 권력과 부의 분배와 같은 불가분한 관련 문제뿐만 아니라 시민 개인의 인격 발달에 결정적으로 영향을 미치는 것”에 있다고 봤다(Culver & Grizzle, 2017, p. 32).

2. 미디어 리터러시로서 프라이버시

지금까지 미디어 리터러시에서 프라이버시 이슈는 주요한 영역은 아니었다. 하지만 프라이버시가 민주주의 사회의 인간의 기본권으로서 미디어 리터러시가 발현될 수 있는 바탕이 된다는 점과 디지털 미디어의 진화와 데이터 환경의 확장 국면에서 정보의 흐름을 이해하고 권한을 갖는 것이 중요하다는 점에서 프라이버시는 미디어 리터러시, 디지털 시민성 교육에서 간과할 수 없는 부분이 되었다.

프라이버시에 대한 유네스코의 입장은 프라이버시와 미디어 리터러시의 접점을 분명하게 드러낸다. 유네스코(2017)는 프라이버시를 표현의 자유, 정보의 자유와 함께 인격의 자유로운 발달을 위한 필수 요소로 보고, 프라이버시 권리가 표현의 자유 권리와 민주주의의 권리를 지지한다고 봤다. 프라이버시가 존중받는 환경에서 외부 압력과 간섭 없이 개인의 생각, 정치적 의견, 예술적 표현을 펼칠 수 있으므로, 프라이버시는 자유로운 의사 표현과 콘텐츠 제작 등 표현과 참여 즉 미디어 리터러시의 근간이고, 표현과 참여는 교육, 재정의 기회 등 다양한 기회에 영향을 미치므로 미디어와 기술의 발전에서 프라이버시와 미디어 정보를 읽고 이해하는 것(literate)의 의미가 중요하다고 강조한다. 프라이버시 권리는 온라인과 오프라인에서 인권과 연결되어있다. 유네스코는 인터넷에 대한 접근과 차별받지 않음, 표현의 자유와 정보의 자유, 집회의 자유,

결사와 참여의 자유, 아동과 청소년을 위한 특별 보호, 인권과 기본적 자유의 제한·침해의 구제권 등이 프라이버시와 관련있다고 본다(Culver & Grizzle, 2017).

미디어 리터러시는 미디어와 기술이 개인의 자유와 개인 행위자성(personal agency)을 지니고 살아가는 능력을 가능하게 하거나 제한하는 방법을 이해하게 한다는 점에서 프라이버시와 직접적인 관련이 있다. 디지털 환경에서 프라이버시에 대한 이해는 데이터와 정보의 생성·분석·배포·적용·사용·자산화 과정에 대한 이해를 포함한다(Culver & Grizzle, 2017, p. 15). 프라이버시 보호 역량은 프라이버시를 요구하는 능력과 정보를 보호하는 방법뿐만 아니라 어떤 정보를 공유할지 판단하고 행동하는 것을 포함한다. 외부에서 어떻게 내 데이터를 접근하고 사용하는지, 의식적/무의식적으로 어떻게 접근을 허용하거나 제한할 수 있는지 등을 질문하거나 이해하는데 미디어 리터러시 능력(지식, 기술, 태도)이 필요하므로, 대부분의 프라이버시 역량은 본질적으로 미디어·정보·디지털 역량이고, 미디어 리터러시는 프라이버시를 이해·보호하며 타인의 프라이버시를 존중할 수 있는 선행조건이다. 즉 ‘온라인에서 개인 프로필과 정보의 상품화·수익화에 대해 인식하는’ 프라이버시 역량은 ‘앱과 서비스의 비즈니스 모델을 인식하고, 인터넷/기술 중계자와 미디어가 프라이버시 정책에 대한 책임이 있다는 것을 아는’ 미디어 리터러시의 맥락에 있다고 볼 수 있다. 프라이버시와 관련된 다양한 혜택과 우려 지점을 판단하려면 미디어 리터러시 역량인 ‘민주주의 사회에서 미디어의 역할과 기능을 이해하는 기술(skill)’이, 상업적 목적으로 개인의 사진을 이용해도 되는지를 결정하려면 ‘윤리적 정보 이용 기술’이 필요하다. 또한 데이터 보안 등을 이해하기 위해서는 정부나 상업적 이해관계의 파악이 필요한데, 이는 미디어 리터러시의 중요한 부분이다(n. d.). 동시에 미디어 리터러시는 데이터 환경, 디지털 추적과 데이터 흐름에 대한 이해뿐만 아니라 프라이버시 권리의 요구 능력도 포함해야 한다. 기술이 프라이버시, 투명성, 표현의 자유와의 관계를 변화시키고 있다는 점에서 정보, 미디어와 기술에 대한 이해는 미디어 리터러시에서 중요해졌다(Cannataci et al., 2016).

미디어 플랫폼에서 프라이버시에 대한 인식은 인터넷의 ‘무료’서비스 이용에 ‘비용’이 들고, 이 비용은 절대 남용되어서 안 되며 투명한 이용자의 동의가 필요하다는 점에서 시작된다. 프라이버시 역량이 있다면, 미디어 산업에 대한 이해(미디어 리터러시)를 근거로 소셜미디어, 전통적인 미디어나 모바일 앱의 무료 서비스에 대한 대가로 개인정보를 제공하는 것을 결정할 수 있어야 하고, 개인정보가 동의하에 이윤 창출에 사용될 경우 공정한 소득 분배나 이익 공유를 요구하거나 협상할 수 있어야 한다. 또한 개인정보나 다른 데이터를 공유할 때와 개인정보에 문제가 생겼을 때 정보에 입각한 결정을 내릴 수 있어야 한다. 특정 정보가 개인으로 식별될 수 있는 상황을 이해하는 능력은 비자발적으로 수집된 메타데이터를 어떻게 처리할지 등을 포함하는 매우 복잡한 판단을 요구한다. 프라이버시는 타인의 접근으로부터 개인정보를 보호하고, 이를 제한할 필요성 차원에서 접근하는 경우가 많지만 현실에서 매우 복잡한 양상을 띤다⁷⁾.

미디어 리터러시는 아동·청소년이 프라이버시를 이해하고 관리하며 보호하는 방법을 익히는데 중요한 역할을 한다. 프라이버시 관련 미디어 리터러시 기술은 자율성, 정체성, 친밀성, 책임감, 신뢰, 친사회적 행동, 회복탄력성, 비판적 사고 등 다양한 아동 발달 영역과 밀접한 관련이 있다(Raynes-Goldie & Allen, 2014; Pradeep & Sriram, 2016; Balleys & Coll, 2017; Livingstone et al., 2019 재인용). 프라이버시는 수년간 위협과 위협의 프레임(금전적 손실, 납치 등)으로 다뤄졌으나(Children’s Commissioner, 2018), 미디어 리터러시 교육에서 프라이버시는 개인 프라이버시 필요성과 가치 이해, 디지털 기술

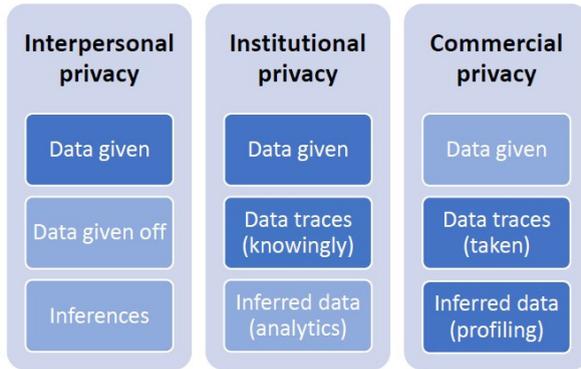
7) 한 예로 정부가 언론의 자유를 제한하는 것은 문제이나 정부가 테러와 전쟁 우려 지역에 머무는 자국민의 소셜미디어 계정에 접속하는 것은 적법한 절차를 따른다면 긍정적일 수 있다. 글로벌 기업이 고객의 구매를 추적해, 정보를 이용해 상품을 추천하는 것은 유용할 수 있지만 쿠키를 사용해 동일한 회사가 소유한 여러 웹사이트에 광고를 내보내는 것은 침해적일 수 있다. 정부 접근은 시민 보호를 목적으로 하지만 시민들은 보안을 대가로 데이터에 대한 통제권을 포기해야 할 수 있다. 상업적 접근은 개인의 의지나 지식에 반해 배경, 관심사, 경제 상태에 기초해 개인 데이터에 대한 접근은 판매될 수 있기 때문에 이 과정을 정확히 이해할 수 있어야 한다. 개인들은 정보를 무차별적으로 공유할 수 있는 다양한 주체들로부터 데이터 통제권을 넘겨달라는 요청을 수없이 받고 있고, 이러한 시나리오를 분석하려면 높은 수준의 미디어 리터러시 역량이 필요하다(Culver & Grizzle, 2017).

사용시 프라이버시 함의 이해, 프라이버시와 투명성의 균형 설명하기, 표현의 자유, 정보에 대한 접근을 포함한다. 리빙스톤(Livingstone, 2014)은 미디어 리터러시는 행위유도성(프라이버시 포함), 커뮤니케이션(생산과 디코딩), 사회적 상호작용(관계, 프라이버시, 익명성 등) 등 여러 영역의 역량을 포함할 필요가 있고, 이러한 미디어 리터러시 발달에 프라이버시 역량이 중요한 역할을 한다고 말한다. 디지털 시대 개인 데이터가 통신과 정보, 데이터 수집·저장·전송 수단(디지털 미디어, 앱, SNS, 데이터베이스, 출판물, 디지털 아카이브, 컴퓨터, 모바일기술, 여러 모바일 장치)에 쌓여있으면서 프라이버시의 폭은 더욱 넓어졌고, 사회경제적 분류를 위해 감시와 마케팅 차원에서 이용되고 있는 데이터화(datafication)는 개인에게 균일하게 영향을 미치지 않는다. 데이터와 프라이버시 관련 정보의 비대칭은 새로운 형태의 위계를 만들어낼 수 있고, 이 과정에서 구성원들은 불이익을 당하거나 소외될 우려가 크다는 점에서 미디어 리터러시 교육에서 프라이버시 교육이 필요하다(Pangrazio & Selwyn, 2020).

3. 아동·청소년 프라이버시의 개념적 이해

아동·청소년의 프라이버시를 보다 입체적으로 이해하기 위해서는 가정, 학교, 미디어 이용 등 아동이 경험하는 디지털 환경에 대한 이해가 필요하다. 아동과 미디어 리터러시에 대한 논의를 주도해온 리빙스톤 등(Livingstone et al., 2019)은 아동의 온라인 프라이버시를 개인의 관계 유형에 따라 △개인과 다른 개인이나 집단(대인 프라이버시) △공공 혹은 제3부문(비영리 프라이버시) △영리 집단(상업적 프라이버시)으로 구분했다. ‘대인 프라이버시(Interpersonal privacy)’는 개인 ‘데이터 자아’ 즉, 개인에 관한 온오프라인에서 이용가능한 정보가 온라인 연결을 통해 생성·접속·증폭되는 과정과 관련이 있고, ‘제도적 프라이버시(institutional privacy)’는 정부, 교육, 보건 등 공공기관의 개인 데이터 수집·처리 과정에 초점을 맞춘 개념이다. 리빙스톤 등(2019)은 정부 차원의 정보 수집도 문제이지만 데이터에 대한 전권이 정부기관에 위임되는

상황에서 학교 등 교육기관을 통한 정보 수집 문제가 심각하다고 보았다. 특히 교육기관의 프라이버시와 관련된 이슈는 대개 보안(security) 같은 기술적 측면에 치중해있고, 데이터 수집 목적, 다른 집단과의 공유 과정, 장기적 결과는 거의 다뤄지지 않았다고 지적했다. 디지털 기기를 이용해 학습(예, 원격교육)과 학사관리가 이뤄지고, 코로나19 이후 이런 과정이 폭발적으로 늘면서 공교육이 상업적 플랫폼과 비즈니스 모델과 결합하는 것에 대한 많은 우려가 있음에도 이에 대한 논의는 대부분 미래지향적 교육모델의 변화 정도로 다뤄지고 있고, 디지털 학습 플랫폼, 출석·학업 성과에 대한 프로파일링 같은 아동 관련된 ‘제도화된 프라이버시’에 대한 논의는 거의 없다.



[그림 2-1] 프라이버시 차원과 데이터 유형 (Livingstone et al., 2019, p. 16)

‘상업적 프라이버시’는 기업이 비즈니스와 마케팅 목적으로 개인 데이터를 수집·사용하는 과정과 관련이 있다. 온라인 활동의 상품화에서 아동의 활동도 예외는 아니어서, 쿠키 배치, 위치기반 광고와 행동 타겟팅을 통해 온라인 활동을 모니터링하고 프로파일링하고, 필요 이상 많은 개인정보를 공개하도록 권장하며(Bailey, 2015; Shin & Kang, 2016), 디지털 서비스와 제품에 대한 참여와 접근을 유도하기 위해 개인정보를 공개하게 한다(Micheti et al., 2010; Lapenta & Jørgensen, 2015). 이것들은 특히 아동의 이해 능력뿐만 아니라 법정대리인의 이해와 동의(한국의 경우 만 14세 미만 아동의 개인정보

관련 모든 권리는 부모에게 있다)와도 관련이 있다(Livingstone, 2018). 아동들은 상업적 프라이버시(온라인 추적, 데이터 영구 저장, 데이터 삭제 불가)에 대한 일부 우려하지만 정부나 민간 기업에 의한 데이터 이용은 크게 우려하지 않았고, 대체로 개인 데이터가 무엇을 의미하는지, 자신의 데이터가 누구에게, 왜 가치가 있는지를 알지 못했다(Lapenta & Jørgensen, 2015). 아동들은 소셜 미디어와 같은 온라인 서비스를 사용할 때 수동적이고 무의식적으로 개인 데이터를 제공했다(Pangrazio & Selwyn, 2018; Selwyn, Pangrazio, 2018).

개인이 맺는 관계 유형에 따라 프라이버시를 분류한 리빙스턴 등(2019)과 달리, 유니세프(2018)는 '온라인 어린이 프라이버시와 표현의 자유에 관한 보고서'에서 아동의 프라이버시 권리가 복합적이라는 점에 주목해, △물리적(physical) △커뮤니케이션(communication) △정보(informational) △의사결정(decisional) 네 차원으로 프라이버시를 분류했다. '물리적 프라이버시'는 아동의 실제 이미지, 행동이나 위치를 추적, 모니터링과 방송하는 기술의 영향을 받는 것과 관련이 있고, '커뮤니케이션 프라이버시'는 아동의 게시물, 채팅, 대화, 메시지나 통화를 정부나 다른 행위자가 감시하는 상황과 관련이 있다. '정보 프라이버시'는 아동의 개인 데이터가 수집·저장·처리될 때의 위험성과 관련이 있고, '의사결정 프라이버시'는 정보에 대한 접근을 제한해, 아동의 독자적 의사 결정이 방해받는 것과 관련이 있다(UNICEF, 2018).

영국 아동위원회(Children's Commissioner, 2018)는 일상적으로 아동을 둘러싼 데이터 환경을 중심으로 △온라인에서 공유되는 데이터 △가정에서 공유되는 데이터 △가정 밖에서 공유되는 데이터로 구분했다. '온라인에서 공유되는 데이터'는 스마트폰과 태블릿, 웹 브라우징과 검색엔진, 부모의 소셜 미디어 프로필에 업데이트되는 내용이고, '가정의 데이터'는 인공지능 스피커, 인터넷과 연결된 장난감, 홈캠(homecam), '가정 밖 데이터'는 위치추적 시계, 학교 데이터베이스, 학습과 습관(예. 운동, 건강) 앱, 학교의 생체인식 데이터, 마트 등의 회원제서비스, 의료보험 및 의료기록 등이고, 주로 교육이나 보건 서비스 같은 공적영역의 데이터인 경우가 많다. 대개 아동에게 혜택을 주는

것이 목적이지만 학교 등 공공부문에서 프라이버시나 투명성, 보안 등을 지키지 않는 경우나 민간과 협력관계 등을 통해 아동과 부모가 모르는 새 아동의 건강이나 교육에 관한 매우 민감한 데이터가 사기업으로 흘러들어가는 경우가 있다. 가정 밖 데이터를 둘러싸고 수많은 행위자가 있고, 아동과 가족과 데이터를 직접적이지 않은 방식으로 사용하는 사람들의 관계의 복잡한 맥락 속에서 아동의 프라이버시와 정체성의 권리가 지켜지는지 다소 회의적이라는 지적이 있다.

〈표 2-1〉 유니세프의 아동의 온라인 프라이버시와 표현의 자유에 관한 일반원칙(UNICEF, 2018, p. 11)

원칙	영향을 미치는 요인
프라이버시와 개인정보 보호 권리 보장	<ul style="list-style-type: none"> •모니터링 기술 •감시기법 및 기술 •정보 수집, 분석, 보유 방식 •프로파일링
표현의 자유와 정보 접근권 보장	<ul style="list-style-type: none"> •비용과 리터러시 포함 인터넷 접근을 가로막는 요소 •콘텐츠 조정 및 편집 •네트워크, 디바이스 차원 필터링 •가명 금지(예. 페이스북) •정보 수집을 전제로 한 콘텐츠 접속 허용
평판 보호 권리 보장	<ul style="list-style-type: none"> •디지털 리터러시 •데이터나 콘텐츠 제거를 위한 절차의 복잡성 여부 •동의없는 아동의 개인정보 공유 가능 여부
이해수준에 따른 권리 보장	<ul style="list-style-type: none"> •설명기반 동의 제공 능력 •약관 내용에 대한 이해 여부 •부모의 모니터링과 의사결정 여부
피해보상을 위한 소송 권리 보장	<ul style="list-style-type: none"> •인권에 미치는 영향에 대한 투명한 보고 •인권교육 여부 •효과적인 신고 수단 존재 여부

4. 아동·청소년의 프라이버시 의미와 현황

앞서 논의한 것처럼 프라이버시 권리는 인간의 기본권이라는 점에서 모든 세대와 연령에 필수적이지만 아동은 성숙하지 않은 상태이자 발달 과정에 있고, 오늘날의 아동이 디지털 환경에서 태어나서 성장하는 점에서 프라이버시는 아동의 발달과 성장에 반드시 필요하다. 데이터 환경 등 디지털 생태계 환경, 기술적 행위유도성, 아동의 미디어 이용 관행은 아동의 프라이버시 위협 요인이 된다(Livingstone et al., 2019). 스마트폰 대중화 이후 출생한 아동은 성인이나 어느 정도 성장한 후 디지털 기기를 접한 세대와 달리 출생과 동시에 관련 데이터가 수집된다. 연령이 적을수록 데이터가 많이 수집되고, 보통 2세 전부터 상당한 양의 정보가 수집되는 경우가 많다(UNICEF, 2018). 21개국 0~8세 아동 대상의 연구에서 선진국의 2세 미만 아동은 대부분 부모의 온라인 활동을 통해 디지털 흔적을 가지고 있는 것으로 나타났다(Chaudron et al., 2018). 평균 13세 자녀를 둔 부모는 소셜미디어에 자녀의 사진과 동영상을 1,300개 가량 포스트하고, 18세까지 거의 7만개를 포스트한다(Children's Commissioner, 2017). 태어난 순간부터 아동의 데이터를 수집할 수 있고, 성인이 되기까지 18년 동안 생성되는 디지털 정보의 양은 엄청나다. 아동 개인은 온라인에서 적극적으로 활동하기 전부터 건강, 교육, 사회복지와 관련된 정부의 플랫폼과 가족들의 디지털 기기 이용 관행에 의해 데이터화되고, 이 과정을 거쳐 아동의 온라인 정체성이 형성된다(Pangrazio & Selwyn, 2020). 아동은 정부 플랫폼의 건강과 심리 데이터, 학교 플랫폼과 교육 앱에서 수집된 데이터, 인터넷과 연결된 장난감과 게임, 디지털 페어링팅(Blum-Ross & Livingstone, 2017), 라이프 스타일과 엔터테인먼트 기술(게임 콘솔, 스마트워치 등)에 노출되어 있고 개인 데이터 수집과 프로파일링에 취약하다. 또한 5~7세 아동부터 이미 데이터를 수집하고 공유하는 서비스를 이용하고, 공식 이용가능 연령이 14세임에도 8~11세 영국 어린이 5명 중 1명 이상(21%)이 소셜 미디어 계정을 가지고 있는 등(Ofcom, 2017b), 소셜미디어를 1차적인 미디어로 이용

하면서 일상적으로 개인데이터가 생성·노출·수집되는 상황에 놓여있다. 페이스북의 아동용 인스타그램 서비스 개발 시도처럼, 거대 플랫폼 기업들은 아동 데이터를 수집하기 위해 다양한 기술적 수단과 서비스를 총동원하고 있다. 유니세프(2020)는 AI와 머신러닝을 결합한 다양한 광고기법이나 강력한 인터페이스와 유명한 아이คอน 등을 사용한 게임플랫폼의 ‘playable ads’와 같은 광고 기술을 사용해 성장한 틱톡, 구글, 페이스북 등 플랫폼 기업을 ‘키드 테크(Kidtech)’로 명명하면서 아동의 프라이버시에 대해 우려를 드러냈다. 이러한 프라이버시 위협은 온라인 마케팅과 데이터 판매 등 상업적 이용, 데이터화 외에도 악성 프로그램 유포, 피싱, 개인정보 도용 및 신원도용, 명예훼손, 협박, 스토킹, 성적학대, 폭력에 노출될 위험을 낳고(Dey et al., 2013; Muruma-Mengel, 2015), 더 나아가 인생의 기회에 영향을 미칠 수 있다(Children's Commissioner, 2018).

아동의 프라이버시 위협은 감시 이슈와도 연관된다. 기기나 앱(예. 홈캠, 스마트폰 감시앱)을 이용한 부모의 아동 모니터링은 대표적 사례이다. 부모의 일상적 모니터링은 아동에게 감시행위를 정상적인 것으로 받아들여지게 하고, 자신의 데이터를 아무 생각없이 넘겨주게 되고, 데이터를 넘기는 행위에 대해 아무런 문제제기를 하지 않게 한다. 자신의 데이터를 너무 자주 넘겨주다보니 타인이 왜 자신의 데이터를 필요로 하는지, 자신의 데이터가 어떻게 사용될지에 대해 의문을 갖지 못하고 데이터를 넘기는데 익숙해져서 오히려 아동을 위협에 빠뜨릴 수 있다. 아동에게서 너무 많은 데이터를 수집하는 상황이 프라이버시가 얼마나 가치있고 민감한지, 그것을 보호하는 것이 얼마나 중요한지를 인식하지 못하게 만든다는 점에서 아동들에게 잘못된 메시지를 줄 수 있다(Children's Commissioner, 2018). 그 뿐만 아니라 부모나 교사가 자신을 지켜보고 있는 상황은 아동 발달이나 가족 역학에 부정적 영향을 미칠 수 있다. 아동이 위협에 처하고 극복하는 과정은 성장의 일부이며, ‘위험 없는 환경 구축’은 불가능한 일이다. 아동들은 디지털 미디어 이용하면서 성장에 필요한 전략을 구축하며, 발달의 기회를 얻는다(Livingstone, 2008). 오히려

규율, 통제의 외피를 쓴 부모의 위협 회피 전략은 아동의 물리적, 사회적, 가상 세계에 대한 탐구를 제한하고(Barron, 2014), 아동의 자율성과 독립성을 침해할 가능성이 높다(Wisniewski, 2018).

아동의 프라이버시에 대한 인식과 실행 전략에 관한 연구에 따르면 아동들은 나름의 전략을 구사하고 있다. 영국의 12~15세의 인터넷 사용자 대상 연구에서 아동의 3분의 1(34%)이 검색기록 삭제 방법, 4명 중 1명(24%)은 브라우저를 프라이버시 모드 등으로 설정하는 방법을 알고 있었으며, 10명 중 1명(10%)은 온라인 필터나 컨트롤을 비활성화하는 방법을 알고 있었다(Ofcom, 2017a). 아동의 프라이버시 보호 기술도 시간이 지남에 따라 향상되는 것으로 보인다. 하지만 아동기는 디지털 기술과 프라이버시 위협에 대한 인식이 부족하고, 개인 데이터 공유가 자신에게 미칠 영향을 이해하는 능력이 형성되는 상태이므로 성인보다 프라이버시 침해에 더 취약하다(Children's Commissioner, 2017; Livingstone et al., 2019). 아동들은 대체로 프라이버시에 대해 정확하게 이해하지 못하고 프라이버시 보호 방법을 알지 못했고(Chaudron et al., 2018), 12세 정도가 되면 정보 노출에 신중해지기도 하지만(Wisniewski et al., 2015), 효과적으로 대응하지 못했다(Livingstone et al., 2019). 아동들은 온라인에 남기는 '데이터 추적'(예: 이전 검색에 따른 광고 보기와 관련된)과 기기 추적(예: 일부 앱이 지리적 위치를 사용함)에 대해 일부 인식하고 있지만(Redden & Way, 2017), 자신의 데이터가 어떻게 공유되는지를 연결시키지 못했다. 데이터 흐름과 인프라에 대한 지식이 없어 대부분의 데이터를 정적이고 흩어진 것(예: 서로 다른 플랫폼의 위치)으로 봤다(Bowler et al., 2017). 특히 데이터 추적이 미래에 미칠 영향에 대해 거의 인식하지 못했다(Livingstone et al., 2019). 또한, 아동은 프라이버시를 주로 대인관계의 데이터 공유 등 대인적 측면에서 이해하고, 데이터의 상업적이거나 제도적 이용을 거의 고려하지 않았다(Davis & James, 2013; Steihn & Vedder, 2015; Livingstone et al., 2018b). 아동들은 낯선 사람이 집주소를 아는 것이 끼칠 위험은 잘 알고 있지만, 어린 시절 수집된 개인 데이터가 장기적으로 개인의 경험과 전망에

어떤 영향을 미칠지 잘 몰랐다. 부모의 쇼핑 습관이 광고를 통해 아동을 겨냥한 상품과 서비스에 영향을 미칠지, 건강 데이터가 미래에 보험에 가입하는데 어떤 영향을 미칠지 알지 못했다(Children's Commissioner, 2017).

아동들은 상업적 프라이버시 영역과 관련해 어려움을 겪는 것으로 나타났다(Bowler et al., 2017; Coleman et al., 2017; Acker & Bowler, 2018). 아동들은 기업의 플랫폼을 신뢰하고, 사이트 설계자가 개인정보 보호 체계를 적절하게 구축했다고 믿고, 기업이 제공하는 개인정보의 설정을 거부감 없이 수용했다(Davis & James, 2013). 이런 것들은 미디어 이용에서 아동의 주도권을 저해할 수 있다. 미국의 11~18세 대상으로 한 질적 연구에서 대다수 응답자가 데이터에 대해 추상적으로 알고 있고 구체적이고 개인적인 수준에서 데이터와 연결하는 것을 어려워했다. 소셜미디어와 관련된 보안 문제를 알고 있지만, 데이터의 디지털 추적(digital trace)과 이것이 미래에 미칠 영향은 거의 생각하지 않았다(Bowler et al., 2017). 오프콤(2017b)이 3~11세 아동의 미디어 이용 관행과 역량을 조사한 결과, 아동들은 복잡한 광고·마케팅 환경으로 진화한 온라인 광고를 잘 알아차리지 못했고, 특히 소셜미디어 콘텐츠와 유사해 보이는 광고를 구분하지 못했다. 아동들은 후원 광고를 통해 광고 수익을 이해했지만 많은 아이들이 광고라는 단어가 나와도 정확하게 파악하지 못했으며, 구글을 신뢰할 수 있는 출처로 믿고 있었다(Ofcom, 2017b). 13~17세 호주 아동을 대상으로 한 참여적 실험 연구에서, 아동들은 소셜미디어 활동을 상대적으로 안전하다고 생각했고, 많은 아동들이 다른 사람들이 자신에 대해 어떤 정보를 볼 수 있는지 확신하지 못했고, 온라인 게시물의 영구성에 대해 우려하고 있는 것으로 나타났다. 아동들은 광고의 표적이 되는 것에 반대하지 않았고, 일반적으로 온라인 프라이버시에 관심이 있고 염려하고, 압도되고 짜증을 느꼈지만 변화시킬 수 있다고 느끼지 않았다(Selwyn & Pangrazio, 2018).

유니세프(2018)는 '디지털 환경에서 아동의 프라이버시'와 관련해 아동이 사적이고 안전하게 온라인으로 정보에 접근할 수 있고, 아동의 커뮤니케이션과

개인 데이터는 무단 접근·침입으로부터 보호되어야 하고, 아동의 프라이버시는 아동에 맞게 설계되거나 아동용 웹사이트, 플랫폼, 제품, 서비스의 설계가 고려되어야 하며, 온라인 프로파일링으로부터 보호받아야 한다고 보았다. 아동의 '정보 프라이버시'와 관련해 아동, 보호자는 데이터 처리에서 자유롭게 정보에 기반한 동의를 제공받아야 하고, 아동의 데이터는 공정하고, 합법적이고, 투명한 방식으로 처리되고, 아동의 데이터는 최소한의 필요한 것으로 정확하고, 시기에 맞게 저장되어야 하고, 아동은 개인데이터를 보호할 수 있도록 교육받고, 정보를 제공받고(informed), 북돋아지는(empowered) 곳에서 아동의 프라이버시가 최상으로 보호될 수 있다고 강조했다(p. 8). 영국 아동위원회는 학교에서 아동에게 데이터 수집과 이용, 데이터 발자국 통제하기 위한 방안을 가르쳐야 한다고 강조했다(Children's Commissioner, 2017).

이 연구는 리빙스톤 등(2019)과 영국 아동위원회(2018)의 아동·청소년의 프라이버시 개념 분류를 종합해, 좁은 의미의 디지털 환경과 더 넓은 의미의 생활세계로서의 디지털 환경으로 아동·청소년의 가정, 학교, 미디어 환경에서 일어나는 아동의 프라이버시 이슈에 대해 진단하고자 한다.

제 3 장

디지털 환경에서 아동·청소년 개인정보 및 프라이버시 침해 위협

제 3 장

디지털 환경에서 아동·청소년 개인정보 및
프라이버시 침해 위험

제1절 • 디지털 환경에서 아동·청소년 개인정보 침해가능성 확대

1. 디지털 신기술 현황과 개인정보 위험

데이터 경제의 발전에서 비롯한 데이터 활용의 극대화는 사회에 다양한 순기능과 함께 역기능을 발생시키고 있으며, 매일 새롭게 생겨나는 온라인 플랫폼과 서비스들은 우리 생활 모든 분야에 접목돼 기존에 한정된 영역에서만 발현되던 개인정보 침해 가능성이 사회 전 영역으로 확대·심화되고 있다. ICT 기술의 확산은 산업적 측면의 혁신을 의미하는 동시에 개인정보 오남용 및 이에 따른 피해 증가 가능성을 동시에 내포한다. 특히 데이터 중 활용 가능성이 가장 높다고 볼 수 있는 개인정보의 활용 가치는 지속적으로 증가하고 있으며, 디지털화된 개인정보는 대규모로 수집·집적할 수 있기에 프라이버시 침해 가능성을 심화시키고 있다. 또한 기술 진보에 따라 개인정보의 수집·이용·보관·제공·파기의 처리 과정의 구체적인 행태가 확연히 변화되고 있고, 그에 따라 개인정보 침해 위험의 사전 예측이 어려워지고 있다. 빅데이터 분석 기술의 발전으로 자동화된 디바이스 및 센서로부터 여러 유형의 개인정보가 자동수집되어 저장·관리되는 개인정보의 양이 증가할 뿐만 아니라, 해당 정보들을 기반으로 한 프로파일링, 추적성 확보가 가능하게 되어 개인의 프라이버시 침해 위험성이 증가한다. 글로벌 협업의 증가는 개인정보의 공유와 이전·유통을 더욱 확대시키고 이용·제공 단계에서 위험 요소를 증가시킨다.

다양한 분야에서 디지털 신기술의 발달은 새로운 유형의 개인정보보호 이슈를 출현시키고 있다. 최근 지속적으로 수요가 늘고 있는 웨어러블 기기는

스마트폰보다 더 다양한 종류의 센서들을 제공하고, 웨어러블 기기의 센서를 통해 수집된 정보들은 이용자의 행동정보나 생체정보 등을 실시간 수집한다는 점에서 민감한 건강정보 및 바이오정보 유출 등에 관한 개인정보 이슈가 나타나고 있다(이근영, 2016). 스마트 보건의료 분야에서도 최근 네트워크 기반의 의료기기와 의료정보시스템이 증가하고 인공지능, 빅데이터 등 최첨단 기술이 빠른 속도로 의료기관 내외의 각종 시스템에 도입되면서, 환자정보를 포함한 민감한 개인정보가 수집·유통·활용되며 강력한 개인정보보호가 요청되고 있다. IoT 기술의 발전과 함께 확산되고 있는 스마트홈 기술은 집안 냉난방부터 조명, 주방, 보안에 이르기까지 가정의 다양한 장치들을 네트워크에 연결해 집안의 모든 정보를 모니터링 및 제어할 수 있도록 도와주는데 이 과정에서 주거자의 행태정보, 민감정보 등을 수집하기 때문에 유출시 개인의 사생활이 적나라하게 노출될 수 있다(조도은·김시정, 2018). 영상정보 촬영과 관련한 프라이버시 이슈도 증가하고 있다. 드론 등 무인이동체는 개인이 소유해 원거리 촬영 목적의 활용이 증가하고 있는데 「개인정보보호법」에서는 영상정보처리기기의 요건으로 '일정한 공간에 지속적으로 설치'를 언급하고 있어 드론과 같이 이동형 영상정보처리기기의 프라이버시 침해 규제에 대한 공백이 존재한다. 체험용·교육용 기기로 많이 활용되는 VR(Virtual Reality)·AR (Augmented Reality) 기기도 기기 착용 후 비공개 장소에 출현하는 경우 착용자 시야에 들어오는 모든 정보가 기록되므로 소형 기기가 불법촬영 등 불법적 프라이버시·개인정보 침해에 동원될 가능성이 있어 문제가 되고 있다. 고정형 CCTV에서 진화해 자동으로 특정인을 식별하고 추적할 수 있도록 개발된 지능형 CCTV 기술 역시 개인을 더욱 쉽게 식별할 수 있고 발전된 형태의 추적기능을 탑재하고 있는 점에서 개인정보 침해 위협이 크다.

이처럼 새롭게 출현하는 디지털 신기술들은 개인정보 위협과 관련해 여러 가지 공통적인 특징을 지닌다. 우선 개인정보 처리 절차가 갈수록 복잡해지고 있다. 기존의 개인정보 수집은 주로 서비스제공자가 수집하는 개인정보 항목을 명시하고 이용자가 직접 입력하는 형태로 이루어졌다면 현재는 위치정보, 음성

정보, 신체관련 정보들이 다양한 센서를 통해 실시간으로 수집되고 IP주소, 쿠키정보, 서비스 이용 기록들이 정보주체도 모르는 새 자동 수집되기도 한다. 또한 개인이 사용하는 기기가 늘면서 디바이스 연동에 의한 개인정보 수집, 서비스가 플랫폼 단위로 통합돼 운영되면서 타서비스와 연동되어 제공되는 개인정보 등 개인정보 수집경로가 상당히 다양해졌다. 게다가 수많은 기능들을 통합해 제공하므로 개인정보를 위탁·제공하는 업체들이 많아졌고 이에 따라 개인정보의 관리의 어려움과 유출 위험성이 증가된다.

인공지능을 통한 데이터 학습과 빅데이터 분석을 하는 서비스가 점점 많아지고 정보를 자동측정·생성할 수 있는 기술이 고도화되면서, 정보주체가 쉽게 인지하지 못하는 새 수많은 정보들을 자동 수집되는 것도 큰 문제이다. 자동생성정보로 인한 프라이버시 침해 위험에 대한 연구가 부족하고 해당 정보 수집에 대한 국민의 이해도가 낮은 만큼, 디지털 환경의 새로운 온라인 서비스들이 자동 수집정보를 얼마나 수집하고, 어떤 목적으로 활용하는지 현황 파악이 안 되고 있으며, 이에 따라 정보주체가 적절한 대응을 하기 어려워지는 상황이 계속되고 있다.

개인정보의 처리를 통한 프로파일링 등 자동화된 의사결정이 본격 적용되는 흐름도 우려가 되는 부분이다. 개인정보 분석에 기반한 자동화된 의사결정이 분야를 가리지 않고 대부분의 서비스에 활용되고 있고 이러한 개인 프로파일링은 개인신용도 평가, 보험료 자동산정, 타깃 마케팅 등 개인에게 민감한 사항들을 분석해 개인이 인지하지 못한 새 개인을 판단하고 다양한 불이익을 주기도 한다. 그러나 유럽연합의 GDPR이 규정하고 있는 프로파일링 거부권이나 개인 정보 분석결과에 대한 설명요구권 등은 우리 법에서 보장하지 않아 이에 대한 대응조차 불가능한 것이 현실이다.

2. 아동·청소년 디지털 활용 특성과 개인정보 침해 우려

아동·청소년은 다양한 범위의 신기술 디지털 네트워크에 접근하고 있고 변화에 가장 민감한 그룹이며 이들이 많이 사용하는 스마트폰, PC, 게임 콘솔과 같은 기기는 그들의 가장 가까운 친구이자 자기표현의 도구이자 교육의 도구, 표현의 도구 등 다양한 역할을 한다. 요즘 세대의 아동·청소년들은 디지털 언어와 장비를 태어나면서부터 자연스럽게 접하고 사용해온 세대로 이른바 디지털 네이티브이다.

디지털 네이티브인 아동·청소년은 온라인 활동에 능숙한 세대이지만 오히려 온라인 위험에는 취약할 수 있어 이들에 대한 개인정보보호 대책이 필요하다(염정윤·정세훈, 2019). 아동·청소년은 모바일 기기 목적에 제한을 받지 않고 성인에 비해 다양한 용도로 모바일 기기를 사용하고 있다. 개인정보 수집은 앱을 켜는 순간부터 웹사이트나 게임에 로그인하는 순간까지 디지털 서비스를 활용하는 모든 단계에서 이루어진다. 다수의 아동·청소년들이 모르는 사람에게 개인정보를 공개하거나 공유한 경험을 가지고 있으며, SNS 계정을 공개상태로 이용한다(Shin, Huh, & Faber, 2012). 아동·청소년 시기 친구의 이름, 위치정보, 감정상태, 나이 등은 앱이나 웹사이트를 통해 쉽게 수집된다. 아동·청소년은 성인보다 데이터 수집에 노출되기 쉽고 개인정보 제공에 대한 거부감도 적어 광고 등의 타겟이 되기 쉽고, 사이버공격 같은 데이터 침해에도 취약하다.

아동은 온라인 환경에 친화적이고 새로운 기술이나 서비스에 대한 적응력이 높아서 이용도도 매우 높으나 프라이버시나 개인정보의 중요성에 대한 인식, 새로운 기술이나 서비스에 내포된 위험요소에 대한 인지능력이 상대적으로 떨어진다. 자신이나 부모의 개인정보를 충분한 고민없이 제공하거나 공개하기도 한다(정찬모, 2014). 급변하는 디지털 시대에 가장 민감하게 영향을 받는 그룹은 소수자 그룹이며, 그중 대부분의 법 테두리 안에서 특별법으로 보호받고 있는 아동·청소년은 디지털과 기술에 가장 쉽게 접근 가능한 집단이므로 그에 따른 위험도 크다. 특히 온라인 사용이 일상화되고 더욱이 COVID-19 시대를

맞아 디지털 접근성 향상 및 디지털 생활로 전환이 가속화되면서 디지털 네이티브 세대는 개인정보와 프라이버시에 대한 위협에 더욱 빈번하게 노출될 수밖에 없다.

실제 아동·청소년은 소셜미디어, 온라인 banking, 인터넷 쇼핑 등 개인정보 노출 정도가 높은 서비스 사용이 빈번한데 반해, 개인정보에 대한 지식이나 보호 행동은 타 연령대에 비해 낮아 개인정보와 관련된 위협에 상당히 취약한 계층으로 평가된다. 또한 10대 인터넷 이용자의 26.1%가 1년 이내에 개인정보 유출을 경험하는 등 전 연령대 중 가장 높은 비율을 차지하기도 한다(행정안전부·개인정보보호위원회, 2018). 오늘날의 최신 기술은 개인정보 처리를 통해 원격학습이나 원격소통을 지원하는 등 긍정적인 측면도 있지만 온라인 행동 추적을 지원해 어린이들을 성착취 등의 범죄나 데이터를 기반한 의사결정을 통해 차별적 상황에 놓이게 할 수 있다. 한편 아동·청소년은 스스로 개인정보에 대한 권리구제 절차를 진행하기 어려울 뿐만 아니라 법정대리인도 적극적으로 구제 절차를 진행하지 않는 경향을 보인다(윤주희, 2014). 개인화된 기기를 통해 이뤄지는 아동의 디지털 활동을 보호자가 충분히 인지하기 어려운 상황에서, 아동·청소년에게 성인과 동일한 수준의 행동을 요구하는 것은 관련 프라이버시 위험 역시 아동이 성인과 동일한 수준으로 책임져야함을 의미한다. 그러나 아동은 성인과 달리 완전한 인지역량을 지니지 못했으므로, 일반 성인과 달리 추가적인 보호조치가 필요하다(전윤선·나종연, 2020).

또한 현행 「개인정보보호법」은 14세 미만의 아동·청소년에 대한 개인정보 수집 시 법정대리인의 동의를 받도록 하고 있으나 상황에 따라 동의 절차를 거치지 않는 경우가 많다. 이는 주로 자동수집장치를 통해 수집되는 아동·청소년의 개인정보(IP정보, 위치정보, 행태정보, 사용습관정보, 선호 콘텐츠 정보 등)였으며, 이를 수집한 서비스 회사는 이를 통해 아동·청소년의 관심을 끄는 타깃 광고를 진행하기도 했다(전창욱·유진호, 2020).

그러나 생체인식 데이터 처리, 디지털 추적·감시, 자동화된 의사결정, 프로파일링 등의 잠재적 영향에 대한 아동·청소년 대책은 여전히 부족한 실정이다

(COMMITTEE OF MINISTERS, 2021). 아동·청소년에 대한 프로파일링 (profiling), 행동기반마케팅(behavioural marketing), 디바이스간 추적·타겟팅 (cross-device tracking and targeting), 실시간 변하는 광고(advertisements changing in real time), 합리적 행동을 우회하도록 고안된 애플리케이션 (applications designed to bypass rational behavior) 즉, 신경마케팅(neuro-marketing), 거대한 데이터 브로커 기업과 마케팅 클라우드 등으로 이루어진 상업적 감시 세계(commercial surveillance world)에서 부정확하거나 차별적인 알고리즘은 아동·청소년의 복지와 자아이미지 형성에 부정적인 영향을 미칠 수 있다. 방송통신위원회가 2017년 발표한 「온라인 맞춤형 광고 개인정보보호 가이드라인」에서 아동의 행태정보 수집과 맞춤형 광고를 원칙적으로 금지하는 내용은 이러한 우려를 반영한 것이라 볼 수 있다(이희정, 2019).

제2절 ● 아동·청소년 개인정보 침해 사례 검토

1. 틱톡 사건⁸⁾

1) 사건 개요⁹⁾

틱톡은 2012년 설립된 베이징 소재 인터넷 기술 기업 바이트댄스(Byte Dance)가 소유하고 있는 중국 동영상 공유 소셜 네트워크 서비스이다. 짧은 음악, 립싱크, 댄스, 코미디, 토크쇼, 챌린지와 같은 영상과 3초에서 3분 이내의 짧은 루핑 영상을 제작·공유할 수 있다.

방송통신위원회는 2020년 7월 틱톡에 대해 법정대리인 동의 없이 만 14세 미만 어린이의 개인정보를 수집했다며 과징금 1억8,000만 원을 부과했다. 틱톡은 만 14세 미만 아동에게 서비스를 제공하지 않는다고 고지하면서도 회원 가입 단계에서 이를 차단할 만한 절차를 제대로 마련하지 않은 것으로 나타났다. 틱톡은 법정대리인의 동의 없이 만 14세 미만 아동의 개인정보를 최소 6,000건 이상 수집한 것으로 확인됐다.¹⁰⁾ 또한 방송통신위원회는 틱톡이 가입자들의 개인정보를 해외로 이전할 때 미리 알려야 할 내용을 공개 및 고지하지 않았다고 과태료 600만원을 추가 부과했다. 현행법은 개인정보를 국외로 이전할 때 이용자에게 알리고 동의를 받거나 개인정보 처리 방침을 통해 공개해야 한다. 하지만 틱톡은 미국과 싱가포르 등에 위치한 클라우드 서비스 사업자에 국내 이용자 정보를 넘기면서 이를 제대로 알리지 않았다.

8) 틱톡은 인도에서 전면 금지된 것을 시작으로 미국 연방거래위원회(FTC)는 틱톡에 아동 개인정보 불법수집 혐의로 570만달러(약 63억8000만원)의 과징금을 부과했다. 관련기사: 차현아(2019.2.28.). 美, 틱톡에 63억 과징금 부과 “아동 개인정보 무단 수집 혐의”. 조선일보, http://it.chosun.com/site/data/html_dir/2019/02/28/2019022801045.html(검색일:2021.5.25.).

9) 이견희(2020.7.16.). ‘아동 개인정보 무단 수집’ 틱톡에 역대 과징금. 동아일보, <https://www.donga.com/news/Economy/article/all/20200716/101990789/1>(검색일:2021.5.25.).

10) 연합뉴스(2020.7.15.). 틱톡 국내서도 개인정보 수집·유출…역대 과징금. <https://www.yna.co.kr/view/MYH20200715011700038>(검색일: 2021.5.25.).

2) 개인정보 침해 요인

이 사건은 법적으로 명시되어 있는 만 14세 미만 아동 개인정보 수집시 법정 대리인의 동의를 구해야 한다는 사항을 위반한 명백한 위법 사례이다. 법에 규정되어 있음에도 이러한 일이 발생한 것은 틱톡이 생년월일을 기입하는 절차를 생략하는 ‘법망 우회전략’을 택했기 때문이다. 이는 우회하는 방식을 차단하는 제도 미비, 안전성조치 미비 더불어 대다수 가입한 10대들의 경우(특히 만14세의 경우) 해당 권리가 있었는지 여부는 확인하기 어려우나 가입에 어려움이 없었던 것으로 보아 인식 부족의 문제까지 결합된 사안으로 판단된다.

3) 시사점

짧은 영상을 공유로 인기를 끌고 있는 틱톡은 전 세계 5억명 이상이 이용하고 있으며 주 이용자층은 10대 청소년이다.¹¹⁾ 주 피해층은 해당 연령의 아동들이다. 사실상 아동·청소년 대상의 개인정보 유출이나 프라이버시 침해의 양상은 이처럼 만14세 미만 아동의 가입을 법정대리인 없이 허락하는 양상으로 나타난다. 법에 명시되었음에도 많은 사이트들이 틱톡과 같이 가입시 나이 확인이 불가한 우회로를 설정한다면, 비슷한 양상의 개인정보 침해는 지속적으로 발생될 것으로 보인다.

2. 이루다 사건

1) 사건 개요¹²⁾

각종 혐오 발언¹³⁾과 개인정보 유출 등으로 논란이 됐던 인공지능(AI) 챗봇

11) 차현아(2019.2.28.). 美, 틱톡에 63억 과징금 부과 “아동 개인정보 무단수집 혐의”. 조선일보, http://it.chosun.com/site/data/html_dir/2019/02/28/2019022801045.html(검색일: 2021.5.25.).

12) 강승현(2021.4.28.). ‘60만명 카톡 대화 사용’ AI 이루다, 과징금·과태료 1억330만원. 동아일보, <https://www.donga.com/news/Society/article/all/20210428/106662670/1>(검색일: 2021.5.25.).

‘이루다’를 개발하는 과정에서 회사 측이 60만 명의 카카오톡 대화를 무단으로 사용한 것으로 드러났다. 특히 서비스 개발·운영 과정에서 14세 미만 아동 20여만 명의 개인정보를 보호자 동의 없이 수집한 것으로 나타났다.¹⁴⁾ 개인정보보호위원회는 ‘이루다’ 개발사인 스캐터랩에 대해 과징금 5,550만 원, 과태료 4,780만 원을 각각 부과하고 시정조치를 명령했다. 이는 정부가 AI 기술을 활용한 기업의 무분별한 개인정보 이용을 제재한 첫 사례다.

개인정보보호위원회에 따르면 스캐터랩은 이루다 AI 모델의 개발을 위한 알고리즘 학습 과정에서 동의를 얻지 않은 개인정보를 무단 사용했다. 스캐터랩은 자사의 앱 서비스인 ‘텍스트앳’과 ‘연애의 과학’에서 수집한 카카오톡 대화를 2020년 1월부터 2021년 1월까지 이루다의 AI 개발과 운영에 이용한 것으로 드러났다. 이 과정에서 카카오톡 대화에 포함된 이름, 휴대전화번호, 주소 등의 개인정보 삭제나 암호화 등의 조치를 전혀 하지 않고, 약 60만 명에 달하는 이용자의 카카오톡 대화 문장 94억여 건을 이용했다.

2) 개인정보 침해 요인

앞선 틱톡 사례와 같이 이루다 업체 또한 만 14세 미만 아동들의 법정대리인 동의절차 없이 가입을 허락했으며, 또 아동들의 개인정보를 무분별 수집·이용했다. 이 역시 명백한 법 위반 행위이다. 특히 AI 개발과 운영에 이용하기 위한 개인정보 수집의 범위에 대한 논의를 불러온 사안으로, 이 역시 만 14세 미만 아동의 가입을 위한 법정대리인의 동의 절차를 표준화하거나 이를 감시할 수 있는 제도의 미비, 나아가 개발업체가 서비스 설계에서 아동에 대한 개인정보

13) 이루다는 20세 여대생으로 설정된 AI챗봇이고, 문제의 발단은 일부 이용자들이 이루다를 성적 도구화하고 성희롱하면서 비롯됐다. 이어 대화과정에서 이루다가 동성애, 장애인, 임신부, 흑인 등에 대해 혐오발언을 쏟아내면서 문제가 더욱 커졌다. 개인정보 유출 논란이 대두되면서 사태가 매우 심각해졌다. 전창배(2021.1.20.). 배운 대로 말한 ‘이루다’는 죄가 없다...문제는 AI윤리실증. 한국일보, <https://www.hankookilbo.com/News/Read/A2021011713510002673> (검색일: 2021.5.25.).

14) 연합뉴스(2021.4.28.). 이루다 개발사, 14세 미만 20만명 정보도 보호자 동의없이 수집(종합). <https://www.mk.co.kr/news/society/view/2021/04/411216/>(검색일: 2021.5.25.).

동의, 아동의 법정대리인에 대한 동의 등에 대한 인식이 미비해 발생한 것으로 추측된다.

3) 시사점

아동·청소년 개인정보 침해 사례가 만 14세 미만 아동의 가입 시 법정대리인의 동의 없이 진행할 수 있는 우회 절차를 마련한다는 것이 밝혀졌다. 이를 막을 사전 보호장치가 있는 것은 아니다. 한편으로 만 14세 미만의 아동의 임의가입이 문제되는 이유는 만 14세가 넘는 청소년의 경우 성인과 같은 법적 처우를 받기 때문이다. 한편 청소년이 자신의 개인정보 보호 및 프라이버시 권리가 구체적으로 어떠한 것인지 인지하고, 대처하는 방법 등을 알기 어렵다. 청소년의 경우 자신의 개인정보가 틱톡이나 이루다 사건을 통해 유출되거나 활용됐는지 인지했을 가능성이 낮다.

3. 부모의 개인정보 침해

1) 사건 개요¹⁵⁾

SNS 등을 통해 자녀의 모습이 담긴 사진 및 영상 콘텐츠를 게시하는 부모들이 늘어나고 있는 가운데, 셰어런팅을 둘러싼 논란도 불거지고 있다. 셰어런팅이란 공유를 뜻하는 영어단어 ‘셰어(Share)’와 양육을 뜻하는 ‘페어런팅(Parenting)’의 합성어로, 자녀의 일상을 공유하는 행위를 일컫는다. 이는 성장하는 자녀의 모습을 기록하기 위한 행동이지만 아동 본인의 의사와 상관 없이 게재되는 사진, 영상이 많기 때문에 사생활과 초상권 등 아동의 권리를 침해한다는 비판이 제기되기도 한다. 신생아나 유아의 경우 자신의 모습이 노출되는 과정을 인지할 수 없는데다, 분별력이 충분하지 못하거나 부모의

15) 김가연(2020.11.13.). 키즈유튜브·SNS부터 방송출연까지...‘셰어런팅’, 아동 권리침해일까. 아시아 경제, <https://www.asiae.co.kr/article/2020111213424741844>(검색일: 2021.5.25.).

요구에 따라 동의를 표했을 우려가 있기 때문이다.

특히 이 같은 미디어 노출이 아동을 향한 인신공격, 악성댓글을 비롯해 신원도용, 납치 등 범죄를 초래할 수 있다는 우려도 있다. 또 자녀의 모습이 담긴 콘텐츠로 수익을 창출할 경우 원하지 않는 행동을 강요하거나 압박하는 등 심리적 학대로도 이어질 수 있다는 지적도 이어진다. 이렇다 보니 일부 시민들 사이에서는 “일종의 학대로 볼 수 있다”는 목소리가 높아지고 있다.

셰어런팅을 둘러싼 논란은 해외에서도 불거졌다. 할리우드 배우 기네스 펠트로스는 지난해 자신의 인스타그램에 딸 애플 마틴과 함께 찍은 사진을 올렸다가 논란에 휩싸였다. 마틴은 댓글을 통해 “애기했었잖아요. 내 동의 없이 것도 올리면 안 돼요”라고 항의했다. 당시 누리꾼들은 “자녀도 사생활을 보호받을 권리가 있다”, “엄마라고 해서 모든 권리를 갖는 것은 아니다”라며 비판했다.

미국 워싱턴대와 미시건대 연구진이 2016년 발표한 ‘가족의 기술이용 규칙에 대한 부모와 자식의 관점’ 보고서에 따르면, 40개주 249쌍의 부모·자녀를 조사한 결과 “무단으로 자녀에 대한 정보를 온라인에 공유해서는 안 된다”고 답한 자녀의 응답이 부모보다 두 배 높은 것으로 파악됐다. 2016년 10월 캐나다 앨버타주 캘거리시에 사는 대런 랜달(당시 13세)은 자신의 부모에게 합의금 35만 캐나다 달러(약 3억 원)를 요구하는 소송을 냈다. 부모가 자신을 당황스럽게 하는 유아시절 사진을 약 10년 넘게 페이스북에 올렸다는 것이 이유였다. 캐나다 국영방송 CBC에 출연한 그는 “(부모가 올린 사진들은) 나의 이미지를 심각하게 훼손했다”며 사진을 과도하게 공유하는 부모들로부터 아기와 앞으로 태어날 아기가 법적으로 스스로 보호할 수 있도록 하기 위해 부모를 고소했다고 밝혔다.¹⁶⁾

16) 박순봉(2019.2.6). [SNS와 초상권③]내 아이 사진 올리는데 뭐 어때? 초상권, 해외선 다르다. 경향신문. http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201902061026001(검색일 : 2021.5.25.).

2) 개인정보 침해 요인

부모를 통한 아동·청소년의 개인정보 침해는 명백한 부모의 인식 부재에서 나타나는 아동·청소년 자녀에 대한 개인정보 및 프라이버시 침해 사례이다. 아동·청소년 역시 불편함을 느끼지만 정확히 자신의 어떤 권리가 어떻게 침해 받고 어떻게 대처해야하는지 모르고 있을 가능성이 매우 높다. 특히 부모가 가해자일 경우에는 더욱 그러할 것으로 예측된다.

3) 시사점

오늘날 부모도 아동도 디지털 사용이 활발해지고, 디지털은 일상의 한 축이 되었다. 자녀 수가 적고, 부모 역시 디지털과 친숙한 세대여서 많은 영상·사진 등의 기록을 남기면서 태어나는 순간부터 자녀의 ‘동의(할 수)없는’ 계사가 무차별하게 이루어지고 있다. 이 행위로 인해 아동 자신은 의도하지 않았음에도 성장 후 지우고 싶은 이른바 ‘흑역사’가 전자지문처럼 디지털 상에 영구히 남아, 아동은 고통을 겪게 된다. 또한 무심코 전체 공개로 올린 자녀 사진은 2차 범죄로 이어진다. 정서가 발달되기 전에 인신공격, 악성댓글에 노출되어 가치관과 인성 형성에 악영향을 끼칠 수 있으며, 신원도용이나 sns에 무수히 드러난 개인정보들로 인해 납치 등의 범죄를 당할 우려도 있다.

이렇듯 아동·청소년의 개인정보 및 프라이버시는 부모도 침해할 수 있고, 부모의 행동은 자녀의 인식 형성에 직접적인 영향을 미치기 때문에 아동·청소년에 대한 개인정보보호 교육은 부모와 연계해 기획되어야 한다.

4. 온라인 그루밍

1) 사건 개요¹⁷⁾

고등학교 2학년인 10대 여성은 랜덤 채팅애플리케이션(앱)을 통해 한 성인

17) 박다혜(2019.6.24.) “엄마한테 말하지마” 청소년 노리는 마수 ‘온라인 그루밍’. 한겨레, <https://www.hani.co.kr/arti/society/women/899011.html>(검색일: 2021.5.25.).

남성을 알게 됐다. 남성은 친절했고, 이름, 다니는 학교 등에 관한 대화를 나눴다. 학생은 남성이 자신을 “예뻐해준다”고 생각했고, 갈수록 대화 수위는 높아졌다. 남성은 성기 사진을 보내며 학생은 “얼굴이 나오는 섹시한 사진을 보내달라”고 요구했다. 학생은 관계가 단절될까봐 거절하기가 어려웠다. 남성은 만남을 요구했고, 학생은 응하려 했다. 다행히 학생 어머니가 대화기록을 발견, 경찰에 신고해 실제 만남까지 이어지진 않았다.

이는 2020년 한국사이버성폭력대응센터가 상담한 ‘온라인 그루밍’ 사례이다. ‘온라인 그루밍’은 성적인 관계를 맺기 위해 이메일, 채팅방, 게임, 데이트·채팅앱, SNS 등을 이용하는 범죄 수법으로 아동·청소년 성범죄의 전조로 꼽힌다. 칭찬을 하며 친밀감을 쌓고 비밀 등을 털어놔 의존하게 만드는 것이 핵심이다. 이후 성적인 이미지와 영상을 요구하고, 나중엔 성매매의 협박 도구로 이용한다.

사실상 성범죄의 통로가 되는 플랫폼 규제의 필요성도 제기된다. 채팅앱 이용자가 최소한의 신상정보를 필수로 입력하게 하고 범죄 사실이 드러나면 사업자가 이를 수사기관에 제공할 수 있게 하거나 플랫폼 사업자를 아동·청소년 대상 성범죄 신고의무자에 포함하는 등 조치가 필요하다는 얘기다. 실제로 실명·성인 인증 절차를 거치지 않아도 되는 채팅앱이 상당히 많다. 대화 내용 갈무리가 어렵거나 채팅방을 나가는 순간 내용이 삭제되는 기능도 신고나 수사를 어렵게 한다. 조진경 대표는 “2016년 앱 7개를 ‘성매매 알선’ 혐의로 신고했는데 증거 불충분으로 무혐의가 나왔다. 항고, 재항고, 재정신청까지 했는데 전부 기각됐다”며 “현재 방송통신심의위원회의 사이트 폐쇄 조치는 음란물에만 초점이 맞춰져 있어 온라인상의 성매매 알선 등에 대해선 신고나 규제가 제대로 이뤄지지 않는다”고 지적했다.

2) 개인정보 침해 요인

일차적으로 데이트앱이나 기타 채팅앱은 가입인증절차가 앞선 사례들과 같이 생략되는 경우가 많다. 이 역시 범망에 걸리지 않았을 뿐 만 14세 미만

아동의 가입이 어렵지 않은 데이트 또는 채팅앱이 상당할 것으로 예측된다. 가입인증절차의 생략은 앱이 범죄의 온상이 되는 것을 촉발하는데 예컨대 상대 남성이 아무런 정보를 기입하지 않아도 미성년자에게 대화결기가 가능하다. 이는 청소년에게 성범죄의 예방을 위해서라도 반드시 프라이버시 교육이 필요하다는 것을 보여준다. 이 역시 인식의 부족, 제도의 미비 요인에 해당된다.

3) 시사점

청소년 대상 성범죄의 3분의 1이 온라인 랜덤 채팅방이나 청소년의 SNS DM(다이렉트 메시지)을 통해 발생한다. SNS에서 학생의 신상정보를 얻은 범죄자는 이를 갖고 협박하거나(집 주소를 안다고 협박하거나¹⁸⁾), 성향을 분석해 치밀하게 접근 후, 결과적으로는 성범죄로 이어지는 등의 각종 범죄의 통로가 되고 있다. 개인정보 침해가 2차 범죄를 위한 도구로 사용되는 것이다.

현행 개인정보보호법은 상업적인지에 구별 없이, 아동 대상 콘텐츠인지에 상관없이 '모든 개인정보처리자'에게 적용된다. 넓은 대상에게 규제 의무가 부과 되면 보호 범위가 넓어지는 면도 있으나, 실제 법 집행에서 규제를 회피하는 자가 증가하고 실효성을 거두기 어려울 수 있다는 지적이 있다(이희정, 2021). 이러한 지적대로 실제 많은 사이트들이 만 14세 미만의 가입과정 절차를 여기는 경우가 많다. 개인정보 유출에서 끝나지 않고 범죄로 이어지는 상황, 특히 디지털 성범죄로 사안이 확대되는 경우를 막고, 올바른 SNS 사용 방법에 대해 지속적으로 교육할 필요성이 제기되는 사안이다.

오늘날 범죄는 과거와는 다른 양상을 띤다. 디지털을 통해 개인정보를 습득한 뒤 이를 무기로 피해자에게 가해를 하고, 더 나아가 온라인에 범죄행위 영상이 남거나 해당 영상이나 사진으로 성매매를 강요하는 등의 범죄로 이어지기도 한다. 전파가능성이 큰 만큼 잔혹성도 크다. 이를 사전에 차단하기 위해 랜덤 채팅앱의 가입인증절차 생략 등의 위법행위를 바로잡고, 아동·청소년의 개인정보보호 및

18) 김도현(2021.2.10.). "집 주소 알고 있어"... SNS서 만난 초등생 성폭행 30대 검거. 뉴시스, https://newsis.com/view/?id=NISX20210210_0001336133(검색일: 2021.5.25.).

프라이버시 보호에 정부가 앞장설 필요가 있다. 또한 청소년 역시 범죄에 노출되지 않도록 개인정보 보호 방법을 인지해야 한다. 이는 교육을 통해 가능한데, 1회성 교육이 아닌 지속적이고 사전예방 교육이 필요하다.

5. 불법도박사이트 인증 및 매매

1) 사건 개요¹⁹⁾

일명 ‘꿀알바’라고 불리는 불법도박사이트 인증 매매가 성행하면서 청소년들이 용돈벌이를 위해 개인정보를 파는 불법에 노출되고 있다. 해당 아르바이트는 SNS 메시지를 통해 휴대폰 번호나 SNS계정을 알려준 뒤 인증번호를 제공하면 돈이 입금되는 방식으로, 수집된 계정과 연락처는 불법도박사이트 홍보에 이용된다. 실시간 스포츠 스코어 중계사이트 인증번호는 건당 3천 원에서 8천 원, SNS계정은 5천 원에서 1만 원까지 거래된다. 복잡한 절차 없이 간단하게 돈을 벌 수 있어 청소년들 사이에서 유행처럼 번졌고, 동급생이나 후배를 협박·갈취하는 학교폭력까지 이어지고 있다.

그뿐만 아니라 ‘무료나눔’이라는 이름으로 불특정 다수를 유인하거나 길거리에서 행인에게 전화기를 빌린 뒤 인증번호를 받기도 하는 것으로 알려졌다. 청소년들이 무방비로 개인정보 유출 범죄와 학교폭력에 노출되자 경기지역 내 한 교육지원청은 지난해 관내 학교에 ‘불법인증을 위한 번호요구 예방 안내문’을 발송하기도 했다.

2) 개인정보 침해 요인

이들 도박업체가 원하는 건 일부 사이트 홍보 계정을 만드는 데 필요한 휴대폰 번호와 가입인증번호이다. 이 사실을 자세히 알 리 없는 청소년들은 돈을 받고

19) 양효원(2021.2.1.) “꿀알바 보장”...청소년 개인정보 노리는 불법도박사이트 알바 성행. 중부일보, <https://www.joongboo.com/news/articleView.html?idxno=363470986>(검색일: 2021.5.25.).

업체에 정보를 넘긴다. 본인도 모르는 새 도박업체 홍보에 일조하는 셈이다²⁰⁾. 이것 역시 피해 학생들의 인식 부족에서 발생한다.

3) 시사점

도박업체들은 라이브스코어 가입에 필요한 정보를 요구한다. 라이브스코어는 회원 수가 100만 명을 웃도는 스포츠 중계, 경기예측 사이트다. 회원 수가 많아 파급력이 크기 때문에 도박업체 사이에서는 최고의 홍보 채널로 꼽힌다. 도박사이트 운영자들은 글을 남기거나 개별 이용자들에게 메시지를 보내며 홍보 활동을 한다. 이러한 활동이 적발돼 계정이 영구정지되면 새 아이디를 만들기 위해 타인의 휴대폰번호와 인증번호를 구하러 나선다. 이 과정에서 청소년은 도박업체에 ‘손쉬운 먹잇감’이 된다. 간편하게 용돈을 벌 수 있다는 생각에 별다른 의심 없이 정보를 넘겨주기 때문이다. 라이브스코어가 본인들에게 친숙한 사이트라는 점도 의심을 내려놓게 한 원인이다.

업체들은 보통 3,500~7,000원의 현금, 문화상품권, 고가의 무선 이어폰을 미끼로 청소년을 유혹한다. 중고거래 사이트에서는 ‘라이브스코어 인증번호 보내면 돈을 주겠다’는 글을 쉽게 찾을 수 있다. 청소년에게 직접 페이스북 메시지를 보내 인증번호를 요구하는 일도 빈번하다. 불법 도박업체에서 청소년의 휴대전화로 개설한 아이디를 통해 음란사진을 합성한 뒤 유포해 도박사이트를 홍보하거나 다른 사람에게 사기를 칠 수 있다. 이때 돈이라는 대가를 받았기 때문에 공범으로 낙인찍힐 우려가 있다.²¹⁾

이렇듯 아동·청소년들은 개인정보의 가치에 대해 가볍게 여긴다. 당장의 작은 금전적 이익을 위해 중요하게 여기지 않는 개인정보를 팔아넘기는 것이다. 본인 것뿐만 아니라 더 많은 돈을 벌기 위해 가족, 친구, 지인 등의 개인정보를 그저

20) 하지수(2020.3.27.). “용돈 벌래”…도박업체에 개인정보 넘기는 청소년들. 조선에듀, http://edu.chosun.com/site/data/html_dir/2020/03/27/2020032702004.html(검색일 : 2021.5.25.).

21) 하지수(2020.3.27.). “용돈 벌래”…도박업체에 개인정보 넘기는 청소년들. 조선에듀

글자를 하나 넘기듯이 파는 것이다. 개인정보와 개인정보보호라는 인식제고의 필요성이 강력하게 대두되는 이유다. 개인정보가 구체적으로 왜 중요한지 정확하게 인지하지 못하기 때문에 경제적 이익에 쉽게 무너진다. 이러한 복잡한 문제를 해결하기 위해 반드시 개인정보보호 및 프라이버시에 대한 교육이 필요하다.

제3절 • 디지털 플랫폼별 개인정보 침해 위험요소 분석

1. 트위터

1) 개요 및 주요 기능

소셜미디어는 사람들이 자신의 생각과 의견, 경험, 관점 등을 서로 공유하고 참여하기 위해 사용하는 개방화된 온라인 톨과 미디어 플랫폼으로, 트위터(Twitter), 인스타그램(Instagram), 페이스북(Facebook) 등이 대표적 서비스다. 소셜네트워크 서비스(Social Network Service)는 이용자들이 자신의 웹페이지를 구축한 뒤 다른 이용자와 연결하거나 콘텐츠를 공유하고 상호작용할 수 있게 하는 서비스로, 소셜미디어의 한 종류이다.

대표적인 소셜네트워크서비스인 트위터는 이용자들이 140자 이내의 짧은 글을 주고받고 공유할 수 있는 플랫폼이다. 트위터는 글을 올리는 사람이나 읽는 사람 모두 빠르게 부담 없이 이용할 수 있는 이용의 편의성, 스마트폰이나 컴퓨터 등으로 쉽게 접근할 수 있는 접근용이성, 팔로우·팔로잉 기능으로 인해 모르는 사람과 인적 네트워크 형성이 가능한 독특한 네트워크 확장방식 등으로 성장해왔다(황혜정, 2009).

트위터 이용은 트윗이라는 짧은 메시지를 작성, 전파하거나 다른 사람의 글을 빠른 속도로 리트윗하면서 이루어진다. 트윗의 재잘거림은 리트윗과 팔로잉으로 엮여지면서 삽시간에 퍼져나가는 위력을 갖는다(김유정, 2013). 트위터는 정보 교환을 통한 사회이슈참여, 상호작용을 바탕으로 한 팔로워 그룹형성, 정보전달의 용이성(심홍진·황유선, 2010) 등이 이용자들의 주요 이용 동인이 되며 주요 기능으로는 팔로잉과 팔로워 관계맺기, 글올리기, 리플받기, 글이 리트윗되는 상호작용 기능 등을 제공한다(Chen, 2011).

2) 아동·청소년 이용 실태

한국갤럽마켓의 조사에 따르면 국내외 주요 소셜네트워크서비스 중 트위터의 연간이용률은 약 14%를 차지하며, 연령대별 트위터 이용률은 10대 남성 25%, 여성 31%로 20대에 이어 전 세대 중 두 번째로 높은 이용률을 보인다(한국갤럽마켓, 2021). 또한 트위터는 Z세대(만 15~24세)의 이용자가 밀레니얼 세대(만 25세~39세)보다 20% 가까이 더 많이 이용하고 있으며, Z세대에서 접속 빈도와 이용 시간이 높은 헤비 유저는 트위터가 타 소셜네트워크서비스보다 압도적으로 많은 것으로 나타났다.

트위터 주 이용자의 접속 빈도를 분석한 결과 60%에 달하는 트위터 주 이용자가 하루 10회 이상 트위터에 접속했으며, 48.5%가 하루 3시간 이상 트위터를 이용하는 것으로 나타났다. 트위터 이용 목적으로는 타인의 게시물이나 콘텐츠를 확인하기 위한 '정보탐색'이 87.8%로 가장 높게 나타났으며, 56.8%의 이용자가 타인의 게시물·콘텐츠에 마음에 들어요를 누르기 위해 트위터를 이용하고 있다고 답했다. 특히 정보검색용으로 트위터를 활용하는 이용자가 인스타그램이나 페이스북에 비해 비교적 높게 나타났다(트위터 대한민국, 2021).

3) 개인정보 침해 요인

(1) 아동·청소년 식별 문제 및 연령별 콘텐츠 구분 미비

GDPR에 따라 유럽연합 회원국은 16세 미만 미성년자가 소셜미디어 등 온라인 서비스를 이용할 경우, 반드시 부모나 보호자의 동의를 받아야 하며 회원국가는 필요할 경우 최대 13세까지 제한 연령을 낮출 수 있다. 이에 따라 트위터는 만 13세 미만 아동의 트위터 이용을 금지하고 있으며, 해당 정책 이전에 가입된 아동의 경우 이용자의 연령을 입력하지 않으면 트위터 계정을 잠근 뒤 부모의 동의 후 잠금을 풀어주는 정책을 취하고 있다.

트위터는 애초 다른 소셜 플랫폼과 달리 개인 프로필에 생년월일 설정 기능이 없었으며, 아동에 대한 별도의 가입 동의를 구별해 받고있지 않았다. 이 때문에

13세 이상 이용자의 콘텐츠를 구분하는 도구가 존재하지 않았고 GDPR 규정 준수를 위해서는 13세 미만 이용자의 계정을 일괄 차단시키는 방법을 택할 수밖에 없었던 것이다. 아동의 서비스 이용을 일괄 제한할 것이 아니라 부모의 동의 절차를 밟아 가입할 수 있는 공식적인 가입 창구를 만들어주고, 연령별로 이용가능한 콘텐츠를 구분해 제공하는 것이 바람직하지만, 이를 위한 노력은 거의 없는 것으로 보인다.

미성년자에 대한 연령별 콘텐츠 구분이 미비한 것도 문제이다. 트위터는 13세 이상만 가입할 수 있지만 별도의 성인인증을 거치지 않기 때문에 미성년자도 손쉽게 음란물 등에 접근할 수 있으며 개인정보 유출·침해 위협에 무분별하게 접근이 가능하다.

(2) 손쉬운 개인정보 노출

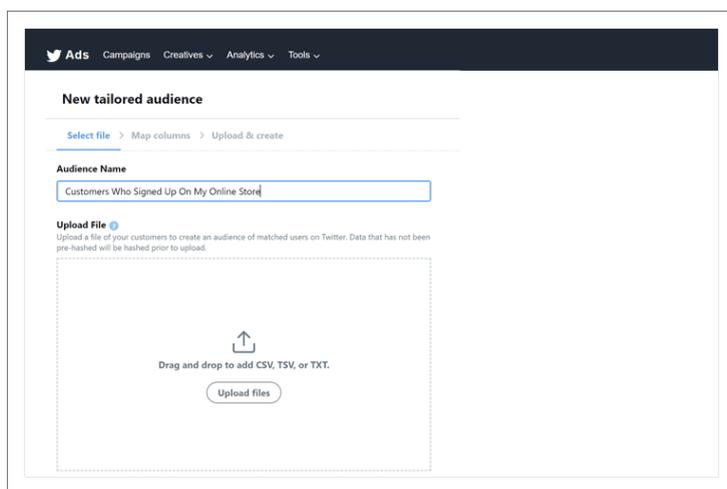
트위터는 일단 글을 올리면 사실상 모두에게 공개되는 형태의 서비스로, 친구부터 범죄의도를 가진 사람까지 모두가 이용자의 활동을 관찰하고 있는 것이나 마찬가지이다.²²⁾ 개인정보 인식이 부족한 아동·청소년은 쉽게 휴대전화번호, 집주소, 주민등록번호 등과 같은 개인정보를 트위터상에 노출할 염려가 있다. 트위터의 리트윗 기능은 내 게시물을 다른 사람의 타임라인에 공유할 수 있도록 해주고, 순식간에 불특정 다수에 의해 온라인에 게시될 수 있도록 만들어주기 때문에 개인정보 노출에 상당히 취약하다. 트위터가 2016년부터 '잊힐 권리'를 수용해 원본 게시물을 삭제하면 리트윗된 사본들도 일괄적으로 지워지는 기능을 업데이트했지만²³⁾, 타인이 리트윗 버튼을 누르지 않고 직접 게시물을 복사해 붙여 퍼나르는 경우 잊힐 권리 행사가 불가능하기 때문에 최초 유의해 개인정보가 포함되지 않도록 게시글을 올리는 것이 중요하다.

22) 권오성(2014.1.29.). SNS에 뒤통수 맞지 않으려면 개인정보 노출 삼가고 공개범위 설정 유념. 한겨레, <https://www.hani.co.kr/arti/economy/it/622098.html>(검색일: 2021.10.1.).

23) 연합뉴스, 김태균(2016.5.15.). 트위터도 '잊힐 권리' 수용... 이용자가 리트윗 일괄 삭제 가능. <https://www.yna.co.kr/view/AKR20160513164400017>(검색일: 2021.10.1.).

(3) 동의 목적 외 맞춤형 광고 사용 문제

트위터는 현재 맞춤형 광고를 위해 몇몇 종류의 데이터를 이용하고 있다. 여기에는 트위터에서 팔로우하는 사람이나 소셜네트워크의 인맥, 트윗 방식, 다른 트윗과의 인터랙션 방식 등이 포함된다. 맞춤형 광고에는 이외에도 이용자의 프로필 정보와 위치, IP 주소 등이 사용된다.²⁴⁾ 이 때문에 동의 목적 외에 트위터가 무단으로 정보를 활용하거나 맞춤형 광고에 활용되면 이용자의 피해가 상당하다.



[그림 3-1] 동의 목적 외 개인정보를 활용한 트위터의 맞춤형 광고 시스템

트위터는 2020년 8월 이용자들이 보안 목적으로 제공한 휴대폰 번호나 이메일 주소를 2013~2019년까지 표적 광고에 활용한 혐의로 미 연방거래위원회(FTC)의 조사를 받은 바 있다.²⁵⁾ 트위터는 실제 이용자 일부가 이중인증(2FA)을 위해 트위터에 제공한 전화번호와 이메일 주소를 표적형 광고에 활용했음을 인정했으며

24) ITWORLD(2014. 11. 27.). 트위터, 설치한 앱 정보 수집... 맞춤 콘텐츠 제공에 활용, <https://www.itworld.co.kr/news/90730>(검색일: 2021.10.01.).

25) 이영섭(2020.8.4.). 트위터, '개인정보 오용' 미정부 조사받아... "3천억원 물 수도". 연합뉴스, <https://www.yna.co.kr/view/AKR20200804048300009?input=1195m>(검색일: 2021.10.01.).

이는 ‘맞춤형 오디언스 및 파트너 대상 광고 시스템’에서 오류가 발생해 이용자가 보안상의 이유로 제공한 정보를 광고주의 마케팅 리스트를 기반으로 한 타겟 광고에 실수로 사용된 것이라고 밝혔다²⁶⁾. 이에 대한 책임으로 FTC는 트위터에 50억 달러의 벌금을 부과했다.

트위터는 이외에도 iOS 이용자의 위치정보를 무단으로 수집하고 공유한 사례가 있으며²⁷⁾, 어떤 앱을 사용하는지에 따라 일부 사람들 사이에서 프라이버시 관련 우려를 불러일으키고 있다. 트위터의 데이터 수집은 자동으로 작동되기 때문에 이용자가 인식하기 힘들며, 이용자가 이미 ‘광고 추적 제한’이나 ‘관심사 기반의 광고 거절’ 옵션을 활성화한 경우에는 적용되지 않지만 해당 설정을 이용자가 적극적으로 식별해 적용하는 것이 쉽지 않다. 또한 이용자가 관련 기능을 차단 하면, 트위터 서버에 저장된 앱 목록 데이터도 삭제되기 때문에 서비스 이용의 편의성도 상당히 떨어진다.

이 때문에 비교적 개인정보가 어떻게 수집되고 어디에 활용되는지에 대한 이해가 높지 않고 개인정보자기결정권 행사에 큰 관심이 없는 아동·청소년은 개인정보의 맞춤형 광고 활용의 희생양이 되기 쉬어, 이를 방지할 수 있는 서비스 설계나 관련 안내와 교육이 필요하다.

2. 페이스북

1) 개요 및 주요 기능

페이스북은 2004년 하버드대 학생들을 대상으로 시작되었지만 점차 이용 참여 범위가 확대되어 현재 가장 활발하게 이용되고 있는 온라인 네트워킹 커뮤니티 서비스이다. 페이스북이 지향하는 것은 “all friends in one-place solution”으로 이름, 비밀번호, 이메일 주소만 입력하면 자동으로 친구를 찾아주고 바로

26) <https://help.twitter.com/en/information-and-ads>

27) 문가용(2019.5.15.). 트위터, iOS 이용자의 위치 정보 실수로 수집하고 공유, 보안뉴스, <https://www.boannews.com/media/view.asp?id=79524>(검색일: 2021.10.01.).

그들과 대화할 수 있다. 가입자들은 프로필을 작성해 자신의 정보와 근황이나 활동 상황을 알릴 수 있으며 담벼락에는 다른 이용자들이 포스트한 메시지가 제공 되고 다른 사이트, 동영상, 사진들에 접속할 수 있는 링크들이 첨부될 수 있다 (김유정, 2013). 관심있는 게시글에 ‘좋아요’를 누르거나 조회를 하는 등 반응한다면 페이스북은 이를 기억하고 추적해 관심있는 광고와 관련 게시글을 추천해준다.

2) 아동·청소년 이용 실태

2020년 조사에 따르면 소셜네트워크서비스 이용자 중 초등학생은 63%, 중학생은 71.9%, 고등학생은 72.4%가 페이스북을 이용했으며, 중·고등학생의 35%가 인스턴트메신저 기능도 활용하고 있었다(통계청·여성가족부, 2021). 한국 껄럽의 조사에 따르면 10대 중 최근 1년 내 페이스북을 이용해본 적 있다고 응답한 비율은 남성 63%, 여성 64%에 달했다(한국껄럽마켓, 2021). 대학내일 20대 연구소가 만 15~34세 남녀 SNS 이용자 900명을 대상으로 진행한 설문조사에서도 한국 10대는 페이스북(73.6%)을 가장 많이 사용했다. 이는 카카오톡 대신 페이스북 메신저(페메)를 주로 사용하는 10대 성향이 반영된 것으로 분석된다²⁸⁾.

3) 개인정보 침해 요인

(1) 상세한 개인정보 입력 요구에 따른 민감정보 노출

페이스북은 경력, 학력, 거주지, 연락처, 가족 및 결혼/연애 상태, 중요 이벤트, 정치적 관심사 등 상세한 개인정보를 입력하도록 안내하고 있으며, 이에 따라 관심사나 광고를 맞춤형으로 추천해주는 알고리즘을 택하고 있다. 이러한 정보는 민감한 내용을 다수 포함하고 있으며 아동·청소년이 해당 정보를 입력하는 것에 아무런 제약을 두고있지 않기에 성범죄, 납치, 거짓소문 등에 쉽게 악용될 소지가 있다.

28) 장준하(2020.10.29.). 한국 10대가 선호하는 페이스북, 미국에서는 꼴찌?, Ai타임스, <http://www.aitime.com/news/articleView.html?idxno=133204>(검색일: 2021.10.01.).

(2) 허위정보로 인한 아동 가입 가능성

「개인정보 보호법」 제39조의3 제4항에 의하면 정보통신서비스 제공자는 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 법정대리인의 동의를 받아야 하고, 대통령령으로 정하는 바에 따라 법정대리인이 동의했는지를 확인해야 한다. 그러나 실제로 아동이 페이스북을 이용하는 경우, 정확한 연령 확인이나 법정대리인의 동의 절차를 통해 회원가입이 이루어지지 않고, 허위로 이메일 주소나 생년월일을 입력해 쉽게 회원에 가입할 수 있다는 문제가 있다.

만 14세 미만 아동이 페이스북 계정을 생성했다면 이에 대한 신고를 받고 검토 후 계정을 삭제하고 있으며, 주기적으로 필터링을 하고 있으나 별도의 휴대폰 인증 등 검증작업이 없는 점은 얼마든지 아동이 연령 검증체계를 우회해 가입할 수 있는 여지를 열어둔 셈이 된다.

(3) 당사자 동의 없는 개인정보 제공

페이스북에서 해킹으로 인해 5억 3,300만명의 개인정보가 유출된 사건 등 해킹에 의한 개인정보 유출 우려도 있지만²⁹⁾, 서비스의 특성과 관련해 가장 문제가 되는 부분은 당사자 동의 없는 개인정보 제공 문제이다.



[그림 3-2] 페이스북의 개인정보 제공 구조
(출처: 중앙일보, 2020)

29) BBC NEWS(2021.4.7.). 페이스북: 개인정보 유출...혹시 내 번호도?, <https://www.bbc.com/korean/international-56646722>(검색일: 2021.10.01.).

개인정보보호위원회는 2020년 11월 25일 페이스북을 수사기관에 고발하고 총 67억 6,600만원의 과징금을 부과했는데 이는 페이스북이 2012년 5월부터 2018년 6월까지 약 6년간 당사자 동의를 받지 않고 다른 사업자에게 개인정보를 제공했기 때문이다. 국내 페이스북 이용자 1,800만명 중 최소 330만명 이상의 개인정보가 유출된 것으로 조사됐다. 제공된 개인정보 항목은 학력·경력, 출신지, 가족 및 결혼·연애상태, 관심사 등이 포함되었다. 정보유출은 이용자가 페이스북 로그인을 통해 다른 사업자의 서비스를 이용할 때 이용자의 '페이스북 친구' 개인 정보도 제3자 개발자에게 함께 제공되는 식으로 이루어졌으며, 개인정보가 제공된 사업자 중에는 약 5,000만명의 개인정보를 영국의 데이터 분석 업체 케임브리지 애널리티카에 제공해 2016년 미국 대선에 사용하도록 한 '글로벌 사이언스 리서치(Global Science Research·GSR)'도 포함됐다³⁰⁾.

이처럼 페이스북 내에서 다양한 형식으로 존재하는 앱들은 제3자에게 개인 선호도와 민감정보가 포함된 개인정보를 제공하는 경우가 많으며, 관련 권리는 물론 개인정보 제3자 공유로 인한 위험성을 이해하고 있지 못한 아동·청소년에게 이와 같은 개인정보 위협 환경은 치명적이라고 볼 수 있다.

(4) 소셜로그인을 통한 제3자 제공 동의 사각지대 발생

페이스북과 같은 SNS 서비스들은 대부분 모바일 앱이나 인터넷 웹사이트에 별도 회원가입 없이 간편하게 접속할 수 있는 '소셜로그인' 기능을 제공하고 있다. 소셜로그인 기능은 페이스북의 API³¹⁾, SDK³²⁾ 비즈니스 방식을 통해 제공하는 대표적인 기능이기도 하다. 페이스북은 SDK를 통해 페이스북을 통한 소셜로그인

30) 허정원(2020.11.25.). '330만명 학력·연애상태 개인정보 유출' 페이스북 형사고발...과징금 67억, 중앙일보, <https://www.joongang.co.kr/article/23929859#home> (검색일: 2021.9.2.)

31) API(Application Programming Interface)란 응용 프로그램에서 사용할 수 있도록 운영체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스로, 앱·서비스 등을 제공하는 매개체와 다른 앱·서비스를 사용하는 매개체의 통신을 위한 다리역할을 수행한다.

32) SDK(Software Development Kit)이란 프로그래머들을 위해 제공되는 개발도구로, 소프트웨어 기술자가 사용해 특정한 소프트웨어 꾸러미, 소프트웨어 프레임워크, 하드웨어 플랫폼, 컴퓨터 시스템, 운영체제 등을 위한 응용 프로그램 등을 만들 수 있게 해주는 개발 도구의 집합이다.

등의 API 기능을 앱 개발자 등에게 제공 중이다. 페이스북 SDK의 경우 페이스북이 지원하는 개발자 그룹 전세계 76개국에 27만명에 달할 정도로 많은 개발자들이 이용 중이다³³⁾.

페이스북은 타사 데이터를 확보하기 위해 API를 활용한 소셜로그인 연동 기능을 적극 제공하며 해당 기능을 통해 확보한 타사 데이터를 정밀한 타겟 광고 실시를 위해 이용한다. 이 때문에 소셜로그인 기능은 간편한 가입을 유도하나 이용자 동의 절차의 지나친 간소화를 통해 정보주체가 본인의 정보를 제3자에게 과도하게 넘기도록 유도한다는 점에서 상당한 주의가 필요하다. 특히 페이스북은 소셜로그인을 통해 제3자에게 최대 70개에 달하는 개인정보를 제공하면서도 제공되는 개인정보의 구체적인 항목을 이용자에게 밝히지 않고 있었으며, 소셜로그인 사용업체의 개인정보 이용 목적이나 보유 기간 등에 대한 고지하지 않아 방송통신위원회의 제도 개선을 요청받기도 했다³⁴⁾.

문제는 소셜로그인 기능이 아동의 서비스플랫폼 가입 시 동의 사각지대를 발생시킨다는 것이다. 소셜로그인 기능은 별도 회원가입 절차없이 개인정보의 제3자 동의만으로 회원가입이 가능한 부가서비스들이 많아 아동 개인정보에 대한 법정대리인의 동의절차를 우회할 수 있는 창구로 활용된다. 소셜로그인을 통해 제3자에게 제공되는 아동개인정보의 현황을 법정대리인이 알 수 없어 법에서 부여한 법정대리인의 권리행사가 불가능해지는 상황이다.

만 14세 미만의 아동이 소셜로그인을 통해 서비스플랫폼에 가입하는 경우, 기존 플랫폼 로그인시 보호자 본인인증뿐만 아니라 새로운 서비스플랫폼 회원가입 시 보호자 본인인증을 추가로 수행해야 한다(총 2번의 보호자 본인인증). 그러나 소셜로그인 기능을 제공하는 서비스플랫폼 중 해당 절차를 지키고 있는 곳은 거의 없다.

33) 김정현·송화연 (2020. 7. 15). “페북 때문에 다른 ‘앱’ 못쓴다고?”…킬 스위치 둔갑한 ‘페이스북 SDK’”, 뉴스1, <https://www.news1.kr/articles/?3994618>(검색일: 2021.9.2.)

34) 노동균(2018. 8. 31.). 페이스북이 ‘소셜 로그인’ 기능으로 제3자에 넘긴 개인정보 항목 70개 달해, IT Chosun, http://it.chosun.com/site/data/html_dir/2018/08/31/2018083101674.html (검색일: 2021.9.2.)

3. 인스타그램

1) 개요 및 주요 기능

인스타그램(Instagram)은 즉석에서 사진을 볼 수 있게 한 방식의 카메라인 ‘인스턴트 카메라(Instant Camera)’와 전보를 보낸다는 의미의 ‘텔레그램(Telegram)’을 합쳐 만든 이름으로, 사진을 손쉽게 다른 사람들에게 전송한다는 뜻을 가진 소셜미디어 플랫폼으로, 사진 및 동영상을 공유할 수 있다. 이용자는 사진과 짧은 동영상을 업로드하고, 다른 이용자의 피드를 팔로잉할 수 있으며, 위치 이름으로 이미지를 지오태그(geotag)할 수 있다. 또한, 이용자들의 인스타그램 계정을 소셜 네트워킹 서비스와 연동할 수 있으며, 다른 이용자와 피드를 주고받을 수 있다. 이용자는 자신의 인스타그램 계정을 다른 SNS 사이트에 연결해 업로드한 사진을 해당 사이트에 공유할 수 있다.

인스타그램의 가장 큰 특징은 부연설명을 덧붙일 수 있는 해시태그 기능이다. 해시태그는 이용자들이 서로를 찾는 것을 도우며 비슷한 흥미를 가진 사람들을 끌어들이도록 유도한다. 직접 팔로우하지 않더라도 해시태그 검색기능을 통해 간접적으로 관련 정보와 관심사를 찾아볼 수 있다. 해시태그는 이러한 특징을 활용해 광고 알고리즘 생성에 활용되며 이용자에게 더 흥미롭고 매력적인 맞춤형 광고를 제공하는데 일조한다.

2) 아동·청소년 이용 실태

2020년 조사에 따르면 인스타그램은 소셜네트워크서비스 이용자 중 초등학교생 45.4%, 중학생 63.2%, 고등학생 70%가 이용하고 있었으며(통계청·여성가족부, 2021), 한국갤럽 조사에 따르면 10대 중 최근 1년 내 인스타그램을 이용해본 적 있다고 응답한 비율은 남성 56%, 여성 63%에 달했다(한국갤럽마켓, 2021).

3) 개인정보 침해 요인

(1) 아동·청소년 사진의 무단 도용 및 유출

인스타그램은 자신의 이미지를 자유롭게 공유하는 것을 기본 기능으로 하며, 인스타그램에 사진을 게시한 이용자는 공유를 동의하는 것으로 본다는 정보처리 안내를 하고 있다. 즉, 인스타그램의 개인정보 취급방침은 “회원님은 서비스를 사용함으로써 인스타그램이 이용자가 사진, 댓글, 기타 내용 등 게시물(이용자 콘텐츠)을 서비스에 게시하고 이용자에게 게시물을 공개적으로 공유할 수 있는 플랫폼을 제공한다는 점을 이해하고 이에 동의하게 됩니다. 즉 서비스를 통해 전체 공개하신 이용자 콘텐츠를 다른 이용자가 이 개인정보취급방침의 약관 및 인스타그램의 이용약관에 따라 검색, 조회, 사용, 공유할 수 있습니다”라고 규정하고 있다.

아동·청소년이 별다른 생각 없이 올린 사진들은 누군가가 캡처해 소장하거나 재가공해 다양한 플랫폼에 공유될 수 있다. 이러한 사진들은 성인이 되어서 삭제하려해도 통제가 불가능하다. 또한 개인의 사진을 도용해 가짜 SNS 계정을 만든 뒤 허위사실을 유포하는 경우도 있다³⁵⁾. 인스타그램에 포스팅해도 괜찮은 사진 일지, 그 게시물이 시간이 지나서 본인에게 어떠한 영향을 줄지에 대해 알고 고민하는 과정이 필요한데 아동·청소년은 이 과정을 거치지 않고 서비스를 이용할 위험이 있다.

(2) 위치정보 및 생체정보의 무분별한 수집

인스타그램에서 사진을 올릴 때는 위치정보를 설정할 수 있다. 위치정보 자체는 별 문제가 없어보이지만 누군가가 인스타그램에 올라온 위치정보를 통해 그 사람의 행동이나 활동 패턴을 찾아내는 것은 간단하다. 아동·청소년을 타깃으로 온라인

35) 신재현(2021.4.16.). 사진도용 SNS에 ‘자작 음란글’…셀프 캡처후 일베 유포, 뉴시스, https://mobile.newsis.com/view.html?ar_id=NISX20210415_0001408191#_enliple(검색일: 2021.10.01.).

그루밍, 납치, 피싱 등을 하려는 행위자는 공개된 계정의 다양한 정보들을 통해 범죄를 구상하는데 이중 위치정보는 가장 다양하고 위험한 정보를 제공한다. 특히 위치태그가 포함된 사진은 대상자가 최근 방문한 장소를 기반으로 정교한 피싱용 정보를 만들어낼 수 있어 더욱 위험하다³⁶⁾.

인스타그램을 인수한 페이스북에는 사진을 올리면 자동으로 사진 속 얼굴을 인식하고 누구인지 알려주는 기능도 존재한다. ‘눈과 눈 사이의 거리’등을 숫자로 환산해 얼굴 정보를 저장하고 분석하며 이를 통해 전 세계 이용자들의 생체정보를 수집하는 것이다. 이러한 생체정보 수집에는 별도의 동의 절차를 보장해야 하지만 신규 가입자에 대해 해당 정보 수집은 자동으로 동의하는 것으로 간주하고, 별도의 거부 없이 지속적으로 정보가 수집되도록 해 문제가 될 바 있다.³⁷⁾

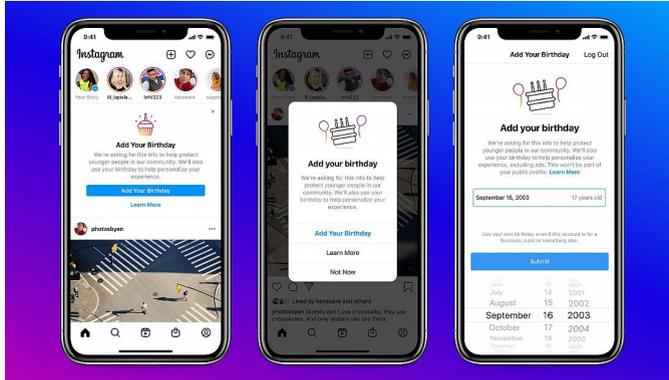
(3) 이용자 활동 추적과 한정된 통제 방법

인스타그램은 이용자가 많이 조회한 게시글과 광고, 해시태그 등을 기반으로 이용자가 좋아할 것으로 추측되는 것을 분석하고 이를 통해 이용자 맞춤형 광고를 제공한다. 활동 추적의 범위는 인스타그램 플랫폼 내부뿐만 아니라 인스타그램이 소유하지 않은 웹사이트와 서버까지 확장되며 이렇게 분석된 정보는 광고주와 앱 개발자, 소셜 플러그인, API 및 SDK 비즈니스 툴을 통해 제3자에게 전송된다. 최근 인스타그램이 18세 미만 이용자에 대해 그들의 관심사 또는 다른 플랫폼에서의 활동 기록을 기반으로 한 타겟팅 광고를 제한하고, 타겟팅 광고 시 활용 가능한 18세 미만 아동·청소년의 개인정보를 연령, 성별, 장소에 한정된 것도 이러한 위험에 아동·청소년이 노출되는 것을 최소화하기 위함이다. 그러나 이러한 조치에도 연령, 성별, 장소에 따른 이용자 활동 추적은 여전히 우려된다. 또한 인스타그램이 아동·청소년 보호정책 적용을 위해 모든 이용자들로부터 ‘생년월일’

36) 구분권(2021.6.13.). SNS ‘사진 태그’ ‘위치정보’는 해커의 ‘먹이’. 한겨레, <https://www.hani.co.kr/arti/science/future/999171.html>(검색일: 2021.10.01.).

37) 윤상문(2021.8.25.). 내 얼굴 알아본 페이스북…알고 보니 20만 명 정보 ‘무단 수집’, MBC, https://imnews.imbc.com/replay/2021/nwdesk/article/6296165_34936.html(검색일: 2021.10.01.).

정보를 수집하고 인공지능(AI)을 활용해 이용자가 생년월일을 허위로 기재하지 않았는지 탐지하고 이용자의 실제 연령을 확인할 방법을 모색 중이라고 하지만,³⁸⁾ 검증의 정확성이 보장되지 않으며 연령별로 차별화된 서비스가 가능할지는 지켜 봐야 할 것이다.



[그림 3-3] 인스타그램의 생년월일 정보 수집 화면

더불어 활동 추적에 대한 온오프 기능과 통제 기능을 충분히 제공해야 하나 인스타그램은 관심사와 업로드한 이용자 정보 수정 기능, 광고선호도 재설정 기능, 광고대상 선정 기능 등을 제공할 뿐이다.

4. 유튜브

1) 개요 및 주요 기능

유튜브는 2005년 시작한 웹서비스로 이용자가 제작한 콘텐츠를 웹플랫폼에 직접 게시하는 형식으로 이용자가 직접 콘텐츠를 생산·공유하는 서비스를 정착 시켰다. 유튜브는 이용자는 직접 콘텐츠를 만들고 확산하는 과정을 통해 적극적

38) Tom Bateman(2021.9.1.). Tell Instagram your birthday or get blocked as app introduces age verification. BIZTECH NEWS, <https://www.euronews.com/next/2021/08/31/tell-instagram-your-birthday-or-get-blocked-as-app-introduces-age-verification>(검색일: 2021.10.01.).

참여가 가능하다.

유튜브는 이용자가 게시한 동영상 조회수에 따른 광고수익을 배분한다. 이에 인기 동영상 업로더는 유튜브 크리에이터로 지칭되면서 수익을 창출할 수 있는 독립적 제작주체로 활동하게 된다. 또한 유튜브는 동영상 콘텐츠에 담겨있는 정보를 빅데이터로 관리하며 빅데이터를 이용해 콘텐츠 큐레이션 서비스를 제공할 수 있다(Rotman et al., 2012). 유튜브 크리에이터의 영향력과 빅데이터 기반의 큐레이션 서비스 제공을 통해 동영상 콘텐츠는 이용자들에게 빠르게 확산될 수 있고 이는 유해 콘텐츠나 부정적 이슈에 대한 영상도 사후에 차단이 어려울 만큼 빠르게 확산될 수 있다는 부작용을 초래하기도 한다(최홍규·고범석, 2021).

2) 아동·청소년 이용 실태

2017년 이후 유튜브는 국내에서 앱 이용시간 1위를 차지하는 등 이용시간은 증가하고 있으며, 전 세계 대상 동영상 스트리밍 앱의 이용시간에서도 유튜브가 최상위권을 차지한다. 특히 가장 높은 순위는 유튜브 키즈(1위)가 차지하고 있다(Apptopia & Braze, 2020). 즉 유튜브는 전 세계에서 가장 많은 사람이 가장 많은 시간 이용하는, 이용자에게 영향력이 큰 동영상 서비스로 자리잡고 있는데, 특히 유아·어린이 등 저연령층에 대한 영향력이 갈수록 더 커지고 있다(최홍규·고범석, 2021). 2020년 세이브더칠드런의 아동·청소년 디지털 플랫폼 경험조사에 따르면 아동·청소년이 가장 많이 이용하는 디지털 플랫폼은 유튜브가 63%로 가장 많았으며, 유튜브 이용자의 약 50%가 하루 평균 3시간 이상 서비스를 이용하는 것으로 조사됐다. 또한 유튜브를 이용하는 아동·청소년의 21.6%가 해킹, 스팸 등 개인정보 노출과 관련한 부정적 경험을 했고, 부정적 영향력이 있다고 답한 비율도 44.8%나 되었다(세이브더칠드런, 2020).

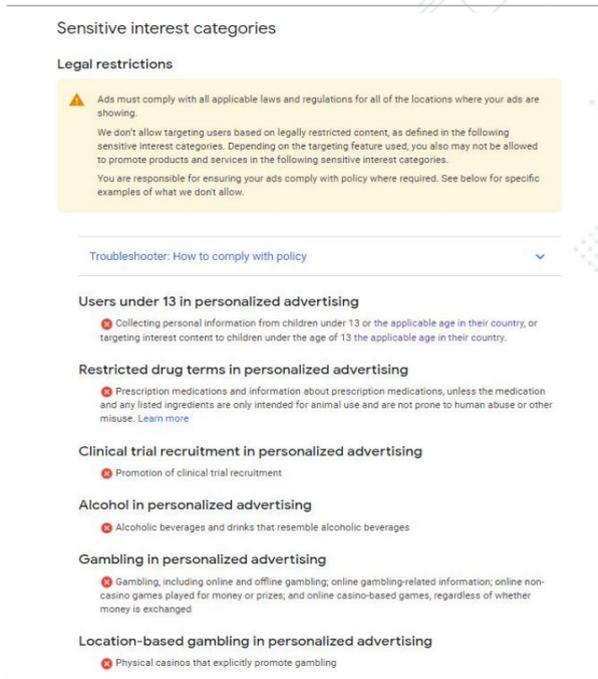
3) 개인정보 침해 요인

(1) 아동 대상 타깃형 광고

미국의 아동 온라인 개인정보보호법(COPPA)은 13세 미만의 아동을 보호하고, 보호 대상에는 아동으로부터 수집한 부모·친구 등 타인의 개인정보를 포함한다. COPPA의 대표적 범집행 사례로, FTC는 유튜브가 아동의 개인정보를 불법으로 수집해 부모 고지나 동의 없이 유튜브의 아동 대상 채널을 시청하는 아동으로부터 쿠키 및 모바일 광고 식별자를 수집하고 이를 맞춤형 광고 등에 이용한 행위에 대해 1억 7,000만달러의 벌금형을 부과했다. 이는 부모 승낙 없이 13세 미만 이용자들의 정보를 수집하거나 이들을 표적으로 삼은 활동을 못하도록 한 COPPA가 마련된 이후 부과된 최대 규모의 벌금이다. 이처럼 추천 알고리즘 기반의 동영상 플랫폼은 더 많은 조회수와 시청시간 확보를 위해 개인의 성향을 추적하고 학습하는데, 아동의 개인정보보호를 위해 아동의 특별 보호를 고려한 설계가 필요하다.

이에 유튜브는 최근 18세 미만 이용자 위치정보 이력 조회와 맞춤형 광고를 적용하지 않기로 발표하고 관련 이용약관을 변경했다. 18세 미만의 연령, 성별, 관심사를 기반으로 한 맞춤형 광고 타깃팅을 중단하고, 구글 설정에 '위치정보' 기능을 꺼두고 활성화 기능까지 삭제했다³⁹⁾.

39) 유동현(2021.8.12.). 특특 “얼굴·목소리 수집합니다”...유튜브는?, 헤럴드경제, <http://m.heraldbiz.com/view.php?ud=20210812000813>(검색일: 2021.10.01.).



[그림 3-4] 유튜브에서 맞춤형광고가 금지된 항목

(2) 아동이 출현하는 콘텐츠에 대한 보호

유튜브가 아동용 콘텐츠에 개인 맞춤형광고를 제한하면서, 아동이 이용하는 콘텐츠에 대해서는 보호가 확대됐으나, 아동이 직접 콘텐츠 제작에 참여하거나 출현해 콘텐츠 생산에 기여하는 경우에 대한 보호도 필요하다. 아동의 경우 개인정보를 스스로 관리하는 방법을 인지하지 못할 확률이 크고, 아동이 직접 콘텐츠를 제작하는 크리에이터가 될 경우 콘텐츠 제작 과정에서 자신에 대한 정보나 영상을 무분별하게 공유할 위험이 있다. 이 경우 아동의 개인정보가 흥미의 소재가 되거나 범죄의 도구가 되므로 각별한 주의가 필요하다(최흥규·고범석, 2021).

이에 유튜브는 ‘아동이 출연하는 콘텐츠를 위한 권장사항’을 배포하고 있는데, 이에 따르면 미성년자를 동영상에 등장시키기 전에 부모나 법적 보호자의 동의를

받아야 한다고 명시하고 있으며, 미성년자의 동영상 참여는 자발적이어야 한다고 강조하고 있다. 구체적으로 유튜브는 만 13~17세 이하 이용자가 동영상 업로드 시 기본 설정을 '비공개(Private videos)'로 한다. 유튜브는 동영상 공개 설정을 공개, 비공개, 일부공개 등으로 구분하고 있으며, 비공개나 일부공개의 경우 검색으로는 해당 영상을 찾을 수 없다(일부공개는 링크로만 접근 가능). 이러한 기능을 통해 청소년은 자신의 모습이나 개인정보가 나온 동영상을 실수로 업로드하는 일을 줄일 수 있으며, 이로 인해 발생할 수 있는 정보 노출이나 부적절한 접근 등을 예방할 수 있다⁴⁰⁾.

5. 틱톡

1) 개요 및 주요 기능

동영상 플랫폼인 틱톡(TikTok)은 2016년 설립된 세계 최초의 숏폼 모바일 비디오 플랫폼으로 한국에는 2017년 11월 출시됐다. 사람들의 영상시청 시간은 늘고 있으나, 한 영상에 체류하는 시간은 짧아지면서 이 패턴을 이용한 숏폼 콘텐츠 플랫폼이 인기를 끌게 됐다.

틱톡은 각종 효과와 편집 프로그램 등이 내장돼, 몇 번의 터치만으로도 간편하게 영상을 제작할 수 있고, 인플루언서를 중심으로 '챌린지'가 유행하면서 일반인도 영상을 손쉽게 제작해 공유하는 문화가 확산됐다. 시청자와 생산자의 경계가 모호하며 스마트폰에 최적화된 세로형으로 구성되어 있으며, 쉽고 직관적인 영상들, 가볍게 접근할 수 있는 콘텐츠로 이루어져 10대에게 인기를 끌만한 요소를 모두 갖췄다는 평가를 받는다⁴¹⁾.

40) 이상우(2021.8.24.). 구글의 아동·청소년 보호 서비스 정책, 어떤 내용 담겼나. 보안뉴스, <https://www.boannews.com/media/view.asp?idx=100042>(검색일: 2021.10.01.).

41) 전유진(2021.4.24.). 거대 IT 기업 총출동한 '숏폼 비디오 플랫폼'...특징, 정의, 틱톡, 서비스, 우려점, 문화뉴스, <https://m.post.naver.com/viewer/postView.nhn?volumeNo=31340209&memberNo=22517376>(검색일: 2021.10.01.).

2) 아동·청소년 이용 실태

틱톡은 2019년 7월 기준 가입자가 10억 명을 넘어섰으며, 주 이용자(51%)는 24세 이하의 대학생과 청소년으로 분석되며, 주된 이용 동기는 정보/오락추구, 소통, 자기표현이었다(샤오진화·이상기, 2020). 이용자들의 틱톡 이용 빈도는 거의 매일(75%), 주 5-6회(16.7%), 주 3-4회(8.3%), 주 1-2회(0%)로 접근성이 높고 콘텐츠의 시간이 짧은 만큼 매일 접근하는 이용자가 많았으며 약 12.3%의 이용자가 해킹·스팸 등 개인정보 노출 경험이 있었다(세이브더칠드런, 2020).

미국은 틱톡이 아동 온라인 개인정보보호법(COPPA)에서 규정하는 13세 미만 자녀의 부모를 대상으로 개인정보 수집 동의를 받도록 하는 조항을 위반했다고 보고 2019년 2월 570만 달러의 벌금을 부과했으며, 틱톡은 아동·청소년의 틱톡 이용을 적극적으로 규제할 것에 합의했다. 틱톡은 16세와 17세 가입자의 다이렉트 메시징(DM) 설정의 기본값을 ‘받지 않는다(No One)’로 설정했으며 이미지나 영상을 메시지로 보낼 수 없도록 제한하는 기능과 16세 미만 계정에 대한 DM을 막는 기능도 업데이트했다. 또한 10대가 공유옵션을 이해할 수 있도록 16세 미만 이용자가 첫 영상을 게시할 때 팝업이 나타나도록 추가했다. 이 팝업에는 영상을 볼 수 있는 사람을 선택하라는 내용이 담긴다. 13~15세 이용자의 계정은 게시물 공개 기본값이 ‘비공개’로 설정되며, 다른 개인 계정은 ‘모두’ 설정이 꺼져 있게 되고, 오후 9시부터 푸시 알림을 받을 수 없다. 더불어 다른 이용자는 16세 미만 계정의 콘텐츠를 다운로드할 수 없다⁴²⁾.

3) 개인정보 침해 요인

(1) 아동·청소년 목소리, 얼굴 정보의 유출 및 악용 문제

틱톡은 2021년 6월 2일 갱신한 ‘미국 거주자용’과 ‘미국과 유럽을 제외한 지역 거주자용’ 개인정보 처리방침에 오디오의 성질(the nature of the audio)과

42) 심두보(2021.8.12.). 애플·구글 이어 틱톡도 청소년 보호장치 마련한다. PAXNetnews, <https://paxnetnews.com/articles/77418>(검색일: 2021.10.01.).

얼굴 이미지(faceprints)를 수집할 수 있다고 명시했다. 틱톡은 ‘자동으로 수집하는 이미지와 소리 정보’ 항목과 ‘당사가 이용하는 개인정보 유형’ 중 ‘이용자 콘텐츠와 행동정보’ 항목에 이러한 내용을 포함했다. 틱톡의 한국어 개인정보 처리방침에도 “당사(틱톡)는 이용자 콘텐츠의 일부로 등장하는 물체와 풍경, 이미지 내 얼굴과 신체의 특징 및 속성의 존재와 위치, 오디오의 성질 및 귀하의 이용자 콘텐츠에서 들려주는 단어 텍스트를 식별하는 이미지와 오디오에 대한 정보를 수집할 수 있다”라고 적시했다⁴³⁾.

개인정보보호위원회가 발간한 「생체정보 보호 가이드라인」(개인정보보호위원회, 2021)에 따르면 ‘생체정보’란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 ①개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 ②특정 개인을 인증·식별하거나 ③개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 ④일정한 기술적 수단을 통해 처리되는 정보를 말한다. 생체정보는 특정 개인을 인증·식별하기 위한 목적으로 처리되는 ‘생체인식정보’와 인증·식별 목적이 아닌, 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 처리되는 일반적인 생체정보로 구성된다. ‘일반적인 생체정보’는 해당 정보가 수집, 전송, 보관 등 처리되는 과정에서 유출되거나 오·남용되는 경우에 예상되는 개인정보 침해 위험성을 고려해 생체인식정보에 준하는 보호 조치 이행이 권장되며, ‘생체인식정보’는 가이드라인에서 제시하는 보호 원칙⁴⁴⁾과 처리 단계별 생체인식정보 보호조치⁴⁵⁾의

43) 이재영(2021.6.5.). 틱톡 “얼굴·목소리 수집할 수 있다”...개인정보 처리방침 개정. 연합뉴스, <https://www.yna.co.kr/view/AKR20210605045300009?input=1195m>(검색일: 2021.10.01.).

44) ①비례성: 생체인식정보 처리에 따른 편익에 비해 개인정보 침해 위험성이 크지 않은지를 고려해 생체인식정보의 활용여부를 판단한다. ②적법성: 생체인식정보의 수집·이용·제공 등 생체정보 처리의 근거는 적법·명확해야 한다. ③목적제한: 생체인식정보를 정보주체에게 동의 받은 인증·식별 이외의 목적으로 무단으로 활용해서는 안된다. ④투명성: 생체인식정보 보호에 관한 사항을 정보주체에게 알기 쉽게 공개한다. ⑤안전성: 생체인식정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전하게 처리하고 관리한다. ⑥통제권보장: 정보주체가 자신의 생체인식정보를 스스로 통제할 수 있는 수단을 제공한다.

45) ①생체인식정보의 필요성 검토 ②개인정보보호 중심 설계(PbD) 적용 ③대체 수단 마련 ④개인정보 영향평가 수행 ⑤적법하게 생체인식정보 수집 ⑥위·변조된 생체인식정보에 대한 대책 마련 ⑦생체인식정보 수집·입력 시 전송구간 보호 ⑧동의받은 목적의 범위 내 이용 ⑨생체인식정보 통제 수단 제공 ⑩생체인식정보 수집·입력 단말에서 처리 ⑪생체인식정보 저장 시 암호화 ⑫생체인식

적용이 권장된다. 그러나 틱톡의 개인정보 처리방침에서 적시하고 있는 생체정보들이 명확히 어떤 정보를 의미하고, 어떤 목적으로 활용되는지를 제대로 설명하고 있지 않기 때문에 해당 정보가 일반적인 생체정보인지, 생체인식정보인지 파악하기 힘들며 그에 따른 최소한의 권장 조치들을 이행하고 있는지도 확인하기 힘들다. 틱톡은 수집한 생체정보를 다른 용도가 아닌 콘텐츠 맞춤추천, 광고추천, 영상 효과나 인구학적 분류, 식별작업을 위해서라고 설명하고 있는데⁴⁶⁾, 모호한 용어설명과 포괄적인 수집 목적은 해당 정보가 얼마나 광범위하게 활용될지에 대해 전혀 예측할 수 없게 만들고 있다.

(2) 데이터의 불법적인 국외이전

방송통신위원회는 2020년 7월 틱톡이 국내이용자 개인정보를 국외 이전하며 이용자에게 알리지 않은 행위를 위반했다고 판단하고 다른 위반행위와 함께 1억 8,000만 원의 과징금 및 과태료 600만원, 시정조치를 부과했다. 틱톡은 알리바바 클라우드, 패스틀리(fastly), 엣지캐스트(Edgecast), 파이어베이스(firebase) 등 4개 클라우드 서비스 업체를 이용하고 있었고 국내 이용자의 개인정보 전체는 중국의 클라우드 서비스인 알리바바 클라우드에 위탁하고 있었으나 이에 대해 이용자에게 고지하지 않았다. 정보가 보관된 서버는 미국과 싱가포르에 위치해 있었다.

미국에서도 관련 소송이 진행된 바 있다. 2019년 미 캘리포니아 북부 지방법원에 제기된 소송에서 틱톡은 GPS정보, IP주소, SIM카드 기반 위치정보, 단말기정보, 주소록, 문자메시지 등 동영상 서비스와 무관한 정보까지 과도하게 수집하면서도, 이용자 데이터를 방대한 규모로 중국에 있는 본사에 이전해 전송한다고 주장했다 (한국인터넷진흥원, 2020).

정보의 파기 ⑬원본정보 보관 시 분리보관 ⑭개인정보 공개 ⑮개인정보취급자에 대한 관리·감독
46) 전다운(2021.8.9.). 틱톡 '생체인식 정보 수집' 논란...삭제가 답?. TECHPLUS, <https://tech-plus.co.kr/60556>(검색일: 2021.10.01.).

6. 인공지능 스피커

1) 개요 및 주요 기능

인공지능 스피커는 주로 음성인식을 통해 하나 이상의 단어의 도움을 받아 상호작용 동작을 제공하는 가상비서가 내장된 음성명령 기기이다(김선기, 2020). 인공지능 스피커 시장의 성장 추세는 매우 빠른 편이다. 글로벌 시장조사업체 카운터포인트리서치는 인공지능 스마트 스피커의 글로벌 출하량은 2025년까지 연평균 21%의 성장률을 보일 것으로 내다봤다. 글로벌 시장조사업체 리서치앤마켓도 2017년 25억달러 규모였던 인공지능 스피커 기반의 AI개인비서(IVA) 시장이 2023년 252억달러에 이를 것으로 전망했다.⁴⁷⁾

많은 사람들이 인공지능 스피커의 음성인식 기술을 통해 정보검색, 날씨 확인, 음식 주문, 택시 호출, 음악과 라디오 청취 등 다양한 서비스를 이용하고 있다. 인공지능 스피커는 사람의 음성을 인지하기 위해 항상 대기상황이어야하고, 대기 상황 중에 명령어를 인식하고 작동을 시작한다. 음성데이터와 단어들을 이용자의 명령과 매칭시켜 구현해나가는 것이다. 많은 데이터 학습을 통해 명령 수행의 정확도를 높인다. 이때 항상 음성을 듣고 있는 대기모드는 이용자가 자신의 프라이버시를 무의식적으로(Unconsciously) 끊임없이(Seamless) 지속적으로(Continuously) 디바이스에 기록 및 저장하게되는 프라이버시 로깅 현상으로 이어지게 되고(심홍진, 2018), 로깅데이터는 개인의 은밀한 사생활에 대한 모든 정보가 저장될 수 있기에 프라이버시 침해에 대한 우려와 개인정보 침해 위험이 상당히 높은 상황이다.

2) 아동·청소년 이용 실태

인공지능 스피커의 인식능력이 점점 진화하고 콘텐츠도 강화되면서 점차 인공

47) 박설민(2021.10.12.). AI스피커 급증하는데...내 개인정보는 괜찮을까. 시사위크, <http://www.sisaweek.com/news/articleView.html?idxno=147890>(검색일: 2021.10.21.).

지능 스피커가 가전의 일부로 자리를 잡아가고 있고, 남녀노소 누구나 쉽게 활용 가능한 기기로 자리잡고 있다. 특히 아동을 겨냥한 교육용 콘텐츠를 탑재하면서 아동 교육용 인공지능 스피커의 출시도 증가하고 있다.

네이버는 인공지능 플랫폼 클로바(Clova)가 탑재된 스피커에 어린이용 콘텐츠 5,700건을 추가해 인기 동요, 인기 캐릭터 동화 등을 제공하고 있으며⁴⁸⁾, 초중고 모바일 알림장 서비스와 제휴해 부모와 아이가 인공지능 스피커를 통해 알림장을 확인할 수 있는 서비스를 시작했다. 여러 명의 자녀를 등록해 아이별로 알림장 정보를 확인할 수 있고, 알림장 알람기능으로 매일 특정시간에 알림장을 음성으로 전달받는 것도 가능하다.

또한 인공지능 스피커는 아동의 언어발달을 촉진하고, 부모-자녀간 상호작용을 돕는 보조수단으로서 역할을 할 수 있으며⁴⁹⁾, 스마트홈 기기와 IoT 연결을 통해 집안에서 이루어질 수 있는 다양한 활동과 음성을 통해 상호작용이 가능하다. 이는 아동·청소년에 대한 교육과 생활 전반에 인공지능 스피커의 영향력이 확대될 수 있음을 의미하며, 동시에 기기와 사람이 상호작용하는 모든 순간의 내용들이 데이터로 기록되고 보관되며 유출될 수 있다는 위험성을 내포한다.

3) 개인정보 침해 요인

(1) 아동·청소년 이용자에 대한 구분된 서비스 제공 불가

인공지능 스피커는 이용자가 아동인지 아닌지 판별하기 어렵기 때문에, 상황에 따라 원치 않는 정보를 기기에 제공할 수 있고, 반대로 인공지능 스피커가 아동에게 부적절한 정보를 전달할 우려가 있다. 인공지능 스피커는 이용자의 기호를 보다 정확하게 수렴하고 서비스 제공자의 이익을 위해 다양한 정보를 사용하게 된다.

48) 김범수(2018.7.13.). 네이버, AI 스피커에 아동용 콘텐츠 5700건 추가...무료 이용, ChosunBiz, https://biz.chosun.com/site/data/html_dir/2018/07/13/2018071301373.html(검색일: 2021.10.01.).

49) 이지원(2021.7.6.). 이화여대 임동선 교수 연구팀, "AI 스피커, 아동 언어발달 보조수단으로 가능성 주목해야", 교수신문, <http://www.kyosu.net/news/articleView.html?idxno=71528>(검색일: 2021.10.01.).

즉, 이용자의 정확한 명령이나 의도 없이 추천이라는 이름으로 서비스 제공자의 이익에 부합하는 방향으로 편향된 정보를 제공하게 될 가능성이 존재한다. 편향된 정보의 제공은 확증편향을 일으키게 되고 서비스 제공자가 부당한 이익을 얻을 수 있게 하는 방법도 제공할 수 있으며(김선기, 2020), 이는 정보를 선별해 수용하는 능력이 부족한 아동·청소년에게 잘못된 인식 형성이나 의사판단을 초래할 수 있다.

또한 인공지능 스피커 업체들이 아동·청소년들의 목소리뿐 아니라 선호하는 콘텐츠, 스피커 사용기록과 같은 민감한 데이터를 어떻게 수집하고 관리하는지 제대로 밝히지 않고 있기 때문에, 성인과 아동·청소년을 구분해 정보를 수집하고 아동·청소년 대상으로는 보다 이용자를 보호할 수 있도록 하는 서비스 설계가 필요하다.

(2) 음성 데이터의 과도한 보관 기간

인공지능 스피커는 이용자의 음성정보를 차곡차곡 모아 데이터화시킨다. 하지만 정보주체인 이용자들은 정작 내 정보가 얼마나 저장되는지에 대해서 인지하지 못하는 경우가 많다. 이용자의 음성정보는 생체정보이며, 개별적인 이용자를 특정해 맞춤형 명령을 인식하면 생체정보 중 더욱 강력한 보호조치가 요구되는 생체인식정보에 해당한다. 수집되는 음성정보 중에는 계좌번호, 주민번호 등의 중요한 정보가 포함될 수 있으며 명령 인식을 위해 음성 데이터가 자연어 처리되는 과정을 거치게 되면 해당 정보는 더욱 위험성이 큰 상태로 보관되게 된다.

〈표 3-1〉 인공지능 스피커별 음성정보 수집·이용 현황

제품 (사업자명)	동의 유무	저장 및 보유		
		서버저장 여부	음성정보 분리보관 여부	보유기간
클로바 (네이버)	회원가입 시 동의	저장	수집 7일 후 음성정보 분리보관 (계정정보 등과 분리)	2년

제품 (사업자명)	동의 유무	저장 및 보유		
		서버저장 여부	음성정보 분리보관 여부	보유기간
카카오미니 (카카오)	회원가입 시 동의	저장	수집 즉시 음성정보 분리보관 (계정정보 등과 분리)	회원 탈퇴 시
NUGU (SKT)	회원가입 시 동의	저장	수집 14일 후 음성정보 분리보관 (계정정보 등과 분리)	2년
기가지니 (KT)	회원가입 시 동의	저장	수집 2개월 후 음성정보 분리보관 (계정정보 등과 분리)	2년
구글 어시스턴트 (구글)	이용자가 음성저장 활성화 시	미 저장	분리보관 하지 않음	3/18/36개월 중 이용자 선택

아마존과 구글은 이용자의 음성명령 수집 시 계정과 연동해 보관하고 있으며, 이용자가 3개월, 18개월, 36개월 중 보관기간을 선택하도록 하고 있다. KT와 네이버는 인공지능 스피커를 통해 수집된 정보를 2년 동안 저장하고, 카카오의 경우 회원탈퇴 시까지 수집된 정보를 보유한다. 민감정보에 대해서는 비식별 조치를 취해야 하는데, 구글은 비식별 조치를 하지 않으며 카카오만 수집 즉시 비식별 조치를 하고, 네이버와 KT는 비식별 조치까지 다소 시간이 걸린다.

개인정보처리자는 음성정보 보유기간을 활용 목적에 필요한 최소한의 기간으로 정해야 하나, 사업자 스스로가 서비스에 필요한 정보활용 기간을 명확하게 정하지 못하고 있으며 비식별 조치 등 음성정보 보호 강화를 위한 조치들을 취하지 않고 있는 것이 큰 문제이다. 카카오와 네이버 등은 중요 개인정보가 감지되면 자동으로 비식별조치나 삭제되는 기능을 적용 중이지만 모든 사업자가 현재 해당 기술을 적용하는 것은 시기상조이며 탐지율과 정확성에 대해서도 장담할 수 없는 상황이다.

제4절 ● 아동·청소년에 대한 보호와 감시의 딜레마

아동·청소년은 보호의 대상이기도 하지만 권리의 주체이다. 유엔아동권리협약은 아동이 다양한 권리를 가지고 있으며 이에 대한 보장을 인정하고 있는데, 자신에게 영향을 미치는 모든 문제에 대해 자유롭게 의견을 표현할 권리와 사생활에 대한 부당한 간섭으로부터 침해받지 않을 권리 역시 포함한다. 아동은 이 협약을 비롯해 여러 선언과 조약에서 특별한 보호를 받을 권리를 인정받고 있다. 부모 등 법적 보호자들은 아동의 능력과 발달 정도에 맞게 지도하고 감독할 책임과 권리가 있다.

그러나 현실에서는 어떠한 조치가 아동 보호를 위한 조치인지, 아니면 아동 보호를 명분으로 한 통제인지, 혹은 아동이 권리의 주체로서 인정되고 자신의 견해를 표현할 자유를 보장받고 있는지 판단하기 쉽지 않다. 그것이 국가나 학교의 정책이든 보호자의 결정이든 아동 보호를 명분으로 종종 매우 통제적인 정책이나 기술이 도입되거나 정당화된다. 이 과정에서 아동은 주로 보호 대상으로 인식될 뿐, 자신의 의견을 당당하게 표현하거나 자신이 원하지 않는 조치를 거부할 수 있는 권리 주체로 인정받지 못한다. 더 큰 문제는 아동 보호를 명분으로 도입된 정책이나 기술이 오히려 아동의 프라이버시와 개인정보 자기결정권을 침해할 수 있다는 점이다.

한국의 아동 관련 정책 역시 가부장적 시각에서 자유롭지 않다. 아동 보호를 명분으로 아동의 스마트폰 사용을 감시하는 앱의 설치를 의무화하거나 얼굴, 지문, 유전자 등 아동의 생체정보를 수집하는 정책을 도입해왔다. 어떤 정책은 아동이나 보호자에게 선택권을 주거나 충분한 안전조치를 취하고 있지만, 그렇지 않은 정책도 존재한다. 과연 아동 보호를 명분으로 도입된 정책이 진정으로 아동 보호에 효과가 있는지, 오히려 아동의 권리를 침해하는 것은 아닌지, 다른 덜 침해적인 수단은 없는지 숙고해볼 필요가 있다.

4절에서는 아동 보호를 명분으로 도입되었지만, 오히려 아동의 권리 침해

위험이 있는 정책의 사례로 아동 스마트폰 감시법 및 기술과 아동의 생체정보 수집을 중심으로, 국제적인 인권 기준에 비추어 해당 정책의 문제와 개선 방안은 무엇인지 검토해보고자 한다.

1. 아동·청소년의 스마트폰 감시

아동의 보호를 명분으로 아동의 프라이버시를 침해하는 대표적인 사례는 부모에게 아동의 온라인 활동에 대한 모니터링 기능을 제공하는 소위 ‘스마트폰 감시앱’이다. 한국에서는 전기통신사업법 개정을 통해 통신사에 스마트폰 감시앱 설치를 의무화하고 있다.

1) 스마트폰 유해매체물 차단수단 설치 의무화

유해매체물 차단수단, 즉 스마트폰 감시앱 설치를 의무화한 전기통신사업법 개정안은 2014년 10월 국회를 통과해 2015년 4월부터 시행되었다. 19대 국회에서 한선교(의안번호 1900279), 심재철(의안번호 1904490), 김상희(의안번호 1906738) 의원 등이 유사한 취지의 개정안을 발의했다. 개정안의 입법 취지를 보면 “스마트폰이나 태블릿PC 등을 통한 전기통신서비스의 제공이 증가하고 있고, 이에 따라 해외사업자들에 의한 음란·폭력적인 어플리케이션이나 웹 등이 청소년에 무방비로 노출되어 사회문제화”되고 있음을 지적하며, “청소년 유해 어플리케이션 등의 유통을 막아 청소년 보호를 강화”하려는 목적을 강조하고 있다.

이러한 취지로 신설된 전기통신사업법 제32조의7은 제1항에서 이동통신사가 청소년과 계약을 체결할 때 청소년유해매체물 및 음란물을 차단할 수 있는 차단수단을 제공하도록 하고 있으며, 방송통신위원회가 이에 대한 실태를 점검할 수 있도록 했다. 전기통신사업법 시행령 제37조의9에서 구체적인 차단수단 제공 방법 및 절차를 규정하고 있는데, 1항에서 차단수단으로 ‘청소년의 이동통신단말 장치에 청소년유해매체물등을 차단하는 소프트웨어 등’을 제공할 것을 규정하고

있다. 그리고 계약 체결 시 청소년과 법정대리인에게 차단수단의 종류와 내용을 고지하고 차단수단의 설치 여부를 확인하도록 하고 있다. 또한, 계약 체결 후에도 차단수단이 삭제되거나 15일 이상 작동하지 않을 경우에는 매월 법정대리인에게 그 사실을 통지해야 한다.

발의된 법안에 대한 국회 검토보고서를 보면, 아동의 프라이버시권에 미치는 영향에 대해서 심도있는 검토를 하고 있지는 않다⁵⁰⁾. “2011년 8월 방송통신심의 위원회가 안드로이드 오픈마켓 내 음란·선정성 애플리케이션을 조사한 결과 총 18,101개 애플리케이션을 확인했으며, 이는 전년 대비 31.6배 증가한 수치임”과 “이러한 유해 애플리케이션 유통에도 불구하고 청소년의 접근을 제한할 수 있는 성인인증장치 등을 제공하고 있는 것은 총 212건(1.2%)에 불과”하다는 점을 지적하며, 입법의 필요성에 대해 인정하고 있다. 또한, 사업자에게 차단수단의 작동여부를 확인하도록 하고, 차단프로그램이 설치·작동되지 않으면 전기통신 역무의 이용을 제한하도록 한 조항에 대해서는 ““사설(외부) WiFi”를 이용해 청소년유해매체물에 접근할 경우, 전기통신사업자는 청소년유해매체물 차단수단의 정상적 작동여부를 판단할 수 없”기 때문에 사업자에게 과도한 부담이 될 수 있다는 점에 대해서만 우려를 제기하고 있다. 다만 한선교 의원 대표발의안에 대한 검토보고서에서는 “사업자가 이용자의 단말기 이용현황을 지속적으로 모니터링하는 것을 전제로 한다는 점에서 이용자의 사생활 침해 논란이 제기될 수 있음”을 간략히 언급하고 있을 뿐이다.

그러나 시민사회단체들은 이 법안이 청소년의 인권을 침해할 수 있음을 비판해 왔다. 2013년 4월 심재철 의원이 전기통신사업법 개정안을 발의했을 때 청소년 인권단체들은 법안을 비판하는 기자회견을 개최하고, “청소년 보호를 빙자했지만 사실상 청소년을 법률상 성인과 동등한 인격체로 존중하지 않는 발상에서 나온 인권 침해적인 법안”이며, 법안 제정 과정에서 정작 “당사자인 청소년의 목소리는 찾아볼 수 없다”고 비판했다.

50) 전기통신사업법 일부개정법률안 검토보고서 - 심재철의원 대표발의 (2013.4.11), 2013.6.

이 정책에 대해 비판적인 입장을 제시해왔던 사단법인 오픈넷은 2016년 8월 전기통신사업법 제32조의7에 대한 헌법소원을 청구했다. 오픈넷은 이 법을 ‘청소년 스마트폰 감시법’이라 지칭하며 다음과 같이 문제를 지적했다. 첫째, 이통사가 청소년의 스마트폰에 차단수단을 의무적으로 설치하고 청소년이 어떤 정보를 검색하고 접근하는지를 상시 감시하게 해 스마트폰을 사용하는 청소년의 사생활의 비밀과 자유를 침해한다. 둘째, 감시앱 제작업체가 청소년과 법정 대리인의 개인정보를 수집·보관·이용해야하므로 개인정보자기결정권을 침해한다. 셋째, 차단수단에 의해 유해정보뿐만 아니라 합법적이고 교육적인 정보도 차단되어 청소년의 알 권리를 침해한다. 넷째, 차단수단 설치 여부에 대해 청소년 및 법정대리인의 선택권을 인정하지 않아 부모의 자녀교육권을 침해한다. 이와 함께, 법에서는 차단수단의 제공만을 언급하고 있는데, 시행령에서 계약 체결 후 차단수단이 삭제되거나 차단수단이 15일 이상 작동하지 아니할 경우 매월 법정대리인에게 그 사실을 통지하도록 한 것은 청소년의 스마트폰에 대한 365일 24시간 상시적인 감시를 요구하는 것으로 이는 법률이 위임한 한계를 벗어난 것이라고 비판했다.

그러나 헌법재판소는 2020년 11월 26일 이 사안에 대해 합헌결정을 내렸다.⁵¹⁾ 헌법재판소는 이동통신사의 차단수단 제공 의무에 대해 “차단수단을 제공받는 자의 의사에 반해 이를 설치해 줄 의무까지 포함되어 있다고 해석하기는 어렵다”고 판단하면서, 차단수단 제공의무 관련 조항들에 대한 청구는 각하했다. 즉, 이동통신사는 차단수단을 제공할 의무만 있을 뿐 설치할 의무가 있는 것은 아니며, 청소년과 법적대리인들이 차단수단 설치를 거부할 수 있는 선택권이 있다는 본 것이다. 그러나 이와 같은 헌법재판소의 판단은 다소 아쉬움이 있다. 이용자가 궁극적으로는 차단수단을 설치하지 않을 수 있다는 점에서는 헌법재판소의 해석이 맞을 수 있지만, 현실의 이동통신서비스 계약 과정에서 이용자 선택권에 대한 충분한 설명이 이루어지지 않을 수 있다. 차단수단 제공은 전기통신사업법

51) 현재 2020. 11. 26. 2016헌마738

개정 이전부터 가능했다는 점에서 입법 후 사실상 차단수단 설치를 의무로 받아들일 수 있다.

또한, 헌법재판소는 시행령의 통지 조항과 관련해 설치에 동의해 차단수단을 설치한 경우에만 적용된다고 전제하면서 “청소년이 청소년유해매체물등 차단수단을 삭제했는지 여부나 차단수단이 작동하지 않도록 했는지 여부 등은 해당 청소년의 사생활의 비밀과 자유에 속할 뿐 아니라 청소년유해매체물등을 대하는 해당 청소년의 성향이나 태도 등을 유추할 수 있는 자료로서 청소년의 실명 등의 자료와 결합해 개인의 동일성을 식별할 수 있게 하는 개인정보에 해당”하기 때문에 통지조항이 청소년의 사생활의 비밀과 자유 및 개인정보자기결정권을 제한한다는 것을 인정했다. 그럼에도 통지 조항만으로 과잉금지원칙에 반하지 않기 때문에 사생활의 비밀과 자유 및 개인정보자기결정권을 침해하지 않는다고 결론을 내렸다. 이와 관련해 오픈넷은 시중에 유통되는 다양한 감시앱들이 청소년 유해매체물 차단을 넘어 청소년의 인터넷 접속내역, 위치정보 등 민감한 개인 정보를 수집하고 있다는 의견을 제출했지만, 헌법재판소는 이를 받아들이지 않았다. 법에서 의무화한 것은 청소년유해매체물의 차단일 뿐, 감시앱들이 제공하는 다른 기능들은 이 법과 무관하다고 본 것이다. 이 역시 법적으로는 그렇게 해석될 수도 있겠으나 현실적으로 청소년의 스마트폰 서비스 계약시 차단수단 제공을 의무화하는 이 법에 의해 다양한 통제기능을 가진 감시앱의 보급을 촉진했음을 부인할 수 있을지 의문이다.

2) 스마트폰 감시앱의 현황

앞서 살펴본 전기통신사업법 개정안에서는 차단수단 애플리케이션의 기능으로 음란물 및 청소년 유해매체물의 차단만을 규정하고 있지만, 실제 활용되고 있는 소위 ‘스마트폰 감시앱’들은 훨씬 다양한 감시 기능을 제공하고 있다.

한국모바일산업연합회(MOIBA)는 음란물과 청소년 유해정보로부터 청소년을 보호한다는 명분으로 2012년부터 스마트폰 감시앱을 개발해 무료로 제공해왔다. ‘스마트보안관’이라는 이름의 스마트폰 애플리케이션은 2015년 4월 차단수단

설치를 의무화한 전기통신사업법 개정안 통과 후, 더 널리 사용되었다. 그러나 스마트보안관의 보안 취약점이 캐나다 토론토대학 연구소인 시티즌랩에 의해 제기되었는데, 시티즌랩이 스마트보안관에 대한 2차 보고서를 공개한 2015년 11월 1일 스마트보안관의 서비스가 중단됐다. 공지사항에 따르면 “모든 전기통신사업자가 유해정보 차단 SW를 무료로 제공함에 따라 민간 앱 시장의 발전과 중복사업 방지를 위해” 신규 가입자를 받지 않고 기존 가입자는 민간사업자의 서비스로 전환한다고 밝히고 있다. 그러나 한국모바일산업연합회는 이후에도 사이버안심존, 사이버안심드림이라는 이름의 애플리케이션을 배포하고 있다. 사이버안심존은 ‘청소년 스마트폰 중독예방 프로그램’이라고 설명하고 있는데, 학교에서는 스마트폰 중독상담 관리프로그램을, 가정에서는 사이버안심존 앱을 통해 스마트폰 이용행태를 점검하고 이용시간을 관리·지도할 수 있다고 설명하고 있다. 사이버안심존은 다음과 같은 기능을 제공하고 있다.

- 자녀의 스마트폰 이용행태 분석 정보 제공: 자녀와 부모 스마트폰에서 자녀의 스마트폰 일평균 이용시간, 주 이용시간대, 주 이용정보 카테고리 등에 대한 분석정보를 확인하고 중독예방 관리 가능
- 자녀 스마트폰에서 불법·유해 앱 실행 및 인터넷사이트 접속 시 차단: 방송통신심의위원회, 여성가족부 등에서 고시한 불법·청소년유해매체물, MOIBA가 방송통신심의위원회의 Safenet 등급 기준에 따라 자체 수집한 불법·유해 정보 등을 차단 데이터베이스(DB)로 구축해 차단
- 프로그램 및 불법·유해 DB 자동 업데이트(최신 DB 유지): 사이버안심존의 불법·유해 콘텐츠 DB는 자동 업데이트를 통해 최신의 DB 유지
- 사이버안심존 앱 삭제방지: 부모 확인 없이 자녀 임의로 삭제방지를 위해 부모가 삭제를 원하는 경우 고객센터를 통해 확인 후 삭제방법 안내
- 보행 중 잠금 설정 ‘스몸비 예방’: 보행 중 스마트폰 사용으로 인한 사고 예방을 위해 보행 중 잠금 설정 가능
- 자녀 스마트폰 몸캠피싱 방지: 채팅앱을 통한 몸캠피싱 피해 예방을 위해 채팅앱의 카메라와 파일 다운로드 기능 차단

- 자녀 사용시간 설정: 휴대폰 사용시간을 설정해 설정한 시간 내에서 앱을 사용하도록 설정 가능
- 자녀 스마트폰에서 다크웹 접속 시 차단: 다크웹 접속 프로그램을 통해 스마트폰으로 다크웹 접속 시도 시 이를 감지해 차단

스마트안심존이 스마트폰 이용행태를 감시하고 유해정보에 대한 접근을 차단하는 앱이라면, 스마트안심드림은 카카오톡, 문자메시지, 인터넷 검색 내용을 모니터링한다. 온라인 언어폭력으로부터 자녀를 안전하게 보호한다는 명분으로 스마트폰 문자메시지, 메신저 등의 내용을 모니터링해 특정한 문구, 예를 들어 “욕설, 따돌림, 협박 등이 의심되는 문자가 수신되거나 자녀가 인터넷 사이트에서 학교폭력, 자살, 가출 등의 단어를 검색했을 때” 부모에게 고지해준다. 스마트안심드림은 다음과 같은 기능을 가지고 있다고 한다.

- 사이버 언어폭력 의심 문자 감지 알림: 자녀의 스마트폰 문자, 카카오톡 등 메신저로 수신하는 메시지 중에서 욕설, 폭행, 협박, 약취, 모욕, 공갈, 따돌림 등과 관련된 내용이 감지되었을 경우 부모 스마트폰으로 정보 제공
- 자녀 고민 검색어 감지 알림: 자녀가 스마트폰에서 인터넷 사이트 접속 후 학교폭력 관련문제, 가정문제, 성적문제, 이성문제, 교우문제, 외모문제, 일탈, 비행, 자살, 범죄 등과 관련 있는 단어 등을 검색할 경우 고민 단어를 감지해 부모 스마트폰으로 정보 제공
- 학교폭력상담 신고 서비스 지원: 부모님 또는 자녀가 학교폭력과 관련된 문제로 상담을 원하는 경우 스마트안심드림 앱에 있는 상담·신고 메뉴를 통해 전화(117)나 상담채팅(117chat) 등을 이용해 상담할 수 있으며, 이메일을 통한 신고 가능
- 사이버 언어폭력과 고민단어 DB 업데이트: 스마트안심드림의 사이버 언어 폭력 및 고민단어 DB는 최신의 DB 유지
- 스마트안심드림 앱 자녀 임의삭제 방지: 자녀 스마트폰에 설치된 ‘스마트안심드림’앱은 임의삭제가 불가하며, 서비스를 해지하거나 부모가 자녀 앱

삭제를 허용할 경우에만 삭제 가능

이 앱과 별개로 통신사들은 각자 개발한 스마트폰 감시앱을 유무료로 제공하고 있다. SKT의 T청소년 안심팩, KT의 KT자녀폰 안심, LGU+의 U+자녀폰지킴이 등의 앱들은 유해 앱/인터넷 사이트 차단, 앱 이용시간 설정, 부모용 통계 및 모니터링 제공 기능 등을 보유하고 있다.

청소년 유해를 차단앱 현황		
SKT	T청소년 유해차단 (무료) · 유해 앱/인터넷사이트 차단	T청소년 안심팩 (무료) · 유해 앱/인터넷사이트 차단 · 앱 이용시간 설정 · 부모용 통계 및 모니터링 제공
	KT자녀폰 안심프리 (무료) · 유해 앱/인터넷사이트 차단	KT자녀폰 안심 (월2,200원) · 유해 앱/인터넷사이트 차단 · 앱 이용시간 설정 · 부모용 통계 및 모니터링 제공
LGU+	U+자녀폰지킴이 (무료) · 유해 앱/인터넷사이트 차단	U+자녀폰지킴이 (월2,200원) · 유해 앱/인터넷사이트 차단 · 앱 이용시간 설정 · 부모용 통계 및 모니터링 제공
	IOS 사이버가디언 (무료) · 유해 앱/인터넷사이트 차단	

[그림 3-5] 청소년 유해물 차단앱 현황
(출처: 방송통신이용자정보포털 와이즈유저)

이 외에도 패밀리링크, 모바일펜스, 스크린타임, 키즈플레이스 등 다양한 스마트폰 감시앱이 유·무료로 서비스되고 있다. 이 앱들은 유해환경이나 스마트폰 중독 등으로부터 자녀보호를 명분으로 내세우고 있다. 그러나 제공 기능을 보면 자녀의 스마트폰 이용을 세세하게 모니터링하고 특정한 방식으로 통제할 수 있도록 하고 있다. 패밀리링크는 구글이 제공하는 앱으로 5,000만회 이상 다운로드 되었다. 이 앱은 자녀의 앱 사용 시간이 표시되는 활동보고서를 제공하고, 자녀가 구글 플레이스토어에서 다운로드하려는 앱을 부모가 승인하거나 차단할 수 있도록 한다. 인앱 구매를 관리하고 자녀의 기기에서 특정 앱을 숨길 수도 있으며, 교사

추천 앱을 표시해 부모가 자녀 기기에 바로 앱을 추가할 수 있는 기능도 제공하고 있다. 또한 앱이나 기기의 사용시간 제한과 설정을 부모가 할 수 있도록 하며, 부모가 원격으로 기기를 잠가 사용을 중단시킬 수도 있다. 물론 자녀의 위치도 언제든지 확인할 수 있다.

100만회 이상 다운로드된 모바일펜스 역시 마찬가지다. 앱 목록 확인·차단, 기기 및 앱의 사용시간 설정기능 뿐만 아니라 스마트안심존과 같이 유해 웹사이트를 차단하고 위험 문자메시지를 감시하는 기능도 포함하고 있다. 자녀의 위치를 추적하고 부모가 설정한 지역, 예를 들어 학교, 학원, 위험지역 등에 자녀가 들어가거나 이탈할 때 부모에게 알려주는 기능도 있다. 카메라, 와이파이, 블루투스 등 스마트폰의 기능을 부모가 원격으로 통제할 수 있을 뿐만 아니라 특정 번호의 수신과 발신도 제한할 수 있다.

아동 청소년의 보호가 목적이라고 하지만 이는 스마트폰 이용자 입장에서 프라이버시에 대한 심각한 침해가 아닐 수 없다. 당연히 이러한 앱들에 대한 청소년들의 불만은 상당하다. 화가 난 아이들은 앱에 '별점 테러'를 가하고 리뷰를 통해 분노를 표출하고 있다. 그러나 어떤 앱은 "아이들의 별점 하나는 이 앱의 진가를 반증한다"고 오히려 홍보에 활용하고 있다. 급기야 스마트폰 감시법 폐지와 모바일펜스앱 삭제를 요청하는 청와대 청원도 등장했고, 인터넷에서는 이러한 앱 삭제 방법들이 공유되고 있다. 반대로 감시 앱들은 자녀가 앱을 삭제하면 부모에게 알리는 기능을 제공하고 있다.

3) 스마트폰 감시앱의 문제점

스마트폰 감시앱은 자녀 보호를 명분으로 하고 있지만 자녀 프라이버시 침해가 자녀를 진정으로 보호하는 것인지에 대한 의문이 제기된다. 청소년들은 이 앱이 자신을 통제하는 것임을 즉각 느낄 수 있고 '인권 침해'라며 반발하게 된다. 이는 부모와 자녀 사이의 갈등을 초래하며 이 때문에 앱 설치를 망설이는 부모들도 많다. 자녀의 반발이 아니라도 이 같은 자녀의 프라이버시 침해를 동의하지 않는 부모들도 있을 것이다.

2021년 발표된 ‘디지털 환경과 관련된 아동의 권리’에 대한 유엔 일반논평 25호(UN Committee on the Rights of the Child, 2021)에 비추어 볼 때, 아동 스마트폰 감시는 여러 원칙과 권고를 위반하고 있다. 우선 일반논평 25호는 4가지 일반원칙 중 하나로 ‘아동의 견해 존중’을 제시하고 있지만 스마트폰 감시앱 설치 의무화뿐만 아니라 가정의 스마트폰 감시앱 설치 과정에서 아동의 견해는 존중받지 못하고 있다. 75절에서는 “아동에 대한 모든 디지털 감시는 아동의 프라이버시 권리를 존중해야 하며, 아동이 알지 못하는 사이나 매우 어린 아동의 경우 부모나 양육자가 알지 못하는 사이에 일상적으로, 무차별적으로 수행되어서는 안 된다. 상업적 환경, 교육 및 보육 환경에서 그러한 감시에 반대할 권리를 보장하지 않은 채 이루어져서는 안 되며, 원하는 목적을 달성하기 위해 이용할 수 있는, 프라이버시 침해를 최소화할 수 있는 수단을 항상 고려해야 한다”고 지적하고 있다. 그러나 스마트폰 감시앱은 이 앱에 대한 아동들의 별점 테러에서 볼 수 있듯이, 감시에 반대할 아동의 권리를 보장하지 않는다. 또한 설사 스마트폰 감시앱을 통해 달성하고자 하는 목적이 정당하다고 할지라도, 그것이 ‘프라이버시 침해를 최소화할 수 있는 수단’인지는 의문이다.

한편, 부모의 폭력으로부터 아이들이 상담을 받고 싶을 수 있는데, 스마트폰 감시앱은 아이들이 상담을 받기 위해 인터넷을 검색하거나 전화를 하는 등 구조 수단을 차단하는 문제도 야기할 수 있다. 이와 관련해 일반논평(76절)에서도 “안전 목적으로 온라인 활동을 감시하는 기술은 신중하게 구현되지 않으면, 아이들이 전화 상담서비스(helpline)에 접근하거나 민감한 정보를 검색하지 못하게 할 수 있다”고 지적하고 있다.

국가인권위원회도 차단앱에 의한 아동·청소년 기본권 침해를 최소화할 방안을 마련할 것을 방송통신위원회 위원장에게 권고했다(국가인권위원회, 2021). 인권위 아동권리위원회는 “스마트폰을 통해 유통될 수 있는 청소년유해매체물 및 음란 정보로부터 청소년을 보호하는 것은 아동의 올바른 성장을 위해 필요한 부분이고, 또 그러한 목적을 달성하기 위해 이와 관련된 앱의 필요성을 부인하기는 어렵다”고 하면서도 “이러한 앱이 추가로 제공하는 스마트폰 사용 실시간 모니터링, 스마트

폰 사용시간 제한, 해당 아동의 위치추적, 와이파이 차단, 인스턴트 메신저 사용 차단 및 법정대리인에 의한 내용 확인, 문자메세지(SMS) 내용 확인, 특정 번호에 대한 수신·발신차단, QR코드를 이용한 본인확인 제한 등 부가적 기능은 아동의 사생활의 자유 및 개인정보자기결정권 등 과도한 기본권 침해를 발생”시킨다고 판단했다. 또한 “부모 등 법정대리인에게 이러한 문제점을 인식할 수 있도록 충분한 정보를 제공하지 않는다”고 지적했다. 이에 인권위는 방송통신위원회 위원장에게 “△관련 앱이 제한하는 부가기능 실태를 점검하고, 인권침해 요소가 있다고 확인되면 해당 앱을 제공하는 부가통신사업자에 대해 개인정보 침해행위 중지 등 필요한 조치를 취할 것, △청소년유해매체물 및 음란정보 차단수단 제공과 관련해 차단수단 이용에 대한 동의 절차, 정보 보관 및 파기 절차 등의 내용을 포함하는 지침을 제작해 배포·홍보할 것”을 권고했다.

방송통신위원회뿐만 아니라 개인정보보호위원회도 아동·청소년의 권리 보호와 관련해 해야 할 역할이 있다. 스마트폰 감시앱 사업자들에 의한 아동과 보호자의 개인정보 수집·처리가 적법하게 이루어지고 있는지 실태를 조사하고, 필요할 경우 시정조치를 명령할 필요가 있다. 예를 들어, 14세 이상 아동의 경우 법적 대리인이 아니라 정보주체의 동의를 받게 되는데, 이들의 동의가 진정한 동의가 아닐 경우 개인정보보호법 위반이 될 수 있으며, 개인정보처리자가 진정한 동의임을 입증해야 한다. 나아가 개인정보보호법에서 아동·청소년의 개인정보 처리와 관련한 규율을 정비할 필요가 있다. 아동에게 적합한 쉬운 용어로 개인정보 처리와 관련한 고지를 하도록 의무화하고, 아동의 개인정보에 기반한 프로파일링과 자동화된 결정에 대한 규율도 포함할 필요가 있다.

그러나 스마트폰 감시앱의 경우, 부모 등 보호자와 아동의 관계가 개입되기 때문에 쉽지 않은 문제이다. 결국 부모가 스마트폰 감시앱의 문제를 인식하고, 감시앱 설치를 강제할 경우 형성되는 부모와 자녀의 관계가 바람직한 것인지, 오히려 자녀의 발달과 자녀와의 관계에 부정적인 영향을 미치지 않을지 고민할 필요가 있다. 이와 관련해 일반논평(85절)의 지적은 경청할 필요가 있다. 즉, “아이들은 종종 디지털 기회를 받아들이고 실험하며 위험에 직면할 수 있지만”,

아동들은 “특히 부모와 보호자의 접근방식이 징벌적이고 지나치게 제한적이거나 아동의 발전하는 능력에 맞추지 못할 경우에, 디지털 활동에서 더 많은 지원과 격려를 원한다”는 것이다.

2. 아동·청소년의 생체정보 수집

빅데이터, 인공지능, 사물인터넷 등 신기술의 발전으로 정보주체의 권리 침해 위험도 증가하고 있다. 사물을 통해 정보주체도 인식하지 못하는 사이에 개인정보가 수집되고, 생성되는 개인정보의 규모가 극대화되고 있으며, 국경을 넘어 서로 다른 개인정보처리자 사이에 개인정보가 유통되고 있다. 위험을 증가시키는 또 다른 요인은 민감한 생체정보의 수집이 증가한다는 점이다. 아동의 생체정보 역시 예외는 아니다.

1) 아동·청소년 생체정보 수집·처리의 위험성

개인정보보호위원회가 발간한 ‘생체정보 보호 가이드라인’(2021)에 따르면, 생체정보는 “지문, 얼굴, 홍채, 정맥, 음성, 필적 등 ①개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 ②특정 개인을 인증·식별하거나 ③개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 ④일정한 기술적 수단을 통해 처리되는 정보”를 의미한다. 특히 생체정보 중 특정 개인을 인증·식별할 목적으로 처리되는 정보를 ‘생체인식정보’라고 한다. 따라서 생체정보는 생체인식정보와 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 처리되는 ‘일반적인 생체정보’로 구성된다.

생체인식정보는 개인을 인증 또는 식별 목적으로 입력장치 등을 통해 수집·입력되는 ‘생체인식 원본정보’와 이로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 ‘생체인식 특징정보’로 구분된다. 예를 들어, CCTV 영상이나 사진 등으로부터 자동으로 사람을 식별할 수 있는 특징점을 뽑아낼 경우, 원래의 영상이나 사진 속의 얼굴은 원본정보, 특징값을 추출해 나온 정보는

특징정보가 될 것이다. 한편, 생체인식정보가 아니더라도 유전정보, 개인의 건강에 대한 정보 등도 사람의 신체적, 생리적, 행동적 특징을 인식할 수 있는 정보라는 점에서 생체정보라고 할 수 있다.

모든 생체정보가 민감정보는 아니지만, 생체인식정보, 유전정보, 건강관련 정보는 국내 개인정보보호법상 민감정보에 해당한다. 생체인식정보는 원래 민감정보에 포함되어있지 않았는데, 2020년 시행령 개정으로 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 즉 생체인식정보와 ‘인종이나 민족에 관한 정보’가 새롭게 민감정보에 추가되었다. 유전정보 및 건강관련정보는 이전부터 민감정보로 규정되어 있었다. 개인정보보호법 제23조는 민감정보의 처리에 대해 특별히 규정하고 있는데, 민감정보는 정보주체의 ‘별도의 동의’를 받은 경우, 그리고 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에만 처리할 수 있도록 제한하고 있다.

생체정보 특히 생체인식정보와 유전정보의 경우 다음같은 특징이 있다. 우선 모든 사람이 가지고 있는 특징이어야 할 것이다(보편성). 대다수 사람들이 가지고 있는 특징이 아니라면 식별이나 인증을 목적으로 활용되기 힘들 것이다. 둘째는 다른 사람과 구별되는 특정 개인에게 고유한 정보이다(고유성). 셋째 평생 변하지 않는 속성을 가지고 있다(영구성). 지문이 없어지거나 성장하면서 얼굴이 변하는 것과 같은 예외적인 경우가 있지만 대체적으로 영구적 속성을 가지고 있다(이상윤 외, 2016).

생체인식 정보의 활용도가 높아지면서 위험성에 대한 우려도 커지고 있다. 생체인식 정보가 본인 식별이나 인증을 위해 활용되는 것은 유일성, 불변성 때문인데, 바로 그와 같은 특성 때문에 개인의 프라이버시에 미치는 영향도 치명적일 수 있다. 즉, 유출되었을 경우 변경할 수 있는 비밀번호나 신용카드 등과 달리 생체인식 정보는 한번 유출되면 피해를 복구하는 것이 거의 불가능하다. 또한 생체정보로부터 다양한 부가정보들이 추출될 가능성이 크다. 예를 들어, 본인인증을 위한 얼굴정보 처리 과정에서 인증, 건강상태 등 본인인증과는 무관한 정보가 추출돼 이용될 수 있다. 이에 따라 본인이 노출하고 싶지 않은

민감한 정보가 정보주체의 의사와 무관하게 활용될 위험성을 배제할 수 없다. 뿐만 아니라, 생체정보는 정보주체가 인지하지 못하는 사이 수집될 수 있는 위험이 있다. 내가 인식하지 못하는 사이 CCTV에 촬영될 수 있고 내가 마신 컵에서 지문이나 DNA를 채취할 수도 있다(이상윤 외, 2016).

생체인식 기술은 시스템 설계나 기술적 제약이나 오류, 데이터의 의도하지 않은 사용을 통해 프라이버시 침해나 배제 등 아동에게 특별한 위험을 야기할 수 있다. 첫째, 생체인식은 주로 성인에 맞춰서 작동하도록 설계되기 때문에, 아동을 식별하는데 항상 적절하지 않을 수 있다. 예를 들어, 매우 어린 아동의 홍채 인식은 쉽지 않고 얼굴 인식도 특정 연령대에서는 성능이 좋지 않다. 둘째, 아동은 성인보다 취약하기 때문에 사회적, 윤리적으로 추가적인 위험을 야기할 수 있다. 예를 들어, 아동은 자신의 생체인식 정보 제공에 대해 적절한 판단을 내릴 수 있는 지식이 부족할 수 있다. 셋째 아동은 빅데이터 혁명의 중심에 있는데, 이에 따라 아동이 평생에 걸친 위험에 노출될 수 있다. 아동은 일생에 걸쳐 더 많은 데이터가 수집될 것이며, 이 데이터가 그들의 삶에 어떠한 영향을 미칠지 예측하기 힘들다(UNICEF, 2019).

아래에서는 아동의 생체정보 수집·처리와 관련해 논란이 되었던 주요 이슈에 대해 검토해보도록 한다. 이 이슈들은 아동보호 등 공공의 목적을 위해 생체정보를 수집·활용하고자 하지만 다른 한편으로 아동의 기본권을 침해할 우려를 야기하고 있다.

2) CCTV 등을 통한 아동·청소년 영상정보의 처리

아동, 장애인, 환자 등 사회적 약자 보호를 명분으로 사회 각 영역에 CCTV 도입이 확대되고 있다. CCTV는 사회적 약자에 대한 폭력을 억제하거나 사후적으로 가해자를 처벌하는데 도움이 될 수 있지만, 다른 한편으로 대상자에 대한 지속적인 촬영을 통해 일거수일투족을 파악할 수 있게 한다는 점에서 인권 침해 위험이 있다. 또한 CCTV와 같은 포괄적인 모니터링 기기는 다른 개인정보와 달리 동의하는 특정 개인만을 대상으로 하기 힘들다. 그래서 개인정보보호법

에서도 CCTV를 통한 개인정보 처리에 대해서는 일반적인 개인정보와 달리 별도 조항에서 다루고 있다. 개인정보보호법 제25조가 그것인데, 그 규율 대상은 ‘공개된 장소’에 설치된 영상정보처리기에 한정된다. 범죄의 예방 및 수사를 위해 필요한 경우 등 제25조 제1항에서 열거하고 있는 목적에 한해 촬영대상자의 개별적인 동의없이 설치할 수 있다. 다만 공공기관이 설치하는 경우에는 ‘공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴’해야 한다(제25조 3항). 만일 사무실과 같이 공개된 장소가 아닌 경우는 해당 공간에서 촬영되는 당사자들의 동의를 받아야 한다.

공개된 장소에 설치되는 CCTV를 일반적으로 규율하는 개인정보보호법 외에, 특정한 그룹을 대상으로 특정한 장소에 CCTV 설치를 의무화한 것은 어린이집 CCTV가 처음이다. 어린이집 보육교사의 아동학대 사건은 국민들의 공분을 불러일으켰고, 어린이집 CCTV를 의무화해야 한다는 목소리가 높아졌다. 물론 이에 대한 반론도 만만치 않았다. 어린이집 CCTV는 보육교사와 아동의 기본권을 제한한다는 점, CCTV를 설치하더라도 확실적인 의무화가 아니라 공동체 구성원(보육교사 및 보호자 등)의 합의에 기반해야 한다는 점, 아동학대가 일어났던 어린이집 역시 이미 CCTV가 설치되어 있었던 바 CCTV가 근본적인 대안이 될 수 없고 CCTV 설치로 인해 보육교사의 스트레스가 증가하는 등 보육의 질을 오히려 저해할 수 있다는 점, 감시와 처벌 중심이 아니라 보육교사의 자질을 높이기 위한 훈련이나 보육교사의 처우개선 등 근본적인 환경 개선이 중심이 되어야 한다는 점 등의 비판이 제기되었다.

이러한 논란에도 어린이집 CCTV를 의무화한 영유아보육법이 2015년 5월 국회를 통과했다. 영유아보육법 제15조의4는 보호자 전원이 설치에 반대하는 경우가 아닌 한, 어린이집에 CCTV를 의무적으로 설치하도록 했다. 제15조의5는 일정한 경우 보호자, 공공기관, 수사기관 등이 CCTV 영상정보를 열람할 수 있도록 허용했다⁵²⁾. 이후 영유아보육법 해당 조항에 대해 위헌소송이 제기되었지만,

52) 제15조의4(폐쇄회로 텔레비전의 설치 등) ① 어린이집을 설치·운영하는 자는 아동학대 방지 등 영유아의 안전과 어린이집의 보안을 위해 「개인정보 보호법」 및 관련 법령에 따른 폐쇄회로

2017년 12월 28일 헌법재판소는 합헌 결정을 내렸다.⁵³⁾

텔레비전(이하 “폐쇄회로 텔레비전”이라 한다)을 설치·관리해야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2020. 12. 29.>

1. 어린이집을 설치·운영하는 자가 보호자 전원의 동의를 받아 특별자치시장·특별자치도지사·시장·군수·구청장에게 신고한 경우
2. 어린이집을 설치·운영하는 자가 보호자 및 보육교직원 전원의 동의를 받아 「개인정보 보호법」 및 관련 법령에 따른 네트워크 카메라를 설치한 경우
- ② 제1항에 따라 폐쇄회로 텔레비전을 설치·관리하는 자는 영유아 및 보육교직원 등 정보주체의 권리가 침해되지 아니하도록 다음 각 호의 사항을 준수해야 한다.
 1. 아동학대 방지 등 영유아의 안전과 어린이집의 보안을 위해 최소한의 영상정보만을 적법하고 정당하게 수집하고, 목적 외의 용도로 활용하지 아니하도록 할 것
 2. 영유아 및 보육교직원 등 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려해 영상정보를 안전하게 관리할 것
 3. 영유아 및 보육교직원 등 정보주체의 사생활 침해를 최소화하는 방법으로 영상정보를 처리할 것
- ③ 어린이집을 설치·운영하는 자는 폐쇄회로 텔레비전에 기록된 영상정보를 60일 이상 보관해야 한다.
- ④ 제1항에 따른 폐쇄회로 텔레비전의 설치·관리기준 및 동의 또는 신고의 방법·절차·요건, 제3항에 따른 영상정보의 보관기준 및 보관기간 등에 필요한 사항은 보건복지부령으로 정한다.

[본조신설 2015. 5. 18.]

제15조의5(영상정보의 열람금지 등) ① 폐쇄회로 텔레비전을 설치·관리하는 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 제15조의4제1항의 영상정보를 열람하게 해서는 아니 된다.

1. 보호자가 자녀 또는 보호아동의 안전을 확인할 목적으로 열람시기·절차 및 방법 등 보건복지부령으로 정하는 바에 따라 요청하는 경우
2. 「개인정보 보호법」 제2조제6호가목에 따른 공공기관이 제42조 또는 「아동복지법」 제66조 등 법령에서 정하는 영유아의 안전업무 수행을 위해 요청하는 경우
3. 범죄의 수사나 공소의 제기 및 유지, 법원의 재판업무 수행을 위해 필요한 경우
4. 그 밖에 보육관련 안전업무를 수행하는 기관으로서 보건복지부령으로 정하는 자가 업무의 수행을 위해 열람시기·절차 및 방법 등 보건복지부령으로 정하는 바에 따라 요청하는 경우

② 어린이집을 설치·운영하는 자는 다음 각 호의 어느 하나에 해당하는 행위를 해서는 아니 된다.

1. 제15조의4제1항의 설치 목적과 다른 목적으로 폐쇄회로 텔레비전을 임의로 조작하거나 다른 곳을 비추는 행위
2. 녹음기능을 사용하거나 보건복지부령으로 정하는 저장장치 이외의 장치 또는 기기에 영상정보를 저장하는 행위

③ 어린이집을 설치·운영하는 자는 제15조의4제1항의 영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획의 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 해야 한다.

④ 국가 및 지방자치단체는 어린이집에 설치한 폐쇄회로 텔레비전의 설치·관리와 그 영상정보의 열람으로 영유아 및 보육교직원 등 정보주체의 권리가 침해되지 아니하도록 설치·관리 및 열람 실태를 보건복지부령으로 정하는 바에 따라 매년 1회 이상 조사·점검해야 한다.

⑤ 폐쇄회로 텔레비전의 설치·관리와 그 영상정보의 열람에 관해 이 법에서 규정된 것을 제외하고는 「개인정보 보호법」(제25조는 제외한다)을 적용한다.

[본조신설 2015. 5. 18.]

53) 영유아보육법 제15조의4 제1항 제1호 등 위헌확인. 2015헌마994, 2017. 12. 28.

그러나 헌법재판소의 합헌 결정이 CCTV 설치를 무조건 정당화하는 것은 아니다. 헌법재판소의 합헌 결정이 가능했던 이유는 영유아보육법 제정 과정에서 인권침해 논란을 반영해 법에 다양한 안전장치를 포함했기 때문이다. 우선 헌법재판소도 “어린이집에 CCTV 설치로 어린이집 원장을 포함해 보육교사 및 영유아의 신체나 행동이 그대로 CCTV에 촬영·녹화되므로 CCTV 설치 조항은 이들의 사생활의 비밀과 자유를 제한한다”는 점을 인정했다. 그러나 “어린이집의 보육 대상인 영유아는 0세부터 6세 미만으로 일상생활에 보호자의 도움이 필요하고 발육 단계상 의사표현 능력이 부족해 자신이 인지한 상황을 제대로 전달하지 못할 가능성이 크고 어린이집은 보육교사 및 다른 영유아들과만 생활하는 공간이기 때문에 문제가 발생하더라도 적발이 쉽지 않다”는 점, 그리고 다른 대안적인 방법이 존재하지 않는다는 점에서 목적의 정당성과 수단의 적합성이 인정된다고 보았다. 또한 일정하게 보육교사와 아동의 사생활이 제한되기는 하지만, 법에서 이를 최소화할 수 있는 다양한 조치를 마련해두었다고 평가했다. 예를 들어 △인터넷망을 통해 실시간 수신자에게 전송되는 네트워크카메라가 아니라 CCTV로 제한하고 있는 점, △설치목적 이외의 목적으로 CCTV를 임의로 조작하거나 다른 곳을 비추는 행위, 이미 지정된 저장장치 이외의 장치나 기기에 영상정보를 저장하는 행위 등을 절대적으로 금지하고 있는 점, △CCTV 영상 정보의 열람은 보호자가 자녀나 보호아동의 안전을 확인할 목적으로 요청하는 경우 등으로 제한적으로 허용하는 점, △법에서 정한 것을 제외하고 개인정보 보호법 상 규정들을 적용하도록 한 점, △보호자 전원이 반대할 경우 CCTV를 설치하지 않을 가능성을 열어두었기 때문에 무조건 강제되는 것은 아니라는 점 등이다.

따라서 인터넷에 연결된 네트워크카메라를 사용하거나 정보주체가 자신이 입은 피해에 대해 진술을 할 수 있는 사람이라든가 보안조치와 같은 여러 안전조치가 미흡할 경우에는 CCTV 설치의 정당성에 대한 판단이 달라질 수 있음을 고려할 필요가 있다. 예를 들어, 2010년경 서울시가 소위 ‘서울형 어린이집’에 SK브로드밴드가 서비스하는 IPTV시스템을 설치할 것을 종용한 적이 있다. 이는 폐쇄형 CCTV와 달리 실시간으로 일정 시간동안 어린이집의 모습을 생중계했다.

당시에는 관련법도 없었기 때문에 보육교사에게 동의를 받았지만, 사실상 동의가 반강제적이었고 학부모들의 의견은 묻지도 않아 문제가 되었다. 학부모들도 이러한 서비스를 무조건 환영한 것은 아니었는데, 아동이 특정질환을 앓고 있거나 다소 활발한 아이를 둔 경우 자신의 아이가 다른 아이의 부모에게 노출되는 것을 부담스러워하는 경우도 있었다⁵⁴⁾. 더구나 인터넷을 통해 전송되기 때문에 해킹 등 보안 위협도 더욱 컸다. 어린이집에 설치되는 카메라가 이러한 IPTV였다면 CCTV와 마찬가지로 정당화될 수 있었을지 의문이다.

대다수 초·중·고등학교에서도 이미 CCTV가 되었다. 2017년 기준 99% 이상의 학교에 설치가 완료되었다.⁵⁵⁾ 전국 시도교육청에 정보공개를 청구해 받은 자료에 따르면, 2021년 9월 현재 약 29만 대에 가까운 CCTV가 설치되어 있다. 학교 CCTV는 교문, 운동장과 같이 건물밖에 설치된 경우도 있고, 복도나 계단 등 실내에 설치된 경우도 있는데, 극히 일부를 제외하고는 교실에는 설치되어 있지 않다.

학교에 설치된 CCTV의 법적 근거는 개인정보보호법과 초·중등교육법이다. 앞서 언급한 바와 같이 개인정보보호법 제25조는 공개된 장소의 영상정보처리장치 설치를 규율하고 있다. 따라서 운동장 등 학교의 공개된 장소에 설치되는 CCTV는 개인정보보호법 제25조를 적용할 수 있다. 그러나 비공개된 장소에 설치되는 CCTV에는 개인정보보호법 제25조가 적용되지 않는다. 개인정보보호위원회와 한국인터넷진흥원이 발표한 ‘공공기관 영상정보처리기기 설치·운영 가이드라인’(2021)에 따르면, ‘학생, 교사 등 학교관계자만 출입이 가능한 학교 시설(교실, 실험실 등)’은 ‘비공개된 장소’에 해당한다. 따라서 교실에 CCTV를 설치할 경우에는 다른 적법 근거가 있어야 하는데, 초·중등교육법 제30조의8은 학교의 장이 학생 안전을 위해 ‘영상정보처리기기의 설치에 관한 사항’을 시행하도록 하고 있다. 이와 관련해 같은 법 시행령 제57조의2는 학생의 안전대책

54) 한국일보(2010.5.3.). 서울형 어린이집 원아 모습 IPTV 증계 논란 “선생님, 저거 우리 감시하는 카메라죠?”. 진보네트웍센터(2010.5.3.). 서울형 어린이집 IPTV 문제점에 대한 기자회견.

55) 베이비타임스(2017.10.11.). 학교 내 설치 CCTV 제 역할 못하는 ‘무용지물’.

등을 수립할 때 “학생, 학부모 및 교직원의 의견을 듣고 학교운영위원회의 심의 또는 자문을 거치”도록 하고 있을 뿐, 다른 구체적인 안전조치를 규정하고 있지는 않다.

좀더 세부적인 기준으로는 <학교 내 영상정보처리기기 설치·운영 표준 가이드 라인>이 있다. 이 가이드라인은 학교의 장이 영상정보처리기기를 설치할 경우 “영상정보처리기기 설치 운영 계획”을 마련하도록 하고, 책임관 지정, 안내판 설치, 사전의견수렴 관련 사항, 설치 업체 및 기기선정 조건, 필수 감시지역 등의 규정을 포함하고 있다. 또한 영상정보의 수집 제한, 처리 제한, 접근 통제, 열람 요청 절차, 보유 및 삭제 절차 등 안전조치를 규정하고 있다. 이 가이드라인은 최소 30일 이상 영상정보를 보유하도록 권고하고 있는데, 정보공개청구 결과 실제 대다수 학교가 보유기간을 30일로 설정하고 있었지만, 일부 학교의 경우 그보다 최소 7일 혹은 최대 1년까지 보유하는 학교도 있었다. 한편, 동 가이드라인의 별지로 있는 점검표에서는 ‘개인의 사생활을 현저히 침해할 우려가 되는 위치’에 카메라를 설치하지 않도록 하면서, 교실, 화장실, 탈의실, 목욕실 등을 예로 들고 있다. 대다수 학교에서 이 가이드라인에 따라 교실에 CCTV를 설치하지 않고 있는 것으로 보인다.

학교에서 CCTV가 제대로 관리되고 있는지 의문이다. 2017년 국정감사에서 이동섭 의원은 CCTV 관제가 학교 자체적으로 이뤄지고 제대로 관리되지 못하고 있는 것을 지적하며, 통합관제센터와의 연계현황을 파악하고 행안부 및 지자체와 정보공유와 협조체계를 갖출 것을 지적한 바 있다⁵⁶⁾. 2021년 현재 약 10%의 학교 CCTV가 통합관제센터와 연계하는 것으로 파악되었는데, 통합관제센터와 연계는 또 다른 문제를 야기할 수 있다. 통합관제센터 자체가 법적 근거가 없어, 통합관제 자체가 개인정보의 목적 외 제공에 해당할 수 있기 때문이다. 이미 2018년 국가인권위원회는 법률적 근거 없는 CCTV 통합관제센터 운영은 인권 침해라고 지적하며, 행정안전부 장관에게 통합관제센터의 설치 운영, 범죄 수사

56) 베이비타임스(2017.10.11.) 학교 내 설치 CCTV 제 역할 못하는 ‘무용지물’.

목적 등으로 개인영상정보를 이용하거나 제3자에게 제공할 경우의 요건과 절차 등에 관한 법률적 근거를 마련할 것을 권고한 바 있다. 그러나 2021년 현재까지 법적 근거가 마련되지 않고 있으며, 행정안전부 소관의 지침 및 지방자치단체별로 조례, 훈령, 예규 등으로 통합관계센터를 규정하는 것에 그치고 있다(최미경·최정민, 2019).

〈표 3-2〉 학교 CCTV 설치현황 (2021.9 현재)

	설치학교수	설치대수 (실내/실외)	교실설치 여부 및 대수	CCTV 연계대수
강원	647	14,606 (6,673/7,933)	32	254
경기	2,444	51,891 (20,671/31,220)		
경남	1002	22,353		3,529 (522개 학교)
경북	917	20,190 (9,252/10,938)	미설치	6,954
광주	320	6156 (2099/4057)	미설치	620 (155개 학교)
대구	464	13,786	미설치	2,407
대전	298	6,428		600
부산	640	18,080 (10,867/7,213)		3,458 (303개 학교)
서울	1,356	42,385		965
세종	143	5,496	미설치	없음
울산	248	5,062	미설치	미연계
인천	537	17,529 (9,450/8,079)	미설치	583 (70개 학교)
전남	882	14,994 (5,401/9,593)		4000
전북	765	13,244		미연계
제주	191	4,651 (1,393/3,258)	미설치	2,299

	설치학교수	설치대수 (실내/실외)	교실설치 여부 및 대수	CCTV 연계대수
충남	738	18,111	7 (5개 학교)	1227 (175개 학교)
충북	495	14,756 (7,434 / 7,322)		881
계	12,087	289,718	39	27,777

출처: 시도교육청 정보공개청구 답변

※ 빈칸은 자료가 존재하지 않음

3) 아동·청소년의 유전정보 처리

유전정보(genetic information)는 개인이나 가족의 인체유래물질에서 나온 유전적 특징에 대한 정보를 말한다. 유전정보는 특정개인을 식별할 수 있는 식별정보를 포함하고 있으며, 이를 통해 개인 식별, 친자 확인, 가족관계도 파악할 수 있다. 머리카락, 타액 등 매우 소량의 신체유래 물질로부터도 유전정보 추출이 가능하다. 이 때문에 당사자의 인지도 동의 없이도 유전정보의 수집과 분석이 이루어질 위험이 있다. 또한, 유전정보를 통해 유전병 등 개인의 생물학적 특징도 파악할 수 있다(이상윤 외, 2016).

이러한 특성 때문에 유전정보는 개인 식별이나 특정한 질병 등을 확인할 목적으로 활용할 수 있으며, 특히 경찰 수사에서도 오래전부터 활용되어왔다. 또한 경찰, 검찰 등 수사기관들은 자체적인 DNA 데이터베이스를 구축하기 위해 노력해왔는데, 데이터베이스의 속성상 규모가 클수록 효용이 높아지기 때문에 이들 기관은 유전정보 수집 대상을 계속 확대해왔다. 범죄현장에서 수집한 유전정보 외에 특정 그룹을 대상으로 한 DNA 데이터베이스의 구축이 법제화된 것은 실종아동 대상 DNA 데이터베이스가 처음이다. 2005년 실종아동등의 보호 및 지원에 관한 법률(실종아동법)이 제정됐고, 이에 따라 경찰청장은 실종아동 등의 발견을 위해 유전자 검사 대상물을 채취할 수 있게 됐다. 경찰이 실종아동 등을 대상으로 유전정보 수집을 시작한 것은 장기미아 부모들의 간절한 요구가 있었기에

사회적 동의를 얻기 쉬웠기 때문일 것이다. 그러나 인권단체들은 경찰청의 DNA 데이터베이스가 확장될 것을 우려했으며, 장기미아를 찾기 위한 목적이라면 아동과 부모에 대한 유전자 채취와 대조가 이루어질 때까지 한시적으로 운영하되 그 이후에는 폐기할 것을 요구했다. 인권단체 우려처럼, 이후 유전정보 수집 대상이 14세 미만 아동 및 장애인에서, 18세 미만 아동, 치매환자로 확대됐고, 범죄자 대상 DNA 데이터베이스도 구축됐다.

실종아동 DNA 데이터베이스의 경우, 유전자 검사의 대상은 보호시설 입소자, 실종아동 등을 찾고자 하는 가족, 보호시설의 입소자였던 무연고 아동을 대상으로 한다. DNA 채취 전에 서면동의를 받으며, 검사대상자가 미성년자, 심신상실자나 심신미약자일 때 본인 외에 법정대리인의 동의를 받아야 한다. 신상정보와 유전정보는 각각 따로 보관된다. 유전자 검사를 통해 수집된 검사대상물은 유전정보 분석 후 폐기된다. 분석된 유전정보는 △실종아동 등이 보호자를 확인했을 때 △검사대상자나 법정대리인이 요청할 때 △유전자 검사일로 부터 10년이 경과되었을 때 폐기된다.

2010년 수형인, 피의자 등의 DNA 데이터베이스의 구축을 허용하는 ‘디엔에이 신원확인정보의 이용 및 보호에 관한 법률(디엔에이법)’이 제정됐다. 그런데 유전정보 채취 대상에 소년범도 포함하고 있다. 보호처분을 받은 소년범의 범죄기록은 전과기록으로 관리되지 않으며, 법원이 추가로 보호처분을 내릴 때만 조회가 가능한데, 이러한 소년범에 대해서도 똑같이 유전정보를 채취하고 있다.⁵⁷⁾ 더구나 디엔에이법은 절도죄에 대해서도 일괄 채취하고 있으며, DNA 채취를 당한 소년범의 절반 이상이 절도범이다. 인권단체는 이는 흉악범죄의 예방이라는 법 제정 취지에 맞지 않다고 비판하고 있다. 특히 아동·청소년들에게 더욱 가혹할 수 있는데, 범죄자 DNA 데이터베이스의 정보는 평생 삭제되지 않기 때문에, 청소년들은 평생 자신이 언제 소환될지 모른다는 두려움을 안고 살아야 하기 때문이다. 이 때문에 법 제정 과정에서 소년범의 DNA 채취 및 신원확인정보

57) 한겨레(2015.3.1.). 소년범 전과 기록도 없앤다더니, DNA 채취 왜 하나.

데이터베이스화에 반대하는 의견이 많았으며, 대법원도 “소년의 교화 및 재사회화를 방해하고 소년에 대한 낙인 효과를 초래하므로 바람직하지 않다”면서 국회에 반대 의견을 제출한 바 있다.

앞서 언급했듯이, 유전정보는 머리카락, 타액 등 우리의 일상적 흔적으로부터 나도 모르게 채취될 수 있기 때문에, DNA 데이터베이스는 나를 언제, 어디서나 추적할 수 있는 수단이 된다. 그렇기에 아동에게 특히 치명적인 영향을 미칠 수 있다. 따라서 미아찾기나 범죄수사와 같은 공공적 목적을 위해 유용할 수 있음에도, 유전정보의 활용은 매우 제한적으로 이루어질 필요가 있다.

4) 지문 등 아동·청소년의 생체인식정보 처리

학생안전, 출입통제 등의 명분으로 지문인식기를 학교에 도입하려는 사례도 있었는데, 이에 대해 국가인권위원회는 수차례 인권침해 결정을 내렸다. 2005년 전라북도 6개 시도 소재 14개 학교에서 급식과 관련해 식당에 지문인식기를 설치하고 학생들에게 일괄적으로 지문날인을 요구하자 이에 대해 시민단체와 전교조가 국가인권위원회에 진정했다⁵⁸⁾. 학교 측은 지문인식기 설치 이유로 “△급식학생과 비급식 학생의 판별 및 정확한 출입현황 파악이 용이하고 △급식 시간 단축 △학생증 분실·훼손·양도의 문제가 없고 △학생출입 통제 관리가 명확하다”는 점을 들었다. 그러나 국가인권위원회는 △지문등록을 요구할 법률적 근거도 없고, 한 학교를 제외하고 학부모 동의도 받지 않은 점 △시·군 교육청, 학교의 관련 규정이나 지침도 마련되어 있지 않은 점 △효율적인 식당 운영·관리가 민감한 생체정보를 요구해 학생들의 개인정보자기결정권을 제한할만큼 중대하지 않은 점 △등록된 지문을 위탁업체에서 관리해 목적 외 활용의 위험이 있는 점 등을 고려할 때 학생들의 인격권, 사생활의 비밀과 자유 등을 침해하는 행위라고 판단했다(국가인권위원회, 2005).

2011년 세종시가 유비쿼터스 정보기술을 도입해 지능화된 학교를 설립하는

58) 오마이뉴스(2005.4.12.). 도둑밥 먹는 학생 잡으려고 지문인식기 설치?

‘u-스쿨 구축사업’을 추진하면서 스마트스쿨 구축을 위한 지문인식시스템 도입의 인권침해 소지에 대해 국가인권위원회에 의견을 요청했다. 지문인식시스템은 학생들의 출결상황을 확인하기 위한 것인데, 이에 대해 국가인권위원회는 도입하지 말 것을 권고하는 의견을 표명했다. 국가인권위원회는 지문정보의 “고유불변성 및 민감성은 불의의 유출사고 시 그 피해가 보다 중대하다”고 보았으며, “명확한 인식과 설명이 부족한 상태에서 지문정보가 수집될 가능성이 있고, 해킹에 의한 유출 가능성을 배제할 수 없으며, 다른 데이터베이스의 결합을 통한 오·남용 피해가 발생할 가능성이 존재한다는 점에서 프라이버시권 침해 소지가 크다”고 판단했다. 반면, 지문인식시스템 도입의 필요성은 크지 않다고 보았다. 학급당 학생수가 20~30명 정도에 불과하고 이동식 수업방식도 아니어서 신속한 출결 관리 효과는 미미하다고 보았다. 또한 담임교사의 육안 확인이나 전자학생증 등 출결확인을 위한 대체수단이 있다는 점도 고려했다(국가인권위원회, 2011).

대구광역시 교육청은 안전한 학교 환경 조성을 목적으로 관내 전체 초등학교 229곳에 지문인식을 통한 건물 출입 통제시스템을 전면 도입하겠다고 밝혔다. 이에 대구지역 시민사회단체와 전교조 등이 반발했고 국가인권위원회에 진정을 냈다⁵⁹⁾. 이에 대해서도 국가인권위원회는 “법률적 근거 없이 아동의 개인정보 자기결정권을 과도하게 제한할 우려가 있고, 아동의 기본권을 최소한으로 제한할 수 있는 다른 다양한 방법으로 학교 내 아동의 안전을 보장하도록 노력하는 것이 바람직하다”는 의견을 표명했다. 또한 초등학생들의 동의를 받더라도 “학교와 학생의 관계에서 학생 등의 동의가 자유로운 의사에 기반하지 않았을 수도 있음이 우려”된다고 보았다. 대구광역시 교육청이 카드인식과 지문인식을 병행하거나 선택적으로 사용하도록 하겠다고 밝힌데 대해서도, 국가인권위원회는 “초등학생들이 출입카드를 항상 가지고 다녀야 하는 것이 △아동의 연령에 부합하는 방식인지 △유엔 아동권리협약 제3조 제1항에서 말하는 아동의 최선의 이익을 최우선적으로 고려한 방식인지 △성인을 기준으로 한 행정편의적인 방식은 아닌지 여부

59) 한겨레(2019.7.29.) 대구시교육청, 초등학교 지문인식 출입시스템 도입 백지화.

등에 대한 면밀한 검토도 필요하다”는 의견을 제시했다(국가인권위원회, 2019). 이후 대구광역시 교육청은 국가인권위원회의 의견을 수용해 지문인식기 도입을 백지화했다.

지금까지 사례를 보면 국가인권위원회는 별도의 법적인 근거 없이 학교 내에서 학생들의 지문정보를 수집하는 것의 정당성을 인정하지 않고 있다. 학생이나 학부모 동의를 받는다면 개인정보보호법의 형식적인 요건을 충족할 수 있을지 몰라도, 학교와 학생의 동등하지 않은 관계를 고려하면 자유로운 동의가 아닐 수 있다는 지적은 의미가 있다. 2020년 개인정보보호법 시행령 개정으로 생체 인식정보가 민감정보로 규정돼 처리요건이 강화되었기 때문에, 생체인식정보의 처리를 규정한 별도의 법률이 있지 않다면, 특히 아동 대상의 생체정보 처리는 정당성을 얻기 힘들다.

지금까지는 주로 지문인식기가 논란이 됐지만, 정맥, 홍채, 얼굴 등 다른 생체 인식 기기의 도입도 논란이 될 수 있다. 이미 2005년 서울대 기숙사에서 학생들의 동의 없이 정맥인식기를 도입해 학생들이 국가인권위원회에 진정하는 사례가 발생하기도 했다⁶⁰⁾.

한편, 경찰은 2011년 실종아동법을 개정해 실종아동의 DNA 수집뿐만 아니라 사전에 아동의 지문과 얼굴정보를 경찰의 정보시스템에 등록할 수 있게 했다. 이는 보호자의 신청에 따라 이루어지는데 아동이 실종될 경우 조속한 발견에 도움이 된다는 이유에서다. 그러나 학부모단체와 정보인권단체는 아동 지문 사전 등록제를 반대했는데, 민감한 생체정보인 지문정보를 경찰이 수집하고 민간업체에 위탁해 유출 위험성이 크고, 실종아동법은 “누구든지 정당한 사유 없이 지문 등 정보를 실종아동 등을 찾기 위한 목적 외로 이용해서는 아니 된다”고 하고 있어 사실상 수사 목적의 활용은 정당화될 수 있고, 이에 따라 시설아동 등 취약계층의 경우 유전정보뿐만 아니라 지문까지 국가에 의해 강제로 수집·이용될 수 있기 때문이다. 또한 지문을 등록하지 않아도 실종아동을 찾을 방법이 없는 것도

60) 한겨레(2005.8.9.). 서울대 기숙사에 정맥인식기, 학생들 “인권침해다” 진정서.

아니었기 때문이다. 2018년 아동의 지문등록을 보호자가 신청하는 것을 넘어 의무화하는 법안(실종아동법 개정안)이 여당 국회의원인 노웅래 의원에 의해 발의됐으나 국가인권위원회는 개정안이 아동의 자기결정권을 침해하고 헌법상 과잉금치 원칙에 어긋난다고 비판했다. 개정안은 임기만으로 폐기됐다⁶¹⁾.

현재 경찰은 ‘안전Dream’이라는 홈페이지에서 아동, 여성, 장애인 등의 사전 등록을 할 수 있게 하고 있으며, 2021년 앱을 통해 집에서도 휴대전화로 지문을 등록할 수 있도록 하고 있다. 코로나19 여파로 현장의 사전 지문등록건수가 2019년 66,387건에서 2020년 17,026건으로 크게 줄었기 때문이다⁶²⁾. 그러나 실종아동 발견이라는 목적의 정당성을 인정하더라도 덜 침해적인 대체수단이 상황에서 아동의 생체정보를 수집할 필요가 있는지, 경찰이 그에 맞는 사회적 신뢰를 획득하고 있는지 의문이다.

61) 뉴시스(2018.6.17.). 인권위 “실종 대비 이유로 아동 지문 의무 등록은 위헌”

62) 연합뉴스(2021.5.24.). “실종아동 예방 지문등록, 집에서 휴대전화로 하세요”

제4장

아동·청소년 개인정보와 프라이버시 교육 현황

제 4 장

아동·청소년 개인정보와 프라이버시 교육 현황

제1절 ● 해외 교육 사례

1. 프라이버시에 대한 접근

코로나 바이러스 팬데믹은 누구도 미처 예기치 못한 속도와 범위와 방식으로 우리 삶의 행태를 변화시켰다. 교육 방식과 업무 행태는 물론, 의료 서비스, 사회복지 서비스, 음식과 식료품 서비스, 그리고 심지어 사회적 관계를 맺고 유지하는 방식까지 바뀌어왔다. 거의 모든 것이 온라인, 디지털 환경으로 이전되었다. 그와 더불어 미디어 리터러시의 중요성도 과거 어느 때보다 더 커졌다.

미디어 리터러시는 단순한 기술적 지식이나 노하우의 수준을 넘어선다. 그것은 온라인 환경에서 회복 탄력성(resilience)과 디지털 시민성 개발에 필수적인 여러 윤리적·사회적·숙려적(reflective) 행위를 포함한다. 따라서 미디어 리터러시를 온라인에 대한 접근성, 표면적인 기술적 지식, 위험을 회피하기 위한 제약 등으로 협소하게 규정하는 대신, 이용자의 이성적 판단 능력을 높이는 데 주목하는 것이 중요하다. 적절한 미디어 리터러시나 지식을 미처 갖추지 못한 채 온라인 환경에 빠져버리는 사람들이 점점 더 많아지기 때문이다. 유네스코는 2017년에 개발한 교육방법론에 따라 미디어 리터러시와 정보 리터러시를 통합한 ‘미디어와 정보 리터러시’ (Media and Information Literacy, MII)이라는 용어를 사용하는데, 시민들이 다양한 형식으로 제공되는 정보와 미디어 콘텐츠에 주체적·비판적·, 윤리적·효과적으로 접근하고, 찾아내고, 이해하고, 평가하고, 사용하고, 공유하는 것은 물론 그로부터 새로운 정보를 창작해낼 수 있는 필수 역량의 묶음 혹은 집합이라고 할 수 있다.

프라이버시에 대한 이해는 필수 역량 중에서도 특히 중요하다. 디지털 환경, 특히 소셜미디어 사용 같은 온라인 활동에서 개인정보의 일정한 공개와 공유는 필수적이기 때문이다. 프라이버시는 매우 다층적이고 가변적이며 맥락 의존적이어서 모두가 이견없이 동의할 수 있는 정의를 찾기는 어렵다. 하지만 아동과 청소년의 디지털 활동, 특히 다양한 소셜미디어 사용의 맥락에서 본다면 대다수 나라들이 개인정보 보호법의 기초 개념으로 삼는 ‘개인정보에 대한 본인의 관리권, 혹은 통제권(right to control of one’s own personal information)’으로 정의하는 것이 가장 포괄적이고 합리적이라고 판단된다. 프라이버시의 ‘구루’로 꼽히는 앨런 웨스틴(Alan Westin)의 표현을 빌리면 “개인, 집단, 또는 기관이 누구와, 언제, 어떻게, 어느 수준의 정보를 소통할지 결정하고 통제할 수 있는 권리”이다. 이는 개인정보보호법을 가진 나라들이 기반으로 삼은 이른바 ‘공정정보 원칙(Fair Information Principles)’의 핵심이기도 하다.

프라이버시는 사람들의 행동에 대한 사회적 비난을 막아줌으로써, 사회의 지배적 규범과 갈등을 빚는 자기표현을 가능케 해준다. 프라이버시 덕택에 사람들은 사회 규범에 속박되지 않고 자유로운 생각과 표현, 행동을 할 수 있다. ‘개인 정보’에 무게 중심을 둔 웨스틴의 이런 규정은 유럽연합 나라들은 ‘정보 자기 결정권’이라는 개념으로 정교화했다. 이는 한 개인이 다른 사람이나 기업, 기관에 자신의 개인 정보를 어느 수준까지 공개하거나 공유할지 결정하고, 설령 이미 제공된 뒤라도 공개나 공유 수준이 타당하지 않다고 판단하면 이를 철회할 수 있는 권리다.

유네스코는 프라이버시를 미디어와 정보 리터러시의 한 요소로서 이렇게 정리했다.

- 사이버공간에서 개인의 프라이버시 권리가 왜 필요하고 중요한지 이해하기
- 개인 정보와 프로필이 특히 온라인에서 급속히 상품화, 상업화해 가는 경향을 인지하기
- 언제, 어떻게 프라이버시와 익명성을 요구할지, 언제 타인의 프라이버시와 익명성을 존중할지 이해하기

- 온라인이나 오프라인에서 언제 개인정보를 공유할지 판단하기
- 온라인 플랫폼을 비롯한 여러 기관들의 프라이버시 정책과 정보 관리 행태를 평가하기
- 디지털 환경의 프라이버시 위험과 혜택을 이해하고, 그에 따라 프라이버시 설정과 수준을 적절히 조정하기
- 타인의 개인정보를 윤리적으로 사용하고 타인의 프라이버시 존중하기

프라이버시에 초점을 맞춘 교육 프로그램은 나라나 법적 관할 지역의 차이에도 불구하고 여러모로 비슷하고 겹치는 부분도 많다. 이들은 공통적으로 프라이버시의 개념과 가치가 현대의 달라진 문화와 끊임없이 변모하는 기술 환경, 그리고 디지털 정보의 경제적·정치적 맥락에 맞춰 새롭게 환기되고 재조정되어야 할 필요성을 인식한다. 프라이버시가 개인이나 그룹에 관한 데이터와 정보의 문제라는 점에 비춰보면 합리적인 판단이고 접근법이다. 온라인과 디지털 환경의 특징 중 하나가 정보·통신·기술 등의 융합과 수렴이라는 점에서 보면, 프라이버시에 관한 교육 프로그램 역시 그런 부분을 충분히 반영해야 한다는 데는 의문의 여지가 없다.

세계 여러 나라와 지역의 프라이버시 교육에서 한 가지 유념해야 할 점은 각 나라와 지역의 사회문화적 특성과 역사적 맥락에 따라 프라이버시에 대한 이해와 가치 평가 또한 상당 부분 달라질 수 있다는 사실이다. 어느 나라에서는 당연시 되는 프라이버시의 가치가 다른 나라에서는 그렇지 않을 수 있다. 예컨대, 지나친 단순화의 위험을 무릅쓰고 말한다면, ‘프라이버시’라는 가치에 대한 유럽 국가들과 북미지역(특히 미국)의 시각은 다르며, 그런 점은 디지털 환경에도 고스란히 반영된다.

2. 미국의 프라이버시 교육

미국의 경우 기업이나 기관이 온라인에서 이용자의 행태를 추적하고 그로부터 프로필을 구축해 표적광고와 다른 상업 목적에 이용하는 일은 당연시되어 왔다.

연방차원의 통일된 프라이버시 법규가 없고, 온라인의 주요 빅테크가 대부분 미국에 있고, 정부는 이들 기업의 급속한 성장과 확장을 우선시해 거의 규제를 하지 않았기 때문이다. 아동과 청소년의 온라인 프라이버시를 보호하기 위한 ‘아동 온라인 프라이버시 보호법(COPPA)’은 그런 환경에서 아동·청소년의 프라이버시를 배려하는 일정 수준의 보호막 역할을 해왔다.

지난 몇 년간 학계와 프라이버시 권리 단체, 일부 의원을 중심으로 연방차원의 프라이버시법 제정을 주장했지만 2021년 현재까지 이렇다 할 성과가 없다. 대신 주정부 차원의 프라이버시법 제정은 꽤 활발하다. 2018년 제정된 뒤 여러 차례 개정돼 2020년 1월1일 발효된 ‘캘리포니아주 소비자프라이버시법(California Consumer Privacy Act, CCPA)’을 비롯해 지난해 3월에는 버지니아주가 ‘버지니아 소비자데이터보호법(Virginia Consumer Data Protection Act)’을 통과시켰고, 그로부터 4개월 뒤 콜로라도주가 ‘콜로라도 프라이버시법(Colorado Privacy Act)’을 제정했다. 다른 주들도 프라이버시법에 관심을 보이지만 입안부터 입법위원회, 상하원 토의와 의결, 주지사 최종서명까지 만만찮은 시간과 노력이 들기 때문에 실제로 발효된 주는 3개 주에 불과하다⁶³⁾.

이중 가장 주목되는 것은 캘리포니아주의 CCPA로, 주의 경제규모가 캐나다 전체와 맞먹을 정도로 크다는 점, 법제가 유럽연합의 일반개인정보보호법(GDPR)에 비견될 만큼 엄격하다는 점뿐 아니라 세계 IT의 중심지인 실리콘밸리의 소위 ‘빅테크’ 기업들이 모두 적용대상이 되기 때문이다. CCPA는 개인정보의 개념을 개별 소비자를 넘어 가구(household)와 관련된 정보로 확대하는 한편, 이들의 프라이버시 권리를 5가지로 범주화했다⁶⁴⁾. △개인정보 수집 전이나 당시, 의도와 목적을 고지 받을 권리(Right to Notice), △수집된 본인의 개인정보에 접근할 수 있는 권리(Right to Access), △개인정보 수집을 거부할(혹은 허락할) 권리

63) 미국 여러 주들의 프라이버시 법안 진전 여부는 프라이버시 옹호 단체인 IAPP의 ‘추적기(tracker)’로 확인할 수 있다. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

64) Davis Wright Tremaine LLP. Consumer Rights under the CCPA, Part 1: What Are They? <https://www.dwt.com/blogs/privacy--security-law-blog/2019/07/consumer-rights-under-to-ccpa-part-1-what-are-they>

(Right to Opt out/in), △수집된 개인정보를 삭제하라고 요구할 권리(Right to Request Deletion), △평등한 서비스와 가격을 요구할 권리(Right to Equal Services and Prices) 등이다. 특히 13세 미만 아동의 개인정보를 수집하기 위해서는 부모의 사전 동의가 필요하며, 13-16세 아동의 개인정보를 판매할 때도 부모의 동의가 요구된다.

미국의 연방차원의 일원화된 개인정보 보호법은 없지만 아동의 개인정보와 프라이버시 보호를 규정한 법은 존재한다. 바로 1998년 제정된 ‘아동 온라인 프라이버시 보호법(Children’s Online Privacy Protection Act, COPPA⁶⁵)’이다. 이 법은 웹사이트 운영자나 온라인 서비스 기관들이 13세 이하 아동의 개인정보를 수집할 때는 반드시 부모의 명시적 동의를 얻어야 한다는 등 여러 요구 사항을 담고 있다. 구체적으로는 개인정보 처리 내용의 고지(Notice), 부모의 동의(Consent), 수집되는 아동의 개인정보에 대한 부모의 검토권(Review), 더 많은 개인정보를 취득하기 위해 아동을 길들이거나 부추기는(conditioning) 행위의 금지, 개인정보 보호와 보안대책, 데이터 보유와 삭제에 관한 의무 사항 등이다. 그러나 소셜미디어 인구가 늘고 인터넷 접속 채널과 환경이 다변화함에 따라, 이 법의 준수 여부를 감독하고 규제하는 기관인 연방거래위원회(FTC)는 그를 따라잡기 위한 노력을 기울이고 있다. 그 중 하나가 아동을 대상으로 한 온라인 기업과 서비스업체들에 대한 6단계 법 준수 가이드로 핵심은 다음과 같다.

- 1단계: 웹사이트나 온라인 서비스는 13세 미만 아동의 개인정보를 수집하는가.
- 2단계: COPPA 규정에 맞춘 프라이버시 정책을 게시하라.
- 3단계: 아동의 개인정보를 수집하기 전에 그 부모에게 직접 고지하라.
- 4단계: 아동의 개인정보를 수집하기 전에 부모로부터 검증가능한 동의를 취득하라.

65) Children’s Online Privacy Protection Rule (“COPPA”). Federal Trade Commission. <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

- 5단계: 수집된 아동의 개인정보에 대한 부모의 지속적인 권리를 존중하라.
- 6단계: 아동의 개인정보를 적절히 보호하기 위한 합리적 절차를 시행하라.

1) 커먼센스 미디어(Common Sense Media)

미국에서 청소년과 가족의 디지털 리터러시를 기르는 데 가장 적극적인 비영리 단체 중 하나인 커먼센스 미디어(Common Sense Media⁶⁶⁾)는 아동에게 안전한 기술과 미디어를 홍보하고 가족 친화적인 교육과 캠페인을 전개한다. 커먼센스가 특히 부모의 자녀 학습에 중점을 두는 분야는 프라이버시와 인터넷 안전이다⁶⁷⁾. 미성년 자녀가 인터넷의 혜택은 최대로 누리면서도 위험성은 최소화한다는 목표로 커먼센스는 어떻게 자녀의 온라인 프라이버시를 보호할 수 있는지에 관해 최근 연구와 팁, 툴 등을 제공한다. 대표적인 주제는 △어떤 프라이버시 설정이 가장 바람직한가? △미성년 자녀에 대한 부모의 통제권(parental control)에는 어떤 것이 있나? △온라인의 이용자 이름은 어떤 것이 바람직하며, 적절한 공유 범위는 무엇인가? △기업들에 대해 자녀의 데이터로 프로필을 만들지 말고, 데이터를 제3자 기업이나 기관에 팔지 말도록 요청하는 방법은 무엇인가? 등이다.

프라이버시와 인터넷 안전을 주제로 한 질의와 응답 코너도 유아(2-4세), 어린이(5-7세), 큰 아이(8-9세), 낀 아이(10-12세), 십대(13세 이상)로 분류해 부모가 해당 연령대에 맞는 내용을 쉽게 찾을 수 있도록 배려했다. 가장 많이 묻는 질문도 따로 모아놓았다. 질문은 다음과 같다.

1. 어떻게 하면 온라인에서 아이의 프라이버시를 보호할 수 있는가?

66) <https://www.common sense.org>

67) 2003년 아동운동가인 짐 스타이어(Jim Steyer)가 설립한 커먼센스 미디어는 시중에 나온 책, 영화, TV 쇼, 비디오게임, 앱, 웹사이트 등을 리뷰해 특정 연령대의 아동들에게 적절한지 평가한다. 평가의 기준이 되는 범주는 6가지로, 긍정적인 롤 모델이 있는가, 긍정적인 메시지를 전달하는가, 폭력과 공포감의 수위는 어느 정도인가, 섹스 관련 콘텐츠의 여부, 사용되는 언어, 소비주의 조장 여부, 음주와 마약, 흡연 장면은 얼마나 나오는가 등이다. 하지만 각 범주의 평점이 낮다고 영화나 드라마의 전체 평점까지 낮아지는 것은 아니다. 가령 디즈니 영화 '크루엘라(Cruella)'는 긍정적인 메시지와 롤모델, 폭력성, 언어 수위, 음주 흡연 등의 범주에서 모두 낮은 점수를 받았지만 영화 자체의 평점은 별 다섯 개 만점이다. '부모가 알아야 할 점'이라는 코너는 그런 평점이 나온 맥락을 친절하게 설명한다. 또 영화와 TV 프로그램에 대해 교육적 가치를 매기는 '학습 평점(Learning Ratings)' 범주도 추가했다.

2. 컴퓨터와 스마트폰에서 최적의 프라이버시 설정은 무엇인가?
3. 아이의 사진을 온라인에 올리는 것은 안전한가?
4. 바람직한 스크린 ID와 비밀번호를 만드는 방법은?
5. 교사가 교육에 디지털 도구를 사용할 때 어떻게 하면 자녀의 프라이버시가 제대로 보호될 수 있는가?
6. 아이의 기기가 해킹을 당했다고 여겨진다면 어떻게 해야 할까?

이 중 특히 1번에 대한 대답은 프라이버시에 대한 미국 사회의 통념을 보여준다는 점에서 좀더 살펴볼 만하다. 커먼센스에 따르면 온라인 프라이버시에는 두 종류가 있다. ‘개인 프라이버시’는 아동의 온라인 평판을 지칭하는 반면, ‘소비자 프라이버시 (consumer privacy)’ 혹은 ‘고객 프라이버시(customer privacy)’는 아동이 온라인에서 다른 사람들과 소통하거나 구매할 때 기업이 수집하는 데이터를 가리킨다. 둘 다 중요하며, 몇 가지 간단한 방법으로 아동이 민감한 개인정보를 비밀로 유지할 수 있게 해준다.

첫째, 아동이 사용하는 앱과 자주 찾는 웹사이트의 프라이버시 설정을 엄격하게 적용하는 것이다. 모든 앱과 웹사이트의 프라이버시 정책과 약관을 꼼꼼히 읽는 것은 현실적으로 어렵지만, 특정한 앱이나 웹사이트, 기기를 사용해 정보를 공유하겠다고 동의하기 전에, 적어도 어떤 정보가 공유·공개되는지는 살펴볼 필요가 있음을 자녀에게 상기할 필요가 있다.

둘째, 온라인에서 어떤 활동이나 소통을 할 때 항상 본인의 개인정보를 어느 수준까지 공유·공개할지 고민하고 판단해야 한다는 점을 자녀에게 가르쳐야 한다. 특히 어린 자녀에게는 주소, 전화번호, 생년월일이 매우 민감하고, 잠재적으로 악용될 수 있음을 알려줄 필요가 있다. 또 무엇이 바람직한 온라인 행태인지 알려주라. 이를테면 사진이나 댓글을 올릴 때 잠재적 영향이나 결과를 한번 더 생각해 보라는 식이다. 특히 온라인에서는 공유와 유포의 용이성 때문에 한 번 올린 글이나 사진을 완전히 삭제하기 어렵다는 점을 일깨워야 한다.

마지막으로 부모는 특히 미성년 자녀의 온라인 프라이버시 보호를 강조하는

‘아동온라인프라이버시보호법 (COPPA)’의 골자를 이해해둘 필요가 있다. 13세 미만의 아동인 경우 부모의 명시적 동의가 필요하다는 점, COPPA의 준수 여부를 감독하는 연방거래위원회(FTC)가 다양한 아동 프라이버시 보호 방안을 계몽한다는 점, 무엇보다 미성년 아동을 주이용자로 둔 서비스나 앱은 해당 연령대에 적절한 디자인과 장치를 웹사이트나 앱에 마련하도록 되어있다는 점을 알아두는 것이 좋다.

2번 질문, 컴퓨터와 스마트폰에서 바람직한 프라이버시 설정 팁도 유익해 보인다. 먼저 ‘컴퓨터 프라이버시’에서 강조하는 것은 쿠키(cookies)에 주목하라는 것이다. 어떤 웹사이트에 접속하는 순간 생성되는 쿠키는 그 접속자/이용자의 움직임을 추적한다. 어떤 쿠키는 이용자의 로그인 정보나 온라인 쇼핑 카트에 담아놓은 상품을 기억하는 경우처럼 유용한 역할을 담당한다. 하지만 어떤 쿠키는 이용자가 원치 않는 내밀한 정보까지 수집하고, 때로는 수시로 삭제해도 완전히 삭제되지 않은 채 숨어 해당 이용자의 프로필을 구성하며, 그런 정보를 광고 회사나 다른 기업들에 본인의 허락 없이 팔아넘긴다(쿠키에 대한 별도의 페이지도 마련되어 있다).

스마트폰의 프라이버시를 조정하는 방법은 운영체제와 기기에 따라 조금씩 다르지만 프라이버시 설정을 가능한 한 엄격하게 해야한다는 점은 같다.

1. 무엇보다 먼저 ‘위치 정보’는 꼭 필요한 경우가 아니면 끄는 것이 좋다.
2. 어떤 앱은 이용자의 전화기에 저장된 정보(예, 연락처)의 공유를 허락해 달라고 요청한다. 거절하라.
3. 인스타그램과 페이스북 같은 서비스의 앱을 내려받은 경우, 웹사이트에 설정한 수준과 마찬가지로 엄격한 프라이버시 설정을 적용하라.
4. ‘소셜 로그인(social login)’을 조심하라. 어떤 사이트에 당신의 페이스북이나 구글의 ID와 비밀번호로 로그인하는 경우, 부지불식간에 해당 앱이나 사이트가 당신의 프로필에서 일정한 정보에 접근하는 것을 허락하는 셈이다. 편의성에 기대어 소셜 로그인을 선택하기 전에, 어떤 정보가 공유되는지 따져보는 것이 바람직하다.

커먼센스 미디어는 디지털 환경과 소셜미디어 플랫폼들에 대한 감시와 비평도 수행한다. 넷플릭스, 디즈니플러스, 애플TV플러스, 로쿠 같은 여러 스트리밍 서비스와 기기들의 약관을 비교하고 프라이버시 관련 기능을 평가해 발표한 보고서 ‘스트리밍앱과 기기들의 프라이버시 비교(Privacy of Streaming Apps and Devices, 2021)’⁶⁸⁾는 그런 사례다. 보고서에 따르면 애플TV를 제외한 모든 스트리밍서비스들의 프라이버시 보호 수준이 미흡한 것으로 드러났다. 심지어 무료 서비스에서 유료로 전환해도 프라이버시 보호 수준은 전혀 향상되지 않았으며, 광고 회사들의 행태 추적 기능은 고스란히 유지되는 것으로 드러났다. 그러한 결과를 바탕으로 커먼센스 미디어는 모든 스트리밍 미디어와 기기들이 ‘프라이버시 중심 디자인’ 원칙을 적용해 가장 높은 수준의 프라이버시 보호를 기본설정(default)으로 삼아야 한다고 주장했다. 이는 개인정보 판매, 제3자를 통한 마케팅과 이용자 추적, 표적 광고, 데이터 프로파일링 등의 활동을 중지해야 한다는 뜻이다. 또 아동 프로필을 설정하는 의도와 목적을 더 명확히 밝히고, 아동의 프라이버시를 더 잘 보호하는 데 프로필을 사용해야 할 것이라고 강조했다.

커먼센스 에듀케이션은 유치원부터 12학년(고 3)까지 아동·청소년의 디지털 시민성 배양을 목적으로 한다. ‘디지털 시민성(Digital Citizenship)’ 커리큘럼⁶⁹⁾은 다양한 멀티미디어를 활용해 학년별로 적합한 교육 프로그램을 제공한다. 프로그램은 아동·청소년의 비교적 짧은 주의력을 감안해 15분 분량의 작은 모듈로 구성했다. 커리큘럼은 △미디어 균형과 복지, △프라이버시와 보안, △디지털 흔적과 정체성, △관계와 소통, △사이버 괴롭힘과 혐오표현, △뉴스 및 미디어 리터러시 등 여섯 분야로 나뉜다. 이중 프라이버시와 보안(Privacy & Security) 분야는 학생들에게 온라인 프라이버시 개념을 소개하고, 개인정보를 친구, 일반

68) Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). Privacy of Streaming Apps and Devices: Watching TV that Watches Us. Common Sense Media. https://www.commonsensemedia.org/sites/default/files/uploads/research/privacy_of_streaming_apps_and_devices-final.pdf
69) <https://www.commonsense.org/education/digital-citizenship/curriculum>

대중, 온라인 플랫폼, 앱 개발사 등 다양한 계층의 사람들과 공유할 때 어떤 결과가 초래될 수 있는지 알려준다. 개인정보 공유는 긍정적 사교와 개인의 성장을 도와주는 자연스럽게 건전한 활동이지만 범위와 속도, 특성이 다른 온라인 환경에서는 정신적, 신체적 위험을 초래할 수 있고, 신상도용이나 금융사기 등의 피해로 이어질 수도 있다는 점을 상기시킨다. 하지만 ‘빅브라더’나 ‘수상한 사람을 위협하다’는 식으로 두려움을 조장하기보다 온라인의 정보 공유의 혜택과 위험을 균형잡힌 시각으로 보여주려 한다.

커리큘럼은 프라이버시 사안을 두 가지 관점에서 다룬다. 하나는 데이터 프라이버시, 다른 하나는 아동과 청소년이 온라인에 남기는 디지털 흔적과 평판으로서의 프라이버시다. 그에 따라, 청소년의 민감한 개인정보를 외부의 위험으로부터 어떻게 안전하게 보호할지에 초점을 맞춘다. 개인정보가 과다 노출되거나 본인 의사와는 상관없이 유출될 수 있는 여러 채널과 위협들, 이를테면 계정등록과 설정, 소셜미디어 포스팅, 온라인 구매, 인터넷 알고리즘, 얼굴·음성 인식 기술, 사물인터넷(IoT) 등을 학생들에게 설명하고 상기시킨다. 또 가족교육권 및 프라이버시보호법(FERPA), 아동온라인프라이버시보호법(COPPA), 캘리포니아주의 학생온라인개인정보보호법(SOPIPA) 등 미국의 여러 프라이버시 보호 법규도 소개한다.

커먼센스의 디지털 시민성 커리큘럼은 유치원부터 12학년까지, 연령대에 적절하다고 여겨지는 수준의 화제와 내용으로 구성되어 있다. 학생들의 관심을 유도·유지하기 위해 실생활에서 흔히 접할만한 사례를 제시해, 그것이 개인정보와 프라이버시 보호에 어떤 도전을 제기하는지 보여준다. 1학년용 학습 자료는 ‘인터넷의 신호등’이라는 제목으로 웹사이트나 앱을 방문했을 때 명심해야 할 안전 수칙을 전달한다. 2학년용 강의는 어떤 유형의 정보를 비밀로 유지해야 하는지 조언하고, 3학년은 복잡하고 쉽게 짐작하기 어려운 비밀번호를 만드는 법을 알려주며, 4학년생에게는 개인정보라도 온라인에서 공유할 수 있는 종류는 무엇인지 귀뜸한다. 더 나아가 온라인의 낚시성 제목이나 정보를 가려내는 방법(5학년), 피싱(phishing, 6학년), 기업들의 개인정보 수집 방식과 위험성(7학년),

온라인 프라이버시(8학년), 온라인 추적과 빅데이터 딜레마(9학년), 신기술에 대한 프라이버시 위험성 평가 (10학년), 부모 허락 없이 소셜미디어를 사용할 수 있는 연령대에 대한 논의(11학년), 소셜미디어와 휴대폰 데이터에 대한 정부의 접근 권한에 대한 논의(12학년)와 같이 다루는 내용의 수준과 복잡성은 학년에 맞게 높아진다.

2) 인간적인 기술 센터(Center for Humane Technology)

넷플릭스의 다큐멘터리 ‘소셜딜레마(Social Dilemma, 2020)’는 소셜미디어의 가공할 위험성을 매우 설득력있게 폭로한 화제작으로 꼽힌다. 실리콘밸리의 여러 소셜미디어 기업의 전직 엔지니어나 프로그래머의 입을 통해 페이스북, 트위터, 유튜브 같은 소셜미디어 서비스가 더 많은 사람들의 더 오랜 주목과 관심을 끌기 위해 얼마나 정교하고 용의주도하고 심지어 음험한 기법과 기술을 서슴없이 사용하는지, 그리고 그렇게 끌어모은 사람들의 관심과 주의를 어떻게 상품화하고 화폐화해 다른 광고사나 정부, 정치 집단에 판매하는지 생생하게 보여주었다. 이 다큐멘터리의 핵심 인물은 트리스탄 해리스(Tristan Harris)로 구글에서 ‘디자인 윤리학자(Design Ethicist)’라는 독특한 직함으로 디지털 기술과 소셜 미디어 서비스의 윤리적 사용을 주창하다 사직하고 ‘인간적인 기술 센터(Center for Humane Technology⁷⁰⁾)’를 설립했다. 그는 구글을 비롯한 소위 ‘빅테크’ 기업들이 윤리적 배려 없이 무차별적으로 사람들의 관심과 주의를 끌어들이 상업적으로 활용하는 데만 혈안이 되어 있다고 비판한다. 인간적인 기술 센터는 이 같은 빅테크들의 ‘주목 경제(attention economy)’와 ‘설득적 기술(persuasive technology)’이 개인 차원을 넘어 거짓정보, 인터넷 중독, 민주주의 훼손 등 사회적 해악으로 확장된다고 지적하면서, 디지털 이용자들의 정신적 복지, 민주주의, 윤리적 정보 공유를 주창한다.

인간적인 기술 센터는 그런 목표를 위해 다양한 매체를 활용해 전방위로

70) <https://www.humanetech.com/>

캠페인을 펼친다. ‘소셜딜레마’ 다큐멘터리가 그 중 하나이고, 빅테크와 소셜 미디어의 위험성을 지적하고 그 대응책을 알려주는 팟캐스트 ‘당신의 온전한 주목이 필요합니다(Your Undivided Attention⁷¹⁾’, 그리고 현직 공학자들을 대상으로 한 온라인 교육 프로그램 ‘인간적인 기술 기초(Foundations of Humane Technology)’ 등이 그런 경우이다. 아동과 청소년을 가르치는 교사와 학부모에게 특히 유용하고 요긴한 정보와 자료를 많이 담고 있다는 점에서 주목할 만하다. ‘코로나-19 팬데믹 중 부모를 위한 디지털 웰빙 가이드라인(Digital Well-Being Guidelines for Parents During the COVID-19 Pandemic⁷²⁾’, 학생과 학부모, 교육자를 위한 페이지⁷³⁾, 정책 개혁안⁷⁴⁾ 등이 그런 사례이다.

이 중 ‘코로나-19 팬데믹 중 부모를 위한 디지털 웰빙 가이드라인’은 다음과 같이 선(禪)이나 명상에 가까운 체계적 접근법으로 구성되어 있다.

1. 느낌: 중요한 것은 디지털 기기와 기술의 ‘사용’만이 아니라, 충동적으로 그것을 집어 들고 만지고 화면을 바라볼 때 맛보는 ‘느낌’에 주목하자. 어떤 감정인가? 호흡에는 변화가 없는가? 가슴은 어떻게 느끼는가?
2. 왜?: 디지털 기기와 기술 자체를 목적이 아닌 수단으로, 도구로 사용하겠다는 의식적 노력을 기울이자. 자녀에게 ‘왜’라는 질문을 던지자. 왜 나는 기기를 집어 드는가? 이 기술은 정말로 내 삶을 개선하는가? 이 기술이 혹시 팬데믹 기간 동안 다른 활동(예, 운동, 교육, 사교)의 대체제로 사용되고 있지는 않은가? 나는 자녀에게 바람직한 기술/기기 사용의 모범이 되는가?
3. 스크린 타임: 부모들은 특히 자녀가 얼마나 오래 디지털 기기를 사용하는지에만 (스크린 타임) 주목하는 경향이 있다. 스크린 타임이 다 같은 것은 결코 아니다. 중요한 것은 스크린으로 접하는 콘텐츠의 내용이다. 따라서 무작정 스크린 타임만 규제하는 것은 현명하지 않다. 이를테면 디지털

71) <https://www.humanetech.com/podcast>

72) <https://www.humanetech.com/digital-wellbeing-covid>

73) <https://www.humanetech.com/families-educators>

74) <https://www.humanetech.com/policy-reforms>

기기로 친구와 나누는 한 시간 동안의 대화가 아무런 생각 없는 30분의 스크롤링보다 훨씬 더 바람직할 수 있다. 그림을 그리고 댄스 비디오를 만들어 온라인에 올리는 행위는 창의적이고 교육적일 수 있지만, 그에 대해 얼마나 많은 ‘좋아요’ 클릭이나 댓글이 달렸는지 끊임없이 체크하는 행위는 자칫 정신 건강에 부정적 영향을 미칠 수 있는 소위 ‘슬롯머신 행태’이다. 정서적 자극이나 쾌감을 기대하며 끊임없이 화면을 스크롤하는 행위, 내 포스팅에 대한 반응을 확인하기 위해 빈번하게 온라인에 들어오는 행위는 모두 그에 해당한다.

4. 기술은 거래임을 기억하라: 편의성이나 연결성을 위해 무엇을 지불하는지 따져보라. 예를 들면 구글 지도를 사용할 때 우리의 위치 정보를 제공하며, 대부분은 그런 거래에 만족해한다. 하지만 다른 경우는 그런 거래가 공정하거나 온당한지 파악하기 어렵다. 예를 들면 다른 사람들의 포스팅을 보는데 시간을 보내는데, 여기에는 화면 옆이나 위, 아래에 놓인 광고에 노출되는 비용도 지불하는 셈이며, 운동이나 다른 활동을 포기하는 부분도 고려되어야 할 것이다. 스마트폰을 사용하는 경우는 화면에 정신이 팔리는 동안 나의 물리적 환경(예컨대 카페에서 함께 앉은 친구나 식탁의 가족들)에 대한 ‘심리적 존재감(mental presence)’은 화면에 내주는 셈이어서, 물리적 환경의 다른 사람들은 화면에서 멀어지는 상황보다 ‘덜 중요하다’라는 인식과 무시당한다는 모욕감을 느낄 수 있다. 이런 정서적 역동성을 비용으로 환산하기는 현실적으로 어렵지만 그것이 정신 건강에 모종의 영향을 미칠 것이라는 추정은 가능하다. 따라서 이런 질문을 던질 가치가 있다.

- 이 편의성을 위해 내가 잃는 것은 무엇인가? 그럴 만한 가치가 있는가?
- 이 시간은 유익하게 보낸 시간인가?
- 지금 하는 일을 디지털 기기나 도구 없이 할 수 있는 대안은 무엇인가?
(예. 손으로 일기 쓰기, 앱의 도움 없이 명상하기)

5. 전향적인 태도를 갖자: 기술은 중립적이지 않다. 우리의 주의를 끌기 위해 경쟁하며, 일단 들어가면 빠져나오기 어렵다는 점을 인식하자.

6. ‘바른’ 기술을 고르자: 어떤 디지털 환경이나 도구는 다른 경우보다 더 효과적일 수 있다. 상황과 맥락을 고려해 가장 효율적인 기술이나 수단을 고르자. 예를 들면 정서적으로 민감한 주제는 텍스트나 이메일보다 대면 접촉이 훨씬 더 효과적이고, 불필요한 오해나 감정적 증폭을 불러일으킬 염려도 더 적다. 이런 경우에 스스로에게 물어보자.
- 이 대화는 텍스트가 더 적합한가, 페이스타임이나 직접적인 대면 접촉이 더 나은가?
 - 이것을 소셜미디어에서 모두와 공유할 것인가, 몇몇 선택된 사람들에게만 알릴 것인가?
 - 문자 메시지를 통한 대화는 얼마나 오래 걸렸으며, 그 와중에서 내 주의를 얼마나 자주 방해받거나 다른 데로 쏠렸는가?
 - 이 디지털 환경은 나와 내 가족에게 적절한가?
7. 성장 중인 두뇌를 보호하자: 우리는 사상 유례를 찾아볼 수 없을 만큼 기술을 사용하고 그에 의존하고 있다. 하지만 아동의 두뇌는 아직 성장하는 중이어서 사용하는 기술과 미디어에 의해 양상과 성격이 달라질 가능성이 크다. 따라서 다음과 같은 요소를 고려해 볼 만하다.
- 지금 이 스크린타임은 정말로 가족과 나를 위한 것인가?
 - 집안에서 디지털 기기를 사용하지 않는 ‘스크린-프리’ 장소와 시간을 설정하고 있는가?
 - 우리는 어떤 유형의 통화나 온라인 사교에 참여하거나 회피해야 하는가?
8. 의심을 품자(Be Skeptical): 코비드-19 팬데믹 동안 실내에서 더 많은 시간을 보내므로, 디지털 기기와 앱을 사용하는 시간도 늘 수밖에 없다. 하지만 그렇게 사용하는 기기와 앱, 특히 ‘무료로’ 제공되는 소셜미디어와 미디어 상품들에 회의적인 태도를 견지해야 한다. ‘무료’를 주장함에도 이들은 어떤 식으로든 수익을 올리고 있기 때문이다. 그와 관련해 품어봄직한 질문은 이런 것이다.
- 이것은 어떻게 나의 삶을 개선해줄 것인가?

- 이것은 나에게 어떤 인간적 가치를 가져다주는가?
- 이 일을 하는데 기술을 이용함으로써 나는 어떤 기술을 포기하는가?
- 광고기업들에 팔릴 것이라는 전제로, 나는 어떤 개인정보를 공유하는데 부담이 없는가?
- 내가 사용하는 앱과 서비스들은 나를 붙들어두기 위해 어떤 기법이나 수단을 사용하는가?

한편 인간적인 기술센터가 제시한 정책 개혁안은 아동 보호, 프라이버시, 플랫폼의 투명성, 해악에 대한 책임, 조작/착취 금지 등을 담고 있다. 이중 아동을 보호하기 위한 대책으로 전국 차원의 계몽 캠페인, 더 효과적인 ID 조회 방식과 연령적합 디자인, 아동·청소년 보호를 우선한 디폴트 설정, 끝없이 이어지는 스크롤 디자인 규제, 콘텐츠 내용에 대한 경고 표시 등이 제시된다. 한편 프라이버시 보호를 위해 미국 전역을 아우르는 연방차원의 프라이버시법을 제정하되, 그 안에 프라이버시 침해 피해자의 소송권, 위치 추적 금지(do-not-track)와 개인정보 판매금지(do-not-sell)를 기본 설정으로 정하고, 데이터 브로커를 금지하고, 프라이버시 보호를 감독하는 연방거래위원회(FTC)의 권한을 강화해야 한다고 제안한다.

3) 티치프라이버시(TeachPrivacy)

‘티치프라이버시(TeachPrivacy⁷⁵⁾)’는 컴퓨터를 기반으로 프라이버시 교육 프로그램을 제공하는 기업이다. ‘캘리포니아 소비자 프라이버시보호법(CPPA)’, ‘의료보험 양도 및 책임에 관한 법(HIPAA)’, ‘가족교육권 및 프라이버시법(FERPA)’, ‘아동 온라인 프라이버시 보호법(COPPA)’, ‘금융서비스 현대화법(GLBA)’, ‘전화 소비자 보호법(TCPA)’ 등 주로 미국의 프라이버시 관련 법제를 알기 쉽게 설명해주는 교육 프로그램들이 많지만 유럽연합의 ‘일반개인정보보호법(GDPR)’이나 캐나다의 프라이버시 체제, 그리고 피싱, 소셜 엔지니어링, 프라이버시와 보안

75) <https://teachprivacy.com/>

등 일반적인 내용도 다수 포함되어 있다.

티치프라이버시는 2010년 세계적인 프라이버시 전문가로 꼽히는 대니얼 솔로브(Daniel Solove) 교수(조지 워싱턴대 로스쿨)에 의해 설립되었다. 솔로브 교수는 국내에도 번역 출간된 <인터넷 세상과 평판의 미래> <숨길 수 있는 권리> 등의 저자로도 유명하며, 평소 프라이버시 교육의 중요성을 논문과 인터뷰, 학회 발표 등을 통해 강조해 왔다. 티치프라이버시는 그런 신념을 비즈니스로 바꾼 결과물이라고 할 수 있다. 이 서비스가 다른 프라이버시 교육 기관이나 프로그램들과 구별되는 대목은 온라인의 특성과 환경을 적극 활용했다는 점이다. 특히 교육 프로그램을 짧게는 2-4분부터 길게는 몇 시간에 이르기까지 여러 단위로 모듈화함으로써 주의 지속 시간이 상대적으로 낮은 아동과 청소년의 특성을 잘 반영했다. 또 뷔페식으로 일정한 주제에 따라 모듈로 나눠 학생의 필요와 목적에 따라 마치 퍼즐 맞추듯 자유롭게 조합해 배울 수 있도록 했다. 현재 웹사이트에 소개된 주제별 프라이버시 교육 모듈만 100개가 넘는다. 교육의 수준도 디지털 지식이 비교적 낮은 사람도 쉽게 배울 수 있는 프라이버시 기초, 사이버보안 기초 등부터 전문 분야의 직업인이나 교사들을 대상으로 한 코스에 이르기까지 다양하다.

티치프라이버시는 서비스의 특성상 프라이버시나 개인정보에 대한 고정된 정의를 따로 정해놓지 않았지만 역시 대부분의 과정은 미국의 법제를 가장 종합적으로 반영하고 있다. ‘트레이닝’ 메뉴를 보면 프라이버시와 데이터 보안 전반을 다루는 ‘프라이버시 코스 라이브러리’와 ‘데이터 보안 코스 라이브러리’를 필두로 프라이버시에 관한 한 미국에서 가장 중요하게 취급되는 ‘의료보험 양도 및 책임에 관한 법(HIPAA)’과 ‘가족교육권 및 프라이버시법(FERPA)’에 대한 별도의 라이브러리가 따로 마련되어 있다. 특히 ‘화이트보드(Whiteboard) 라이브러리⁷⁶⁾’는 나라별 주요 프라이버시 법제나 구조를 가르치려는 교사나 학부모가 특히 유의하다고 여길 만한 자료 창고이다. 티치프라이버시만의 독특한 서비스라고 할 만한

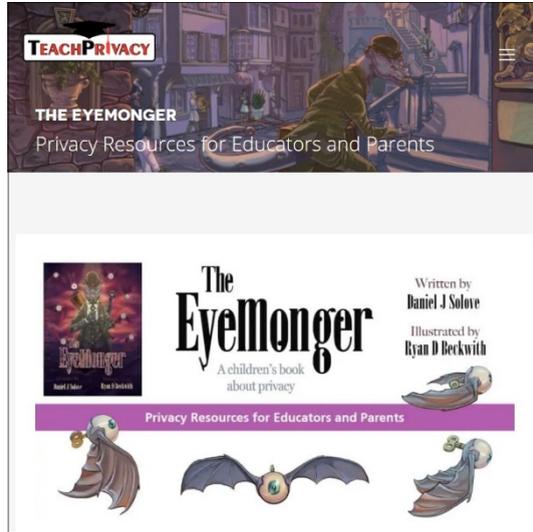
76) <https://teachprivacy.com/privacy-security-training-programs/whiteboards/>.

화이트보드는 말 그대로 흰색 한 면에 특정 법규나 한 나라의 프라이버시 법제를 그림을 곁들여 요약했다. 미국의 경우 연방차원의 부문별 프라이버시 법들, 주정부 차원의 프라이버시 법규를 요약한 화이트보드가 준비되어 있다. 미국과 캐나다의 프라이버시 법을 비교한 그래픽 자료도 있다. 전세계의 프라이버시법도 나라별로 정리했는데, 한국의 개인정보보호법(PIPA)의 그림 설명서도 여기에 포함되어 있다.

또 트레이닝 주제별 묶음에는 캘리포니아 소비자 프라이버시 보호법(CCPA), GDPR, 프라이버시 실드(Privacy Shield), HIPAA, FERPA, 브라질의 최신 프라이버시 법인 LGPD, 그리고 '프라이버시 중심 설계' 등에 대한 트레이닝 코스가 나와 있다.

대니얼 솔로브 교수는 최근 4-11세 아동을 대상으로 <아이몽저: 아동용 프라이버시 계몽서(The Eyemonger: A children's book about privacy⁷⁷)> 라는 제목의 프라이버시 계몽서도 펴냈다. 책에서 아이몽저는 우리의 일거수 일투족을 항상 감시하는 온갖 시스템과 기기를 포괄하는 단어다. 것처럼 누군가에 의해 24시간 감시된다면 우리는 어떤 기분일까? 그런 감시로부터 벗어나 각자 숨기고 싶어하는 내용은 무엇일까? 어떤 내용을 비밀로 유지하는 게 바람직할까? 비밀을 간직하는 게 잘못일까? 왜 사람들은 비밀을 유지할까? 어려운 법률 용어나 복잡한 설명 없이 판타지 소설 같은 일러스트를 곁들여 프라이버시의 중요성을 자연스럽게 일깨우는 구성이 눈길을 끈다.

77) <https://teachprivacy.com/the-eyemonger-privacy-resources-for-educators-and-parents/>.



[그림 4-1] 아동용 프라이버시 계몽서 아이몽거(The Eyemonger)

프라이버시에 대한 정의도 평이하다. ‘프라이버시는 무엇인가를 비밀로 유지하고 싶어하는 사람들의 의도를 존중하는 것’이며 ‘프라이버시는 얼마나 많은 정보를 남과 공유할지 경계선을 정하고, 다른 사람들의 경계선을 존중하는 것’이라고 〈아이몽거〉는 설명한다.

솔로브 교수는 아동과 청소년을 대상으로 한 프라이버시 교육에 포함되어야 할 내용⁷⁸⁾도 (1) 인지(awareness) (2) 보호(protection) (3) 수집(collection) (4) 공유(sharing) 네 가지 범주로 요약했다. 각 범주에 포함된 교육 아이템은 다음과 같다.

1. 인지: 일반적인 프라이버시 이해

- ① 디지털 시대의 프라이버시: 어떻게 개인정보가 수집되고 사용되는가.
- ② 온라인 서비스와 상품의 이용: 다양한 기술의 사용에 따른 혜택과 위험 평가.

78) <https://teachprivacy.com/the-eyemonger-privacy-resources-for-educators-and-parents/>.

2. 보호: 안전과 보안

- ① 신상 도용(identity theft): 신상 도용을 당한 경우 어떻게 대응할 것인가.
- ② 피싱(phishing)과 온라인 위협: 온라인 환경의 다양한 위협을 어떻게 판별하고 회피할 것인가.
- ③ 프라이버시와 신체 안전: 온라인에서 낯선 사람과 만난 탓에 초래될지 모르는 신변의 위협을 어떻게 예방할까. 어떤 개인정보를 온라인에 올리는 것이 위험할 수 있나.
- ④ 데이터 보안: 해커, 피싱, 바이러스 등을 판별하고 막는 방법. 바람직한 보안 대책.

3. 수집: 프라이버시의 경계선을 존중하기. 훔쳐보기와 다른 형태의 정보 수집 편법

- ① 타인의 프라이버시 경계선에 대한 윤리적 존중: 어떻게 기술은 프라이버시 침해를 더 쉽게 만들었는가. 개인정보 공유의 경계선을 설정하고 존중하는 것이 왜 중요한가.
- ② 정보 수집과 사용에 관한 법률적 경계선: 타인의 프라이버시 침해는 심각한 피해를 초래할 수 있음. 특정한 프라이버시 침해는 사법적 처벌을 초래할 수도 있음.
- ③ 정부의 수색과 감시: 정부의 수색과 감시로부터 시민이 요구할 수 있는 기본 권리는 무엇인가.

4. 공유: 자신과 타인의 개인정보 공유

- ① 기밀성(confidentiality): 개인정보의 기밀성을 유지해야 할 의무.
- ② 온라인 가십과 자기 과시/노출: 어떻게 온라인 가십은 타인에게 피해를 입힐 수 있는가. 자기 노출이나 공개가 초래할 수 있는 부정적 결과는 무엇인가.
- ③ 온라인 괴롭힘과 온라인 학대: 온라인 괴롭힘(사이버불링)과 온라인 학대는 심각한 피해를 초래할 수 있음. 괴롭힘이나 학대의 피해자가 된 경우 어떻게 대응할 것인가, 또 다른 피해자를 어떻게 도와줄 수 있는가.

- ④ 섹스팅과 ‘청소년들이 생산한 성적 이미지(Youth Produced Sexual Images)’: 섹스팅의 위험성. 심각한 정서적 스트레스는 물론 법적 처벌로 이어질 수도 있음.

4) 세계프라이버시전문인협회(IAPP)

세계프라이버시전문인협회(IAPP⁷⁹⁾)는 개인정보 보호와 프라이버시 전문가들로 구성된 세계 최대 규모의 비영리회원단체로 미국 뉴햄프셔의 포츠머스⁸⁰에 본사를 두고 있다. 전세계를 아우르는 만큼 데이터 프라이버시에 관한 한 가장 방대하고 전문적인 정보와 다양한 온라인 교육 프로그램을 제공하며, 해마다 미국과 유럽, 아시아태평양 지역에서 프라이버시 컨퍼런스를 개최한다. 아동과 청소년에 특화된 프라이버시 교육 프로그램은 없지만 ‘프라이버시 프로 프루던스(Prudence the Privacy Pro⁸⁰⁾’라는 제목의 프라이버시 계몽 만화를 꾸준히 연재해 젊은층의 관심을 유도하고 있다.

5) 대학과 공공 도서관

여러 도서관의 웹사이트들이 아동과 청소년을 대상으로 한 프라이버시 교육의 창구로 기능한다는 점도 주목할 만하다. 그 중 한 사례는 캘리포니아주 산호세 공공도서관에서 꾸린 ‘가상 프라이버시 랩(Virtual Privacy Lab⁸¹⁾’이다. 이들은 온라인 프라이버시를 주제 별로 묶은 툴킷을 제공한다. 온라인 프라이버시란 무엇인가, 소셜미디어와 온라인 공유, 보안-인터넷은 어떻게 작동하는가, 데이터는 어떻게 공유되는가, 당신의 정보 흔적(information footprint), 익명성과 추적(tracking), 온라인 프라이버시 현황 등이 툴킷의 주제들이다. 기본 내용을 습득한 다음 더 깊이 파고들고 싶은 사람에게는 그에 부합하는 툴킷을 제공한다. 한 가지 흥미로운 대목은 산호세 공공도서관에서 사용하는 다른 온라인 서비스

79) <https://iapp.org>

80) <https://iapp.org/resources/article/prudence-comic-1/>

81) <https://www.sjpl.org/privacy>

기관과 기업들의 개인정보 보호 정책을 하이퍼링크로 제공한다는 점이다.

하버드대학 산하 버크만 클라인 센터(Berkman Klein Center)는 인터넷 분야의 다양한 연구와 프로그램들로 명성이 높는데, 청소년을 대상으로 한 프로젝트 ‘청소년과 미디어(Youth and Media⁸²)’는 디지털 시민권, 인공지능(AI), 콘텐츠 생산, 데이터, 디지털 접근, 디지털 경제, 디지털 리터러시, 정체성 탐사와 형성, 법률, 안전과 복지 등 디지털 환경의 다양한 이슈와 주제를 폭넓게 다룬다. 프라이버시와 평판, 보안도 여기에 들어있다. 청소년과 미디어 사이트는 그런 범주의 커리큘럼을 연령대/학년에 맞춰 세분화하고, 그에 적절한 난이도로 콘텐츠를 정리했다.

프라이버시와 평판 분야는 △프라이버시 개요, △평판 개요, △소셜미디어와 공유, △커뮤니케이션 관리 네 과정으로 구성된다. 이중 프라이버시 개요를 보면 11-18세(6-12학년)를 대상으로 예상 소요 시간 70분(활동 30분, 과제 수행 40분)이며, 총 35개 언어로 제공된다고 나와 있다. 이와 관련된 내용은 프라이버시를 주로 개인정보, 특히 내밀한 정보의 공개나 비공개의 관점에서 다룬다. 그리고 공개 범위의 적절한 설정이 프라이버시와 평판 관리에 어떤 영향을 미치는지 고민해보도록 유도한다. 국내 중고등학교에서 참조할 수 있을 법한 내용과 자료가 많다. 평판 개요는 공개된 온라인 정보가 어떻게 다른 사람들에 대한 평판을 형성할 수 있는지 알려주며, 활동 내용으로 (1) 누가 나의 비밀을 알고 있는지 고려하는 것, (2) 나의 온라인 평판은 어떤 내용일지 조사해 보는 일, (3) 누군가가 나에게 대한 의견이나 콘텐츠를 올렸지만 그것이 부적절하다고 판단하는 경우 어떻게 해야 할지 논의하기, (4) 나에게 대해 부정적인 내용의 온라인 정보, 남이 보기를 원치 않는데 공개된 정보에 어떻게 대응해야 하는지 논의하기 등이 나와 있다.

소셜미디어와 공유 과정은 이를 현명하게 이용하는 방법을 여러 그룹 활동을 통해 알아낼 수 있도록 구성했다. 온라인에 어떤 유형의 소셜미디어가 있고, 그들의 특성은 무엇인지 조사하는 일, 친구 신청에 얽힌 여러 이슈를 파악하고, 그 해법을

82) <http://youthandmedia.org>

논의하는 일, 소셜미디어를 통해 어떤 성격의 정보를 누구와 어느 정도까지 공개할지 판단하는 문제, 소셜미디어 플랫폼들에서 이용자의 취향과 관심에 맞춰 프라이버시 설정을 바꾸는 일 등이 이 코스의 골자다. 마지막 커뮤니케이션 관리는 나에 대한 정보 중 어떤 유형을 남들과 공유하거나 비밀로 유지할지 판단하는 일, 소셜미디어의 프라이버시 설정을 바꾸는 방법(왜 어떤 콘텐츠는 ‘친구하고만 공유’이고, 다른 콘텐츠는 ‘공개’인지 그 기준을 고민해 보기), 그리고 매체의 성격에 따라 소통이 원활하거나 그렇지 못한지, 왜 오해나 갈등을 불러 일으키는지 조사하고, 그에 따른 해법을 찾아보는 일 등을 포함한다. 청소년과 미디어 프로젝트는 주제와 성격에 따른 모델 커리큘럼을 제시하는 데 그치지 않고, 그에 대해 더 심층 연구하고 싶은 사람을 위해 폭넓고 방대한 관련 자료와 연구 결과, 사이트들을 소개해준다. 교사와 학부모에게 참고가 될 법하다.

3. 캐나다의 프라이버시 교육

캐나다의 법규와 여러 정부 정책에서 정의한 정보 프라이버시는 전세계적으로 공통된 공정정보 원칙(Fair Information Principles), 즉 자신의 개인정보에 대한 일정 수준의 통제권(right to control)에 기반을 둔다. 다시 말해 나의 개인정보 중 어떤 부분을 누구와 언제 얼마만큼, 그리고 얼마동안 공유하거나 공개할지 결정할 수 있는 권리라고 정의한다. 여기에서 개인정보는 그 사람의 신원을 파악하고 식별할 수 있는 모든 정보 요소를 포함한다. 흔한 예로는 이름, 주소, 생년월일, 성별, 좋아하는 것, 하는 일, 나를 담은 사진과 비디오 등이다.

캐나다 청소년의 디지털 리터러시는 OECD 평균보다 높은 편이다. 코로나 바이러스 팬데믹이 벌어지기 이전인 2018년의 경우 15세 캐나다 청소년의 94%가 집에서 컴퓨터로 학교 숙제를 할 수 있다고 대답해 OECD 평균인 89% 보다 높았다⁸³⁾. 또 설문 응답 학생의 70%가 주관적이거나 편향된 정보를 판별하는

83) <https://www150.statcan.gc.ca/n1/daily-quotidien/201214/dq201214a-eng.htm>

방법을 배웠다고 대답해 OECD의 55%보다 높은 수치를 보였다. 인터넷의 특정 정보의 신뢰성을 판단하는 방법(79% 대 69%), 페이스북이나 인스타그램같은 소셜미디어에 정보를 올리면 어떤 결과가 나올 수 있는지에 대한 이해(81% 대 76%)에서도 다소 우위를 보였다. 하지만 피싱(phishing)이나 스팸을 판별하는 방법을 배웠느냐는 질문에는 OECD(41%)보다 낮은 38%만이 그렇다고 대답했다.

1) 캐나다 개인정보보호위원회(OPC), 주/준주 단위 정보공개 및 개인정보 보호 위원회(OIPC)

이웃한 미국에 비해 캐나다는 개인정보 보호를 보장한 법제가 매우 잘 갖춰져 있다. 캐나다 전국 규모의 비즈니스를 제공하는 기업과 비정부 기관들에 적용하는 ‘개인정보보호 및 전자문서법(Personal Information Protection and Electronic Documents Act, PIPEDA)’가 있고, 각 주 단위로 해당 주에서만 비즈니스를 하는 기업들에 적용하는 ‘개인정보보호법(Personal Information Protection Act, PIPA)’이 있다. 그런 법을 갖춘 브리티시 콜럼비아주, 알버타주, 퀘벡주는 주차원의 비즈니스에는 PIPA를 적용하고, 전국 규모의 은행이나 방송국 등에는 PIPEDA를 적용한다. 그에 반해 주차원의 개인정보보호법이 없는 온타리오주, 뉴브런즈윅주 등 다른 주들은 비즈니스의 범위와 상관없이 일괄적으로 연방차원의 PIPEDA를 적용한다. 온타리오주는 법제의 부족함을 인식하고 주차원의 개인정보보호법을 준비 중이다.

한편 정부기관과 공기업은 다른 유형의 법제에 묶인다. 연방 정부는 공개정보법(Access to Information Act)과 개인정보보호법(Privacy Act)의 적용을 받으며, 주/준주 정부와 공기업들은 해당 주/준주 차원의 ‘정보공개 및 개인정보보호법(Freedom of Information and Protection of Privacy Act, FIPPA)’을 준수해야 한다(주마다 이름은 조금씩 다르지만 정보공개 분야와 개인정보 보호 분야를 한데 묶은 법 구조는 비슷하다). 연방과 주차원의 개인정보 보호 실태를 감독하는 기관도 다르다. 연방은 ‘개인정보보호위원회(Office of the Privacy

Commissioner of Canada, OPC⁸⁴), 각 주는 ‘정보공개 및 개인정보보호 위원회(Office of the Information and Privacy, OIPC)가 해당 관할 지역의 개인정보 보호 실태를 감시하고 감독한다.

캐나다는 이처럼 개인정보 보호를 위한 법제는 잘 마련되어 있지만, 제때 개정되지 않아 급속한 기술 진보와 사회 변화에 너무 뒤처진다는 지적을 받는다. 가령 PIPEDA는 제정된 이후 30년이 넘도록 한 번도 개정되지 않았으며, 주 정부 단위의 개인정보 보호법제 역시 개정이 더더 소셜미디어를 비롯한 디지털 환경을 적절히 반영하지 못한다는 우려를 낳는다. 개인정보보호위원회 관계자, 프라이버시 학계와 전문가들은 특히 대중 교육, 아동과 청소년들에 대한 프라이버시 교육을 명시적으로든 묵시적으로든 법으로 강제하거나 권장해야 한다고 입을 모은다. 현재 캐나다의 중고등 학교에서 시행되는 프라이버시와 디지털 리터러시 교육은 학교 자율에 맡겨져 있지만, 일정한 시사 문제나 화제를 학생들이 정하고, 그 사안을 다양한 렌즈와 온라인 정보를 통해 바라보고 분석하고 토론하는 가운데 건전하고 명석한 디지털 시민의 자격을 갖추게 한다는 목표는 비슷하다.

위에 설명한 것처럼 캐나다의 개인정보 보호 체계는 다소 복잡해 보이지만 연방과 주 단위의 감독기관들은 서로 원활하게 협조하고 공동 프로젝트도 적극 전개하기 때문에 눈에 띄는 갈등이나 문제는 불거지지 않는다. 이들 감독 기관들은 서로 다른 관할권과 관할 지역을 가졌지만 적어도 개인정보 보호방안을 모색하고 개인의 프라이버시 권리를 홍보하고 계몽하는 일에는 매우 적극적이다.

캐나다 개인정보보호위원회는 일반 성인은 물론 특히 피싱이나 스팸 사기를 당하기 쉬운 노년층을 대상으로 다양한 계몽 활동을 전개한다. 그에 못지않게 아동과 청소년의 디지털 리터러시, 특히 프라이버시에 대한 지식을 높이기 위해 그들의 눈높이에 맞춘 미디어와 채널을 활용한다. 학부모를 위한 프라이버시 팁, 온라인 프라이버시를 위한 DIY, 연령대에 따른 학교 커리큘럼 등도 제공한다. ‘소셜 스마트: 프라이버시, 인터넷, 그리고 당신⁸⁵’이라는 제목의 12페이지

84) <https://priv.gc.ca/en/>

85) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and>

그래픽 노블은 그런 고민이 잘 반영된 결과물이다. 특히 이 만화는 대상 독자층인 청소년들의 의견과 질문, 우려 사항 등을 수렴해 현실감을 높였다.

캐나다 개인정보보호위원회는 새 학기가 시작되는 9월을 맞아 아동·청소년의 프라이버시 지식을 높이기 위한 ‘온라인에서 안전하게 놀아요(play safe online⁸⁶⁾)’ 캠페인을 전개했다. 이들은 복잡하고 거창한 행사를 주최하는 대신 온라인에서 자신의 프라이버시와 평판을 적절히 관리하면서 즐겁게 놀 수 있는 ‘팁’을 학부모와 교사, 학생들에게 알려준다. 팁은 다음과 같이 간단하고 이해하기 쉽게 범주화했다.

- 당신의 평판을 보호하세요.
- 누구를 신뢰할지 신중하게 판단해요.
- 클릭하기 전에 한 번 더 생각해요.
- 스스로를 보호하세요: 비밀번호는 복잡하고, 쉽게 들키지 않도록 만들고, 자신에게 맞도록 프라이버시를 설정하세요.
- 흔적을 남기지 말아요. 소셜미디어에 민감한 개인정보는 올리지 말아요.
- 익명을 유지해요. 학교 계정에는 실명을 써야 하지만, 온라인 게임이나 소셜미디어에는 가명을 쓰는 것도 좋은 아이디어입니다.

-events/privacy-education-for-kids/social-smarts-privacy-the-internet-and-you/
86) <https://www.priv.gc.ca/en/blog/20210902/>



[그림 4-2] 캐나다 온타리오주 OIPC의 아동·청소년 프라이버시 프로그램

한편 캐나다 인구의 3분의 1 정도가 거주하는 온타리오주의 ‘정보공개 및 개인정보보호위원회(OIPC)’는 9월23일 ‘프라이버시 추구! 아동을 위한 게임과 활동(Privacy Pursuit! Games and Activities for Kids⁸⁷⁾’을 펴냈다. 아동 청소년의 프라이버시 리터러시를 높일 목적으로 제작된 18페이지 분량의 소책자는 친근한 일러스트와 크로스워드 퍼즐, 암호문 풀기(Cryptograms), 상관되는 항목 연결하기, 글자찾기 등 다양한 게임을 적절히 섞어 ‘놀이를 통한 교육’의 효과를 꾀했다. 이 작업은 온타리오주 OIPC가 설정한 우선 과제들 중 하나인 ‘아동과 청소년의 디지털 리터러시 높이기’의 일환이다.

이 캠페인에서 돋보이는 것은 어려운 법률 용어를 최소화하고 아동과 청소년이 쉽게 이해할 수 있는 단어와 표현을 사용했다는 점이다. 가령 소셜미디어에 개인 정보를 제공하는 사안에 대해서는 “(온라인에서) 개인정보가 가치 있는 이유는 기업들이 그것으로 돈을 벌기 때문입니다. 그게 늘 나쁜 것은 아니지만, 어떤 게임이나 앱이 공짜라면 그것은 우리의 개인정보 중 일부를 비용으로 지불하고,

87) https://www.ipc.on.ca/wp-content/uploads/2021/09/privacy-pursuit-activity-book-for-kids_ipc.pdf

원치 않는 광고를 봐야 한다는 뜻입니다”라고 설명한다. 또 이른바 스마트 장난감 (smart toys)들은 대개 작은 카메라와 마이크를 탑재해서 우리의 개인정보를 수집할 수 있다고 경고한다.

2) 미디어스마트스(Media Smarts)

캐나다에서 청소년의 디지털과 미디어의 리터러시를 높이기 위해 가장 적극적으로 활동하는 비정부, 비영리 단체 중 하나는 ‘미디어스마트스(Media Smarts)’이다⁸⁸⁾. 미디어스마트스 웹사이트의 주요 메뉴는 디지털 및 미디어 리터러시, 연구 정보, 부모 코너, 교사용 자료, 그리고 블로그이다. ‘디지털 및 미디어 리터러시’ 메뉴는 다시 일반 정보와 미디어 이슈, 디지털 이슈로 구분된다. 일반 정보는 디지털 리터러시와 미디어 리터러시의 차이와 접점을 설명하고, 그런 리터러시를 요구하는 주요 (디지털) 미디어를 열거한다. 인터넷과 모바일, 텔레비전, 영화, 비디오 게임, 음악이 그들이다. 이들은 별개인 듯 하지만 서로 겹치거나 연결된다. 특히 디지털 리터러시는 미디어 리터러시에 비해 새로운 개념이다. 미디어스마트스에 따르면 디지털 리터러시는 단순히 기술적 노하우만 가리키는 것이 아니다. 온라인 환경에 기민하게 적응하고 여러 공격이나 곤경을 극복할 수 있는 ‘회복 탄력성(resilience)과 윤리적인 디지털 시민의 자격을 갖추는 데 필수적인 여러 인종적, 사회적, 숙려적(reflective) 지식과 행동을 포괄한다.

미디어스마트스는 또 빠르게 변화하는 기술 지형에 기민하게 적응하고 대처하기 위해서는 디지털 리터러시가 필수라고 강조하면서 디지털 환경을 다음과 같이 정리했다.

1. 디지털 미디어는 네트워크로 연결되어 있다. 이 연결은 양방향이어서 데이터 교환과 참여의 벽이 현저히 낮아졌다.
2. 디지털 미디어는 지속적이고, 검색과 공유가 가능하다. 디지털 콘텐츠는 영구적이다. 전송된 모든 것은 어딘가에 저장되어 검색되고 색인화될 수 있다.

88) <https://mediasmarts.ca>

3. 디지털 미디어는 알 수도 예상할 수도 없는 관객을 가진다. 위 특징들 때문에 당신이 온라인에서 공유하는 내용은 의도하거나 예상하지 못했던 이들에게도 공개될 수 있다. 관객을 관리할 수 없기 때문에 콘텐츠는 때로 맥락을 벗어난 오해를 살 수 있다.
4. 디지털 미디어를 통한 경험은 사실이지만 항상 그렇게 느껴지는 것은 아니다. 네트워크를 통한 상호 작용의 특징 중 하나는 ‘공감의 덫(empathy traps)’이다. 익명의 느낌, 혹은 상대의 목소리나 얼굴 표정을 느낄 수 없는 데서 오는 공감 부족은 악성댓글과 사이버 괴롭힘을 유발하는 한 원인으로 작용한다. 또 물리적 실체가 결여된 온라인의 특징은 현실 사회의 법, 윤리의식, 권리 등을 잊게 만들기 쉽다.
5. 디지털 미디어를 사용할 때 우리가 대응하는 방식은 해당 플랫폼의 아키텍처에 좌우된다. 그리고 그 아키텍처는 개발자의 편향과 가치관을 반영하고 있다.

미디어스마츠에 따르면 이와 같은 디지털 미디어의 특성은 정보 인증, 온라인 괴롭힘, 사이버 보안, 지나친 인터넷 사용, 도박, 온라인 혐오표현, 온라인 윤리, 온라인 마케팅, 프라이버시, 포르노, 성적 착취, 그리고 섹스팅 같은 이슈를 촉발한다.

디지털 리터러시의 장을 통해 경제적, 사회적, 문화적, 시민적 간극을 줄일 수 있다는 점에서 사회 정의의 문제라고 볼 수도 있다. 일정 수준의 디지털 리터러시를 갖출 권리를 공식 인정하는 것은 따라서 온라인 기회에 대한 접근, 특히 소외 계층이나 그룹(여성, 흑인, 원주민, 기타 소수 인종이나 민족, 신규 이민자)의 온라인 접속을 높일 수 있다. 미디어스마츠의 디지털 리터러시 이니셔티브는 이런 연구를 지원한다. 예컨대 YWCA 캐나다와 제휴해 진행하는 ‘디지털스마츠’ 프로그램은 소위 ‘디지털 경제’에서 상대적으로 소외되는 인구(예. 노년층, 저소득층, 이민자, 비영어 사용자, 시골이나 격오지 거주자, 원주민)를 돕자는 취지로, 온라인 환경에 대한 참여자의 이해와 자신감을 높이는

데 기여한다는 평가다. 이 프로그램을 통해 참여자들은 정보의 신뢰도와 적실성을 제대로 판단하는 방법을 배우고, 온라인상의 권리와 개인정보 보호 방법도 익힌다.

미디어스마트스의 프라이버시 프로그램은 ‘디지털 이슈’ 중 하나로 분류되어 있다. 온라인 환경이 가진 감시의 위험성과 더불어, 많은 성인들이 오해하는 것과 달리 청소년들 또한 프라이버시를 매우 중요한 권리로 인식한다는 점을 강조한다. 흥미로운 점은 온라인 프라이버시를 소셜미디어의 사용과 긴밀히 연계된 ‘소셜 프라이버시’와, ‘데이터 프라이버시’로 구분했다는 사실이다. 또 광고와 마케팅, 소비주의, 미성년자의 온라인 활동이 가진 잠재적 위험성도 다루고 있다.

미디어스마트스는 교육용 게임, e-튜토리얼과 워크숍도 개최해 교사와 학부모의 참여를 북돋운다. 매년 10월 말은 ‘미디어 리터러시 주간⁸⁹⁾’으로 정해 다양한 교육 프로그램과 캠페인 활동을 전개한다. 올해는 10월 25-30일로 학년별로 특화된 주제를 짚는다. 첫날인 25일의 주제는 데이터의 ‘사용’이며, 화요일은 미디어와 프라이버시 가치의 ‘이해’, 수요일은 ‘참여’, 목요일은 정보 판별과 접근, 그리고 금요일은 보안에 초점을 맞춘 ‘인증’이다. 교사나 학부모가 아동과 청소년의 프라이버시는 물론 미디어 리터러시 교육을 위한 커리큘럼을 짤 때 도움을 받을 만하다.

4. 영국의 프라이버시 교육

영국의 프라이버시 법은 유럽연합 회원국이었던 동안은 ‘일반 개인정보보호법’ (GDPR)과 동일했다. 그러나 유럽연합을 탈퇴한 영국 정부는 프라이버시 법을 개정할 것이라고 최근 발표했다. 이는 브렉시트(Brexit) 이후의 무역 성장을 촉진하기 위한 노력의 일환이며 “그저 체크 박스에 체크만 하는데 그치지 않고 상식에 기초한 법”으로 개선할 것이라고 취지를 밝혔다.

89) <https://mediasmarts.ca/mlw-teachers-hub>

유럽연합의 ‘일반 개인정보보호법(General Data Protection Regulation)’은 1995년의 ‘개인정보보호지침(Data Protection Directive)’을 개선하고 강화한 법률로 개인의 프라이버시 권리를 강조하고, 개인정보를 수집하는 기업에 대해 투명성과 더불어 필요한 경우 개인정보 삭제를 요구할 수도 있다. 또 회원국별로 다른 프라이버시 법을 제정하도록 허용한 지침과 달리, 모든 회원국에 동일한 규칙을 적용하며, 개인정보 침해에 따른 벌금을 대폭 높여 법적 강제력을 한층 강화했다. 따라서 자동으로 영국의 프라이버시 법이 되었던 GDPR는 영국이 유럽연합을 탈퇴하는 순간 효력을 잃은 셈이 되지만, GDPR에 맞춰 2018년 영국 의회가 개정한 ‘개인정보보호법(Data Protection Act)’은 계속 유효하다. 영국은 이 법을 다시 개정하겠다는 복안이다.

영국 정부의 법 개정 결정은 브렉시트의 상징성을 강조하기 위해서도 필요한 조치로 보인다. 하지만 다른 한편, 프라이버시법 개정의 한계도 명백할 것으로 보인다. 유럽연합 회원국들과 정상적인 무역 관계를 유지하고 개인정보를 원활하게 공유하기 위해서는 GDPR과의 적정성(adequacy)을 인정받아야 하기 때문이다. 영국 정부가 GDPR 전반을 비판하기보다 쿠키 수집 내용을 알리면서 이용자의 동의를 구하는 배너의 비효율성을 지적하는 데서 드러나듯 영국 프라이버시 법 개정은 실질이나 보호원칙에 칼을 대기보다, 이용자의 현실적 편의성을 높이는 쪽에 치중할 것으로 전망된다.

1) 파이브라이츠 재단(5Rights Foundation)

“아동은 성숙기에 도달할 때까지 아동이다, 스마트폰을 집어들 때까지가 아니라90).”

“아동의 권리는 그것이 얼마나 불편을 끼치든, 선택 사항이 아니다.”

파이브라이츠재단 웹사이트에 나와 있는 이 같은 선언은 재단의 의도와 목적을 잘 보여준다. “현재 10억 명 이상의 어린이와 청소년이 온라인을 이용한다. 매일

90) <https://5rightsframework.com/>

또 다른 17만 명이 생애 처음으로 온라인에 접속한다”는 말로 온라인 환경이 이미 중요한 현실이 되었음을 지적한다. 재단의 비전은 ‘아동과 청소년에게 적합한 디지털 세계, 이들이 창의적으로, 충분한 이해를 가지고, 두려움 없이 접속할 수 있는 디지털 세계’를 건설하자는 것이다. 재단의 설립자이자 의장인 비반 키드론(Beeban Kidron)은 영화 제작자이자 영국 상원의원으로 2012년 영국 아동의 인터넷 사용 실태를 다룬 다큐멘터리 ‘인리얼라이프(InRealLife)’를 감독하면서 온라인 상의 아동 보호 운동을 본격 시작했다. 9월 2일부터 시행되는 ‘연령적합 설계 규약(Age Appropriate Design Code)’의 입법을 주창하고 주도한 주인공이기도 하다. 모두 15가지 표준으로 구성된 설계 규약은 아동의 이익을 최우선으로 내세워, 온라인 서비스 제공사의 데이터 수집과 이용은 최소화 하되 서비스에 대한 접근은 최대화한다. 서비스 제공에 반드시 필요한 데이터만을 최소한으로 수집 및 저장하고, 아동의 개인정보를 공유해야 할 이유가 없는 한 데이터 공유를 금지하며, 18세 이하 아동에 대해서는 프로파일링기능의 해지를 기본 설정으로 삼아야 한다. 이를 어기는 경우 GDPR의 프라이버시 침해 벌금과 같은 규모의 과징금을 물게 된다.

파이버라이츠(5 rights)라는 재단의 이름은 아동과 청소년이 온라인에서 보장 받아야 할 5개 권리⁹¹⁾를 지칭한다. 권리들은 다음과 같다.

1. 온라인에 올린 내용을 쉽게 지울 수 있는 삭제의 권리(Right to Remove).
온라인에서 개인은 자신의 공간과 활동 내역을 의식적으로 통제할 수 있어야 한다. 이는 개인의 프라이버시 보호와 밀접하게 연계되는 대목이다.
2. 온라인에서 내 개인 데이터를 누가, 왜, 어떤 부분을, 무슨 목적에 사용하는지 알 권리(Right to Know). 그와 같은 데이터 교환에 참여할지에 대해 의미 있는 선택을 내릴 수 있어야 한다.
3. 안전의 권리(Right to Safety and Support). 불법행위는 법적 처벌을 받아야 하지만, 온라인에서 청소년의 마음을 쪼먹고 괴롭히는 정보나 활동은 불법으로

91) <https://5rightsframework.com/the-5-rights/>

규정하기 어려운 경우가 많고, 그에 대한 지원도 드물고 열악하다. 아동·청소년이 온라인에서 안전하게 활동할 수 있는 지원이 필요하다.

4. 인지되고 의식적인 사용의 권리(Right to Informed and Conscious Use). 도박장의 슬롯머신처럼 청소년의 집착과 중독을 유발하도록 설계된 기술을 사용하는 것은 비윤리적이고 비민주적이다. 기업들은 특정 기술이나 서비스, 제품의 그런 성격을 이용자에게 명확히 알려야 한다.
5. 금융 리터러시 권리(Right to Financial Literacy). 자동차 보험부터 가계 재무 관리까지, 금융 리터러시는 청소년이 자신이 이용하는 기술의 목적을 이해한다는 뜻이다. 이는 충분한 이해력을 갖춘 소비자로서뿐 아니라 창작자로, 온라인 기여자로 성장하기 위한 기본 토대다.

이 중 1, 2, 3번 항목은 온라인 프라이버시의 권리와 직접 연계된다. ‘연령 적합 설계 규약’에서 드러나듯, 파이브라이츠 재단은 디지털 세계의 구조적 변화를 꾀한다. 재단 측은 “디지털 세계는 지금까지 아동들의 성장 환경으로 진지하게 고려된 적이 없었다”면서, “그것은 어른이 어른을 위해, 모든 이용자들은 동등하다는 전제로 발명한 것이다. 하지만 모든 이용자를 동등하게 취급한다면 어린이와 청소년 역시 어른으로 취급된다”라고 강조한다. 재단은 (1) 아동과 청소년이 온라인에서 안전하게 자신을 표현하고 자아를 실현하기 위한 실질적 규제와 국제 협약을 옹호하고, (2) 세계 곳곳의 공학자, 정책전문가들과 제휴해 기술 표준과 프로토콜을 개발하며, (3) 재단이 우선순위로 내세운 서비스 설계 문제, 온라인의 아동 보호, 아동과 청소년의 권리 신장, 그리고 데이터 리터러시를 주제로 한 연구서와 가이드를 펴낸다.

‘파이브라이츠 재단’은 온라인에서 아동을 보호할 수 있는 문화적, 기술적, 법률적 조건을 개발하는데 필요한 단계를 설정하기 위해 ‘글로벌 아동 온라인 보호정책 핸드북(Global Child Online Protection Policy Handbook)’을 만들고 있다. 핸드북은 온라인 환경에서 아동을 적절히 보호하는 데 필요한 로드맵, 모범 사례, 바람직한 행동양식 등을 소개해 나라별 편차와 간극을 줄이는

데 주안점을 두고 있다.

15개월 예정의 이 프로젝트는 알바니아, 가나, 요르단, 페루, 베트남 등 참여 의사를 밝힌 나라들과 협력해 온라인상의 여러 아동 학대 문제를 협의하고 해결 방안을 논의한다. 파이브라이츠 재단은 2년전 이스트런던대학, 르완다 정부와 제휴해 ‘아동 온라인 보호 정책과 시행 계획⁹²⁾’을 개발한 바 있다. 2019년 르완다 정부가 채택한 정책과 계획은 이 프로젝트에도 기반이 될 전망이다.

2) 진화프로젝트(ProjectEVOLVE)

프로젝트이발브(ProjectEVOLVE⁹³⁾)는 온라인의 방대한 자원 창고다. 영국 인터넷안전위원회(UK Council for Internet Safety, UKCIS⁹⁴⁾)가 연구하고 개발한 프레임워크 ‘연결된 세계에 대비한 교육(Education for a Connected World⁹⁵⁾’의 내용과 긴밀히 연계해 보완자료, 연구내용, 추천활동, 전문 개발 자료 등을 모아놓았다. 개발비 일부는 유럽연합의 지원을 받았다.

프로젝트이발브에 담긴 방대한 콘텐츠를 관리하는 곳은 ‘사우스웨스트 그리드 포 러닝(South West Grid For Learning, SWGfL⁹⁶⁾)’으로 아동의 온라인 안전과 보안을 돕는 활동을 하는 비영리기관이다. 초기 화면의 메뉴는 자원(Resources), 지식 지도(Knowledge Map), 플래너(Planner), 대시보드(Dashboard)로 구성되지만 일부 메뉴는 아직 개발 중이다. 이중 자원 메뉴를 선택하면 다시 주제(strand), 연령대(Phase), 학년(Year Group), 테마(Theme), 자원(Resources)별로 나뉘어진다. 주제별 메뉴를 따라가 보면 자아이미지와 정체성, 온라인관계, 온라인평판, 온라인괴롭힘, 온라인 정보관리, 건강과 복지, 프라이버시와 보안, 저작권과 소유권 등으로 다시 나뉜다. 이 중 프라이버시와 보안을 선택하면 어떤

92) Child Online Protection Policy and Implementation Plan. <https://5rightsfoundation.com/uploads/cop-in-rwanda-report.pdf>

93) <https://projectevolve.co.uk/>

94) <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

95) <https://www.gov.uk/government/publications/education-for-a-connected-world>

96) <https://swgfl.org.uk/>

요구 사항들을 충족해야 이 분야에 대해 건전한 이해력을 갖추었다고 평가되는지 보여준다. 일종의 경쟁력 지표들의 모음인 셈이다.

프로젝트이발브의 콘텐츠는 영국의 ‘더 안전한 인터넷 센터(UK Safer Internet Centre⁹⁷)의 전문가들이 연구·개발한 내용을 바탕으로 한다. 학교와 학부모, 민간단체에서 디지털 환경에 대한 교육 커리큘럼을 짜고자 할 때 참고하고 도움을 얻을 수 있는 정보센터라고 할 수 있다.

3) 놀이 중심 설계 (Playful by Design)

‘놀이 중심 설계(Playful by Design⁹⁸)’은 특정 기관이나 단체, 서비스를 소개하는 것이 아니라 아동과 청소년의 디지털 교육과 권리 분야의 전문연구자인 소니아 리빙스톤(Sonia Livingstone) 교수와 크루아케 포통(Kruakae Pothong), 파이브라이츠 재단 설립자 비반 키드론이 공동으로 제안한 개념이다. ‘놀이 중심 설계’라는 표현은 기술이나 서비스, 제품을 설계하는 초기 단계에서 프라이버시와 안전 대책, 보안 방안을 강구하고 내장해야 한다는 개념의 ‘프라이버시 중심 설계(Privacy by Design), ‘안전 중심 설계(Safety by Design), ‘보안 중심 설계(Security by Design)’ 등에서 영감을 얻었다. 이 개념은 아동은 선천적으로 새롭고 다른 놀이 방식을 추구하고 발견한다는 사실을 보여준 연구 결과를 바탕으로 어른이 주도, 주입하거나 몰아가는 방식이 아닌, 아동의 자유로운 사고와 창의성을 가능한 활짝 열어줄 수 있도록 놀이 환경을 조성해야 한다는 제안이다. 부주의하고 위험하게 디자인된 제품과 서비스에 대한 경계심을 일깨우는 ‘설계부터 위험한 제품이나 서비스(Risky-by-Design⁹⁹)’의 개념도 그와 연결된다.

아동·청소년의 디지털 권리와 프라이버시 보호를 위한 이 같은 연구와 접근법은

97) <https://www.saferinternet.org.uk>

98) <https://digitalfuturescommission.org.uk/blog/its-time-to-make-the-digital-world-playful-by-design/>

99) <https://www.riskyby.design/introduction>

국내에서도 참고할 만한 내용을 담고 있다고 판단된다. 디지털 환경의 권리와 혜택, 위험에 대한 연구를 장려, 지원하는 ‘디지털 미래 위원회(Digital Futures Commission¹⁰⁰)’나 ‘인터넷안전위원회’같은 공공 기관의 업무와 활동 내용 또한 주목할 만하다. 또 하나 언급할 만한 기관은 영국의 개인정보 보호를 규율하는 독립 기구인 ‘영국정보위원회(ICO¹⁰¹)’이다. 영국의 개인정보보호법을 유럽연합의 GDPR과 동등한 수준이 되도록 개정하고 준수 여부를 감독하는 ICO는 9월부터 발효된 ‘연령적합 설계규약’ 마련에 주도적 역할을 했다. 영국정부가 브렉시트를 계기로 GDPR과 구별되는 영국만의 개인정보보호법을 만들겠다고 선언한 만큼 그런 개정 작업의 한 축인 ICO에 쏟아지는 세간의 관심도 높아질 것으로 보인다.

5. 호주의 프라이버시 교육

1) 아동과 미디어 위원회(ACCM)

호주의 비영리 단체인 ‘아동과 미디어 위원회(Australian Council on Children and the Media, ACCM¹⁰²)’는 ‘아동이 보는 스크린의 콘텐츠는 중요하다’라고 선언한다. 위원회는 아동과 청소년을 디지털 미디어와 스크린 미디어의 이용자로 상정한다. 그래서 극장에 걸린 영화, 넷플릭스 같은 스트리밍 서비스들에서 제공하는 아동용 영화, 스마트폰용 앱 등 아동이 이용할 만한 ‘스크린 콘텐츠’를 평가한다. 콘텐츠가 아동이 이용하기에 얼마나 적합하거나 추천할 만한지 판단한다.

위원회의 초기 메뉴에는 프라이버시도 빠지지 않는다. 앱은 이용자의 행태를 추적하므로 조심해야 한다는 메뉴, 호주의 법규는 아동의 프라이버시를 보호하는지, 그렇지 않은지 알려주는 메뉴가 포함되어 있다. 그래서 앱을 다운받으면 어떤 일이 발생하는지, 해당 앱이 아동의 개인정보를 요청하는 경우 어떻게 대응해야 하는지 등 실질적인 부분을 코치해준다. 호주에서 아동에게 추천하는 안드로이드용

100) <https://digitalfuturescommission.org.uk>

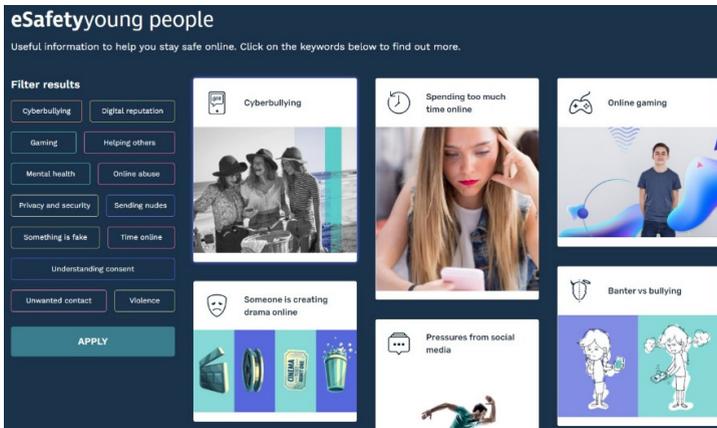
101) <https://ico.org.uk>

102) <https://childrenandmedia.org.au>

앱 50개의 목록은 덩이다.

호주도 법상으로 아동의 프라이버시 권리 보호에 구멍이 많다. 연방차원의 개인정보보호법이 있지만 아동의 프라이버시 권리를 특정하고 있지 않으며, 스마트폰 앱들이 이용자를 추적하는 행위를 명시적으로 금지하지 않으며, 이미 수집된 아동의 개인정보에 대한 삭제 요구의 권리도 없다. 15세 미만의 아동에 대해서는 개인정보를 수집하기 전에 명시적 동의를 얻어야 한다고 요구한 점은 다른 나라의 개인정보보호법과 별반 다르지 않다.

2) 온라인 안전 위원회(eSafety Commissioner)



[그림 4-3] 호주 온라인 안전위원회

‘온라인 안전위원회(eSafety Commissioner¹⁰³)’는 호주가 아동과 청소년의 디지털 권리나 교육에 특별히 더 관심을 쏟는다는 증거처럼 보인다. 이들은 여러 산하 기구와 프로젝트, 연구 활동을 통해 더 효과적인 아동의 디지털 권리와 프라이버시 보호 대책을 모색한다.

온라인 안전 위원회는 교육자, 부모, 아동, 청소년, 여성, 노인 등과 같이, 메뉴를 대상 관객에 맞춰 설정했다. 이 중 청소년 메뉴를 누르면 청소년들이 공감할 만한

103) <https://www.esafety.gov.au/>

여러 온라인 이슈를 화면 왼쪽에 버튼 모양으로 제시해 놓았다¹⁰⁴). 사이버불링, 게이밍, 온라인학대, 누드사진 전송, 가짜정보, 폭력 등이 여기에 들어 있다. 프라이버시와 보안도 물론 그 중 하나다. 프라이버시와 보안을 선택하면 ‘온라인 계정을 안전하게 관리하는 방법’과 ‘신원(identity)을 보호하는 방법’ 두 메뉴로 이어진다. 온라인 계정을 안전하게 관리하는 방법으로 나온 조언은 이렇게 요약된다¹⁰⁵).

- 주로 사용하는 소셜미디어 사이트/앱의 프라이버시 설정 내용을 정기적으로 점검해, 내 의도대로 설정되어 있는지 확인하라.
- 남들이 짐작하기 어렵게 비밀번호를 만들고, 오래된 비밀번호는 바꿔라.
- 비밀번호를 남에게 알려주지 말라.
- 앱과 소프트웨어를 최신 버전으로 업데이트해 보안 취약성을 최소화하라.
- 오프라인에서 만난 적이 없는 사람을 온라인 친구로 받아들이지 말라.
- 웹사이트나 앱이 개인정보를 묻는다면 허위나 가짜가 아닌지 확인하라.
- 광고회사들이 당신의 개인정보에 접근할 수 있다는 점을 명심하라.

한편 자신의 신원을 보호하는 방법은 다음 몇 가지로 요약된다. 프라이버시 보호와 연계된 만큼 온라인 계정 관리법과 겹치는 대목이 있다.

- 남들이 짐작하기 어렵도록 강력한 비밀번호를 설정하라.
- 쿠키를 지워라.
- 웹을 브라우징하는 동안은 소셜미디어 사이트와 이메일을 로그아웃하라. 당신의 행태가 추적될 수 있다.
- 브라우저의 사용 방식을 비밀(incognito)모드로 설정하라. 이는 당신의 브라우징 내역이 기록되지 않는다는 뜻이다.
- 페이스북이나 구글 같은 소셜미디어 사이트의 ID와 비밀번호를 사용한 ‘소셜 로그인’을 삼가라.

104) <https://www.esafety.gov.au/young-people>

105) <https://www.esafety.gov.au/young-people/keeping-your-online-accounts-secure>

- 스마트폰 설정을 강화하라.
- 가능한 최소한의 개인정보를 제공할 수 있도록 의식적으로 노력하라.
- 소셜미디어 사이트나 빅테크들은 이용자에게 알리지 않은 채 설정을 바꿀 때가 있다. 정기적인 ‘디지털 검진’이 필요한 이유다.

3) 디지털 차일드(Digital Child)

디지털 차일드(Digital Child¹⁰⁶)의 정식 명칭은 ‘호주 디지털 차일드 연구위원회 센터(Australian Research Council Centre of Excellence for the Digital Child)’로 아동에게 긍정적인 디지털 유년기를 제공하는데 중점을 둔 연구센터이다. 이들의 비전은 아동이 급변하는 디지털 세계에 건강하게 적응하고 이를 현명하게 활용할 수 있도록 도와주는 것이다.

이 기관의 대표 연구 프로젝트는 어린이가 있는 3천 가구를 대상으로 출생부터 8세까지 어떤 잠재적 문제가 있는지, 특히 유년기에 디지털 기술로 충족되지 않는 부문은 무엇인지 지근거리에서 연구하는 작업이다. 어린 시기에 디지털 기술과 환경을 적용하는 것이 이들의 건강과 교육, 연결성에 어떤 영향을 미치는지 파악하고자 한다.

아동의 디지털 복지, 온라인 프라이버시와 관련된 사안에 대한 논평도 주요 업무 중 하나이다. 가령 최근 인스타그램이 아동 보호를 명분으로 프라이버시를 업데이트한 내용(박스 글 참조)을 두고 디지털 차일드는 “프라이버시 업데이트의 내용은 전체적으로 긍정적이지만, 13세 이하의 아동을 대상으로 한 앱을 계획하고 있다는 발표는 결국 인스타그램이 아동의 안전이나 프라이버시 보호보다 회사의 수익을 우선한다는 사실을 입증하는 것”이라고 비판했다.

4) 리셋 오스트레일리아(Reset Australia)

리셋 오스트레일리아(Reset Australia¹⁰⁷)는 호주의 민주주의에 대한

106) <https://www.digitalchild.org.au>

107) <https://au.reset.tech>

디지털 위협을 판별, 해소하는데 목적을 둔 비영리기관이다. 이들의 활동은 두 갈래로 나뉜다. 하나는 주로 실리콘밸리의 빅테크 기업의 비즈니스 활동이 호주의 법제를 준수 하고, 공정한 규칙과 기준을 따르도록 압력을 넣는 작업이고, 다른 하나는 인터넷과 소셜미디어, 빅테크가 사회적으로 어떤 부작용을 낳는지, 그에 대한 대응책은 무엇인지 대중에게 설득하는 작업이다.

아동의 안전에 대한 온라인 위협은 리셋이 디지털 환경의 주요 위협 요소 중 하나이다. 인터넷에서 소비되는 악성 콘텐츠, 특히 거짓정보와 음모 이론들은 빅테크와 소셜미디어 플랫폼의 알고리즘을 통해 억제되는 것이 아니라 오히려 증폭되고 있다고 리셋은 지적한다. 그리고 부모들이 자녀에게 제공되는 콘텐츠의 성격을 제대로 파악하지 못할 때가 많으며, 유해콘텐츠에 대한 노출을 적절히 규제하거나 제한할 능력이 없다. 리셋은 이런 부분을 대중에게 홍보하는 한편, 어떻게 디지털 감시와 데이터 프로파일링, 행태에 기반한 표적 광고가 사회적으로 부정적 영향을 미치는지 분석해 대응책을 제시하려 한다.

아동의 디지털 권리 외에 리셋이 꼽은 온라인 해악 요소들은 (1) 블랙햇 해커 같은 악의적 세력이 거짓정보를 확대 재생산해 호주의 민주주의를 훼손하는 일, (2) 온라인 이용자들의 감정에 호소하는 자극적인 허위 콘텐츠로 극단주의자들의 주의주장을 증폭하는 현재의 디지털 트렌드이다.

6. 시사점

온라인광고 분석기관인 픽셀레이트(Pixelate)의 최근 보고서에 따르면 2021년 상반기 앱 시장에서 제거된 애플용앱의 59%, 구글 안드로이드앱의 25%는 프라이버시 정책이 없는 것으로 밝혀졌다¹⁰⁸⁾. 구글의 경우 제거된 러시아산 앱의 26%가, 애플의 경우 중국산 앱의 60%가 프라이버시 정책이 없었다. 그뿐 아니라 앱스토어 등에서 제거된 구글 앱의 66%는 적어도 하나의 ‘위험한 허락’을 이용자

108) <https://venturebeat.com/2021/09/18/59-of-kids-apps-removed-from-apple-store-didnt-have-a-privacy-policy/>

에게 요구했으며, 27%는 GPS 좌표 정보, 19%는 카메라에 대한 접근을 요청한 것으로 드러났다.

제거된 앱은 총 81만3천 개로 앱 시장에서 제거되기 전까지 90억 번 이상 다운로드됐으며, 그 중 무려 86%는 12세 이하의 아동을 표적으로 삼았던 것으로 밝혀졌다. 더욱이 일단 이용자의 스마트폰에 설치된 앱은 애플앱스토어나 구글 플레이에서 제거된 뒤에도 여전히 남아 사용될 위험성이 지적되었다.

이러한 자료는 아동과 청소년이 디지털 환경에서 어떤 위험에 노출될 수 있는지 잘 보여준다. 정부 기관과 비영리 프라이버시 권익 단체, 디지털 교육 서비스 기관 등이 적극 공조해 대응해야 할 필요성도 그만큼 더 절박하다. 특히 디지털 프라이버시에 관한 한, 캐나다와 미국, 영국의 사례가 보여주듯이 개인정보보호 위원회나 온라인 안전위원회의 주도 아래 커먼센스미디어나 디지털스마트츠 같은 비영리단체들이 일선 학교와 학부모단체와 협력해 아동-청소년의 연령대에 맞는 교육 커리큘럼을 개발하고 실험하고 서로 공유하면서 개선하는 일은 끊임없이 변화하는 디지털 환경에 대응하는 최선의 접근법으로 보인다.

• 빅테크의 아동·청소년 개인정보 대책

최근 주요 테크 플랫폼들이 잇따라 아동의 온라인 안전, 특히 아동 개인정보의 사용과 보호를 보장하기 위한 대책을 내놓았다. 전세계에 공통으로 적용되는 만큼 한국도 그런 대책의 혜택을 받게 된다. 이런 변화의 배경에는 북미와 유럽연합에서 아동의 온라인 보호를 위한 여러 규제안이 작용한 것으로 보인다. 특히 GDPR와 연계해 영국에서 발표한 '아동 규약(Children's code)' 혹은 '연령 적합 설계 규약(age appropriate design code)'은 기본적으로 아동과 청소년에 대해서는 특별한 배려와 더 엄격한 수준의 프라이버시 보호가 필요하다는 점을 전제로 한다. 예를 들면, 이용자가 아동이나 청소년인 경우 그들의 정확한 위치 정보를 노출해서는 안 된다. 그들을 위험에 노출할 수 있기 때문이다. 또 이들의 정보를 경제적, 상업적으로 악용해서는 안 된다. 틱톡과 인스타그램은 신원미상의 성인이 16세 이하 미성년자에게 직접메시지(DM)를 보낼 수 없게 했다. 유튜브는 성인용 콘텐츠에 대해 연령검증 절차를 거치도록 했다.

• 페이스북과 인스타그램

페이스북과 인스타그램은 7월말 ‘청소년 이용자들에게 더 안전하고 더 사적인 경험’을 제공한다는 취지로 플랫폼에 변화를 꾀했다. 16세 이하 이용자들에게는 ‘디폴트’로 비밀 계정(private account)을 부여함으로써 본인이 직접 설정에 가서 정보공유 수준을 바꿀 때까지 정보가 공개되지 않도록 만들었다. ‘잠재적으로 수상한 계정’을 가진 사람들에게 대한 제한규정도 강화했다. 이를테면 ‘청소년 이용자에 의해 차단’을 당했거나 신고된 성인 이용자의 계정’이 그런 경우다.

페이스북은 또 청소년 대상 광고의 기준도 바꿨다. 18세 이하 이용자들은 인스타그램에서 오직 ‘나이, 성별, 그리고 위치’에 기반한 광고만을 보게 된다. 훨씬 더 정교하고 세분화된 페이스북의 감시와 추적 틀은 광고주들에게 제공되지 않는다. 인스타그램은 이런 결정의 배경으로 “이용자들은 자신들의 관심사나 다른 웹사이트와 앱들에 남긴 활동 기록을 바탕으로 한 광고들을 보고 싶어 하지 않으며 … 청소년들은 이런 유형의 결정을 내리기에 아직 충분히 성숙하지 않았기 때문”이라고 밝혔다. 그간 수많은 비판을 받으면서도 타깃 광고의 유해성을 인정하지 않았던 페이스북이 돌연 이런 결정을 내린 배경에 관심이 쏠리지만, 대체적인 관측은 정부의 강경한 규제 방침에 대응한 결과라는 것이다.

하지만 아동·청소년의 온라인 안전을 부르짖는 비영리단체들은 페이스북이 그보다 한 발 더 나아가야 한다고 강조한다. 이들은 인스타그램이 13세 이하 아동을 이용자로 받아들이는 것 자체를 반대한다. 아동은 놀고 배우고 사귄 수 있는 창의적 공간이 필요하며 인스타그램의 콘텐츠와 구조는 그에 적절하지 않다는 주장이다. 여기에는 인스타그램을 사들인 페이스북의 여러 부정적 전력, 특히 프라이버시 보호를 등한시한 여러 스캔들도 한몫한 것으로 보인다.

최근 <월스트리트저널>이 심층보도려 화제가 된 ‘페이스북 파일(The Facebook Files)’은 소셜미디어의 상징인 페이스북과 인스타그램이 사회적으로 얼마나 심각한 부작용을 초래하는지 잘 보여준다(2021. 9). 그중 아동과 청소년에게 미치는 영향만 추려보면, 10대 소녀 10명 중 3명꼴로 인스타그램을 사용하면서 자신의 신체에 대해 열등감을 갖는다고 대답했다. 또 자살 충동을 느끼는 영국 청소년의 13%, 미국 청소년의 6%는 그 원인이 인스타그램 사용에 있는 것으로 파악됐다.

• 구글과 유튜브

유튜브도 놀랄만큼 페이스북과 비슷한 변화 방침을 발표했다. 10대 청소년 이용자에 대한 기본 프라이버시 설정을 바꾼 것이다. 이제 18세 이하 이용자가 올리는 비디오는 공유되지 않는 비밀(private) 상태가 디폴트여서, 이를 더 널리 공개하려면

본인 스스로 설정을 찾아가 공유 수준을 바꾸도록 했다. 광고에 대한 제한도 강화되어, ‘지나치게 상업적인 콘텐츠’는 유튜브키즈에 올라가지 못한다. ‘아동에게 적합하다’(made for kids)라고 명시된 경우라도 유료 광고를 포함한 콘텐츠는 유튜브키즈에 올릴 수 없다.

또 하나 유튜브에 더해진 것은 ‘디지털 웰빙’ 기능이다. 유튜브는 “13-17세의 모든 이용자들에게는 잠시 휴식을 하라거나 잠잘 시간임을 알려 지나치게 오랜 사용을 자제시키는 한편, 자동으로 연속 재생되는 ‘오토플레이(autoplay)’ 기능도 디폴트로 꺼놓을 것”이라고 밝혔다. 물론 이런 기능들은 언제든지 이용자가 바꿀 수 있지만 유튜브가 개선한 디폴트 설정은 의미가 크다.

- 틱톡(TikTok)

틱톡은 다양한 아동 안전 대책을 발표하면서 그 중 하나로 청소년 이용자들이 취침 시간을 넘어 공지를 받을 수 없게 한 결정을 내세웠다. 틱톡의 발표는 영국이 1년의 유예 기간을 거쳐 2021년 9월2일부터 시행하기로 한 ‘연령 적합 설계 규약’(Age Appropriate Design Code)과 연관된 것으로 보인다.

틱톡은 더 이상 13-15세 연령대의 이용자들에게는 밤 9시 이후에 아무런 푸시 공지도 하지 않는다. 16-17세의 경우는 10시 이후다. “청소년 이용자들이 일찍부터 긍정적인 디지털 습관을 붙일 수 있도록 도와주려는 의도”라고 틱톡의 아동안전공공 정책 책임자는 말했다. 이런 변화는 앞서 중국의 아동 이용자들이 밤 10시 이후에 게임을 할 수 없도록 차단한 텐센트(Tencent)의 조치와 비견된다. 하지만 아동이 어른인 척 가장하는 것을 막기 위해 얼굴인식 기술까지 동원하기로 한 텐센트와 달리, 틱톡은 거기까지는 나가지 않았다.

그밖에도 틱톡은 아동 이용자들을 보호하기 위한 여러 조치를 발표했다. 16-17세 사용자들의 DM 기능은 디폴트로 꺼놓아서 본인이 직접 설정에 들어가 켜야만 쓸 수 있게 했으며, 16세 미만은 아예 쓸 수 없도록 막아버렸다. 그리고 모든 16세 미만 사용자들은 비디오를 올릴 때 누가 이를 볼 수 있는지 명시적으로 선택하게 해 의도치 않게 공개해버리는 사태를 최소화했다.

아동·청소년 권의 단체들은 주요 소셜미디어의 이런 움직임을 환영하면서도, ‘연령 적합 설계규약’ 같은 정부기관의 압력이 나온 다음에야 떠밀리듯 보호 대책을 내놓은 데 대해서는 비판적이다. 이들은 소셜미디어 플랫폼들이 아동·청소년 이용자 보호에 지금보다 더 적극적으로 나서야 한다고 주문한다. 아동·청소년 정보를 비즈니스에 활용하려 하기보다 신원미상의 성인이 미성년이용자에게 DM을 보낼 수 없도록 차단하는 식의 구체적 아동보호 대책이 더 실효성 있다는 주장이다.

제2절 • 국내 아동·청소년 개인정보 교육

1. 학교 교과 교육의 현황과 내용

1) 학교의 개인정보 교육

국내 개인정보 교육은 초등학교와 중학교 등 의무교육 차원에서 이뤄지고 있다. 2015년 개정 교육과정에서 소프트웨어 교육이 강화되면서 중학교에 '정보'교과가 신설됐고, 초등학교 실과(17시간)와 중학교 정보교과(34시간)에서 정보(Informatics) 관련 수업이 시행 중이고, 교과 내용 중 하나로 개인정보 보호 교육이 이뤄지고 있다(2018년 중학교 1학년부터 시행). 고등학교에도 정보 교과가 있으나 선택 과목이어서, 학교의 개인정보 교육은 초중학교가 전부이다.

중학교 '정보'는 초등 5~6학년군 '실과'에서 이수한 소프트웨어 기초 소양 교육을 바탕으로 중학교 1~3학년에서 이수하며, 고등학교 일반 선택과목인 '정보' 및 과학계열 전문교과 I 과목인 '정보과학'의 선수 과목으로서 연계성이 있다. 이 장에서는 중학교 정보 교과를 중심으로 의무교육에서 이뤄지는 개인정보 교육에 대해 다루고자 한다.

〈표 4-1〉 학교급별 '정보' 교육 상황

학교급	정보교육 과정	필수 이수시간
초등	실과 통합·편재	연 17시간 이상
중등	정보교과	연 34시간 이상
고등	정보(일반 선택)	-

2) 중학교 정보 교과의 개인정보 교육¹⁰⁹⁾

중학교 정보 교과 내용은 '정보문화', '자료와 정보', '문제 해결과 프로그래밍',

109) 실과(기술·가정)/정보과 교육과정[교육부 고시 제2015-74호 [별책10], 2015.9.23]

‘컴퓨팅 시스템’ 영역으로 구분되며, 정보 교과에서 추구하는 교과 역량은 ‘정보 문화소양’, ‘컴퓨팅 사고력’이고, 역량별 의미와 하위 요소는 <표3-2>와 같다. ‘정보문화’와 ‘자료와 정보’ 영역은 정보사회 구성원으로서 갖추어야 할 기본 소양을 증진하는 데 중점을 두고, ‘문제 해결과 프로그래밍’, ‘컴퓨팅 시스템’ 영역은 컴퓨터과학을 토대로 한 실생활 및 다양한 학문 분야의 문제해결 능력을 신장하는데 중점을 둔다.

‘정보문화소양’은 정보사회의 가치를 이해하고 정보사회 구성원으로서 윤리의식과 시민의식을 갖추고 정보기술을 활용해 문제를 해결할 수 있는 능력으로, ‘정보윤리의식’, ‘정보보호능력’, ‘정보기술활용능력’을 포함한다. ‘정보문화’에서는 정보기술의 발달로 인한 개인의 삶과 사회의 변화를 분석해 관련 진로와 직업 변화를 탐색, 정보사회에서 소프트웨어의 중요성과 가치를 인식하게 하고, 정보 윤리의식과 정보보호능력을 함양하기 위해 개인정보 보호, 저작권 보호, 사이버 윤리 실천 방안을 탐색, 실천에 중점을 둔다고 소개하고 있다.

<표 4-2> 2015년 개정 교과 중학교 정보교과 내용체계

영역	핵심 개념	일반화된 지식	내용 요소
정보 문화	정보사회	정보사회는 정보의 생산과 활용이 중심이 되는 사회이며, 정보와 관련된 새로운 직업이 등장하고 있다.	• 정보사회의 특성과 진로
	정보윤리	정보윤리는 정보사회에서 구성원이 지켜야 하는 올바른 가치관과 행동 양식이다.	• 개인정보와 저작권 보호 • 사이버 윤리
자료와 정보	자료와 정보의 표현	숫자, 문자, 그림, 소리 등 아날로그 자료는 디지털로 변환되어 컴퓨터 내부에서 처리된다.	• 자료의 유형과 디지털 표현
	자료와 정보의 분석	문제 해결을 위해 필요한 자료와 정보의 수집과 분석은 검색, 분류, 처리, 구조화 등의 방법으로 이루어진다.	• 자료의 수집 • 정보의 구조화
문제 해결과 프로그래밍	추상화	추상화는 문제를 이해하고 분석해 문제 해결을 위해 불필요한 요소를 제거하거나 작은 문제로 나누는 과정이다.	• 문제 이해 • 핵심요소 추출
	알고리즘	알고리즘은 문제 해결을 위한 효율적인 방법과 절차이다.	• 알고리즘 이해 • 알고리즘 표현

영역	핵심 개념	일반화된 지식	내용 요소
	프로그래밍	프로그래밍은 문제의 해결책을 프로그래밍 언어로 구현해 자동화하는 과정이다.	<ul style="list-style-type: none"> • 입력과 출력 • 변수와 연산 • 제어 구조 • 프로그래밍 응용
컴퓨팅 시스템	컴퓨팅 시스템의 동작 원리	다양한 하드웨어와 소프트웨어가 유기적으로 결합된 컴퓨팅 시스템은 외부로부터 자료를 입력받아 효율적으로 처리해 출력한다.	<ul style="list-style-type: none"> • 컴퓨팅 기기의 구성과 동작 원리
	피지컬 컴퓨팅	마이크로컨트롤러와 다양한 입·출력 장치로 피지컬 컴퓨팅 시스템을 구성하고 프로그래밍을 통해 제어한다.	<ul style="list-style-type: none"> • 센서 기반 프로그램 구현

[9정01-01] 정보기술의 발달과 소프트웨어가 개인의 삶과 사회에 미친 영향과 가치를 분석하고 그에 따른 직업의 특성을 이해해 자신의 적성에 맞는 진로를 탐색한다.

[9정01-02] 정보사회 구성원으로서 개인정보와 저작권 보호의 중요성을 인식하고 개인정보 보호, 저작권 보호 방법을 실천한다.

[9정01-03] 정보사회에서 개인이 지켜야 하는 사이버 윤리의 필요성을 이해하고 사이버 폭력 방지와 게임·인터넷·스마트폰 중독의 예방법을 실천한다.

정보문화의 성취기준으로 “개인정보 유출로 인한 피해 사례 조사를 통해 개인정보 보호의 중요성을 인식하고 개인정보를 관리하고 보호하기 위한 방법을 알고 실천할 수 있어야 한다. 저작물의 개념과 저작물을 보호해야 하는 이유를 알고 디지털 저작물을 올바르게 이용하기 위한 방법을 찾아 실천할 수 있어야 한다”고 설명하고 있다. 교수학습 방법으로 “개인정보 유출로 인한 피해 사례를 조사하고, 각 사례별 문제점에 따른 개인정보 보호 실천 방안을 수립하도록 한다”고 되어 있다.

3) 중학교 정보교과 개인정보 교육에 대한 평가

2015 개정 교육과정에서 중학교의 정보 교과가 신설되었으나, 초등학교와 고등학교는 정보 교과가 별도로 존재하지 않고, 다른 교과에 통합되어 있거나 선택과목으로 되어 있는 등 교육의 연결성 차원에서 정보 교과에는 한계가

존재한다. 초등 실과수업의 경우 5-6학년에서만 이뤄지고, 초등학교 6년 동안 17시간 밖에(전체 수업 시수 중 0.3%) 확보되지 않아 대부분의 초등학교에서 정보교육이 제대로 이뤄지고 있다고 보기 어렵고, 실과에서 교육 분야를 ‘가정 생활’과 ‘기술의 세계’로 구분해 중학교 ‘기술’과 ‘가정’과 연계될 뿐 ‘정보’교육과의 연계성이 없고(정영식·유정수·김철, 2021), 이로 인해 내용 체계가 중복되거나 학습 요소의 위계가 맞지 않는 등의 문제가 있다(이은경, 2018).

중학교 정보교과 또한 34시간에 불과하고, 이중 개인정보 보호 교육에 할애 되는 시간은 1차시 정도로 관련 교육을 하기에 시간이 매우 부족하다. 무엇보다 정보 교과가 소프트웨어 교육 강화 목적으로 신설되어, 기술중심적 접근이 매우 강하게 드러나고 있고 이는 개인정보 이슈에 대한 서술에서도 마찬가지이다. 기술을 개인이나 사회와 유리된 것으로 보고 기술의 효과적 활용에만 관심을 두고, 그 외의 개인정보 이슈를 포함한 기술과 직접적 연관성이 없는 이슈들 단순한 도덕의 문제로 치환하는 경향이 짙다. 이런 관점을 취하고 있어 성취기준에서도 개인 정보를 개인의 권리가 아닌 ‘정보사회에서 구성원이 지켜야 하는 올바른 가치관과 행동’으로 설정하고, “개인정보 유출로 인한 피해 사례를 통한 개인정보 보호의 중요성 인식”으로 정해, 보호와 피해에만 초점을 두고 있다¹¹⁰⁾.

2. 개인정보보호위원회 등의 교육 현황과 내용

현재 개인정보 침해나 해킹 사건의 처리 과정에서 법정대리인의 동의 없는 아동의 개인정보 수집 및 이용 등 아동·청소년과 관련한 다양한 개인정보 침해 문제가 나타나고 있으나 아동·청소년 개인정보가 잘 보호되고 있는지에 대한 현황 파악조차 제대로 이루어지고 있지 않다. 또한 아동·청소년 대상의 개인정보 및 프라이버시 침해 유형, 아동·청소년의 개인정보보호와 관련된 법적 권리와 사례에 따른 대처 방안 등에 대한 연구가 부족한 실정이며 자연스레 아동·청소년에

110) 학교 개인정보 교육에 대한 평가는 7장 전문가 인터뷰에서 자세하게 다루고 있다.

대한 개인정보보호 교육 또한 구체화되지 않은 상황이다(유지연, 2013).

개인정보보호 교육은 정보주체들이 개인정보 노출의 위험성을 인식하고 이에 능동적이고 주체적으로 대응할 수 있는 방법을 교육함으로써 위험한 온라인 행동을 최소화시킬 수 있다. 교육적 접근은 규제적 접근에 비해 사회적 반발이 적고 건전한 온라인 생태계 구축의 토양을 마련한다는 점에서 교육적 접근은 보다 근본적인 해결책이 될 수 있기에(염정윤·정세훈, 2019), 아동·청소년에 대한 개인정보보호 교육은 상당히 중요한 영역이라고 할 수 있다.

법률상으로는 「개인정보 보호법」 제7조의8, 제9조에 따라 개인정보보호위원회가 개인정보보호 교육을 소관 사무로 하고 있고 이를 위한 기본계획을 수립하도록 되어 있다. 실제 아동·청소년 대상으로 한 개인정보보호 및 프라이버시 교육은 주로 개인정보보호위원회와 한국인터넷진흥원에서 운영하는 개인정보보호 포털(privacy.go.kr)에서 이루어지고 있다. 개인정보보호포털에서는 상시적으로 개인정보보호 단체교육이 이루어질 수 있도록 이용자 대상 온라인 교육 프로그램을 운영하고 있으며, 현장교육이 어려운 경우 초·중·고·일반인 온라인 콘텐츠를 공동활용해 상시 교육이 진행될 수 있도록 지원하고 있다. 또한 사업자, 국민을 대상으로 온라인 교육 콘텐츠를 제공하고 있으며 어린이, 초등학교, 중학교, 고등학교, 일반인, 다국어 교육으로 분류된 교육과정과 그에 맞는 교육을 실시하고 있다. 학교에서도 활용할 수 있도록 단체 온라인 교육도 가능하도록 콘텐츠를 제공한다.

이 중 아동·청소년에 해당하는 교육과정 및 주요 내용은 다음과 같다.

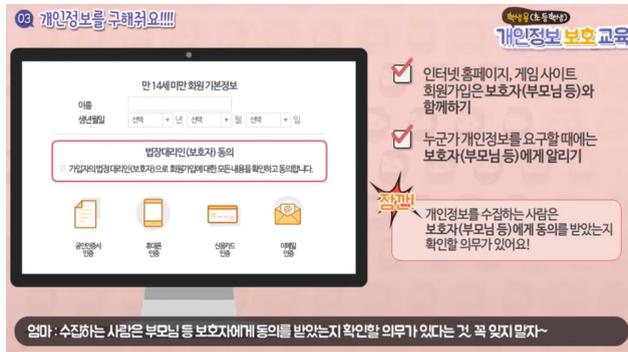
〈표 4-3〉 연령별 교육 내용(출처 : 개인정보보호 포털)

대상 및 교육과정명		주요 내용
어린이	미취학 아동	- 6-7세 어린이 대상 개인정보 유출사례 및 보호방법
학생	초등	- 초등학교 개인정보 유출사례 및 보호방법
	중등	- 중학교 개인정보 유출사례 및 보호방법
	고등	- 고등학교 개인정보 유출사례 및 보호방법

6~7세 미취학 아동에 대한 개인정보보호 교육은 크게 아동 대상 교육과 부모 대상 교육으로 나뉜다. 아동 대상 교육에서는 아동의 눈높이에서 개인정보는 어떤 것들이 있는지, 개인정보는 어떻게 악용되는지 교육하고 궁금한 사항이 있거나 문제가 생길 경우 부모님께 물어보도록 교육해 개인정보에 대한 최소한의 자각을 갖도록 하는 것을 교육의 목표로 삼고 있다. 또한 아동의 눈높이에 맞게, 개념 교육보다는 만화를 통한 사례 위주로 이해할 수 있도록 교육을 수행한다. 개인정보로 발생하는 범죄의 예시를 보여주면서 개인정보를 활용하거나 공유할 때 허락을 구하고, 모르는 사람이 개인정보를 취득하고자 할 때 어른에게 물어보는 등의 실제 사례를 보여준다. 또한 개인정보보호 관련 내용이 담긴 동요와 울동을 통해 쉽고 재밌게 이해할 수 있도록 안내한다.

부모 대상 교육에서는 부모들이 미처 인식하지 못했던 자녀의 개인정보 문제에 대해 일깨워주고 실제 아동의 눈높이에 맞게 교육을 수행하는 방안을 훈련할 수 있도록 교육하는 것에 초점을 맞추고 있다. 법률에 대한 이해보다는 아동의 개인정보가 노출되었을 시의 상황에 대해 주로 설명하고 자녀들이 개인정보가 '자신의 것'임을 이해하도록 하는 교육, 온라인 활동에 대해 부모와 자연스럽게 소통하도록 교육한다.

초등학생 대상 개인정보보호 교육은 총 3개 강의로 이루어져 있으며, 1차시는 개인정보의 개념에 대해, 2차시는 실제 개인정보 유출 사례에 대해, 3차시는 개인정보보호 방법에 대한 교육을 실시하고 있다. 마찬가지로 초등학생을 만화의 주인공으로 설정하고 유튜브 등 초등학생이 접하기 쉬운 온라인 플랫폼을 사례 대상으로 선정해 일상적이고 구체적인 예시들을 위주로 개인정보의 개념과 유출 시 위험성을 설명한다. 개인정보보호 방법으로 휴대전화 잠금설정, 개인정보 제공시 법정대리인에게 동의받기(만 14세 미만 가입), 개인정보를 쉽게 알려주지 않기, 궁금한 개인정보는 118에 전화해서 물어보기 등 기본적이고 실천 가능한 사항 위주로 교육을 수행하고 있다.



[그림 4-4] 초등학교 대상의 개인정보보호 교육콘텐츠(KISA)

중학생 대상 개인정보보호 교육 또한 초등학교 대상 교육의 큰 틀에서 벗어나지 않는 선에서 마찬가지로 중학생에 맞는 사례를 만화 형식으로 제작해 교육하고 있다. 특히 온라인게임 이용 시 개인정보보호 주의사항을 주로 다루고 있으며, 개인정보보호 방법과 관련해서는 법정대리인의 의미, 개인정보 처리방침 확인 방법 등 기본적인 법률 지식을 교육 내용에 포함하고 있었다.



[그림 4-5] 중학생 대상의 개인정보보호 교육콘텐츠(KISA)

고등학교 대상 개인정보보호 교육도 초, 중등 교육과 동일한 형식의 만화로 진행되며 인스타그램이나 중고거래 등 현실의 온라인 플랫폼 활용 사례가 교육에 활용되었다. 특히 무료 인터넷 강의 제공을 가장한 사기사이트 사례, 탈퇴한 사이트에서 개인정보 이용 또는 제3자에게 제공한 경우의 사례 등을 소개하며

정보주체가 법적으로 가지고 있는 권리들을 보다 구체적으로 설명하고 본인의 권리를 어떻게 보장받아야 하고 요구해야 하는지에 대해 더욱 자세히 교육하고 있다.



[그림 4-6] 고등학생 대상의 개인정보보호 교육콘텐츠(KISA)

아동·청소년 대상의 교육과정과 주요내용을 상세히 정리하면 다음과 같다.

〈표 4-4〉 연령별 세부 교육 내용

대상 및 교육과정명		주요 내용
어린이	미취학 아동 (아이 대상)	<ul style="list-style-type: none"> - '나의 개인정보는 소중한요' - 개인정보의 개념 (이름, 주소, 스마트폰 번호, 유치원 이름) - '이상하면 부모님, 어른들께 물어봐요' - 사례소개 1(동호수-주소-, 유치원 이름, 전화번호 묻기 등으로 얻은 개인정보로 발생하는 범죄 예시) - 사례소개 2(친구의 동의 없이 사진 찍기, 공유할 때 부모, 당사자의 허락구하기) - 사례 소개3(카톡으로 모르는 사람에게 사진 및 개인정보 알려주지 말기, 이상한 문자나 화면이 멈춘 경우 어른에게 물어보기) - 어린이 개인정보송, 울동
	미취학 아동 (부모 대상)	<ul style="list-style-type: none"> - 개인정보에 대해 설명해주기 <ul style="list-style-type: none"> • 개인정보에 포함되는 사항 쉽게, 자주, 반복 설명 • 개인정보 노출 시 일어날 수 있는 위험한 상황에 대해 이야기하기 - 개인정보가 '나의 것'이라는 것 알려주기 <ul style="list-style-type: none"> • 자녀도 개인정보 소유 주체임을 이해하기 • 개인정보 노출 위험이 있는지 확인하기 • 가족 개인정보 공유 전 부모님께 묻도록 지도하기

대상 및 교육과정명		주요 내용
		<ul style="list-style-type: none"> • 가까운 사이라도 아동 본인 또는 법정대리인의 동의 없이 아동 개인정보 노출 금지 - 온라인 활동 및 그날 있었던 일에 대해 대화하기 • 모르는 사람의 연락, 이상한 광고, 이해하기 어려운 상황이 생기면 부모님과 상담하도록 하기 • 부모와 온라인 활동에 대해 자유롭게 이야기할 수 있는 분위기 조성 해주기
학생	초등	<ul style="list-style-type: none"> - 초등학교 개인정보 유출사례 및 보호방법 - (1차시) 개인정보의 개념 - (2차시) 개인정보 침해, 유튜브 댓글 이벤트 피해사례, 모바일 메신저 사칭 피싱 사례 외 실제 초등학교 대상 개인정보 유출 사례 유형화 - (3차시) 개인정보보호 방법 <ul style="list-style-type: none"> • 휴대폰 잠금설정 • 만14세 미만, 회원가입, 이벤트 응모 등 개인정보 제공시 법정대리인에게 동의 받기 • 개인정보 알려주지 말기(sns 전체공개 금지) • 궁금한 개인정보 해결하기(118 전화하기)
	중등	<ul style="list-style-type: none"> - (1차시) 개인정보의 개념 - (2차시) 개인정보의 중요성, 중학생 맞춤 교육으로 아이디와 패스워드, 게임의 대리 결제 등의 사례와 결합해 설명, 소셜네트워크 개인정보 관련 전체공개 위험성을 다룬다. - (3차시) 개인정보 보호방법 5가지 <ul style="list-style-type: none"> • sns 개인정보 최소 등록, 개인정보 노출 유무 확인 • 만14세 미만, 회원가입, 이벤트 응모 등 개인정보 제공시 법정대리인에게 동의 받기 • 스마트폰 안전하게 사용하기(잠금설정, 개인정보저장금지) • 개인정보 처리방침 확인하기 • 궁금한 개인정보 해결하기(118 전화하기)
	고등	<ul style="list-style-type: none"> - (1차시) 개인정보 개념, sns상 개인정보 유출 예시를 통한 개념 및 유형 이해하기 - (2차시) 개인정보 유출 사례 <ul style="list-style-type: none"> • (사례1) 무료인터넷강의 제공을 가장한 사기 사이트 사례 • (사례2) 중고물품 거래시 제공한 개인정보를 통한 스미싱 사례 • (사례3) 탈퇴한 사이트에서도 개인정보 이용 또는 제3자에게 제공한 경우 - (3차시) 개인정보 관리 방법 <ul style="list-style-type: none"> • 스미싱 주의하기, 공개된 사이트에 개인정보 공개하지 않기 등

2021년 3월부터 개인정보보호위원회와 한국인터넷진흥원이 아동복지 전문기관 ‘초록우산 어린이재단’과 함께 미취학 아동과 부모를 대상으로 개인정보보호 교육 콘텐츠를 제작해 보급하고 있다. 콘텐츠는 아동편과 부모편으로 구성되었으며 미취학 아동의 눈높이에 맞춰 개발되었고, 국내거주 외국인 가족을 위해 영어로도 제작되었다. 해당 콘텐츠는 개인정보보호포털, 한국인터넷진흥원, 초록우산 어린이재단 유튜브 채널, 주니어네이버 등을 통해서 이용할 수 있다.

방송통신위원회 또한 정보통신서비스 제공사업자(개인정보취급자 등)의 개인정보 관리 역량을 통한 개인정보보호 수준 제고를 위해 교육 수강자의 특성별·수준별 맞춤형 교과과정을 개발하고 있다. 이중 정보주체이자 향후 ‘개인정보 처리자’가 될 수 있는 초·중·고등학생을 중심으로 찾아가는 개인정보보호 현장 교육을 지원한다.

3. 국내 개인정보 보호 교육에 대한 평가

아동·청소년은 스스로 개인정보를 보호하기 힘든 미성숙한 상태에 있으며 단계적인 발달을 거쳐 성인이 되는 과정이므로 발달과정에 맞춰 정보주체로서의 역량을 강화시켜주는 교육이 필요하다(이희정, 2021). 아동·청소년은 연령에 따라 발달 상태와 온라인 이용행태가 다르기 때문에 다른 관심사항을 고려해 연령별 세분화된 개인정보보호 교육이 필요하다(나종연·김지혜·한슬기, 2020).

그러나 개인정보보호위원회와 한국인터넷진흥원에서 실시하고 있는 아동·청소년 개인정보보호 교육은 1회성으로 수행하는 교육 배포자료 혹은 홍보자료 형태에 가깝다. 개인정보자기결정권은 헌법으로 보장하는 독자적 기본권이며¹¹¹⁾, 우리 법은 14세 미만의 아동·청소년들에 대해 개인정보에 대한 자기결정권 판단이 미성숙하다고 판단해 법으로서 특별히 이들의 행동을 보호하고 있다. 그러나 개인정보보호 교육을 소관 사무로 하는 개인정보보호위원회는 개인정보보호 담당자인

111) 헌재 2005.5.26. 99헌마513 결정

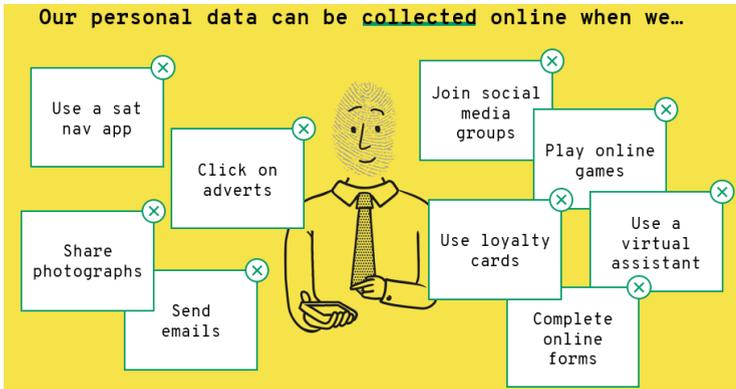
성인 대상 또는 근로자의 법정 의무로서의 교육만 진행할 뿐, 아동·청소년 연령의 정보주체를 위한 체계적이고 지속적인 개인정보보호 교육을 시행하고 있지 않다.

호주는 2021년 5월 2일 아동·청소년에게 체계적인 개인정보 관리 및 보안 교육을 필수적으로 수행하도록 하는 국가 커리큘럼 개정안을 발표했다(Sharwood, 2021)¹¹²⁾. 호주의 아동·청소년들은 5세-16세까지 연령에 따라 “실명이나 생년 월일 같은 개인정보를 아무에게나 공유하지 말 것”, “온라인에 개인정보를 기입할 때는 부모나 보호자에게 먼저 상의할 것” 등의 개인정보 취급 원칙에 대해 교육 받는다. 또한 이용자명/패스워드 사용법, 팝업창을 함부로 클릭할 때의 위험, 온라인 서비스에 의해 저장될지 모르는 개인정보의 종류, 이를 기반으로 하는 위치/신원 추적의 원리 등 개인정보에 대한 위협과 작동 방식에 대해서도 교육 받는다. 초등학교 3, 4학년이 되면 아이들은 개인정보보호에 대한 제대로 된 교육을 받기 시작한다. “온라인 서비스에 의해 저장되는 개인정보를 식별하는 방법과 위치 또는 신원이 노출되는 방식”에 대해 교육받으며, 교사들은 “온라인 게임을 할 때 별명 설정이 중요한 이유” 등에 대해 교육한다(Ropek, 2021).

영국의 정보위원회(ICO)는 초등학교 및 중학교 학생들에게 개인정보보호 기초 교육을 위한 별도의 수업용 자료를 배포하는데, 해당 자료는 개인정보의 기본 개념과 웹사이트나 모바일앱의 이용자 개인정보 활용방식을 살펴보고, 온라인에서 개인정보를 보호하기 위해 유의해야 할 사항을 숙지하도록 구성되어 있다. 이를 통해 영국의 아동·청소년들은 ‘내가 누구인지, 내가 무엇을 하는지에 관한 모든 정보’가 개인정보에 속한다는 사실과 일상적인 온라인 활동 곳곳에서 그런 정보가 어떻게 수집돼 어떤 목적으로 활용(혹은 악용)되는지를 쉽게 이해할 수 있다.(ICO, 2021, July 5)¹¹³⁾

112) 보다 자세한 내용은 https://www.australiancurriculum.edu.au/media/7126/ac_review_2021_technologies_whats_changed_and_why.pdf 참조

113) 보다 자세한 내용은 <https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/school-resources/> 참조



[그림 4-7] 영국 ICO 초중고생 개인정보보호 기초교육 자료 중 일부

이처럼 해외 주요국들은 단순히 아동·청소년과 관련된 개인정보 유출사례를 소개하고 이를 방지하는 방법을 제시하는 교육이 아니라 아동·청소년 연령에 따라 주로 이용하는 온라인 플랫폼으로부터 어떤 프라이버시 위협이 발생하는지, 이에 대한 작동원리는 무엇인지, 이러한 작동 방식이 어떻게 악용되는지 등을 연구하고 이에 대해 연령별 아동·청소년이 관련 사항에 대한 개인정보자기결정권을 행사할 수 있는 역량을 키울 수 있도록 교육하는 방식을 택하고 있다. 2020년 1월 영국 ICO가 온라인상에서 아동의 개인정보보호를 위해 인터넷 서비스에 적용해야 하는 사항들을 담아 발표한 ‘연령적합설계규약’(Age Appropriate Design Code), 18세 미만 아동이 온라인상에서 처한 위험을 분류하고, 아동이 이해하기 쉽게 간결하고 명확한 정보를 제공하기 위해 2021년 5월 OECD가 발표한 ‘디지털 환경 아동 권고안’ 등이 이러한 노력의 일환이라고 볼 수 있다.

이처럼 우리나라도 급변하는 디지털 환경에서 새롭게 발생하는 아동·청소년 대상의 프라이버시 위협에 대해 심도깊은 연구가 필요하고, 아동·청소년의 특수성을 고려한 내용들을 별도로 분리해 아동·청소년을 위한 프라이버시 보호 역량 교육을 실시할 수 있도록 해야 한다. 연내 개인정보보호위원회가 아동·청소년에 특화한 「아동·청소년 보호 가이드라인」의 제정을 추진 중인데¹¹⁴⁾, 해당 가이드라인은 온라인서비스사업자에 대한 최소한의 아동·청소년 보호지침을 제시하는 것

이외에도 아동·청소년에 해당하는 서비스이용자들에 대한 인식교육과 보호자에 대한 안내 등 개인정보보호 교육과 관련한 내용도 반드시 포함되도록 구성해야 할 것이다.

또한 아동·청소년 대상 개인정보보호 교육이 1회성·단기 교육이 아닌 연령별로 체계적·지속적 교육이 시행되기 위해서는 교육 기반도 확충될 필요가 있다. 현재 개인정보보호포털은 사업자를 대상으로 민간이 자율적으로 수행할 수 있도록 개인정보보호 교육자료를 업데이트해 배포하고 있고, 개인정보보호 전문강사 풀도 지역별, 분야별로 선발해 조회할 수 있게 하고 있다. 현재 배포·제작한 아동·청소년 개인정보보호 교육자료와 참고자료들을 지속적으로 업데이트해 배포해 민간 자율교육이 활발히 진행될 수 있도록 유도하고, 개인정보보호위원회가 강사를 연결하는 거점으로 기능할 필요가 있다. 장기적으로 아동·청소년 개인정보보호 교육의 주요 내용과 효과성 연구, 해외 제도·정책·교육 동향과의 연동 및 표준화, 연령별 교육의 체계화 연구 등이 필요하다.

114) 권수현(2021. 8. 4). 개인정보위원장 “연내 아동·청소년 개인정보보호 가이드라인 제정”. 연합뉴스. <https://www.yna.co.kr/view/AKR20210804103300530?input=1195m>(검색일: 2021.9.2.)

제 5 장

아동·청소년의 개인정보와 프라이버시 보호 규범 현황

제 5 장

아동·청소년의 개인정보와 프라이버시
보호 규범 현황

제1절 • 아동·청소년과 개인정보와 프라이버시 보호 규범

개인정보의 상업적 이용이 증가하고 있는 디지털 환경에서 아동은 개인정보 보호와 관련해 취약한 상황에 처할 가능성이 크다. 개인정보를 이용한 맞춤형 서비스나 광고의 증가는 아동을 쉽게 현혹해 상업적 대상으로 전락시킬 가능성이 있다(전윤선·나종연, 2020). 이에 세계 각국과 국제기구는 물론 국내에서도 아동·청소년의 개인정보보호권 및 프라이버시권을 보호하기 위한 여러 규범을 마련해왔다.

아동·청소년의 개인정보보호권 및 프라이버시권에 대한 일반 규범은 1948년 세계인권선언으로 대표되는 국제인권규범과 대한민국 헌법에서 기본권으로 보호하고 있는 사생활에 대한 권리 규범에서 유래한다. 특히 보호의 객체이자 권리의 주체로서 아동·청소년의 프라이버시를 보호하기 위한 규범이 함께 발전되어왔다. 한편, ICT 기술의 발전으로 개인정보에 대한 권리가 발전했고, 세계 각국은 개인 정보보호에 대한 법체계에서 아동·청소년의 개인정보를 보호하고 있다. 지방자치단체 또한 아동·청소년의 인권을 보호하기 위한 자치법규를 두고 제도적으로 보호하고자 한다.

일부 규범의 경우 전문기구를 두고 침해사건에 대한 진정 접수·조사·시정 등 구제를 담당하고 있으며, 아동·청소년의 개인정보보호 및 프라이버시 침해 문제도 함께 다루었다. 다만 대다수의 규범과 구제사례는 디지털 환경에 대한 고려가 아직 크게 반영되지 않은 것으로 나타났다. 코로나19의 확산으로 아동·청소년의 온라인 이용이 크게 늘면서 이에 대한 우려와 제도적 개입이 확대되는 모습이다.

이 장에서는 관련 규범과 구제 현황을 국제규범과 국내법제, 자치법규 수준에서 각각 살펴본다.

1. 아동·청소년의 프라이버시 보호 관련 국제 규범

1) 유엔 국제인권규범의 아동·청소년 프라이버시 보호

유엔 등 국제인권규범은 우리나라도 준수 의무가 있다. 「초·중등교육법」은 “학교의 설립자·경영자와 학교의 장은 「헌법」과 국제인권조약에 명시된 학생의 인권을 보장해야 한다”고 규정하고 있다(제18조의4). 아동·청소년의 권리에 대한 가장 권위있는 국제인권규범은 1989년 11월 20일 유엔총회에서 채택된 ‘유엔 아동권리협약(UN Convention on the Rights of the Child)’이다. 이 협약은 세계에서 가장 많은 국가들이 가입한 인권협약으로, 2019년 현재 196개국이 가입했다. 우리나라는 1991년 이 협약을 비준한 만큼, 초·중등교육법에 따른 학교의 장 뿐 아니라 국가와 지방자치단체 모두 원칙적으로 아동권리협약의 조항과 해석을 이행·준수할 의무가 있다. 또한 국내 아동의 개인정보보호 수준을 강화하기 위해 아동권리협약 등 국제인권규범을 수용해야 한다는 지적이 있어 왔다(전윤선 외, 2020). 따라서 국제인권규범에서 제시하는 아동·청소년 권리에 대한 규정과 해석을 국내 아동·청소년의 프라이버시권 보호 규범에서 실현할 필요가 있다. 특히 최근의 국제인권규범이 디지털 아동인권과 관련해 여러 기준을 제시하고 있다는 점은 주목할 만한 부분이다.

유엔 아동권리협약은 18세 미만의 사람을 ‘아동’으로 정의하는데(제1조) 미취학 아동 뿐 아니라 학령기 청소년을 포함한다. 이 협약은 아동을 성인과 마찬가지로 권리 주체로 인식했다는 점에서 큰 주목을 받았다. 다만 사회적 취약계층으로서 적절한 사회적 보호와 도움을 받을 필요가 있기 때문에 심리적, 육체적 성숙도에 따라 보호자가 대리하도록 했다.

아동권리협약에 가입한 국가의 정부는 ① 생존의 권리, ② 보호의 권리, ③ 발달의 권리, ④ 참여의 권리 등 협약에 명시된 모든 아동의 권리를 보장할 의무를 지고 있다(국가인권위원회, 2018). 이 가운데 발달의 권리와 참여의 권리는 특히 보호 대상으로서의 아동을 넘어 능동적인 권리 행사의 주체로서 아동을 강조한다.

발달의 권리는 아동이 잠재능력을 최대한 발휘하는데 필요한 권리를 말하며, 교육받을 권리, 여가를 즐길 권리, 문화생활을 하고 정보를 얻을 권리, 생각과 양심과 종교의 자유를 누릴 수 있는 권리 등을 포함한다. 참여의 권리는 자신의 생활에 영향을 주는 일에 대해 의견을 말하고 존중받을 권리를 말하며, 표현의 자유, 양심과 종교의 자유, 평화로운 방법으로 모임을 자유롭게 열수 있는 권리, 사생활을 보호받을 권리, 유익한 정보를 얻을 권리 등을 포함한다.

특히 아동권리협약 제16조는 “1. 어떠한 아동도 사생활, 가족, 가정 또는 통신에 대해 자의적이거나 위법적인 간섭을 받지 아니하며 또한 명예나 신망에 대한 위법적인 공격을 받지 아니한다. 2. 아동은 이러한 간섭 또는 비난으로부터 법의 보호를 받을 권리를 가진다”고 규정해 아동의 프라이버시권을 보호하고 있다. 아동과 보호자의 권리나 이해가 충돌할 경우에는 ‘아동 최선의 이익(Best Interests of the Child)’ 원칙을 따라야 한다. 유엔 아동권리협약 제13조에 규정된 아동 최선의 이익과 관련해 유엔 아동권리위원회는 “권리들 사이에 갈등이 발생할 경우 국가는 아동에게 최선의 이익이 되는 해결책이 무엇인가를 확인하기 위해 주의를 기울여야 한다”고 설명했다¹¹⁵⁾. 아동은 성인에 비해 자신의 이익을 강력히 주장할 수 있는 가능성이 적기 때문에, 아동의 이익이 간과되기 쉽기 때문이다. 아동 최선의 이익을 평가할 때에는 (a) 아동의 견해 (b) 아동의 정체성 (c) 가정환경의 보존 및 관계유지 (d) 아동의 돌봄과 보호 및 안전 (e) 취약한 상황 (f) 아동의 건강권 (g) 아동의 교육권을 고려해야 한다. 유엔 아동권리 위원회는 아동이 더 많이 알고 경험하고 이해할수록, 부모, 법정 후견인 또는 아동에 대해 법적 책임이 있는 여타 사람은 감독과 지도를 하는 입장에서 주의와 조언하는 입장으로 바뀌게 되고, 나아가 동등한 위치에서 의견을 교환하는 방향으로 나아가게 된다고 밝혔다. 아동이 성숙해질수록 아동의 견해에 더 많은 비중을 부여해야 한다. 이러한 고려사항은 디지털

115) Committee on the Rights of the Child (2013). General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). 유엔문서번호 CRC/C/GC/14.

환경에서 아동이 자신의 개인정보 처리에 대한 권리와 프라이버시권을 행사할 때에도 주의를 기울여야 할 요소일 것이다.

아동권리협약은 가입국이 협약의 내용을 얼마나 잘 이행하고 있는지 모니터링 하기 위해 유엔아동권리위원회를 구성해 운영하고 있다(제43조). 2019년 10월 3일 유엔 아동권리위원회는 대한민국 아동권에 대한 최종견해를 발표하면서 스마트폰 사용에 대한 권리를 비롯해 한국 아동의 프라이버시권 보호 문제를 처음으로 언급해 주목을 받았다. 이 무렵 유엔은 2016년 12월 총회에서 ‘디지털 시대의 프라이버시권 결의안’을 채택하고 디지털 시대의 프라이버시권의 침해가 여성, 아동 및 소외계층에게 특히 영향을 미친다는 점을 강조한 바 있다¹¹⁶⁾.

25. 위원회는 학교가 성적, 징계조치와 같은 학생의 개인정보를 공개하고, 학생의 사전동의 없이 소지품을 검사하며, 복장 제한을 시행하고 있다는 보고에 주목한다. 이에 위원회는 학교에서 아동의 스마트폰을 포함한 사생활 및 개인정보보호를 협약 제16조에 따라 법과 관행에서 보장하고, 사전동의를 수집함에 있어 아동 친화적인 절차를 개발하고 적용할 것을 당사국에 권고한다.

- 유엔아동권리위원회, 2019. 10. 3. 대한민국 제5·6차 정부보고서의 심의 및 최종견해

특히 유엔 아동권리위원회가 2021년 3월 발표한 일반논평 제25호는 디지털 환경에서 아동의 권리를 보장하기 위한 기준을 종합한 국제규범으로 크게 주목을 받고 있다¹¹⁷⁾. 아동권리위원회는 일반논평에서 기존의 유엔 아동권리협약이 디지털 환경에서 어떻게 이해되고 이행되어야 하는지를 개관하고, 디지털 환경에서 아동의 권리를 증진, 존중, 보호, 충족하기 위한 입법, 정책, 조치의 지침을 제시 하고자 했다(7문). 또한 디지털 환경을 아동에 대한 일방적 위협으로 간주하기 보다 아동이

116) Committee on the Rights of the Child (2019). Concluding observations on the combined fifth and sixth periodic reports of the Republic of Korea. 유엔문서번호 CRC/C/KOR/CO/5-6; 오픈넷 (2019). 유엔 아동권리위원회, 대한민국 아동의 프라이버시권에 대해 최초로 권고. <https://opennet.or.kr/16708> (검색일: 2021. 6. 30).

117) 유엔의 일반논평(general comments)은 국제조약 규정을 해석하는 기준으로 볼 수 있다.

자신의 권리와 의견 피력을 능동적으로 행사해야 하는 환경으로 보았다. 논평은 디지털 환경에서 아동의 개인정보보호권 및 프라이버시권의 보장을 위한 기준도 폭넓게 다루었는데, 아래에서는 관련 내용을 살펴본다.

우선 유엔아동권리위원회는 일반논평 제25호를 위해 전 세계 709명의 아동을 상담했는데 아동 당사자들은 디지털 기술이 자신들의 현재의 삶과 미래에 필수적이라고 보고했다(1문). 또한 아동들은 디지털 환경에 자신들이 안전하고 공정하게 참여할 수 있어야 한다는 입장을 표명했으며(3문) 동시에 디지털 환경에서 자신의 프라이버시권과 개인정보에 대한 권리 침해에 우려를 표했다.

디지털 환경에서도 모든 아동의 권리는 존중되고 보호받고 충족되어야 한다는 원칙 아래, 일반논평은 디지털 환경에서 아동권리 보장을 위한 일반원칙으로 (A)차별 금지, (B)아동 최선의 이익, (C)생명권·생존권·발달권, (D) 아동의 의견 존중을 제시했다. 특히 국가는 디지털 환경에서 아동을 보호하거나 디지털 환경에 대한 접근을 촉진하는 조치를 취할 때, 연령에 적합한 설계 등 아동이 디지털 환경에 독자적으로 참여할 수 있는 여건을 고려해야 한다(제19문). 디지털 서비스 제공업체들은 아동의 발달 능력에 적합한 서비스를 제공해야 하고(제20문), 부모와 보호자들은 아동의 발달하는 자율성, 능력, 프라이버시를 존중해야 한다(제21문).

일반논평은 기업 부문에서 아동의 프라이버시권 존중의 필요성을 강조했다. 디지털 환경과 관련된 서비스와 제품의 제공으로 아동의 권리에 직간접적인 영향을 미치는 기업은 아동의 권리를 존중하고 디지털 환경에서 아동의 권리 침해를 방지 및 구제해야하고, 국가는 이를 보장할 의무가 있다(35문). 기업은 자신의 네트워크 및 온라인 서비스가 아동의 프라이버시권 및 보호받을 권리 등을 침해하는 원인이 되거나 이를 악화시키는 것을 방지해야한다(36문). 기업이 상업광고와 마케팅을 위해 아동의 행동을 예측해 보다 극단적인 콘텐츠로 유도하는 광고를 설계하거나, 자동알림으로 수면을 방해하거나 아동의 개인정보나 위치를 이용해 유해할 수 있는 상업적 콘텐츠로 타깃팅하는 등 아동의 권리를 침해하는데 대해 특별한 주의가 요구된다(40문). 국가는 아동의 실제적 또는 추론된 특성에

대한 디지털 기록에 기반해 아동을 상업적 목적으로 프로파일링하거나 타깃팅 하는 것을 법률로 금지해야 한다. 뉴로마케팅, 감정 분석, 몰입형 광고, 가상·증강 현실 광고에 아동을 직간접적으로 참여시키는 것 또한 금지되어야 한다(42분).

아동에 대한 디지털 서비스는 아동의 개인정보 처리를 서비스 수행에 필요한 범위로 제한하는 데이터 최소화 원칙을 보장해야 하고(55분), 콘텐츠 조정과 규제는 아동의 표현의 자유와 프라이버시권 등의 보호와 균형을 이루어야 한다(56분). 국가는 필터링, 프로파일링, 마케팅 및 의사결정의 자동화된 처리가 디지털 환경에서 아동이 자신의 의견을 형성하고 표현하는 능력을 대체하거나 조작하거나 간섭하지 않도록 보장해야 한다(61분). 또한 감정분석과 추론 등 디지털 환경에서 아동의 사상과 신념의 자유를 조작하거나 간섭하는 관행을 식별, 정의하고, 금지하는 개인정보보호 규정 및 설계 기준을 도입하거나 개선해야 한다. 자동화 시스템은 아동의 내적 상태를 추론하는 데 사용될 수 있다. 자동화 및 정보필터링 시스템이 아동의 행동이나 감정에 영향을 미치는데 사용되어서 안 되고 아동의 기회나 발달을 제한하는데 사용되어서 안 된다(62분).

무엇보다 일반논평 제25호는 디지털 환경에서 아동의 프라이버시권 보호와 관련한 상세한 내용을 담았다. 일반논평은 아동을 식별하는 개인정보의 처리뿐만 아니라 자동화된 개인정보 처리, 프로파일링, 행동 타깃팅, 의무적 신원확인, 정보 필터링, 대량감시 등의 디지털 관행이 일상화되고 있어 아동의 프라이버시권에 대한 침해를 낳고, 그 부정적 결과는 아동의 삶 후반부까지 영향을 미칠 수 있다고 우려했다(68분). 국가는 개인정보를 처리하는 모든 기관과 환경에서 아동의 사생활이 존중되고 보호될 수 있도록 법률적, 행정적 및 기타 조치를 취해야 하며, 법률에는 강력한 안전장치, 투명성, 독립적 감독, 구제수단을 규정해야 한다. 아동에게 영향을 미치는 디지털 제품 및 서비스에는 프라이버시 중심 설계(privacy by design)를 적용해야 한다(70분). 아동의 개인정보 처리에 동의를 구하는 경우, 동의는 사전에 충분히 정보를 제공해 자유롭게 이루어져야 하고, 아동의 연령과 발달 능력에 따라 부모 및 보호자가 동의하도록 할 수 있다(71분). 아동의 개인정보 처리에 대한 아동, 부모 및 보호자의 열람, 정정 및 삭제권

행사가 보장되어야 하고, 아동이 사후에 개인정보 수집에 대한 동의를 철회하거나 반대할 수 있는 권리를 보장해야 한다(72문). 디지털 환경의 범위가 옷이나 장난감 등 더 많은 제품과 서비스로 확대되고 아동이 자동화된 시스템에 '연결'되는 상황인 만큼, 이러한 제품과 서비스에 개인정보 및 사생활 보호 규정과 기준을 적용해야 한다(74문). 자동화된 개인정보 처리 등 아동에 대한 디지털 감시는 프라이버시권을 존중해 일상적으로나 무차별적으로나 아동이나 부모 및 보호자의 인지 없이 이루어져서는 안 되며, 매우 어린 아동을 대상으로 해서도 안 된다. 상업시설 또는 교육과 보호시설은 프라이버시 최소 침해 수단에 대해 고려해야 한다(75문). 아동의 안전을 위해 부모 및 보호자가 아동의 디지털 활동을 감시하는 것은 아동의 상담이나 민감정보 검색을 억제할 우려가 있다. 디지털 감시는 아동의 안전과 사생활 존중 및 보호를 함께 달성해야하고 아동의 발달 정도에 따라 균형 있게 이루어져야 한다(76문).

일반논평은 그밖에도 디지털 리터러시 교육을 통해 아동이 인프라, 영업관행, 설득기법 및 개인정보 및 자동화된 처리의 이용, 감시 등 디지털 환경을 이해하고 사회의 디지털화에 따른 부정적인 영향을 이해하는 것이 점점 더 중요해지고 있다고 강조했다(105문).

이상과 같은 유엔 인권규범은 유럽연합과 영국의 개인정보보호 법체계에서 법률적인 규범으로 수용하고 있다. 유럽연합 개인정보보호 감독기관들은 아동의 개인정보 침해 여부를 판단할 때 아동 최선의 이익 등을 기준으로 인정해왔으며, 영국 개인정보보호법은 유엔 아동권리협약에 따른 영국정부의 의무를 명시적으로 규정하고 있다. 다음 절에서 유럽과 영국의 규범을 좀 더 구체적으로 살펴본다.

2. 유럽의 아동·청소년 프라이버시 보호 규범

컴퓨터와 통신 기술이 발전하면서 개인정보에 대한 디지털 처리가 크게 증가하고 이로 인한 개인정보 침해 및 오남용도 함께 늘었다. 이에 개인정보에 대한 권리를 보호하기 위한 국제규범이 꾸준히 발전해왔으며 특히 유럽평의회와

유럽연합을 위시한 유럽의 제도가 이 분야에서 두드러진 규범력을 발휘해왔다. 유럽평의회는 1981년 최초의 개인정보보호 국제협약인 108호 협약¹¹⁸⁾을 채택했는데 이 협약은 자동화된 개인정보 처리에서 정보주체를 보호하는 적절한 구제 수단 마련을 요구했다. 유럽연합 또한 1995년 <개인정보보호 디렉티브>¹¹⁹⁾를 채택함으로써 강력한 개인정보보호 법규범을 수립했고, 2000년 선포한 <기본권 헌장>에서 사생활과 가족생활의 존중에 대한 권리(제7조)와 분리해 개인정보 보호권(제8조)을 규정했다.

유럽연합과 유럽평의회는 개인정보보호에 대한 법률적 통제는 유럽연합의 개인정보보호 일반규정(General Data Protection Regulation, 이하 GDPR)에서 통일된 규범으로 수립되었다. GDPR은 역외 제3국의 개인정보보호 수준의 적정성을 평가하는 ‘적정성 평가’ 제도를 실시하며 국제규범화했다. 유럽평의회는 GDPR이 발효한 2018년 개인정보보호 국제협약을 현대화하며 GDPR과의 일치성을 더욱 높였다¹²⁰⁾. 특히 유럽에서는 인공지능 등 신기술 환경이 확산됨에 따라 이로부터 아동의 권리를 보호하기 위한 노력들이 이루어지고 있다. 이하에서는 유럽연합을 중심으로 아동의 개인정보보호에 대한 국제규범을 살펴본다.

1) 유럽연합 개인정보보호 법제의 아동 보호 규정

유럽연합에서 아동·청소년의 개인정보보호 규범을 비교적 상세히 다룬 문건으로는 제29조 실무단(Article 29 Working Party)¹²¹⁾이 2009년 발간한 <아동의 개인정보 보호에 대한 의견: 일반 지침 및 학교에서의 특수 사례(이하 ‘실무단 의견서’)>¹²²⁾를

118) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

119) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

120) Convention 108 + : Convention for the protection of individuals with regard to the processing of personal data.

121) 제29조 실무단은 개인정보보호 디렉티브에 의거해 유럽연합 개인정보보호 규정의 해석을 담당해 왔으며, 2016년 제정된 GDPR이 2018년 발효된 이후로 유럽정보보호이사회(European Data Protection Board)로 이관되었음.

122) EU Article 29 Data Protection Working Party (2009). Opinion 2/2009 on the protection

들 수 있다(김기중·임완철·장여경, 2019). 당시 실무단 의견서를 기반으로 하는 유럽연합 1995년 개인정보보호 디렉티브의 경우 아동·청소년의 개인정보 처리에 대한 명시적인 규정을 두고 있지는 않았다. 그러나 의견서는 아동 최선의 이익, 발달의 권리 등 아동의 권리에 대한 유엔 협약의 원칙을 일반원칙으로 포함하고, 공정성 등 개인정보 처리 원칙에 대한 규정에 기반해 아동의 개인정보 처리에 대해 개인정보처리자가 준수해야 할 기준을 제시했다.

우선 일반원칙으로 아동은 인간으로서 모든 권리를 누릴 수 있어야 하며, 자신의 개인정보보호에 대한 권리도 이에 포함된다. 다만 아동이 처해 있는 특수한 상황에 대해 정적이고 동적인 관점 모두를 고려해 살펴봐야 한다. 정적인 관점에서 아동은 신체적, 정신적 성숙에 아직 이르지 못한 사람인 반면 동적인 관점에서 아동은 신체적, 정신적으로 성인에 이르기까지 발달하는 과정에 있는 사람이다. 개인정보보호에 대한 아동의 권리는 두 가지 관점을 모두 인식하는 방식으로 행사되어야 한다. 이때 유엔 아동권리협약에 규정된 아동 최선의 이익 또한 항상 고려되어야 한다.

아동과 법정대리인의 권리 관계도 아동 최선의 이익 측면에서 살펴볼 필요가 있다. 일반적으로 아동이 자신의 권리를 행사하려면 법정대리인을 필요로 한다. 그러나 이는 아동의 법정대리인 상태가 아동에 대해 전적이고 무조건적인 우선 순위에 있다는 의미는 아니다. 아동 최선의 이익 원칙에 따르면 어떤 경우 부모나 법정대리인의 요구보다 아동의 개인정보보호와 관련된 권리가 우선할 수 있다. 법정대리인의 필요성이 아동이 자신과 관련된 문제에서 절대적으로 협의할 수 없다는 것을 의미하는 것이 아니다. 아동의 개인정보 처리가 법정대리인의 동의에 기반해 시작되었다면 관련 아동 당사자가 성년 도달시 그 동의를 철회할 수 있다. 정보주체 아동 스스로 처리가 계속되길 바란다면 새로 명시적인 동의권을 보장할 필요도 있다. 개인정보에 대한 권리는 아동에게 귀속된 것이고 이를 단순히 행사하는 법정대리인에게 귀속된 것이 아니라는 사실을 기억해야한다. 다만 아동

of children's personal data (General Guidelines and the special case of schools).
Adapted 11 February 2009, 398/09/EN, WP 160.

최선의 이익 차원에서 보았을 때 아동이나 법정대리인의 개인정보에 대한 권리가 후순위로 밀릴 수도 있다. 예를 들어 아동방임이나 학대에 대해 청소년복지서비스가 관련정보를 처리할 수 있고, 학교 교사가 아동의 신체적, 정신적 보호를 위해 아동의 개인정보를 관련기관에 제공할 수 있다.

아동은 발달하고 있는 사람이기 때문에 개인정보에 대한 권리 등 권리의 행사는 그들의 신체적, 정신적 발달 수준을 고려해야 한다. 아동은 발달하는 과정에 있을 뿐 아니라 발달에 대한 권리 또한 가지고 있다. 이런 과정을 법제도에서 다루는 방식은 국가별로 다양하지만, 모든 사회에서 아동은 자신의 성숙 정도에 부합하는 대우를 받아야한다. 아동이 성장에 따라 동의권 행사는 최소 아동에 대한 협의로 시작해 아동과 법정대리인의 공동 동의, 아동이 충분히 성숙한 경우에는 단독 동의까지 나아갈 수 있다. 이 권리 행사의 첫 단계는 아동과의 협의이다. 개인정보 처리자에게는 아동과 협의해야 할 의무가 필수적이지 않지만, 아동의 개인정보를 처리할 때 아동 본인의 의견을 고려해야한다는 것을 항상 염두에 두어야한다.

아동의 개인정보를 처리할 때는 유럽연합 개인정보보호법 체계가 규정하고 있는 공정성, 비례성, 관련성, 보관기간 제한 등의 원칙을 준수해야한다. 특히 아동과 관련된 개인정보는 공정성의 원칙을 엄격하게 준수할 필요가 있는데, 이는 아동이 아직 완전한 성숙하지 못했기 때문에 개인정보처리자가 이를 인식하고 최선의 선의를 가지고 아동의 정보를 처리해야한다는 의미이다. 또한 아동은 발달하고 있기 때문에 그들에 관한 정보도 변화하며, 수집의 본래 목적에 비춰 정보가 빠른 속도로 과거의 것이 되거나 상관없는 정보가 되어 버릴 수 있다는 점에 주의해야한다. 개인정보처리자는 관련성이 사라진 아동의 정보를 보관해서는 안 된다. 또 아동의 개인정보를 처리할 때 개인정보처리자는 정당성 원칙과 정보 보안 원칙을 준수해야한다. 정보주체의 이익이나 기본적 권리 및 자유에 과도하게 부담을 지우지 않는 한 개인정보처리자나 제3자에게는 개인정보를 처리할 수 있는 '정당한 이익'이 있지만 정보주체가 아동인 경우 아동 최선의 이익을 지침으로 사용하는 특별한 보호 조치가 취해져야 한다. 아동의 개인정보와 관련한 보안 조치는 아동의 조건에 맞아야한다.

정보주체로서 아동이 가질 수 있는 권리는 설명을 제공받을 권리, 열람권, 정정·삭제·처리정지권, 반대권 등이 있다. 특히 설명을 제공받을 권리와 관련하여 개인 정보처리자가 아동이나 법정대리인에게 정보를 제공할 때는 쉽게 이해할 수 있는 간단하고, 간결한 교육용 언어로 이루어진 통지를 제공해야 한다. 이런 설명은 법정대리인에게 항상 제공되어야 하며 적절한 능력에 도달한 아동에게도 제공되어야 한다. 열람권을 비롯해 정정·삭제·처리정지권은 보통 아동의 법정대리인에 의해 행사되지만 늘 아동의 이익을 위해 행사되어야 하며, 아동의 성숙도에 따라 아동이 독자적으로 또는 공동으로 행사할 수 있다. 의료적인 처치나 상담 서비스 등에서 아동이 성적·약물·자살 등 매우 사적인 정보를 제공한 경우 아동은 자신의 정보를 법정대리인에게 알리지 않을 것을 요청할 수 있다. 아동의 사생활권이 법정대리인의 열람권을 넘어서는지 여부를 판단하려면 아동 최선의 이익 등을 중요하게 고려해야 한다.

제29조 실무단은 아동·청소년의 주된 생활공간으로서 학교의 개인정보 처리 문제를 특별히 주의 깊게 살펴보았다. 학교에서 학생의 정보는 과도하게 수집되어선 안 된다. 항상 필요한 목적에 제한적으로 비례적이고 최소한 수집, 이용해야 한다. 인종, 이민자 출신, 장애, 종교 등 어떤 정보는 학생에게 차별을 초래할 수 있다. 보통 이런 유형의 정보는 문화적·경제적 어려움에 처한 학생의 상황을 학교가 인식하고 필요한 주의를 기울이기 위해 수집되지만 처리에서 아동 이익 최선의 원칙과 강력한 목적제한의 원칙이 준수되어야 한다. 학생 가계의 복지와 수입에 대한 정보는 수업료 지원이나 경감 등 법정대리인의 요청에 따라 아동의 이익을 위해 처리될 수 있지만 이처럼 차별을 유발할 수 있는 유형의 개인정보 처리에 대한 동의는 명백하고 명시적으로 이루어져야 한다.

아동의 개인정보 공유와 관련해 학교는 엄격한 목적구속의 원칙을 준수해야 한다. 아동의 정보는 수집을 정당화한 목적과 양립하지 못하는 목적으로 사용할 수 없다. 학교가 학생 이름과 주소를 고객을 유치하려는 은행이나 보험회사 등 제3자에게 마케팅용으로 제공하는 경우도 있다. 이는 학교 교육 목적으로 수집한 개인정보를 양립하지 않는 목적에 이용하고 제공한 것이다. 학생의 개인정보는

엄격한 정보보안의 원칙을 준수해야 하지만 특히 징계절차, 학교폭력 기록, 보건 의료 조치, 장애인 특수교육, 빈곤학생에 대한 사회적 지원 정보 등에는 더 엄격한 보안조치가 적용되어야 한다. 학교성적에 대한 정보 역시 학생의 개인정보로서 학교성적을 기밀로 보호하는 국가들의 경우에는 이 정보를 법정대리인과 학생 본인에게만 공개하며 제3자 등에 공개하려면 법정대리인이나 충분히 성숙한 학생 본인의 동의를 요구한다. 학생의 개인정보 보관에 대해 학교는 수집 목적달성에 필요한 이상으로 개인정보를 보관해선 안 된다. 따라서 학교는 교육이나 직업상 사유로 학교 파일에 어떤 개인정보를 보관해야 하는지, 징계절차나 제재조치와 관련해 어떤 정보를 어느 시점에 삭제해야 하는지 세심하게 검토해야 한다.

실무단 의견서는 학교 구성원, 특히 학생을 통제하기 위한 수단 중 일부가 특히 침해적일 수 있다고 지적한다. 생체인식정보, CCTV, RFID 정보의 수집과 관련한 경우 특히 그렇다. 이런 통제수단 도입 시 교사, 부모 등 법정대리인과 충분히 협의해야 하며 제시된 목적과 수단의 적절성에 대해 고려해야 한다. 예를 들어 단순히 출입통제를 위해 학생의 신체일부인 지문, 홍채, 손 윤곽 등 생체인식 정보를 수집하는 것은 목적에 비례적이지 않을 수 있다. CCTV 역시 목적 달성에 필요하고 덜 침해적인 다른 수단이 없을 때에만 도입되어야 하며 위치나 촬영시간 선정도 처리목적에 비춰 밀접하고 적절하며 과도하지 않아야 한다. 특히 교실내 CCTV는 학생의 수업권, 표현의 자유뿐만 아니라 교사의 수업권도 간섭할 수 있다. 만약 아동이 어린 나이부터 CCTV의 감시받는 것이 정상이라고 가정하게 되면 발달 중인 그들의 권리에 대한 기본 소양이 손상될 수도 있다. CCTV가 정당하게 운영되는 경우 학생, 학교 구성원 및 법정대리인은 CCTV 유무, 처리자와 처리 목적에 대한 모든 정보를 제공받아야 한다. CCTV 시스템을 계속 유지해야 할지 여부를 결정하기 위해 학교 당국이 정기적으로 CCTV의 정당성과 관련성을 검토할 필요가 있다. 학교가 식별된 아동의 이미지를 공개하거나 제공하려면 부모와 법정대리인 또는 성숙한 아동의 사전동의를 받아야 한다.

마지막으로 실무단 의견서는 우리 사회가 진정한 개인정보와 사생활 보호 문화를 형성하려면 아동기부터 시작해야 한다는 점을 강조한다. 이는 아동이 보호를

필요로 하기 때문만이 아니고, 이런 과정을 통해 이들이 타인의 개인정보를 존중해야 할 의무를 배워가야 하기 때문이다. 이런 목표를 달성하기 위해 학교는 매우 중요한 역할을 수행해야 한다. 아동과 학생은 정보사회의 자율적인 시민으로 성장해야 한다. 이러한 목표를 위해 아동이 어릴 때부터 개인정보와 사생활 보호의 중요성에 대해 배우는 것이 중요하다. 이러한 관념은 이들이 나중에 어떤 정보를 누구에게 어떤 조건으로 공개할지 설명을 듣고 의사결정하는 것을 가능케 할 것이다. 개인정보보호는 학교 교육에 체계적으로 반영되어야 한다. 학생이 보안상 이유로 자신의 자율성을 축소시키는 과잉감시에 직면해서도 안 된다. 아동이 교우관계의 친밀성과 프라이버시를 보장받는 한편 그들의 안전도 지킬 수 있는 균형점을 찾아야 한다.

2016년 제정된 GDPR은 실무단 의견서의 해석을 이어가고 있으며, 아동의 개인정보 처리에 대한 명시적인 규정도 몇 가지 포함했다.

유럽연합 <개인정보보호 일반규정(GDPR)> 중 아동의 개인정보 처리 관련 규정

(전문38) 아동은 개인정보 처리와 관련한 위험, 그 결과와 관련 보호장치 및 권리에 대한 인지가 부족할 수 있으므로 개인정보와 관련해 특별한 보호를 받아야 한다. 그러한 특별한 보호는 특히 마케팅 목적이나 성격 또는 사용자 프로필을 만들기 위한 목적으로 아동의 개인정보를 사용하는 경우와 아동에게 직접 제공되는 서비스를 사용할 때 아동에 관한 개인정보를 수집하는 경우에 적용되어야 한다. 아동에게 직접 제공되는 예방 또는 상담 서비스의 경우에는 친권자의 동의가 필요하지 않아야 한다.

(전문58) (중략) 아동이 특별한 보호를 받아야 한다는 점을 고려해, 정보 처리가 아동과 관련된 경우 모든 정보와 알림은 아동이 이해하기 쉽도록 명확하고 평이한 표현을 사용해야 한다.

(전문65) 정보 주체는 자신에 관한 개인정보가 수정되도록 할 권리와, 해당 정보를 보유하는 것이 본 규정이나 정보관리자가 준수해야 하는 유럽연합이나 회원국 법률에 위배될 경우 '잊혀질 권리'를 가져야 한다. (중략) 해당 권리는 특히 정보 주체가 정보

처리에 수반되는 위험을 충분히 인지하지 못한 어린 시절에 동의를 제공하고 나중에 특히 인터넷에서 그러한 개인정보를 제거하고 싶어 하는 경우와 관련이 있다. 정보 주체는 해당자가 이제 아동이 아니라는 사실에 관계없이 해당 권리를 행사할 수 있어야 한다. 하지만, 표현과 정보의 자유에 대한 권리 행사에 필요한 경우, 법적 의무를 준수하는 데 필요한 경우, 공익 또는 정보 관리자에게 부여된 공식 권한 행사를 위한 업무 수행에 필요한 경우, 공중보건 분야에서 공익을 근거로 필요한 경우, 공익을 위한 자료 보관 목적, 과학 또는 역사 연구 목적이나 통계 목적에 필요한 경우, 법적 청구권의 제기, 행사 또는 방어를 위해 필요한 경우에는 개인정보를 계속 보유하는 것은 합법이어야 한다.

(전문71) 정보 주체는, 온라인 신용 거래 신청 자동 거절이나 인간의 개입이 없는 전자 채용 절차 등과 같이, 자동화된 처리만을 바탕으로 정보 주체의 개인적 요소를 평가하는 조치를 포함할 수 있으며 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리를 가져야 한다. (중략) 그러한 조치는 아동과는 관련이 없어야 한다.

(전문75) 자연인의 권리와 자유에 대한 위험은 가능성과 심각성의 정도가 다양하며, 개인정보 처리에서 발생해 물리적, 물질적 또는 비물질적 피해로 이어질 수 있다. 이는 특히 (중략) 취약한 자연인, 특히 아동의 개인정보가 처리되는 경우(중략)에 발생할 수 있다.

제8조 (정보사회 서비스와 관련한 아동의 동의에 적용되는 조건)

1. 아동에게 직접 제공되는 정보사회 서비스와 관련해서 제6조제1항제(a)호가 적용되는 경우, 아동의 개인정보 처리는 해당 아동이 16세 이상이면 합법적이다. 해당 아동이 16세 미만인 경우, 그러한 처리는 해당 아동의 친권자가 동의하거나 허가한 경우 그 범위 내에서만 합법적이다. 회원국은 이와 관련해 더 낮은 나이 기준을 법률로 규정할 수 있지만, 이는 최소한 13세 이상이어야 한다.
2. 해당 경우 정보 관리자는 이용 가능한 기술을 고려해 아동의 친권자가 동의하거나 허가했는지 확인하기 위해 합리적 노력을 기울여야 한다.
3. 제1항은 아동과 관련한 계약의 유효성, 성립, 효과에 관한 규칙 등 회원국의 일반 계약법에 영향을 미치지 않는다.

제12조 (정보 주체의 권리 행사를 위한 투명한 정보, 알림 및 세부원칙)

1. 정보 관리자는 정보 처리와 관련해 제13조 및 제14조에 언급된 정보와 제15조~제22조 및 제34조에 따른 알림을 정보 주체에게 간결하고 투명하며 이해하기 쉽고 접근이 용이한 형태로 명확하고 평이한 표현을 사용해 제공하기 위해 적절한 조치를 취해야 한다. 특히 아동에게 특정해 전달되는 정보의 경우 이를 준수해야 한다. 정보 주체가 요청한 경우에는 정보를 구두로 전달할 수도 있으나, 이때 정보 주체의 신원은 다른 수단으로 입증되어야 한다.

GDPR의 아동 관련 규정은 다음과 같이 요약할 수 있다. GDPR은 일반적인 국제규범에 따라 18세 미만 아동을 특별히 보호하며, 특히 16세 미만이나 각국별로 최소 13세 미만의 아동이 인터넷 서비스에 가입할 때 친권자의 동의를 받는 것을 원칙으로 한다. 다만 아동 최선의 이익에 따라 아동을 위한 예방이나 상담서비스에는 친권자 동의가 필요하지 않다.

그러나 그 외에 아동은 자신의 개인정보 처리에 대해 성인과 마찬가지로의 권리를 가지고 있다. 즉, 통지권, 열람권, 정정권, 삭제권, 처리제한권, 정정·삭제·처리 정지권제한고지권, 이동권, 반대권, 완전 자동화 의사결정에 대한 권리, 침해 통지권을 모두 행사할 수 있다. 다만 개인정보처리자가 아동에게 개인정보 처리에 대해 통지하고 알릴 때 아동이 이해하기 쉽게 명확하고 평이한 표현을 사용해야 한다. 특히 아동 시기의 동의에 기반해 처리된 개인정보에 대한 삭제권의 행사가 일정하게 보장되어야 한다.

아동은 개인정보 처리에 따른 위험에 대한 인지가 부족할 수 있기 때문에 아동의 개인정보를 수집하고 처리하는 자는 시스템 설계와 처리 과정에서 특별한 주의를 기울여야 한다. 아동의 개인정보를 처리하는 자는 개인정보보호법을 준수하고 공정성 원칙에 더욱 주의를 기울여야 하며, 아동 본인이나 친권자의 동의 등 개인정보 처리의 적법한 근거를 갖춰야 한다. 개인정보처리자나 제3자의 '정당한 이익'을 목적으로 개인정보를 처리하는 경우 정보주체의 동의가 없어도 적법한 처리 요건으로 인정되지만, 아동의 개인정보에 대해서는 정당한 이익에 기반해

처리하는 것이 허용되지 않는다. 특히 마케팅 목적이나 프로파일링 처리에서 아동의 이익에 대한 특별한 보호가 필요하다.

특히 GDPR은 앞서 서술한 프라이버시 중심 설계의 개념을 법정화했다는 점에서 주목받았으며, 이를 아동 관련 서비스와 제품에 적용할 것을 요구하고 있다. GDPR이 규정한 개인정보보호 중심 설계(data protection by design)와 기본 설정(data protection by default)이란 개인정보처리자가 정보주체의 권리와 자유를 보호하기 위해 적절한 기술적·관리적 조치를 시행해 개인정보 보호법을 준수하는 조치를 취하는 것을 의미한다. 개인정보의 처리를 기반으로 하거나 작동 중에 개인정보를 처리하게 되는 제품·서비스·애플리케이션의 생산자는 이를 개발, 설계하는 시점부터 개인정보보호 원칙을 효율적으로 이행하고 필요한 안전조치를 개인정보처리에 통합할 수 있도록 설계(design)해야 한다(GDPR 전문78 및 제25조(1)). 또한 개인정보처리자는 기본설정(default)을 통해 특정 처리목적에 필요한 개인정보만 처리되도록 적절한 기술과 관리 조치를 이행해야 한다(제25조(2)). 영국 개인정보보호 감독기관 ICO는 애플리케이션 프라이버시 설정에서 “공유하지 않음”을 기본설정으로 두고, “공유”를 활성화하기 위해 기능 확장과 위험성에 대해 아동 친화적인 명확한 설명을 제시할 것을 권장했다.

2) 아동 개인정보보호 침해에 대한 유럽연합의 대응

GDPR 제정 후 유럽연합의 개인정보보호 감독기관들은 아동 등 ‘취약한 정보 주체’에 대한 개인정보보호 침해로부터 보호를 강력히 요구해왔다. 특히 제29조 실무단은 <동의에 대한 가이드라인>에서 취약한 정보주체인 아동의 개인정보가 처리될 경우 추가적인 보호조치를 요구했다¹²³⁾. 우선 개인정보처리자가 아동으로부터 ‘설명기반 동의(informed consent)’를 얻었다고 인정받기 위해서는 반드시 아동이 이해할 수 있는 명확하고 평이한 언어로 개인정보를 어떻게 처리할지

123) EU Article 29 Data Protection Working Party (2018). Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017, As last Revised and Adopted on 10 April 2018.

설명해야한다.

동의를 기반으로 정보사회서비스를 아동에게 제공할 때 개인정보처리자는 사용자가 디지털 동의를 제공할 수 있는 연령 이상임을 확인하기 위한 적절한 노력을 기울여야 하고, 이러한 조치는 해당 개인정보 처리의 성격과 위험에 비례해야 한다. 위험성이 낮은 경우에는 신규 서비스 가입자에게 생년월일을 제공하거나 본인이 ‘미성년자이다/아니다’라고 명시하는 양식을 작성하도록 요구하는 것만으로 적절할 수 있다. 이용자가 동의대상 연령 미만이라고 진술하는 경우 처리자는 친권자의 승인을 받아야하며, 연령 확인이 과도한 개인정보처리로 이어져서는 안 된다. 아동을 대신해 동의하는 자가 친권 보유자인지 확인하는 절차의 합리성 역시 개인정보 처리에 내재된 위험성에 따라 다를 것이다. 위험성이 적은 경우 이메일로 친권을 확인하는 것만으로도 충분할 수 있으나 위험성이 높은 경우 더 많은 증빙자료를 요구하는 것이 적절하다. 아동이었던 정보주체가 개인정보 처리에 대해 동의권을 행사할 수 있는 연령이 되면 친권 보유자가 제공한 동의를 확인·변경·철회할 수 있다. 개인정보처리자는 공정성과 투명성 원칙에 따라 반드시 해당 정보주체에게 동의 철회 가능성에 대해 통지해야 한다.

한편, 공공기관이 개인정보 처리를 위해 동의에 의존하는 것은 부적절하다. 공공기관인 처리자와 정보주체의 관계는 권력 불균형이 명백하고, 대부분 정보주체는 공공기관인 개인정보처리자의 처리를 수락하는 것 외에 대안을 갖고 있지 않기 때문이다. 다만 일정 조건 하에서 동의가 전적으로 배제되지 않는다. <동의 가이드라인>은 그 사례로 학교가 학생의 개인정보를 처리하는 경우를 들고 있다. 어느 공립학교가 학생들에게 학생잡지에 본인의 사진을 이용하는 것에 대한 동의를 구했을 때, 학생들이 교육이나 서비스를 거부당하는 불이익 없이 이를 거부할 수 있다면 이 동의는 진정한 동의로 인정된다.

이상의 규범에 기반해 유럽 각국 개인정보보호 감독기관들은 아동의 개인정보보호 침해에 대해 특별한 보호를 요구하는 결정례를 발표해왔다. 우선 디지털 플랫폼이 아동에게 적합한 연령적합성 설계를 갖추었는지를 중요하게 취급하고

있다. 최근 틱톡의 아동 개인정보 처리 관련 논란이 불거지자, 여러 국가 개인정보 보호 감독기관들이 이 문제에 개입했다. 이탈리아에서는 10세 아동이 틱톡에서 질식게임인 ‘블랙아웃 챌린지’를 하다가 사망한 사건이 발생하자, 2021년 1월 22일 이탈리아 개인정보보호 감독기관이 틱톡에 대해 연령이 불확실한 개인들의 개인정보 처리를 금지할 것을 명령했다¹²⁴⁾. 네덜란드 개인정보보호 감독기관은 2021년 4월 9일 대다수가 16세 미만 아동인 네덜란드 이용자들에게 개인정보보호 지침을 영어로만 제공한 것은 GDPR 12조(1)를 위반한 것으로 보고 750,000유로(약 10억원)의 과징금을 부과했다¹²⁵⁾.

SNS에서 아동 개인정보 공유에 대한 결정도 잇따랐다. 아이슬란드 개인정보보호 감독기관은 2020년 6월 25일 어린이 축구대회 사진을 페이스북에 게재하려는 한 은행의 계획이 GDPR을 위반한다고 결정했다. 이 감독기관은 아동과 함께 일하는 사람들이 페이스북에 아동에 관한 개인정보를 공유하지 말아야 한다고 지도해 왔다. 해당 은행은 “아이들의 부모와 보호자가 사진 게시에 동의했”고 “페이스북에 사진을 공유하는 것은 처리자의 정당한 이익”이라고 주장했다. 그러나 감독기관은 아동의 부모나 보호자가 처리자인 은행으로부터 사전에 충분한 정보를 받지 못했기 때문에 합법적인 동의로 볼 수 없고, 아동의 개인정보를 마케팅 목적으로 사용하는 것은 정당한 이익으로 인정할 수 없다고 보았다. 특히 페이스북에 게시된 아동 사진에 대한 향후 이용을 처리자가 완전히 통제할 수 없다는 점이 고려되었다¹²⁶⁾. 덴마크 개인정보보호 감독기관은 2021년 3월 1일 ‘에픽 부킹’이 아동의 사진을 페이스북에 광범위하게 게재하고 보관한 것이 위법이라고 발표하고 해당 사진의 삭제를 명령했다. 정보주체에게 사전에 페이스북 게시 등 개인정보 이용에 대한 충분한 정보를 제공하지 않았으며, 개인정보 보유기간도

124) https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_-_9524194 (검색일: 2021. 8. 31).

125) [https://gdprhub.eu/index.php?title=AP_\(The_Netherlands\)_-_TikTok](https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_TikTok) (검색일: 2021. 8. 31). 틱톡은 이 결정에 이의를 제기했고 이 사건은 현재 틱톡 유럽사무소가 개소한 아일랜드의 감독기관으로 이관된 상태임

126) https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_-_2020010425 (검색일: 2021. 8. 31).

설정하지 않았다는 것이다¹²⁷⁾. 스페인 개인정보보호 감독기관은 2021년 3월 15일 미성년인 자녀의 사진을 부모 동의 없이 촬영하고 위챗에 공유한 외국어 교실에 3,000유로(약 4백만 원)의 과징금을 부과했다¹²⁸⁾. 스페인 개인정보보호 감독기관은 2021년 8월 9일 부모가 동의를 거부했음에도 2명의 아동 사진을 인스타그램에 게시한 리듬체조 클럽에 5,000유로(약 6백80만원)의 과징금을 부과했다고 발표했다¹²⁹⁾.

디지털 환경으로 인한 아동학생의 개인정보 유출도 늘었다. 때로는 공공부문에서 민간부문으로 유출되기도 했다. 노르웨이 개인정보보호 감독기관은 2020년 7월 7일 지방자치단체가 아동의 민감정보를 유출한 것에 대해 500,000NOK(약 6천6백만 원)의 과징금을 부과했다. 이 사건으로 유출된 개인정보는 특수학급 학생과 부모의 민감한 건강정보로서 디지털 학습 플랫폼으로 유출되었다¹³⁰⁾.

학교에서 전자적으로 학생의 개인정보를 처리하는데 대한 감독기관의 시정 요구도 있었다. 벨기에 개인정보보호 감독기관은 2020년 6월 16일 한 교육 위원회가 12세 학생을 대상으로 '스마트스쿨' 시스템을 통해 설문조사를 하면서, 학생의 개인정보를 불법적으로 처리하고 데이터 최소화 및 투명성 원칙을 위반했다고 판단했다. 교육위원회는 법적 의무로서 개인정보를 처리했다고 했으나, 감독기관은 설문조사가 그에 해당하지 않으므로 학생 부모의 동의를 받았어야 했다고 보았다. 또한 아동과 보호자에게 충분한 정보를 제공하지 않았고 괴롭힘 등에 대한 설문을 처리하면서 익명도 보장하지 않았다고 지적했다¹³¹⁾. 아이슬란드 개인정보보호 감독기관은 2021년 5월 4일 424명의 아동의 개인정보를 유출한 학교전자관리시스템의 관리 회사에 23,585유로(약 3백만 원)의 과징금을 부과했다¹³²⁾. 슬로베니아 개인정보보호 감독기관은 2021년 12월 16일 체육교사가

127) https://gdprhub.eu/index.php?title=Datatilsynet_-_2019-431-0052 (검색일: 2021. 8. 31).

128) https://gdprhub.eu/index.php?title=AEPD_-_PS/00405/2020 (검색일: 2021. 8. 31).

129) [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-_PS/00209/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00209/2021) (검색일: 2021. 8. 31).

130) https://gdprhub.eu/index.php?title=Datatilsynet_-_20/02191 (검색일: 2021. 8. 31).

131) https://gdprhub.eu/index.php?title=APD/GBA_-_31/2020 (검색일: 2021. 8. 31).

132) [https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_\(Iceland\)_-_2020010355](https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_2020010355) (검색일: 2021. 8. 31).

온라인 수업에서 아동인 학생의 댄스영상을 촬영한 후 제출하게 한 것의 GDPR 준수 여부를 검토했다. 우선 학교가 학생의 개인정보를 처리하는 법적 근거로 동의는 부적절하지만, 학교와 교사는 법률에 따른 학교 교육을 위해 학생의 개인정보를 합법적으로 처리할 수 있다. 다만 데이터 최소화 원칙을 준수해 교육 과정에 필요한 것보다 더 많은 개인정보를 처리해서는 안 되고, 적절한 보안을 보장해야 한다¹³³⁾. 학교 시스템이 민감정보 처리와 관련한 문제를 발생시키는 경우 더 높은 행정제재가 적용된다. 노르웨이 개인정보보호 감독기구는 2019년 11월 10일 시교육청에서 사용하는 모바일 애플리케이션이 63,000명 이상의 학생 개인정보를 노출한 사건에서 120,000유로(약 1억6천4백만 원)의 과징금을 부과했다. 학생과 보호자는 애플리케이션을 통해 학교 교사와 관리자와 통신할 수 있으나, 승인되지 않은 사용자가 애플리케이션에서 건강정보를 비롯한 학생의 개인정보에 접근하는 보안 문제가 발생했다¹³⁴⁾. 스웨덴 개인정보보호 감독기관은 2020년 11월 24일 학생 50만 명과 보호자, 교직원의 민감정보를 비롯한 개인정보를 처리하는 스톡홀름 교육위원회의 교육관리시스템이 취약한 보안으로 GDPR을 위반했다고 보고, 약 392,000유로(약 5억3천6백만 원)의 과징금을 부과했다¹³⁵⁾.

3. 영국의 아동·청소년 프라이버시 보호 규범

영국의 개인정보보호 법체계는 2018년 유럽연합 GDPR의 발효와 동시에 이를 국내에서 이행하기 위해 제정시행한 2018년 영국 개인정보보호법(Data Protection act 2018, 이하 'DPA')과 유럽연합 탈퇴 후 GDPR과 동일한 개인정보보호를 보장하기 위해 2021년 1월 1일 제정시행한 영국 GDPR(UK General Data Protection Regulation)로 이루어져 있다. 이들 영국 개인정보보호 법체계는

133) https://gdprhub.eu/index.php?title=IP_-_07121-1/_2020/2263 (검색일: 2021. 8. 31).

134) https://gdprhub.eu/index.php?title=Datatilsynet_-_18/34319 (검색일: 2021. 8. 31).

135) https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-7024 (검색일: 2021. 8. 31).

GDPR의 규범을 기초로 하되 법집행, 아동 등 부문적으로 GDPR보다 구체적인 규정을 두고 있다.

영국 개인정보보호 법체계는 아동의 개인정보는 특별한 보호 대상이며 유엔 아동권리협약에 따른 영국 정부의 의무를 고려해야 한다고 규정했다(DPA 제123조 및 제189조). 이에 영국 개인정보보호 감독기관인 ICO(Information Commissioner's Office)는 아동의 개인정보 처리에서 아동 최선의 이익을 비롯한 아동의 권리를 보장하기 위한 지침들을 발표해왔다.

영국 개인정보보호법은 정보사회서비스에서 아동 친권자의 동의가 필요한 연령을 만 13세 미만으로 규정하고 있다(DPA 제9조(a)). 그러나 ICO는 아동을 보호하는 조치는 정보사회서비스 친권자 동의권을 넘어 개인정보 처리 전반에서 이뤄져야 한다고 보았으며, 대상은 유엔 아동권리협약에 따라 만18세 미만 미성년 아동 전체로 규정했다¹³⁶⁾.

이때 ICO는 ‘특별한 보호’로서 아동의 개인정보를 처리하는 모든 자에게 GDPR에서도 규정한 바 있는 개인정보보호 영향평가를 실시하고 아동친화적인 개인정보보호 중심 설계와 설정을 적용할 것을 권장했다. 특히 아동의 개인정보를 마케팅 목적이나 프로파일링과 자동화된 의사결정에 사용하거나, 아동에게 직접 온라인 서비스를 제공하는 경우는 고위험 가능성이 있는 개인정보 처리로서 의무적으로 개인정보보호 영향평가를 실시하고 위험을 완화하는 조치를 취하거나 완화가 불가능할 경우 개인정보보호 감독기관과 협의해야 한다. 아동과 친권자에게는 개인정보 처리에 대한 투명성, 공정성, 합법성 등 영국 GDPR 상의 개인정보보호 원칙을 보장하고 열람권, 정정·삭제권, 반대권 등 정보주체의 권리를 보장해야 한다. 특히 아동에게 개인정보 처리에 대해 알릴 때는 성인에게 제공하는 내용과 같은 정보를 아동이 이해할 수 있는 간결하고 명확하며 평범한 문구로 작성해야 한다. 도표, 만화, 그래픽과 비디오의 사용이 권장된다. 개인정보 처리자는 아동의 인지 부족이나 취약성을 악용해서 안 되며, 불량식품을 선택

136) Information Commissioner's Office (2018). Children and the GDPR. 8.

하거나 쓸모없거나 감당할 수 없는 물품을 구입하는 결과로 이어져서는 안 된다. 일반적으로 기업은 마케팅 목적으로 아동의 개인정보를 프로파일링 하지 않도록 해야 한다.

여기서 더 나아가 영국 개인정보보호법은 ICO에 “아동이 접근할 가능성이 있는 관련 정보사회서비스의 연령에 적합한 설계기준에 대해 적절하다고 판단하는 지침”을 마련하도록 했다(DPA 제123조). 이때 ‘연령에 적합한 설계’란 아동의 사용에 적절하고 아동의 발달 요구를 충족하는 서비스 설계를 의미하고, ‘관련 정보사회서비스의 연령에 적합한 설계기준’이란 ICO가 유엔 아동권리협약에 따른 아동의 최선의 이익을 고려해 바람직하다고 보는 설계기준을 의미한다. ICO는 ‘연령적합설계 실행규칙(Age Appropriate Design Code: a code of practice for online services)’을 마련해 1년의 경과 기간을 거쳐 2021년 9월 2일부터 시행했다¹³⁷⁾. 이 규칙은 영국을 넘어 미국 상하원에서 빅테크와 게임 기업이 자발적으로 채택하도록 요청하고 있다는 점에서 국제적 영향력을 발휘하고 있다¹³⁸⁾.

규칙은 18세 미만의 아동이 접근할 수 있는 모든 온라인 서비스에 적용되며, 개인정보를 처리하는 온라인 제품이나 서비스(앱, 프로그램, 웹 사이트, 게임 또는 커뮤니티 환경, 커넥티드 장난감 또는 장치 등을 포함)를 제공하고 해당 제품이나 서비스에 영국의 아동이 접근할 가능성이 있는 경우에 적용된다. 특히 규칙은 연령별 아동의 이익, 요구 및 발달 능력을 고려해 아동의 연령을 ① 0~5세(유아기, pre-literate and early literacy), ② 6~9세(초등기, core primary school years), ③ 10~12세(전환기, transition years), ④ 13~15세(10대 초반,

137) Information Commissioner's Office (2020). Age appropriate design: a code of practice for online services: 한국인터넷진흥원 (2020). 아동의 개인정보보호를 위한 ICO의 ‘연령적합 설계규약’ 분석 (1). <해외 개인정보보호 동향 보고서> 수시동향 보고서 2020년 3월; 한국인터넷진흥원 (2020). 아동의 개인정보보호를 위한 ICO의 ‘연령적합설계규약’ 분석 (2). 2020 최종 보고서.

138) Information Commissioner's Office (2021, 8, 25). Blog: As the Children's code comes in - what's next?. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/08/as-the-children-s-code-comes-in-what-s-next/> (검색일: 2021. 10. 1).

early teens), ⑤ 16~17세(예비 성인기, approaching adulthood)로 구분해 서비스를 설계하고 기준을 적용하도록 했다.

규칙의 기준은 총 15가지로 구성되었고, 주요 요구사항은 다음과 같다.

〈표 5-1〉 영국 연령적합설계 실행규칙의 기준과 요구 사항

기준	주요 요구 사항
(1) 아동 최선의 이익	○ 아동의 권리를 고려하고 지원할 것
(2) 개인정보보호 영향평가	①영향평가의 수행 시점 식별 ②개인정보 처리에 대해 기술 ③아동 및 부모와 협의 ④개인정보 처리의 필요성, 비례성, 준수성 평가 ⑤ 개인정보 처리에서 발생하는 위험의 식별 및 평가 ⑥위험 완화 조치 식별 ⑦평가 결과 기록
(3) 연령에 적합한 적용	○ 개인정보 처리로 인해 아동에게 미치는 위험을 고려하고 이용자 연령 파악의 확실성 수준을 검토할 것
(4) 투명성	○ 영국GDPR에 규정된 명확한 프라이버시 통지를 제공할 것 ○ 개인정보 사용이 활성화되는 시점에 '강력한' 설명을 제공할 것 ○ 명확한 이용약관, 처리방침, 서비스 기준을 제공할 것 ○ 아동친화적 방식으로 정보를 제시할 것 ○ 아동의 연령에 설명을 맞출 것
(5) 개인정보의 해로운 이용	○ 관련 최신 기준 및 규칙을 준수할 것 ○ 명백히 해롭거나 기준에 반하는 방식으로 아동의 개인정보를 처리하지 말 것
(6) 처리방침 및 서비스 기준	○ 개인정보처리방침을 준수해 개인정보를 이용할 것 ○ 이용자 행동에 적용되는 정책을 공개하고 준수할 것 ○ 콘텐츠 및 기타 정책을 공개하고 준수할 것
(7) 기본 설정	○ 높은 프라이버시 수준을 기본 설정으로 제공할 것 ○ 아동이 설정을 변경하면 추가적인 개입을 검토할 것 ○ 이용자가 설정을 영구히 변경할 것인지 일시적으로 변경할 것인지 선택할 수 있도록 허용할 것 ○ 소프트웨어 업데이트시 이용자 선택이나 높은 프라이버시 기본 설정을 유지할 것 ○ 여러 이용자가 사용하는 기기에서는 이용자별 선택을 허용할 것
(8) 데이터 최소화	○ 서비스별 요소 제공에 필요한 개인정보가 무엇인지 식별할 것 ○ 아동이 이용을 희망하는 서비스 요소 각각을 선택할 수 있도록 할 것 ○ 서비스 요소를 아동이 능동적이고 의도적으로 이용할 시에만 개인정보만을 수집할 것

기준	주요 요구 사항
(9) 개인정보 공유(제공)	<ul style="list-style-type: none"> ○ 아동의 개인정보 공유시 아동 최선의 이익을 우선적으로 고려해야 하며, 여기에는 아동 보호, 아동에 대한 성착취 및 학대 방지, 온라인 그루밍 범죄의 탐지와 예방 등이 포함됨 ○ 영향평가 단계별로 제기되는 구체적인 문제와 위험을 고려할 것
(10) 위치정보	<ul style="list-style-type: none"> ○ 기본 설정에서 위치정보 선택을 해제(OFF)할 것 ○ 아동에게 위치가 추적된다는 사실을 명백히 밝힐 것 ○ 아동의 위치가 타인에게 노출되는 설정은 개별 이용 후 다시 해제할 것
(11) 부모의 통제	<ul style="list-style-type: none"> ○ 부모가 통제중이어서 추적되거나 관찰되고 있을 경우 아동에게 명확히 밝힐 것
(12) 프로파일링	<ul style="list-style-type: none"> ○ 목적별로, 프로파일링 유형별로 구분되는 설정을 제공할 것 ○ 프로파일링 기반 기능들은 불가피한 사유를 제외하고 기본 설정에서 해제해 둘 것 ○ 프로파일링이 활성화되는 시점에 적절히 개입할 것 ○ 프로파일링이 설정되면 아동을 보호하기 위한 적절한 조치를 시행할 것
(13) 넛지((Nudge) 기법	<ul style="list-style-type: none"> ○ 아동에게 나쁜 프라이버시 선택을 유도하는 넛지 기법을 사용하지 말 것 ○ 친프라이버시 설정을 위해 넛지를 적절하게 사용할 것 ○ 건강과 복지를 향상시키는 넛지 사용을 고려할 것
(14) 커넥티드 완구 및 장치	<ul style="list-style-type: none"> ○ 개인정보 처리자 및 책임 소재를 명확히 할 것 ○ 대화형 스피커 등 다양한 연령의 여러 이용자가 사용할 경우를 예상하고 공급할 것 ○ 구입 및 설치 시점에 개인정보 이용에 대한 명확한 정보를 제공할 것 ○ 자동재생 오디오 메시지나 대화형 로봇 등에서 '적시에' 의사소통할 방안을 마련할 것 ○ 온라인 연결 장치의 '청취' 모드 등에서 무의식적인 개인정보 수집을 방지할 것
(15) 온라인 도구 ※ 온라인 도구를 아동이 온라인 상태에서 쉽고 간단하게 자신의 권리를 행사할 수 있도록 하는 메커니즘으로, 개인정보 열람권과 수정권 등을 행사하도록 지원	<ul style="list-style-type: none"> ○ 온라인 도구는 눈에 띄어야 함 ○ 온라인 도구는 아동 연령에 적합하고 손쉽게 사용할 수 있어야 함 ○ 온라인 도구는 '나의 데이터 다운로드', '모든 데이터 삭제' 또는 '삭제할 데이터 선택', '나의 데이터 사용 중지', '수정' 등 지원 하는 권리 행사에 대해 구체적이어야 함 ○ 아동 및 부모의 불만이나 요청사항에 대한 진행 상황을 추적할 수 있는 기법과 연락 메커니즘을 포함할 것

전반적으로 규칙은 아동 대상 서비스에서 높은 개인정보보호 기준을 기본 설정(data protection by default)으로 제시했다. 이 기준은 설계 과정의 처음부터 적용되어야 하며, 후속 업그레이드, 서비스 개발 프로세스, 개인정보보호 영향 평가 프로세스에도 반영돼야 한다. 또한 규칙은 아동 최선의 이익 원칙하에 연령별로 적합한 서비스 적용과 정보 제공, 권리 행사 보장을 요구했다. 아동의 개인정보는 최소한만 수집하고 설득력 있는 이유(compelling reason)가 없는 한 공유가 원칙적으로 금지되며 위치정보와 프로파일링 기능은 기본 설정에서 해제해줘야 한다. 아동에게 해로운 방식이나 나쁜 선택을 유도하는 설계는 금지된다.

4. 미국의 아동·청소년 프라이버시 보호 규범

미국은 개인정보보호에 대한 일반법이 없음에도 불구하고 1998년 아동의 온라인 개인정보를 보호하기 위해 ‘아동 온라인 프라이버시 보호법(Children’s Online Privacy Protection Act, 이하 COPPA)¹³⁹⁾를 특별법으로 제정하고, 2000년부터 시행하고 있다. 해당 법의 집행기관은 연방거래위원회(Federal Trade Commission, ‘이하 FTC’)이다.

COPPA는 영리 목적의 웹사이트나 온라인 서비스 운영자 중에서 아동을 대상으로 서비스를 제공하는 경우에 적용되며, 직접 개인정보를 수집하지 않더라도 다른 서비스 운영자 등을 통해 수집하는 경우에도 적용된다. COPPA의 보호 대상은 13세 미만 아동으로, 아동으로부터 수집한 부모·친구 등 타인의 개인정보도 포함된다. 주요 보호 원칙으로는 ① 개인정보 처리방침의 공개, ② 부모에 대한 고지 및 동의, ③ 개인정보 열람·삭제 요청 등 부모의 검토권(Review), ④ 정보 보안 및 보유·파기 등을 규정하고 있다(개인정보보호위원회, 2020: 345).

특히 보호대상 연령 아동을 대상으로 하거나 아동의 개인정보를 수집한 운영자는

139) Children’s Online Privacy Protection Rule (“COPPA”).

아동의 개인정보 수집내용, 사용방법, 공개절차 등에 대해 고지하고 이에 대한 법정대리인의 동의를 받아야 한다. 이때 법정대리인에게 수집된 정보의 사용이나 보유를 거절할 수 있는 합리적 수단을 제공해야하며 합리적으로 필요한 수준보다 더 많은 개인정보의 공개를 요구하지 않아야 한다. 고지 방법은 법정대리인에게 직접 고지하는 것과 아동이 이용하는 온라인서비스 각 영역에서 고지하는 것을 병행하도록 했다. 고지 내용은 명백하고 이해하기 쉬워야 하고 혼동을 유발할 수 있는 내용은 제외해야한다. 이러한 아동의 개인정보 수집관련 고지 및 동의는 이전에 동의를 받았더라도, 변동사항이 발생할 경우 다시 고지와 동의를 획득해야 한다. 이 법에 따라 FTC는 2019년 틱톡과 유튜브가 13세 미만 아동의 개인정보를 부모의 동의 없이 수집한 것에 대해 각각 570만 달러, 1억 7천만 달러의 벌금을 부과했다. 벌금 외에도 FTC는 틱톡 관계사인 뮤직컬리(Musical.ly)사에게 연령에 따라 서비스를 분류하고, 아동 개인정보의 공유를 금지하며 콘텐츠와 이용자 간 상호작용에서도 제한을 두도록 했다. 유튜브 역시 아동 대상 콘텐츠에 대해 수정된 '아동 개인정보보호 강화' 정책을 제시했는데, 대표적으로 아동 대상 콘텐츠에 대해서는 맞춤형 광고와 댓글을 금지하고, 아동 대상 콘텐츠를 식별하기 위한 매커니즘을 개발하기로 했다(전윤선 외, 2020).

미국 내 개인정보보호와 관련한 대표적 주법인 캘리포니아주 소비자 프라이버시 보호법(California Consumer Privacy Act 2018) 또한 13세 미만 아동 개인정보 수집을 위해서는 부모의 사전 동의를 요구하고, 13~16세 아동의 개인정보는 부모의 동의 없이 판매를 금지하는 등 아동보호 조항을 포함하고 있다¹⁴⁰⁾.

5. 국내 아동·청소년 프라이버시 법제와 침해 구제

우리나라에서는 인권과 개인정보보호 관련 법률과 자치 법규에서 아동·청소년의 인권침해에 대한 전문기구를 설치하고 상담, 조사, 권고 등 권리구제를 담당하고

140) CCPA를 수정한 캘리포니아주 프라이버시 권리법(The California Privacy Rights Act of 2020, CPRA)이 2020년 11월 3일 캘리포니아주 주민투표에서 통과되어 2023년 1월 1일 시행 예정임.

있다. 우선 국가인권기구로서 국가인권위원회가 국제규범과 「국가인권위원회법」에 따라 설치되어 있으며, 국가 개인정보보호 감독기관으로서 개인정보보호위원회가 국제규범과 「개인정보보호법」에 따라 설치되어 침해 사건에 대한 권리구제를 소관하고 있다. 그밖에 서울특별시 등 지방자치단체가 아동·청소년 인권관련 조례에 따라 아동·청소년 인권침해에 대한 권리구제 활동을 하고 있으며, 서울특별시교육청 등 교육 지방자치단체가 학생인권조례에 따라 각급 학교 학생 인권 침해에 대한 권리구제 활동을 하고 있다.

이하에서는 국가인권위원회, 개인정보보호위원회, 지방자치단체의 아동·청소년이나 학생인권 관련 권리구제기구의 활동과 관련 규범을 중심으로 아동·청소년의 프라이버시권과 개인정보보호의 침해와 구제 상황을 살펴본다¹⁴¹⁾.

1) 국가인권위원회 침해 구제

국가인권위원회는 「국가인권위원회법」에 따라 각급 학교를 비롯한 공공기관의 인권침해나 차별행위, 법인·단체·사인(私人)에 의한 차별행위, 성희롱에 대해 상담과 조사·구제를 실시하고, 인권관련 법령·정책·관행의 조사·연구와 개선 권고나 의견을 표명한다.

우선 2001년~2020년까지 각급 학교의 인권침해 관련 국가인권위원회에 진정·접수된 건수는 5,334건이며, 그중 아동·청소년인 학생의 프라이버시권과 관련한 처리사례를 취합해 본 결과는 <표 5-2>와 같다.

<표 5-2> 각급 학교 학생 프라이버시권 관련 진정 처리 사례

(기간: 설립후 ~ 2020년)

의결 연도	유형	건수	피권고기관
2006	성폭력 피해학생 사생활의 비밀 침해	1	교육감
2009	두발 단속	1	중학교장

141) 이 장의 서술 내용은 정보공개청구를 통해 각 기관이 공개한 자료에 기반함.

의결 연도	유형	건수	피권고기관
2010	교내 휴대전화 사용 제한	1	고등학교장
2012	고정식 명찰 부착	1	중학교등 11개기관학교장, 교육감
2013	학교폭력 조치사항 학내게시	1	중학교장, 교육감
2014	휴대전화 사용 제한	1	고등학교장
	교실내 캠코더 등 촬영	1	교육감
2016	교내 휴대전화 사용 제한	1	중학교장
	기숙사 휴대전화 사용 제한	2	고등학교장
	교내 흡연단속시 소변검사	1	고등학교장
	상담내용 공개로 인한 사생활의 비밀과 자유 침해	1	고등학교장, 교육감
2017	교내 휴대전화 사용 제한	3	중학교장, 고등학교장, 교육감
	기숙사 휴대전화 사용 제한	1	고등학교장
	학교 급식소 내 CCTV 설치	1	중고등학교장
	소변검사	1	고등학교장
2018	교내 휴대전화 사용 제한	10	중학교장, 고등학교장, 교육감
	기숙사 사생활 침해	1	고등학교장
	두발 단속	1	고등학교장
2019	교내 휴대전화 사용 제한	12	중학교장, 고등학교장, 교육감
	두발 단속	2	중학교장, 고등학교장, 교육감
	학생 일기 등 공개로 인한 사생활의 비밀과 자유 침해	1	초등학교장, 교육감
	대학 합격자 명단 공개	1	고등학교장
2020	교내 휴대전화 사용 제한	13	중학교장, 고등학교장, 교육감
	기숙사 통신의 제한	1	고등학교장
	기숙사 소지품 검사	1	고등학교장
	두발 및 복장 단속	9	중학교장, 고등학교장, 교육감
	개인정보 누설	1	초등학교장

자료: 국가인권위원회 정보공개 수정(사유 중복 집계)¹⁴²⁾

이상의 사례를 살펴보면, 학생 프라이버시권 관련 진정 처리가 양적으로 증가했음을 알 수 있다. 국가인권위원회 통계 전체적으로 아동을 구분해 집계하고 있지

142) 2021년 8월 9일 정보공개. 다만, 통계 전체적으로 아동을 구분해 집계하지 않았으며, 각급학교 인권침해 통계 역시 초중고는 물론 대학 이상 고등교육기관 및 교직원 인권침해 사례도 포함되어 있었음.

않다는 한계가 있으나 개별적으로 취합한 결과 2013년까지 0~1건으로 집계되었던 사례수가 조금씩 증가해 2020년에는 25건(사유 중복 집계)에 이르렀다.

증가 배경으로는 우선 학생의 프라이버시권에 대한 인식 증진을 꼽을 수 있다. 2010년 이후 국가적으로는 개인정보보호법이 제정되고 교과과정에 개인정보 보호에 대한 교육이 포함되어 왔으며, 지방자치단체별로는 학생인권조례가 제정되고 각급 학교에서 학생인권교육이 실시되어 왔다. 다른 한편으로는 학생의 프라이버시권이 관련된 디지털 환경의 변화를 이유로 들 수 있다. 아동·청소년의 스마트폰 보유율은 2012년부터 크게 상승하기 시작해, 2017년 기준 초등저학년생 37.2%, 초등고학년생 74.2%, 중학생 92.0%, 고등학생 93.5%을 보이며, 중학생과 고등학생의 하루 평균 스마트폰 이용시간 또한 증가해 2017년 기준 2시간 가량으로 전연령대 스마트폰 유저의 평균 이용시간(1시간 43분)보다 높게 나타났다(정보통신정책연구원, 2018). 전반적으로 아동·청소년의 스마트폰 보유율과 이용시간이 계속 증가하는 환경 변화는 진정 사유의 양상에도 반영되어 있다. 2020년까지 학생 프라이버시권과 관련된 전체 진정 사유(중복 집계) 71건 중 휴대전화와 통신 제한에 대한 사유가 45건으로 63.4%를 차지했으며 최근으로 올수록 관련 진정 건수가 큰 폭으로 증가해 왔다. 이는 학내 두발과 복장 단속 및 소지품과 신체 검사, 신상노출 등 다른 사생활 침해 사유에 비해 압도적인 비중이다.

국가인권위원회는 휴대전화 사용제한의 필요성이 인정된다고 할지라도, 현대사회에서의 휴대전화는 단지 통신기기의 기능을 하는데 그치지 않고 개인간의 상호작용을 증대시키고 활성화시켜 사회적 관계를 생성·유지·발전시키는 도구이자 각종 정보를 취득할 수 있는 생활필수품의 의미를 가진다는 점, 아동이 성장 과정에 있는 존재인 점 등을 고려하면, 학교는 학생들의 자유로운 의사에 의해 희망자에 한해 수거하거나 수업시간에만 사용을 제한하고 휴식시간과 점심시간에 사용을 허용하는 등 학생의 기본권 침해를 최소화하면서도 교육적 목적을 달성할 수 있는 다른 방법을 고려할 수 있다고 보았다.

한편, <2020 국가인권위원회 통계>에 따르면, 정책 권고, 의견표명, 의견제출이 이루어진 전체 413건 중 아동·청소년·학생의 프라이버시권 및 개인정보

보호권 관련으로 확인되는 사례는 <표 5-3>의 21건이다.

〈표 5-3〉 국가인권위원회 아동·청소년·학생 프라이버시 및 개인정보보호 관련 의견

(기간 : 설립후 ~ 2020년)

의결 연도	권고(의견표명)제목	피권고기관
2003	NEIS에 대한 국가인권위원회의 권고	교육인적자원부장관
2005	초등학교 일기장 검사관련 의견표명	교육인적자원부장관
2006	학업중단 청소년관련 정보의 제공	교육인적자원부장관 국가청소년위원회위원장
2011	입양대기아동 영상 방영 관련 위원회 의견표명	보건복지부장관 (사)한국○○○○회
2012	교실내 CCTV 설치의 인권 침해 여부에 대한 의견표명	서울시교육감
2013	학교 밖 학업중단 청소년 지원에 관한 법률안에 대한 의견표명	여성가족부장관
2015	영유아보육법 일부개정법률안에 대한 의견표명	국회 보건복지위원장
	「학교 밖 청소년 지원에 관한 법률」일부개정법률안에 대한 의견표명	여성가족부
2016	안심 알리미서비스 사업의 인권침해 여부 검토요청에 대한 의견표명	부산광역시 기장군수
	학교 밖 청소년 지원에 관한 법률 일부개정법률안에 대한 의견표명	여성가족부장관
2017	저소득층학생 정보화지원시 인터넷 사용양태 정보수집 관련 의견표명	경기도교육감
	특성화고 취업관련 홍보계시물과 관련한 의견표명	17개 시도 교육감
2018	「아동복지법 일부개정법률안」에 대한 의견표명	국회의장
	학교폭력 사건 축소·은폐에 의한 인권침해	1. ○○초등학교장 2. 군포의왕교육지원청교육장
2019	중학교 배정 시 민감정보 요구	1. 광명교육지원청 교육장 2. 경기도교육감
	초등학교 지문인식 출입시스템 설치로 인한 인권침해	대구광역시교육감
	아동에 대한 수사내용 언론공표로 인한 인격권 등 침해	경찰청장

의결 연도	권고(의견표명)제목	피권고기관
2020	학생상담시스템 운용에 대한 정책권고	교육부장관
	중학교 전학 시 교육지원청의 개인정보 요구에 관한 의견표명	1. 강서양천 교육지원청 교육장 2. 서울특별시교육감
	스마트폰 통제 어플리케이션 사용에 따른 아동의 사생활 등 기본권 침해 방지를 위한 정책 권고	방송통신위원회위원장
	아동복지시설 CCTV 설치 및 운영 관련 의견표명	보건복지부장관

자료: 국가인권위원회 정보공개 수정¹⁴³⁾

이 가운데 국가인권위원회가 2003년 5월 교육행정정보시스템(NEIS)의 개선을 권고한 사례는 정보화 환경에서 개인정보 자기결정권을 중요한 인권으로 인정했다는 점에서 큰 주목을 받았다¹⁴⁴⁾. NEIS 결정은 국가가 학생을 비롯한 정보 주체의 민감한 개인정보를 수기 또는 비통신 데이터베이스 방식으로 수집·관리 하던 환경으로부터 통신망을 통해 단일한 데이터베이스에 집적하는 환경으로 변화했을 때 기본권에 미치는 효과 및 이를 제한하는 요건에 대한 문제를 다루었다. 국가인권위원회는 학교행정의 전산화와 개인정보 처리에 관한 초·중등 교육법과 교육기본법의 일반적인 규정에도 불구하고 NEIS에 대해 특별히 규율하는 법적 근거가 필요하다고 보았으며, 사생활 침해가 큰 보건 등의 영역은 NEIS의 처리 대상에서 제외하고 종전의 비통신데이터베이스 방식인 CS방식을 사용할 것을 교육인적자원부 장관에게 권고했다. 이후 2003년 국무총리 산하에 설치된 교육정보화위원회에서 정부와 교원·학부모·시민단체가 NEIS 시스템에 대한 개선에 합의했다. 또 2005년 3월 24일 NEIS에 대한 법률적 근거 규정으로 초·중등교육법 제30조의4(교육정보시스템의 구축·운영 등)가 신설되면서 현재는 이러한 법적 근거를 기반으로 개인보건의록을 비롯한 교육개인이정보가 NEIS에서 처리되고 있다.

143) 2021년 8월 9일 정보공개

144) 국가인권위원회 2003. 5. 12. 교육행정정보시스템 관련 권고

2) 개인정보보호위원회 침해 구제

한국에서 개인정보보호권은 국민의 기본권으로 법률로 보호하고 있다. 헌법재판소는 2005년 ‘개인정보 자기결정권’을 새로운 기본권으로 선언했고(헌법재판소 2005.5.26, 99헌마513), 2011년 「개인정보보호법」이 제정되었다.

개인정보보호법은 만 14세 미만 아동인 정보주체로부터 개인정보의 수집과 이용에 대한 동의를 받을 때 법정대리인의 동의를 받도록 했다(제22조, 제39조의3). 이때 개인정보처리자는 △개인정보의 수집·이용 목적 △수집하려는 개인정보의 항목 △개인정보의 보유 및 이용 기간 △동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 불이익의 내용 등에 대해 정보주체에게 알려야 하며(제15조 제2항), 특히 정보통신서비스 제공자가 아동으로부터 이와 관련한 동의를 받을 때는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용해야 한다(제39조의3 제5항). 더불어 아동을 비롯한 정보주체는 자신의 개인정보에 대한 열람(제35조), 정정·삭제(제36조), 처리정지(제37조) 등의 권리를 행사할 수 있으며, 아동의 법정 대리인은 개인정보처리자에게 아동 개인정보에 대한 열람 등을 요구할 수 있다(제38조 제2항).

3) 개인정보보호법 아동의 개인정보 처리 관련 규정

제22조(동의를 받는 방법)

⑥ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위해 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위해 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

제38조(권리행사의 방법 및 절차)

② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람 등 요구를 할 수 있다.

제39조의3(개인정보의 수집·이용 동의 등에 대한 특례)

- ④ 정보통신서비스 제공자는 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 대통령령으로 정하는 바에 따라 법정대리인이 동의했는지를 확인해야 한다.
- ⑤ 정보통신서비스 제공자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용해야 한다.
- ⑥ 보호위원회는 개인정보 처리에 따른 위험성 및 결과, 이용자의 권리 등을 명확하게 인지하지 못할 수 있는 만 14세 미만의 아동의 개인정보 보호 시책을 마련해야 한다.

개인정보보호위원회는 개인정보보호법에 따라 설치된 독립적인 개인정보보호 감독기관으로서 정보주체의 권리침해에 대한 조사와 이에 따른 처분권, 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정권 등을 보유하고 있다(제7조의8 제3호 및 제4호). 또한 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리나 이익을 침해받은 사람은 보호위원회에 침해 사실을 신고하고 상담을 받을 수 있다(제62조)¹⁴⁵⁾.

개인정보보호법이 제정·시행된 2011년 9월 30일부터 2020년 12월 31일까지 만 14세 미만 아동의 개인정보 처리와 관련해 개인정보침해 신고센터에 접수된 침해 현황은 <표 5-4>와 같다. 법정대리인의 동의가 없는 아동 개인정보 수집 신고가 전체 침해 접수건수에 비해 매우 적은 비율이지만 꾸준히 접수되고 있다.

145) 다만, 2020년 2월 4일 개인정보보호법이 개정되기 전까지 개인정보보호위원회의 조사 및 처분권은 공공기관에 한정되어 있었으나, 행정안전부로부터 개인정보보호위원회로 순차적으로 이관된 개인정보분쟁조정위원회, 개인정보침해 신고센터의 경우 그 설립시부터 공공기관과 민간사업자를 아울러 업무를 수행해왔음.

〈표 5-4〉 만 14세 미만 아동의 개인정보침해 신고 및 상담 접수 현황

(기간: 2011 ~ 2020)

사유	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
법정대리인 동의없는 수집	71	47	36	33	34	33	49	92	78	60
전체	122,215	166,801	177,736	158,900	152,151	98,210	105,122	164,497	159,255	177,457

자료: 개인정보보호위원회 정보공개¹⁴⁶⁾

한편, 같은 기간 만 14세 미만 아동의 개인정보 처리와 관련해 개인정보 분쟁 조정을 신청한 사례는 〈표 5-5〉와 같았다. 비록 매우 적은 사례이지만 실제 분쟁 사유는 만 14세 미만 아동에 대한 법정대리인의 동의권 행사보다 더 다양한 것을 볼 수 있다.

〈표 5-5〉 만 14세 미만 아동의 개인정보 분쟁조정 현황

(기간: 2011 ~ 2020)

신청 년도	분쟁내용	조치결과
2019	게임회사가 신청인의 개인정보를 동의 없이 수집하고 미파기한 행위	법정대리인으로부터 개인정보 수집 동의를 받았고, 법률에 따른 개인정보 보존의무가 있어 미파기한 것으로 보호법 위반사항이 없으므로 기각
2020	CCTV에 촬영된 마스크 미착용한 신청인의 사진을 승강기에 게시	신청인의 요구에 의해 신청취하
2021	신청인의 대화 수상내용(학교, 학년, 이름)이 적힌 현수막을 학원 외벽에 게시	현수막 제거하는 것으로 조정전 합의

자료: 개인정보보호위원회 정보공개¹⁴⁷⁾

더불어 개인정보보호위원회는 2015년 7월 24일 신설된 법 제8조의2(개인정보

146) 2021년 5월 16일 정보공개. 다만, 아동과 관련한 항목으로 '법정대리인 동의 없는 아동개인정보 수집' 항목 하에서만 통계가 집계되고 있었음.

147) 2021년 5월 16일 정보공개

침해요인 평가) 조항에 따라 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하려는 중앙행정기관 소관 법령의 제정이나 개정안에 대해 개인정보 침해요인을 분석·검토해 법령의 소관기관의 장에게 개선을 위해 필요한 사항을 권고할 수 있다. 제도 신설 후 2020년 12월 31일까지 개인정보 침해요인 평가가 이루어진 경우는 6건이었다. 대부분은 원안에 동의하는 가운데 「학교 밖 청소년 지원에 관한 법률」 일부개정안에 대해 청소년 정보주체의 권리 행사를 좀 더 보장할 것을 요구했다.

〈표 5-6〉 만 14세 미만 아동 관련 개인정보 침해요인 평가

(기간 : 2015 ~ 2020)

의결 연도	의안명	결과
2016	학교 밖 청소년 지원에 관한 법률 일부개정안에 대한 개인정보 침해요인 평가 결과	<ul style="list-style-type: none"> - '친권자' 용어를 '법정대리인'으로 변경 - 친권자등과 연락이 되지 않는 경우에는 청소년 본인의 의사와 관계없이 청소년의 개인정보를 지원센터에 제공할 수 있도록 하고 있는데, 이는 청소년의 개인정보자기결정권을 침해할 소지가 있다 할 것이므로, 법정대리인 뿐 아니라 청소년과도 연락이 되지 않는 경우에 한해 청소년의 개인정보를 지원센터에 제공할 수 있도록 변경할 필요가 있음. - "연락이 되지 않을 때"의 구체적 기준을 하위법령에 위임할 수 있도록 위임 근거를 마련할 것 - 청소년 및 친권자등의 동의 없이 청소년의 개인정보가 제공된 경우 사후 동의를 받도록 할 때, 개인정보자기결정권을 보호하기 위해 고지사항에 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 추가하고 동의를 거부할 경우 개인정보를 즉시 파기해야 함을 명시할 필요가 있음 - 개인정보 처리 기준과 절차를 하위법령에 구체적으로 규정하는 위임 근거를 마련할 필요가 있음

의결 연도	의안명	결과
2018	정보통신망이용촉진 및 정보보호등에 관한 법률 시행령 일부개정안에 대한 개인정보 침해요인 평가 결과	원안 동의
	보호시설에 있는 미성년자의 후견 직무에 관한 법률 시행령 일부개정안에 대한 개인정보 침해요인 평가 결과	원안 동의
2019	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부개정안에 대한 개인정보 침해요인 평가 결과	원안 동의
	위치정보의 보호 및 이용 등에 관한 법률 시행령 일부개정안에 대한 개인정보 침해요인 평가 결과	원안 동의
2020	마리나항만의 조성 및 관리 등에 관한 법률 시행규칙 일부개정안에 대한 개인정보 침해요인 평가 결과	원안 동의

자료: 개인정보보호위원회 정보공개¹⁴⁸⁾

한편 방송통신위원회는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 ‘정보통신망법’)에 따라 정보통신서비스 제공자의 개인정보 처리에 대해 조사하고 처분해왔으나, 2020년 8월 5일 개인정보보호법이 개정·시행되면서 해당 권한을 개인정보보호위원회로 이관했다. 이관 전 방송통신위원회가 만 14세 미만 아동의 개인정보 처리와 관련해 조사하고 처분한 사례는 <표 5-7>과 같다.

<표 5-7> 만 14세 미만 아동 관련 정보통신망 개인정보 침해 처분

(기간: 2008 ~ 2020)

의결일자	처분 대상	위반 내용
2008. 11. 14.	야후코리아	14세 미만 아동의 개인정보 수집 시 정당한 법정 대리인 여부를 확인할 수 있도록 업무처리 절차개선 명령, 과태료 2천만 원

148) 2021년 5월 16일 정보공개.

의결일자	처분 대상	위반 내용
2008. 11. 14.	SK커뮤니케이션즈(주)	14세 미만 아동의 개인정보 수집 시 정당한 법정 대리인 여부를 확인할 수 있도록 업무처리 절차개선 명령, 과태료 2천만 원
2008. 11. 14.	(주)다음커뮤니케이션	14세 미만 아동의 개인정보 수집 시 정당한 법정 대리인 여부를 확인할 수 있도록 업무처리 절차개선 명령, 과태료 3천만 원
2008. 11. 14.	NHN(주)	14세 미만 아동의 개인정보 수집 시 정당한 법정 대리인 여부를 확인할 수 있도록 업무처리 절차개선 명령, 과태료 3천만 원
2010. 10. 20.	(주)잉카인터넷	만 14세 미만 아동의 개인정보를 수집하면서 법정 대리인의 동의를 받지 않음, 과태료 5백만 원(다른 위반 종합)
2011. 11. 23.	한국옵손(주)	만 14세 미만 아동의 개인정보를 수집하면서 법정 대리인의 동의를 받지 않음, 과징금 3,300만원 및 과태료 900만 원(다른 위반 종합)
2020. 6. 4.	익명	만 14세 미만 아동의 개인정보를 수집하면서 법정 대리인의 동의를 받지 않음, 과태료 4백5십만 원(다른 위반 종합)
2020. 7. 15.	익명	만 14세 미만 아동의 개인정보를 수집하면서 법정 대리인의 동의를 받지 않음, 과징금 1억8천만 원 및 과태료 6백만 원 (다른 위반 종합)

자료: 개인정보보호위원회 정보공개¹⁴⁹⁾

우리 개인정보보호법 체계에 따라 이루어진 침해와 구제 사례를 종합하면, 공적 구제기관이 아동의 개인정보 침해를 접수하고 처리하는 사례 대다수는 만 14세 미만 아동 법정대리인의 동의권과 관련한 사항으로서 관련 통계 항목도 해당 표제로만 집계되고 있었다. 현행 법률에 따라 만 14세 미만 아동의 개인정보 처리에 대한 권리는 법정대리인만이 행사할 수 있으며 성숙도에 따라 아동이 법정대리인과 공동으로 행사하는 것은 허용되지 않는다. 반면 만 14세 이상 만 18세 미만 아동의 개인정보는 별다른 보호 규범 없이 전적으로 성인과 동일하게

149) 2021년 8월 11일 정보공개

처리된다.

그러나 일회성으로 끝나는 법정대리인의 동의는 이후 지속적으로 이용되는 아동의 개인정보에 대한 충분한 보호조치로 보기 어려운 한계가 있다(전운선 외, 2020). 취약한 정보주체인 아동의 개인정보가 디지털 환경에 항상 연결되어 있고 상업적 목적으로 처리되는 경우가 늘면서 앞서 유럽 규범에서 살펴보았듯이 아동을 보호하기 위해 보다 정교한 규범 수립이 필요하다. 앞서 아동의 개인정보 처리와 관련한 실제 분쟁 사례 또한 법정대리인 동의권 행사를 넘어 파기, 게시 등 보다 다양한 쟁점을 아우르고 있었다.

만14세 미만은 물론 성년에 도달하지 않은 아동은 취약한 정보주체로서 개인정보 처리 문제를 일반 성인의 개인정보 처리 사례와 구분해 취급하고, 특히 디지털 개인정보 처리 환경이 대규모로 확산되는 만큼 아동의 개인정보 처리에 기반한 마케팅, 프로파일링과 자동화된 의사결정에 대한 금지 방안을 마련할 필요가 있다. 개인정보처리자는 능동적으로 아동 최선의 이익과 발달의 권리를 존중하며 아동의 개인정보를 공정하고 투명하게 처리해야 한다. 아동의 민감정보 처리 또한 더욱 엄격하게 제한되어야 한다. 아동의 개인정보는 시간이 지남에 따라 정확성과 관련성이 떨어지기 때문에 특히 “개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리해야 하며, 그 목적 외의 용도로 활용해서는 아니 된다.(개인정보보호법 제3조 제2항)”는 원칙과 “개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 해야 한다(법 제3조 제3항)”는 원칙이 아동의 개인정보에 대해 더욱 엄격하게 준수될 필요가 있다. 아동의 개인정보에 대한 유출 등 보안성 보장은 아동의 전 생애에 걸쳐 영향을 미칠 우려가 있으므로 더욱 엄격한 기준이 필요하며, 개인정보보호 중심 설계와 기본 설정 도입이 바람직하다.

더불어 프로파일링과 자동화된 의사결정을 비롯해 갈수록 복잡해지는 개인정보 처리 전반과 효과에 대한 정보를 아동과 법정대리인에게 보다 명확하고 투명하게 제공해야 한다. 만 14세 미만 아동이더라도 자신의 개인정보 처리에 대해 해당

연령에 적합한 정보를 제공받고, 성숙도에 따라 법정대리인과 동의권을 공동으로 행사하는 제도 개선도 검토해볼 만하다. 나아가 만 14세 미만 시점에 법정대리인이 개인정보 처리에 동의했더라도, 정보주체인 아동 본인의 동의나 동의철회 의사가 추후 반영될 수 있도록 보장될 필요도 있다. 즉, 아동의 개인정보보호 규범은 일회적 법정대리인의 동의권 보장이라는 소극적 수준을 넘어 아동의 개인정보 처리 주기 전반에 대한 규범으로 수립될 필요가 있다. 관련해 2021년 8월 5일 개정시행된 개인정보보호법은 아동에게 직접 효력을 미치는 “정보통신서비스 제공자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용해야 한다.”는 규정을 정보통신망법으로부터 이관해 규율하기 시작했다(법 제39조의3 제5항). 나아가 정부는 2021년 9월 28일 국회에 발의한 「개인정보보호법 일부개정법률안」(의안번호: 2112723)에서 아동 정보주체의 보호 규정을 정비했다. 개정안은 국가 등의 책무로 “국가와 지방자치단체는 만 14세 미만 아동이 개인정보 처리가 미치는 영향과 정보주체의 권리 등을 명확하게 알 수 있도록 만 14세 미만 아동의 개인정보보호에 필요한 시책을 마련해야 한다(안 제5조 제3항)”는 규정을 신설하고, 각 조항에 분산된 아동의 개인정보보호 규정을 하나의 규정으로 종합했다(안 제22조의2).

무엇보다 아동을 위한 개인정보보호 시책에 의무가 있는 개인정보보호위원회(법 제39조의3 제6항)가 보다 적극적으로 관련 정책을 개발, 시행할 필요가 있다. 최근 개인정보보호위원회는 아동의 개인정보보호를 강화하기로 하고 2021년 3월 30일 미취학 아동 교육용 콘텐츠인 <개인정보보호 첫걸음>을 보급한 데 이어¹⁵⁰⁾, 아동·청소년 정보보호 가이드라인(지침)을 개발 중이다¹⁵¹⁾.

150) ‘개인정보보호 첫걸음’ 미취학 아동 교육용 콘텐츠 보급 (2021. 3. 30). <개인정보보호위원회 보도자료>

151) 연합뉴스(2021. 8. 4). 개인정보위원장 “연내 아동·청소년 개인정보보호 가이드라인” 제정

4) 자치법규 침해 구제

아동·청소년과 학생의 인권을 보호하기 위해 제정된 자치법규들은 모두 사생활에 대한 보호 규정을 포함하고 있다. 특히 각급 학교 학생의 개인정보 보호와 프라이버시권 침해 문제는 교육자치단체들의 학생인권조례에 따라 다루어져왔다.

〈표 5-8〉 아동·청소년과 학생 권리 관련 자치법규

분류	자치단체	조례	제정
학생 인권조례	경기도교육청	경기도 학생인권 조례	2010. 10. 5. 제정
	광주광역시교육청	광주광역시 학생인권 조례	2011. 10. 28. 제정
	서울특별시교육청	서울특별시 학생인권 조례	2012. 1. 26. 제정
	전라북도교육청	전라북도 학생인권 조례	2013. 7. 12. 제정
	충청남도교육청	충청남도 학생인권 조례	2020. 7. 10. 제정
	제주특별자치도교육청	제주특별자치도교육청 학생인권 조례	2021. 1. 8. 제정
아동· 청소년 인권조례	서울특별시	서울특별시 어린이·청소년 인권 조례	2012. 11. 1. 제정
	경기도부천시	부천시 아동·청소년 인권 조례	2016. 4. 4. 제정
	강원도동해시	동해시 아동·청소년 인권 보장에 관한 조례	2019. 3. 15. 제정
	경기도성남시	성남시 아동 인권 조례안	2021. 4. 5. 제정

제정 이후 2020년 12월 31일까지 아동·청소년의 프라이버시권과 개인정보 보호권에 대한 침해 구제 실적이 실제 있는 자치법규는 경기도 학생인권조례, 광주광역시 학생인권조례, 서울특별시 학생인권조례, 전라북도 학생인권조례이다. 다만 사생활과 관련된 침해 및 권리 구제 사례 대부분은 학생의 용모와 소지품 등에 대한 문제로 개인정보 처리와 디지털 환경에 대한 침해 사례는 유의미하게 나타나지 않았다¹⁵²⁾. 다만 경기도교육청의 경우 휴대전화와 개인정보에 대한 침해, 구제 통계를 따로 집계하고 관련 실태조사를 한 바 있다. 이하

152) 2021년 5월~8월 정보공개를 종합한 서울특별시 어린이·청소년 인권 조례, 동해시 아동·청소년 인권 보장에 관한 조례, 부천시 아동·청소년 인권 조례의 경우 제정 이후 2020년 12월 31일까지 침해 및 구제 사례가 없었음. 성남시 아동 인권 조례안, 충청남도 학생인권 조례, 제주특별자치도 교육청 학생인권 조례의 경우에는 관련 통계 생성이 1년 이내로 유의미하지 않았음.

에서는 경기도교육청의 관련 사례를 중심으로 살펴본다.

경기도교육청 「경기도 학생인권 조례」는 제2장 학생의 인권에서 제4절 사생활의 비밀과 자유 및 정보에 관한 권리를 두고, 제11조(개성을 실현할 권리), 제12조(사생활의 자유), 제13조(사생활의 비밀을 보호받을 권리), 제14조(정보에 관한 권리)를 규정하고 있다¹⁵³⁾. 권리구제기구로는 학생인권옹호관을 두고 학생 인권 침해에 대한 상담, 조사, 권고 및 구제를 소관한다.

153) 제12조(사생활의 자유) ① 학생은 부당한 간섭 없이 개인 물품을 소지·관리하는 등 사생활의 자유를 가진다.

② 교직원은 학생과 교직원의 안전 등을 위해 긴급히 필요한 경우가 아니면 학생의 동의 없이 소지품 검사를 해서는 아니 된다. 교직원이 교육목적으로 필요해 불가피하게 학생의 소지품 검사를 하는 경우 그 검사는 필요한 최소한의 정도에 그쳐야 하며, 전체 학생을 대상으로 하는 일괄검사를 해서는 아니 된다.

③ 교직원은 일기장이나 개인수첩 등 학생의 개인적인 기록물을 열람하지 않는 것을 원칙으로 하며, 교육목적상 필요한 경우에도 신중을 기해야 한다.

④ 교장 등은 학생의 휴대전화 소지 자체를 금지해서는 아니된다. 다만, 교육활동과 학생의 학습권을 보장하기 위해서 수업시간 등 정당한 사유와 제18조에 따라 휴대전화 소지 및 사용을 규제할 수 있다.

⑤ 교장 등은 다른 방법으로는 안전 등 목적을 달성하기 어려운 경우에만 폐쇄회로 텔레비전(CCTV)을 설치할 수 있으며, 설치 여부나 설치 장소에 관한 학생의 의견을 수렴하고 설치장소를 누구나 쉽게 알 수 있게 표시해야 한다.

제13조(사생활의 비밀을 보호받을 권리) ① 학생은 가족, 교우관계, 성적, 징계기록, 교육비 납부여부 등 개인정보를 보호받을 권리를 가진다.

② 교장 등은 학생에게 교외에서의 이름표 착용을 강요해서는 아니 된다.

③ 교육감, 경영자, 교장 등은 학생에 관한 정보를 수집·처리·관리함에 있어서 적법하고 적정한 수단과 절차에 따라야 한다.

④ 교장 등은 학생에 관한 개인정보를 본인 또는 보호자의 동의 없이 공개하거나 타인에게 제공해서는 아니 된다.

⑤ 누구든지 학생에게 불이익이 될 수 있는 개인정보를 알게 된 경우에는 이를 함부로 누설해서는 아니 된다.

제14조(정보에 관한 권리) ① 학생 또는 보호자는 학생 본인에 관한 학교 기록을 언제든지 열람할 권리를 가진다.

② 학생은 학교에 대해 학생에게 영향을 미치는 정보의 공개를 청구할 권리를 가진다. 이 경우 학교의 장은 「개인정보보호법」, 「공공기관의 정보공개에 관한 법률」 및 「교육관련기관의 정보공개에 관한 특례법」에 따른 절차에 따라 처리해야 한다.

③ 학생 또는 보호자는 학생 본인에 관한 기록 중에 부정확한 내용, 교육활동과 직접적인 관련성이 없는 내용, 학생의 권리를 부당하게 침해하는 내용 등에 대해 정정이나 삭제할 권리를 가진다.

④ 학교의 장은 예·결산 등 학교 재정 관련 정보를 학생이 쉽게 알 수 있는 내용과 방법으로 공개해야 한다.

경기도교육청 학생인권옹호관이 2019년~2020년에 걸쳐 사생활의 비밀과 자유와 정보에 관한 권리 규정과 관련해 상담·조사·구제한 현황은 <표 5-9>와 같다. 사생활 관련 침해 및 구제건수는 전체 754건 중 103건(2019년)과 전체 411건 중 62건(2020년)으로 나타났다. 2020년에는 코로나19로 비대면수업이 실시되어 상담·조사·구제 건수가 전체적으로 감소했음에도 사생활 관련 침해, 구제 비중은 13.7%에서 15.1%로 오히려 증가했다.

<표 5-9> 경기도교육청 사생활 권리 관련 학생인권 상담·조사·구제 건수

구분	2019년			2020년		
	상담	조사	구제	상담	조사	구제
사생활의 비밀과 자유 및 정보에 관한 권리 (제4절) 관련 건수	76	15	12	53	4	5
전체 건수	646	69	39	375	23	13

자료: 경기도교육청 정보공개¹⁵⁴⁾

이러한 환경 변화 속에서 <2020년 경기도 학생인권 실태조사>는 디지털 환경과 비대면 온라인 환경의 증가가 학생인권에 미친 실태를 조사했다(이정연·김명랑·권경림·최보미, 2020). 우선 사생활과 개인정보 관련 학교 환경이라고 할 수 있는 교내 CCTV 안내, 개인정보 공개, 학교기록 열람권 행사에 대한 질의에서 경기도 학생의 응답은 <표 5-10>과 같다. 학교가 가족관계·가정형편 등 개인 정보를 동의 없이 공개하는 문제는 과거 많은 논란이 되었으나 이에 대해 ‘전혀 그렇지 않’거나 ‘그렇지 않은 편’이라고 답변한 학생이 전체 90.9%에 달했다는 사실은 개인정보 무단노출 사례가 줄어든 것으로 평가할 수 있을 듯하다. 다만 학생의 가정형편에 대한 개인정보 뿐 아니라 학생과 가족구성원의 인종, 출신 국가, 장애, 종교 등에 대한 개인정보는 학생에 대한 차별을 초래할 수 있다는

154) 2021년 5월 26일 정보공개. 통계는 조례 제4절을 모두 포함하는 관계로 사생활의 자유(휴대폰 등) 및 사생활의 비밀(개인정보 등) 관련 사안 뿐 아니라 개성을 실현할 권리(복장, 두발 등)도 포함되어 있었음.

점에서 학교 측에서 계속 주의할 필요가 있어보인다. 한편, CCTV 안내나 학교기록 열람권의 경우에는 개인정보보호법 등 관련 법률이 보장하고 있는 권리임에도 전혀 그렇지 않거나 그렇지 않은 편이라고 답변한 학생이 각 53.4% (학교에서 교내 CCTV에 대한 안내가 되어 있는지)와 40.7%(본인의 학교기록을 언제든지 볼 수 있는지)로 상당히 높게 나타났다. 2011년 개인정보보호법이 제정 되는 등 개인정보 관련 법제도가 최근 크게 발전해왔고 학생들의 권리의식 또한 높아진 만큼, 학교당국이 개인정보보호법을 준수하고 학생의 개인정보에 대한 권리 행사를 보장하기 위해 인식과 관행을 개선하는 조치를 취할 필요가 있어 보인다.

〈표 5-10〉 교내 사생활 권리 보장 관련 경기도 학생 응답

질의	구분	전혀 그렇지 않다	그렇지 않은 편이다	그런 편이다	매우 그렇다	전체
학교에서 교내 CCTV에 대한 안내가 되어 있는지	초	842	1,979	2,256	995	6,072
		13.9	32.6	37.2	16.4	100.0
	중	1186	2,647	2,387	542	6,762
		17.5	39.1	35.3	8.0	100.0
	고	804	1,760	1,543	297	4,404
		18.3	40.0	35.0	6.7	100.0
합계	2,832	6,386	6,186	1,834	17,238	
		16.4	37.0	35.9	10.6	100.0
학교에서 동의 없이 개인정보를 공개하는지	초	4,442	1,163	250	217	6,072
		73.2	19.2	4.1	3.6	100.0
	중	3,868	2,248	499	147	6,762
		57.2	33.2	7.4	2.2	100.0
	고	2,263	1,686	367	88	4,404
		51.4	38.3	8.3	2.0	100.0
합계	10,573	5,097	1,116	452	17,238	
		61.3	29.6	6.5	2.6	100.0

질의	구분	전혀 그렇지 않다	그렇지 않은 편이다	그런 편이다	매우 그렇다	전체
본인의 학교기록을 언제든지 볼 수 있는지	초	1,366	2,217	1,855	634	6,072
		22.5	36.5	30.6	10.4	100.0
	중	548	2,109	3,440	665	6,762
		8.1	31.2	50.9	9.8	100.0
	고	109	673	2,764	858	4,404
		2.5	15.3	62.8	19.5	100.0
	전체	2,023	4,999	8,059	2,157	17,238
		11.7	29.0	46.8	12.5	100.0

자료: 2020년 경기도 학생인권 실태조사 수정

실태조사는 학생들이 중요하게 생각하는 휴대전화 지도와 관리 방식에 대한 조사를 포함했다. 앞서 국가인권위원회는 휴대전화는 학생에게도 생활필수품인 만큼, 교내 휴대전화 사용제한 필요성이 있더라도 학생들의 자유로운 의사를 존중하고 기본권 침해를 최소화할 수 있는 방법을 고려해야 한다고 보았다. 그러나 아직도 학생이나 학급이 휴대전화를 자율관리하기 보다 일괄 수거하거나 금지하는 비중이 49.8%에 달하는 것으로 나타났다.

〈표 5-11〉 학교에서 휴대전화 지도와 관리 방식에 대한 경기도 학생 응답

구분	학생 자율관리	학급별 자율결정	수업 중 일괄수거 (수업별로 제출)	학교생활 중 일괄수거 (등교 후 일괄제출)	학교반입 금지	기타	전체
초	3,440	1,050	129	192	162	1,099	6,072
	56.7	17.3	2.1	3.2	2.7	18.1	100.0
중	801	269	200	5,290	40	162	6,762
	11.8	4.0	3.0	78.2	0.6	2.4	100.0
고	1,568	201	90	2,470	18	57	4,404
	35.6	4.6	2.0	56.1	0.4	1.3	100.0
전체	5,809	1,520	419	7,952	220	1,318	17,238
	33.7	8.8	2.4	46.1	1.3	7.6	100.0

자료: 2020년 경기도 학생인권 실태조사 수정

특히 실태조사는 온라인 교육환경에 대한 인권 실태에 주목했다. 실태조사는 코로나19 위기로 교육 분야에서도 비대면 온라인수업이 확대되었고 온라인 공간도 교육의 주된 환경으로 자리잡게 되었다고 진단했다(이정연 외, 2020). 그간 온라인 공간에서 나타난 학생의 인권침해는 공교육이 진행되는 교육과정 문제라기 보다 또래간의 관계와 생활 속에서 일어나는 문제가 대부분이었다. 하지만 이제는 온라인이 수업과 교육활동이 진행되는 공간인 만큼 인권침해의 현장으로 새로운 주의가 요구된다는 것이다.

관련해 실태조사는 학생과 교사 이미지의 온라인 유포, 온라인 수업의 개인정보 노출 경험에 대해 질의했다. 이에 대한 학생 응답은 전체 17,238명 중 1,123명이 온라인에서 자신이나 친구의 얼굴이 캡처·합성·유포된 것을 본 적이 있다고 답변했고, 교사 이미지의 경우 763명이 본 적이 있다고 답변했다. 또한 온라인수업 중에 개인정보가 동의 없이 공개된 적이 있다는 답변은 298명이었다. 이처럼 그렇다고 답변한 학생의 비율은 높지 않지만 절대적인 답변수가 적지 않았다는 사실에 주목할 필요가 있다. 실태조사는 교사도 유사한 경험을 한 것을 확인했고, 경험한 교사의 비율이 학생보다 더 많았다고 지적했다. 학생과 교사를 비롯한 학교 구성원들이 온라인 학교생활을 계속해 접할 것으로 예상되는 점에서 온라인 개인정보의 노출에 대해 학생은 물론 학교당국의 주의를 요한다고 볼 수 있다. 실태조사는 온라인 교육환경에 대한 인권침해의 기준과 지침 등의 정비를 제언했다.

〈표 5-12〉 온라인 이미지 및 개인정보 노출 경험에 대한 경기도 학생 응답

질 의	구분	그렇다	아니다	전체
온라인에서 자신 또는 친구의 얼굴이 캡처·합성·유포된 것을 본 적이 있는지	초	199	5,873	6,072
		3.3	96.7	100.0
	중	634	6,128	6,762
		9.4	90.6	100.0
	고	290	4,114	4,404
		6.6	93.4	100.0
전체	1,123	16,115	17,238	
	6.5	93.5	100.0	
온라인에서 선생님의 수업장면이나 얼굴이 캡처·합성·유포된 것을 본 적이 있는지	초	155	5,917	6,072
		2.6	97.4	100.0
	중	387	6,375	6,762
		5.7	94.3	100.0
	고	221	4,183	4,404
		5.0	95.0	100.0
전체	763	16,475	17,238	
	4.4	95.6	100.0	
온라인수업 중에 개인정보가 동의 없이 공개된 적이 있는지	초	103	5,969	6,072
		1.7	98.3	100.0
	중	123	6,639	6,762
		1.8	98.2	100.0
	고	72	4,332	4,404
		1.6	98.4	100.0
전체	298	16,940	17,238	
	1.7	98.3	100.0	

자료: 2020년 경기도 학생인권 실태조사 수정

제2절 ● 인공지능 관련 규범과 아동·청소년

교육 분야를 비롯한 사회 각 영역에서 인공지능 기술의 적용과 자동화된 의사결정이 빠른 속도로 확대되면서 이러한 환경 변화가 아동·청소년의 권리에 미치는 영향에 대한 관심과 우려 또한 커지고 있다. 아동권리 옹호를 위해 활동하는 유엔기구인 유니세프는 오늘날 아동들이 이미 인공지능과 다양한 방식으로 상호작용하고 있다고 강조한다(UNICEF, 2020)¹⁵⁵⁾. 인공지능 기술은 장난감, 가상 비서, 비디오 게임에 내장되어 있고 챗봇과 적응 학습 소프트웨어를 구동하는 데에도 사용된다. 알고리즘은 아이들에게 다음에 어떤 비디오를 볼지, 어떤 뉴스를 읽을지, 어떤 음악을 들을지, 누구와 친구가 될지를 추천한다. 아동의 권리는 인공지능과 이러한 직접적인 상호작용 외에도, 복지 보조금, 의료와 교육서비스 접근, 가족의 주택 신청에 대한 자동화된 의사결정 시스템에 의해 간접적인 영향을 받는다. 유니세프는 인공지능이 혁신적인 힘으로 지속가능한 개발 목표의 달성을 지원할 수 있지만, 동시에 아동의 사생활, 안전, 보안에 대한 위험을 내포하고 있다고 경고한다. 특히 인공지능 시스템은 눈에 띄지 않고 대규모로 작동할 수 있기 때문에 광범위한 배제와 차별의 위험이 현실적이다.

지난해 영국에서는 코로나로 인해 취소된 대학입학시험 대신 인공지능으로 성적을 부여했다가 부유한 지역 학생이 높은 점수를 받고 가난한 지역 학생이 낮은 점수를 받은 것으로 드러나 큰 사회적 논란이 일어났다¹⁵⁶⁾. 미국에서는 십대 흑인 여성 청소년이 얼굴인식에 실패해 가게에 들어가지 못하는 사례가 발생했고¹⁵⁷⁾, 카메라와 마이크 등을 통해 학생 정보를 수집하고 부정행위를 판단하는

155) UNICEF(2020). Policy guidance on AI for children: Draft 1.0. 초안은 계속 업데이트될 예정이며 다음 버전은 2021년 하반기 발표 예정.

156) 이향규(2020. 9. 7). 사는 곳으로 성적을 결정했다: 가난한 지역 공립학교 학생들에게 낮은 점수 준 알고리즘, 실패한 실험이 남긴 과제. <한겨레21> 제1329호.

157) WATCH: This Teenager was Misidentified by Facial Recognition and Thrown out of a Roller Rink. *Fight for the Future*. <https://www.fightforthefuture.org/actions/watch-this-teenager-was-misidentified-by-facial-recognition-and-thrown-out-of-a-roller-ri>

인공지능 시험감독이 학생의 피부색을 인식하지 못해 부정행위로 표시하는 등 프라이버시 침해와 불공정성 논란이 일었다¹⁵⁸). 대화형 인형 등 인공지능 장난감이 아이들과의 대화는 물론 부모, 주변 사람들과의 대화를 모두 녹음하고 이를 제3자인 회사와 공유하는 아동온라인프라이버시보호법(COPPA) 위반 논란이 제기되었다¹⁵⁹).

이에 유엔은 물론 세계 각국이 인공지능과 아동·청소년의 권리 보장을 위한 규범들을 수립하고 있다. 이하에서는 인공지능과 아동·청소년의 프라이버시권 문제를 중심으로 해당 규범들을 살펴보고자 한다.

1. 국제규범과 인공지능

1) 인공지능 관련 국제인권규범과 아동·청소년

유니세프는 2019년부터 세계 각지에서 전문가 및 아동 워크숍을 개최하고 세계적인 실태조사를 거쳐 2020년 9월 <아동을 위한 인공지능에 대한 정책 지침 (Policy guidance on AI for children)> 초안을 발표했다¹⁶⁰). 유니세프는 이 지침에서 인공지능 시스템과 상호작용하는 아동을 보호하고 역량을 강화해 삶의 모든 측면에서 인공지능의 혜택에 접근할 수 있도록 지원하고자 했다. 인공지능 정책과 시스템은 아동을 보호하고, 필요와 권리에 공평하게 응하고, 아동이 인공지능의 발전과 사용 과정에 참여할 수 있도록 역량을 강화해야 한다. 특히 유니세프는 이 지침에서 디지털 환경에서 아동의 권리를 보장하기 위해 9가지

nk/?link_id=0&can_id=263ccb09bfb263fde931e703e9051c10&source=email-facial-recognitions-racismon-kids-2&email_referrer=email_1239932&email_subject=facial-recognitions-racismnilnilon-kids (검색일 : 2021. 9. 1).

158) Schools Are Abandoning Invasive Proctoring Software After Student Backlash (2021. 2. 26). VICE. <https://www.vice.com/en/article/7k9ag4/schools-are-abandoning-invasive-proctoring-software-after-student-backlash> (검색일: 2021. 9. 1). 미국 정보 인권단체 EPIC은 콜롬비아 법무장관에 Proctorio, Respondus, Examity, ProctorU, Honorlock 등의 시험 감시 서비스에 대한 조사를 요청했음

159) (2021. 7. 12). 말하는 장난감 ‘헬로 바비’... 개인정보 유출 위험 <한국경제TV>.

160) UNICEF(2020). 앞의 자료.

아동 중심 인공지능(child-centered AI)에 대한 요구사항을 정부와 기업에 제시했다.

그 중 아동의 개인정보와 프라이버시권 보호에 대한 요구사항도 다음과 같이 포함되었다. 우선, 인공지능 정책과 시스템은 아동 개인정보와 사생활의 가치와 고유한 취약성을 인식해야 한다. 아동의 개인정보는 아동이 생성한 콘텐츠, 아동에 대해 수집된 정보들, 알고리즘을 통해 추론된 사항을 포함한다. 아동의 개인정보보호에 대한 규정 준수에서 더 나아가 출신지역과 생체인식정보 등 소외집단과 민감한 정보에 대한 특별한 보호가 요구된다.

따라서 정부와 기업은 아동을 위한 데이터와 아동에 대한 데이터 처리에서 책임있는 데이터 접근법을 취할 필요가 있다. 아동이 취약계층이라는 점을 감안할 때, 아동의 개인정보는 최고 수준으로 보호되어야 한다. 또한 아동 개인정보 이용에 대한 거버넌스는 인공지능 시스템이 아동에 대한 충분한 데이터를 사용해 아동에게 최고의 혜택을 제공해야 할 필요성과 프라이버시와 보안에 대한 최소한의 위험을 보장하기 위해 데이터 수집을 최소화해야 할 필요성 사이에 균형적으로 수립되어야 한다. 또한 정부와 기업은 아동의 개인정보에 대한 권한을 알려야 한다. 아동의 연령과 성숙도에 따라 개인정보를 열람하고, 안전하게 공유하며, 이용에 대해 이해하고 통제, 삭제하는 기능을 갖춰 아동과 대리인이 개인정보에 대한 권한을 행사할 수 있도록 지원해야 하는 것이다. 개인정보 처리 동의에 대한 아동의 이해는 변화할 수 있기 때문에, 아동의 생애 주요 발달단계에서 동의절차가 다시 제공되어야 한다.

프라이버시 중심 설계의 채택도 중요하다. 정부와 기업은 아동의 프라이버시 문제를 명시적으로 인식하고 이를 인공지능 시스템의 설계와 구현에 적용해야 한다. 아동의 프라이버시와 개인정보에 대한 보호는 표현의 자유, 정보접근권 및 프로파일링과 디지털 마케팅 등을 통한 경제적 착취로부터의 보호와 복잡하게 얽혀 있다. 특히 인공지능 환경에서 집단 수준의 보호도 고려될 필요가 있다. 프로파일링은 더 이상 개인에게만 국한된 문제가 아니라 개인의 민족적 출신, 위치, 온라인 행동과 연령 등 광범위한 특성을 기반으로 한 개인들의 집합과도

관련된다. 개인의 프라이버시권을 보호할 뿐 아니라 집합적 관점을 취해 문화적 다양성과 같은 집단의 특성을 보호할 필요가 있는 것이다.

한편, 지침은 최근 인공지능 규범에서 많이 언급되는 설명가능성과 투명성에 대한 상세한 요구사항도 제시했다. 설명가능성과 투명성은 아동 이용자와 부모나 보호자를 비롯한 일련의 이해관계자가 인공지능 시스템의 목적과 잠재적 영향을 이해할 수 있어서 이러한 플랫폼의 사용여부를 결정할 수 있는 역량을 갖추게 한다는 점에서 중요하다. 그러나 이 요구사항은 설명에 사용되는 언어를 단순화 하는 것만으로 달성될 수 없다. 자녀의 시스템 사용을 동의하는 부모와 보호자에게 더 나은 정보를 제공할 수 있어야 하고, 인공지능 제품의 작용과 영향에 대해 책임있는 인공지능 정책과 서비스의 입안자, 규제자, 설계자, 개발자, 운영자와 조달자의 책임구현이 이루어져야 한다. 인공지능 시스템의 설명가능성과 투명성은 아동을 명시적으로 다루는 것이 바람직하다. 장난감, 챗봇, 온라인 시스템 등 인공지능 시스템과 직접 상호작용하는 아동에게 시스템이 어떻게 작동하고 그들의 개인정보를 어떻게 사용하고 관리하는지를 이해할 수 있도록 애니메이션을 비롯한 연령에 적합한 설명이 제시되어야 한다. 아동이 인공지능 시스템과 직접 상호작용 하면서 자신이 인간과 상호작용하고 있다고 착각하는 상황을 방지하기 위해, 솔직한 방식으로 그 사실을 통지해야 한다. 또한 의료 진단, 복지 결정 또는 학교 신청 등 아동의 중요한 인생 결정에 영향을 미치는 인공지능은 인간의 개입 없이 사용되어서는 안 되며, 아동과 보호자에게 그러한 중요 의사결정에 인공지능 시스템이 사용되었음을 알려야 한다. 더불어 인공지능 시스템의 개발이 아동의 이해 부족이나 취약성을 무시하거나 악용할 수 없도록 법적이고 정책적인 규제와 감독 체계가 마련되어야 한다.

2021년 9월 유엔 인권최고대표가 유엔인권이사회 제48차 회기에서 인공지능과 프라이버시권에 대한 보고서를 발표했다¹⁶¹⁾. 최고대표는 보고서에서 인공지능 시스템이 프라이버시권을 침해하게 되는 기능적 요인을 살펴보았다.

161) The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights. 유엔문서번호 A/HRC/48/31.

인공지능 시스템은 일반적으로 개인정보를 포함한 대용량 데이터세트에 의존한다. 데이터 수집은 온라인 서비스와 사물인터넷을 비롯해 사적이고 공적인 장소를 가리지 않고 이루어진다. 데이터에 포함된 개인정보가 수집·결합·분석·공유되는 규모는 전례없는 비율로 증가했다. 이러한 데이터세트의 유통은 기업과 국가에 사람들의 사생활을 노출하는 것 외에도 여러 가지로 개인들을 취약하게 만든다. 개인에 대한 무수한 분석과 제3자 공유는 종종 추가적인 프라이버시 침해로 이어지고 인권에 부정적인 영향을 끼친다. 다양한 출처의 데이터를 결합함으로써 기존에 익명이었던 개인이 식별될 가능성이 증가한다. 정량적 데이터세트 설계는 개인에게 특정한 정체성 분류를 강요하기도 한다. 또한 개인정보의 장기간 보관은 수집 당시 예상하지 않았던 장래의 악용가능성을 낳는다. 시간이 지나면서 데이터가 부정확해지거나 부적절해지거나 편견에 따른 오인을 초래해 향후 편향되고 오도된 결과를 초래할 수도 있다.

인공지능 시스템은 개인정보가 관련되지 않았더라도 인권에 부정적인 영향을 미칠 수 있다. 인공지능 도구는 개인의 정신적, 신체적 상태를 비롯해 광범위한 추론을 수행할 수 있으며 특정 정치적·개인적 성향을 가진 사람들 집단을 식별할 수 있다. 인공지능은 또한 미래의 행동이나 사건이 일어날 가능성을 평가하기도 한다. 인공지능이 만든 추론과 예측은 확률적 특성에도 완전히 자동화된 방식으로 사람들 권리에 영향을 미치는 의사결정의 기반이 될 수 있다. 인공지능의 추론과 예측은 사람들의 자율성과 자신의 정체성에 대한 세부사항을 확립할 권리를 포함해, 프라이버시권 향유에 깊은 영향을 미친다. 사상과 의견의 자유에 대한 권리, 표현의 자유, 공정한 재판 관련 권리 등 다른 권리에도 문제를 야기할 수 있다.

인공지능 기반 결정은 오류에서 자유롭지 않다. 인공지능 솔루션의 확장성은 작아보였던 오류율의 부정적인 영향을 극적으로 증가시킬 수 있다. 인공지능 알고리즘의 출력에는 확률적 요소가 있으며, 결과물에도 불확실성이 포함되어 있다. 사용된 데이터의 관련성과 정확성이 의심스러운 경우도 있다. 결함이 있는 데이터에 의존하는 인공지능 시스템의 출력물은 예를 들어, 한 개인을 부정수급자로

잘못 지목해 추가적인 인권 침해의 원인이 될 수 있다. 인공지능 시스템의 편향된 데이터세트가 차별적 의사결정으로 이어지는 경우가 특히 우려된다.

무엇보다 많은 인공지능 시스템의 의사결정과정은 불투명하다는 점이 큰 문제이다. 인공지능 시스템의 개발과 운영을 뒷받침하는 정보환경, 알고리즘, 모델의 복잡성은 물론 정부와 민간행위자들의 의도적인 비밀주의가 일반대중이 인공지능 시스템의 영향을 이해하는 과정을 방해한다. 불투명성으로 인해 인공지능 시스템을 유의미하게 조사하는 것이 어려워지고 인공지능 시스템이 위해를 야기하는 경우에도 효과적인 책무성 확보가 어려울 수 있다.

이처럼 최고대표는 인공지능의 특성이 프라이버시권리에 영향을 미치는 방식과 양상을 다양한 측면에서 검토했으며, 최고대표의 지적 사항은 발달과 성장 과정이 특히 중요한 아동의 프라이버시권을 인공지능 환경에서 능동적으로 보호해야 할 필요성을 시사한다. 이들 문제를 해결하기 위한 최고대표의 권고는 ‘인권 기반 접근’으로 요약할 수 있다. 최고대표는 데이터 기반 인공지능 시스템에서 개인정보보호법으로 정보주체를 효과적으로 보호해야 할 필요성을 강조했다. 설명에 대한 권리와 완전 자동화 의사결정에 반대할 권리 등 개인의 권리를 강화하고 인공지능 기술의 발전에 부응하는 더 많은 안전장치를 개인정보보호 체계 내에 수립할 필요가 있다. 방대한 정보 비대칭성을 비롯한 글로벌 데이터 환경의 복잡성과 불투명성 증가에 대응하기 위해 독립적인 개인정보보호 감독기관의 중요성 또한 더욱 커졌다.

특히 최고대표는 기업이 원인이 되었거나 초래했거나 직접 관련된 부정적인 인권 영향을 식별, 평가, 방지, 완화하기 위한 인권영향평가의 실시를 강조했다. 인권영향평가를 실시할 때에는 인공지능이 십대 여성 등 취약한 상황에 있는 사람들에게 불균형한 영향을 미치는 것에 각별한 주의를 기울여야한다.

2) 인공지능 관련 유럽 규범과 아동·청소년

유럽평의회 인권위원장은 2019년 보고서에서 회원국 인공지능 시스템의 발전과 구현에서 중대하게 영향을 받는 당사자들(affected individuals) 특히

아동의 의견수렴, 정보제공, 권리구제를 요구했다(Council of Europe Commissioner for Human Rights, 2019)¹⁶²⁾. 이 보고서에서 인권위원장은 회원국들이 인공지능으로부터 권리에 부당한 영향을 받을 위험성이 큰 ‘아동’ 등의 사회집단에 대한 차별을 방지해야 한다고 강조했다.

특히 유럽연합은 인공지능 사용환경에서 권리주체를 보호하는 법제도를 도입해왔으며 아동 보호에 대해 강조해 왔다. 관련 유럽연합 규범은 크게 인공지능 의사결정에서 정보주체의 권리를 보장하는 개인정보보호 관련 법률 규범과 인공지능 관련 시장규제를 추진하는 법률 규범으로 나뉘볼 수 있다. 우선 2016년 제정된 유럽연합 개인정보보호 일반법인 GDPR은 인적 개입이 전혀 없는 완전 자동화된 의사결정에서 정보주체가 대상이 되지 않을 권리를 규정했다(제22조). GDPR은 ①정보주체에게 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 의사결정이고 ②자동화로 처리되는 의사결정을 ③오로지 자동화된 처리 방식에만 의존해 이루어지는 경우를 일반적으로 금지했다. 다만 계약의 체결이나 이행을 위해 필요한 경우, 법률이 허용하는 경우, 정보주체의 명시적인 동의에 근거한 경우는 예외적으로 완전 자동화 의사결정이 허용된다. 이때 GDPR은 아동의 개인정보를 프로파일링 등 자동화된 방식으로 처리하거나 자동화된 의사결정에서 이용할 경우 처리자에게 추가적인 의무를 부과한다. 원칙적으로 완전 자동화 의사결정은 아동에 적용되어서는 안 된다(전문71). 다만 아동의 복지보호 등을 위해 개인정보처리자가 프로파일링을 포함해 법적 효력이나 이와 유사하게 중대한 영향을 미치는 자동화 방식에만 근거한 의사결정을 내려야 하는 경우가 있을 수 있다. 이 경우 해당 처리는 위 예외 조항을 근거로 시행될 수 있다. 그럼에도 GDPR은 아동이 사회 내 취약계층에 속하기 때문에, 일반적으로 기업은 마케팅 목적으로 아동의 개인정보를 프로파일링하지 않을 것을 권장한다. 아동은 온라인 환경에 특히 취약할 수 있고 행태 맞춤형 광고에 더 쉽게 영향을 받을 수 있다. 예를 들어 온라인게임에서 맞춤형 광고 제공이나

162) Council of Europe Commissioner for Human Rights (2019). Unboxing artificial intelligence: 10 steps to protect human rights.

프로파일링은 해당 게임에 돈을 가장 많이 지출할 것 같은 이용자를 대상으로 활용될 수 있다. 이러한 마케팅의 숨겨진 의도나 이로 인한 결과를 이해할 수 있는 능력은 아동의 나이나 성숙도에 영향을 받을 수 있다¹⁶³⁾.

예외적으로 완전 자동화 의사결정을 실시하는 경우 정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 보호조치가 반드시 마련되어야 한다. 특히 아동에 대한 완전 자동화 의사결정에 대한 보호 조치는 아동에게 반드시 적절해야 한다. 이때의 보호조치는 프로파일링과 완전 자동화 의사결정 유무, 관련된 로직에 관한 구체적이고 유의미한 정보, 처리의 중대성과 이로 인해 발생할 수 있는 결과 등을 정보주체에게 사전적으로 설명하고, 그에 대해 정보주체가 인적 개입을 요구할 권리, 본인의 의견을 피력할 권리, 결정에 대한 설명을 들을 권리, 결정에 이의를 제기할 권리 등을 보장하는 것을 포함한다. 더불어 처리자는 처리한 데이터 세트에서 편견이 있는지 확인하고, 이를 해결할 수 있는 방법을 개발해야 한다. 또 알고리즘을 검사하고 자동화 의사결정의 정확성과 관련성을 주기적으로 검토해 개선에 반영해야 한다.

최근 학교에서 도입한 인공지능 얼굴인식 시스템과 개인정보보호법 위반 논란이 커졌다. 2019년 7월 프로방스알프코트다쥐르(PACA) 지역 당국은 프랑스 개인정보보호 감독기관 CNIL에게 마르세유 암페어 고등학교 출입관리용 얼굴인식 시스템의 사용의 허가를 요청했다. 이 시스템의 도입 취지는 신분도용 사실을 적발하고 비인가자의 학교 접근을 방지하는 학교 보안요원의 업무를 원활히 해 학생과 교직원의 보안을 강화하고 학생들이 학교 진입에 걸리는 시간을 단축하는데 있었다. 이 사업은 같은 지역 다른 학교에서도 동일하게 실시되는 1년간의 '시범 사업'이었으며, 학생과 학부모의 동의에 근거해 실시될 예정이었다. 그러나 CNIL과 마르세유지방법원은 이 시스템이 위법하다고 판단했다. 시스템이 표방하고 있는 출입통제 목적 그 자체는 공공기관의 정당한 목표라고 할 수 있지만, 명찰을

163) EU Article 29 Data Protection Working Party (2017). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation. 2016/679, V.Children and Profiling. 29.

사용하는 등 덜 침해적인 대안이 있을 경우 학교 얼굴인식 시스템이 필요하지 않다는 것이 CNIL의 지적이었다. 나아가 단지 학교 출입을 목적으로 대규모로 미성년자를 대상으로 얼굴인식을 사용하는 것은 침해적 감시로서 비례적이지 않다고 보았다. 법원도 암페어 얼굴인식 시범사업이 이 두 기준을 크게 위반했다고 판단했다. 특히 공공기관과 학생 사이의 권력 관계로 인해 동의는 개인정보 처리의 합법적 근거가 되지 못한다고 보았다. 또한 유럽연합법 전반에 걸쳐 아동·청소년에 대해 강화된 보호가 적용되어 있고 생체인식정보는 GDPR상 매우 민감한 정보이기 때문에 미성년자 생체인식정보는 최고 수준의 보호가 필요한데 비해 암페어는 이를 충족시키지 못했다고 지적했다.

2019년 8월 20일 스웨덴 개인정보보호 감독기관이 학생 출석 확인에 안면인식 기술을 사용한 셸레프테오 시 고등학교위원회에 벌금 20만 크로나(약 2천500만 원)의 과징금을 부과했다. 해당 교육위원회는 이 지역의 한 고등학교에서 약 3주에 걸쳐 학생 22명을 대상으로 안면인식 기술을 이용한 출석확인을 시범 실시했다. 교육위원회는 학생과 부모의 동의를 받았다고 주장했으나 감독기관은 유효한 동의로 보지 않았다. 감독기관의 결정에 대해 교육위원회는 법원에 항소했으나 행정법원이 이를 기각해 확정됐다¹⁶⁴).

유럽연합은 개인정보보호법 체계와 별도로 인공지능에 대한 구체적인 규율 또한 추진해왔다. 유럽연합 인공지능 규제 프레임워크는 특히 아동 등 취약한 사람들의 권리 보장에 주의를 기울여왔다. 우선 유럽연합이 2019년 4월 채택한 ‘신뢰가능 인공지능 가이드라인’은 신뢰가능 인공지능의 기반으로 ‘아동’ 등 인공지능 기술이 불이익을 주거나 기술 혜택으로부터 배제될 가능성이 있는 취약한 집단을 고려하고 권력과 정보 불균형에 대응할 것을 요구했다. 나아가 유럽 집행위원회는 2021년 4월 21일 “인공지능법안”을 유럽의회에 발의했다¹⁶⁵).

164) 스웨덴, ‘안면인식 기술로 학생 출석 확인’ 시당국에 벌금 (2019, 8, 28). <연합뉴스>. https://gdprhub.eu/index.php?title=KamR_Stockholm_-_Case_No._5888-20 (검색일 : 2021. 8. 31).

165) Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

유럽연합은 인공지능 규제법에서 고위험 인공지능에 대해 법적 의무 부과를 추진하고 있다. 이때 학교 등 교육 및 직업 훈련과 관련해 사용되는 인공지능은 고위험에 속하며, (a) 교육 및 직업 훈련 기관에 대한 접근을 결정하거나 자연인을 할당할 목적으로 사용되는 인공지능 시스템 (b) 교육 및 직업 훈련 기관의 학생을 평가하고 교육기관 입학에 대해 일반적으로 요구되는 시험참가자를 평가하기 위한 목적으로 사용되는 인공지능 시스템은 일정한 요구사항을 충족해야 시장에 출시될 수 있다. 얼굴인식 등 모든 원격 생체인식 시스템 또한 고위험으로 간주된다. 이 법과 별개인 법률에 따라 규제되는 장난감 제품의 안전 구성요소로 인공지능이 사용되는 경우에도 고위험 인공지능 요구사항이 적용된다.

고위험 인공지능에 대한 요구사항으로는 우선 위험관리 시스템과 품질관리 시스템을 갖추도록 하고, 위험성과 차별적 결과를 완화, 최소화하기 위해 사용 데이터세트의 고품질을 보장하도록 하며, 기술문서를 작성하고 로그기록을 보관해 인공지능 결과물을 추적하고 감독기관에 필요한 정보를 제공할 수 있도록 했다. 또한, 사용자에게 명확하고 적절한 정보를 제공해 투명성을 보장하도록 하고, 위험성을 최소화하기 위해 적절한 인적 감독조치를 마련하도록 했으며, 높은 수준의 견고성·정확성·보안성을 보장하도록 했다. 특히 고위험 인공지능 시스템에 대한 위험관리 시스템의 구축·시행에서 아동이 고위험 인공지능 시스템에 접근하거나 영향을 받을 가능성이 있는지 여부에 각별한 주의를 기울여야 한다(법안 제9조(8)). 고위험 인공지능 시스템을 시장에 출시하거나 서비스를 제공하기 전 인공지능 시스템이 법률의 요구사항을 준수하고 있다는 것을 보장하는 적합성 평가를 자체적으로 수행해야 하는데, 인공지능 시스템이 장난감의 구성요소로 사용되는 경우에는 제3자 적합성 평가 절차를 거쳐야 한다.

무엇보다 인공지능법안은 아동이나 장애인과 같은 취약집단의 약점을 이용해 정신적·신체적 피해를 초래하는 방식으로 그들의 행동을 현저히 왜곡할 잠재성이 큰 인공지능을 금지했다(전문16).

2. 국내 법제와 인공지능

1) 개인정보보호법과 인공지능

국내에서는 인공지능 챗봇 ‘이루다’의 개인정보보호법 위반 논란이 크게 불거졌다. 특히 이 인공지능 챗봇은 만 14세 미만 아동의 개인정보를 위법하게 사용해 높은 행정 제재가 부과되었다. ‘이루다’는 2020년 12월 출시된 인공지능 챗봇으로, 스무살 여대생과 대화를 나누는 것 같은 자연스러운 대화 능력을 선보여, 출시 2주 만에 약 75만 명에 달하는 이용자를 모으며 10~20대 사이에서 크게 인기를 끌었다. 그러나 일부 남성 이용자들이 이루다를 성적 대상으로 취급하고, 이루다 발화내용에 여성·성소수자·장애인·흑인을 혐오하는 내용이 포함되어 인공지능 윤리와 차별 논란을 빚었다. 무엇보다 회사가 이루다를 개발하는 과정에서 이전에 출시한 다른 애플리케이션 이용자의 개인정보를 불법적으로 이용했다는 혐의가 불거져 개인정보보호위원회의 조사를 받게 되었다¹⁶⁶⁾.

2021년 4월 28일 개인정보보호위원회는 인공지능 챗봇 ‘이루다’ 개발사 (주)스캐터랩에 대해 총 1억 330만원의 과징금과 과태료 등을 부과했다. 전체 과징금과 과태료 비중 중 법정대리인의 동의 없이 만 14세 미만 아동의 개인정보를 수집한 행위를 내용으로 한 처분은 총 5,120만원으로 전체의 49.6%에 달한다. 스캐터랩은 2013년 출시한 ‘텍스트앳’과 2016년 출시한 ‘연애의과학’의 회원 개인정보를 위법하게 이용해 인공지능 챗봇 이루다를 학습시키고 출시했다. 이때 카카오톡 대화 메시지에 대한 감정분석서비스를 내세운 ‘텍스트앳’을 이용한 만 14세 미만 아동은 4만 8천 명으로 추정되고, 마찬가지로 카카오톡 대화메시지에 대한 연애심리검사를 내세운 ‘연애의 과학’을 이용한 만 14세 미만 아동은 12만 명에 달하는 것으로 추정되었다. 이루다를 이용한 만 14세 미만

166) 개인정보위, ‘이루다’ 개발사 (주)스캐터랩에 과징금·과태료 등 제재 처분 (2021, 4, 29). <개인정보보호위원회 보도자료>; 성희롱·혐오논란에 3주만에 멈춘 ‘이루다’…AI윤리 숙제 남기다 (2021, 1, 11). <연합뉴스>.

아동은 3만 9천 명으로 추정되었다¹⁶⁷⁾.

‘텍스트엣’은 이용자가 회원으로 가입할 때 직업을 초중고/대학생/일반인 중에서 선택하도록 하면서, 이용자가 직업을 초중고로 설정하거나 회원가입 후 저장된 직업을 초중고로 변경하는 경우에도 별도의 법정대리인 동의 절차를 두고 있지 않았다. 직업을 초중고로 입력한 이용자 숫자에는 만 14세 미만인 자와 만 14세 이상인 자가 모두 포함되므로 스캐터랩과 개인정보보호위원회는 만 14세 미만이 식별되는 ‘이루다’와 ‘연애의 과학’의 전체 이용자 대비 만 14세 미만 아동 비율의 평균 수치를 적용해 ‘텍스트엣’ 전체 이용자를 4만 8천 명으로 추정했다. ‘연애의 과학’의 경우 이용자가 회원으로 가입할 때 버전 1.0에서 출생연도를 입력하도록 하고 있고, 버전 2.0에서는 ‘관심을 두고 있는 연령대’ 정보를 수집했는데, 이 경우 별도의 법정대리인 동의 절차를 두고 있지 않았다. 스캐터랩과 개인정보보호위원회는 해당 이용자 숫자에 생일이 지난 만 14세 이용자가 포함되어 있고, 관심연령이 실제 나이와 일치한다고 할 수 없다는 이유로 만 14세 미만임을 인정할 수 있는 이용자는 12만 명으로 추정했다. 한편, 페이스북 기반의 챗봇인 ‘이루다’의 경우 페이스북 회원만을 대상으로 제공했으나, 이용자가 ‘이루다’ 챗봇을 이용할 때 페이스북 가입절차와 별도로 이름, 나이, 성별 등을 입력하도록 하면서 이용자가 나이를 만 14세 미만으로 설정하는 경우에도 ‘이루다’ 서비스를 이용할 수 있도록 했으며 별도의 법정대리인 동의 절차를 두고 있지 않았다¹⁶⁸⁾.

이에 대해, (주)스캐터랩은 ‘텍스트엣’과 ‘연애의 과학’은 애플 앱스토어, 구글 플레이스토어, 윈스토어에서 서비스되고 있는데, 앱스토어와 플레이스토어의 경우 만 14세 미만 아동 이용자가 앱 구입을 요청하거나 다운로드할 때 부모의 승인을 요구하고, 윈스토어는 19세 미만 이용자 사용을 제한하므로, 만 14세 미만 아동 개인정보 수집에 대한 법정대리인의 동의가 결여되어 위법한 것이라고 볼 수는 없다고 주장했다. 그러나 개인정보보호위원회는 개인정보보호법 제22조

167) 국회의원 배진교 요청자료 회신(2021. 9. 1).

168) 개인정보보호위원회 2021. 4. 28. 제2021-007-072호 심의·의결서.

제6항의 입법취지 등에 비추어 볼 때 개인정보처리자는 앱스토어의 기능과 상관없이 스스로 제공하는 서비스와 관련해 만 14세 미만인 아동의 개인정보를 수집하는 경우에는 법정대리인의 동의를 받아야 할 의무가 있다고 보았다.

이 사건 이후 개인정보보호위원회는 2021년 5월 31일 <인공지능(AI) 자율 점검표>를 발표하고 인공지능의 개발·운영에 참여하는 자의 개인정보보호에 대한 인식을 제고하고 개인정보보호법 준수를 요구했다. 특히 이 지침에서는 우리 법률에 아직 도입되어 있지 않았으나 국제적으로 통용되는 개인정보보호 중심 설계 원칙 등을 반영했다¹⁶⁹⁾. 인공지능 서비스 특성상 예상치 못한 개인정보 침해가 발생할 수 있으므로 기획 단계부터 사전점검과 예방을 위해 개인정보보호 중심 설계원칙을 적용하고, 침해가 우려되는 경우 개인정보 영향평가를 수행하도록 했다.

더불어 개인정보보호위원회는 개인정보보호법 개정을 통해 완전 자동화 의사결정에서 정보주체의 권리를 보장하기 위한 방안을 추진하고 있다. 정부가 2021년 9월 28일 국회에 발의한 「개인정보보호법 일부개정법률안」(의안번호: 2112723)은 '자동화된 결정에 대한 정보주체의 권리 등'에 대한 조항을 신설하고 정보주체가 완전 자동화 의사결정에 대한 거부, 설명 등을 요구할 수 있도록 했다(안 제37조의2)¹⁷⁰⁾. 다만 입법예고안은 정보주체가 사전적으로 프로파일링은 물론 자동화 의사결정의 로직과 그 결과에 대한 정보를 통지받고 자신의 의견을 피력하거나 인적 개입을 요구할 수 있는 권리를 보장하고 있지 않다는 점에서

169) 개인정보위, 인공지능(AI) 자율점검표 발표 (2021, 5, 31). <개인정보보호위원회 보도자료>.

170) 개인정보보호위원회 공고 제2021-1호, 개인정보보호법 일부개정법률(안) 입법예고안.

“제37조의2(자동화 의사결정에 대한 배제등의 권리) ① 정보주체는 다음 각 호에 따른 자동화된 개인정보 처리에만 의존해 특정 정보주체에게 개별적으로 법적 효력 또는 생명·신체·정신·재산에 중대한 영향을 미치는 의사결정을 행한 개인정보처리자에 대해 그 거부, 이의제기, 설명 등을 요구할 수 있다. 다만, 거부 요구는 제2호에 한한다.

1. 제15조제1항제1호, 제2호, 제4호

2. 제15조제1항제3호, 제5호, 제6호, 제7호

② 제1항에 따른 요구를 받은 개인정보처리자는 특별한 사정이 없는 한 그 요구에 따라 배제, 재처리, 설명 등 필요한 조치를 해야 한다.

③ 개인정보처리자는 제1항에 따른 자동화 의사결정의 기준과 절차를 대통령령이 정하는 바에 따라 정보주체가 사전에 쉽게 인식할 수 있도록 알리는 등 필요한 조치를 해야 한다.”

한계가 있다. 또한 국가인권위원회는 입법예고안에 대한 의견에서 정보주체에게 완전 자동화 의사결정을 받지 않을 권리가 있음을 원칙적으로 규정하고, 자동화 의사결정을 바로 정보주체에 적용하기보다 예외적으로 합리적이고 정당한 범위 내에서만 허용되는 것이 바람직하다고 보았다. 또한 자동화 의사결정에 의해 생성된 민감정보를 처리할 때 ‘중대한 공익상의 목적을 위해 법률이 허용하는 경우’와 ‘정보주체의 명백한 동의’ 등 더 엄격한 조건을 규정할 필요가 있다고 지적했다¹⁷¹⁾.

2) 서울특별시교육청 인공지능 가이드라인

2021년 9월 서울특별시교육청은 <인공지능(AI) 공공성 확보를 위한 현장 가이드라인>을 발표했다. 교육청은 학교에서 인공지능(AI)을 활용한 교육이 활발해짐에 따라 전국 최초로 학생의 개인정보보호와 데이터 처리 과정의 투명성과 안전성을 확보하기 위해 현장 가이드라인을 개발했다고 밝혔다¹⁷²⁾. 특히 가이드라인은 학교에서 인공지능을 도입할 때 ‘인공지능(AI) 등급 평가 매트릭스’와 ‘인공지능(AI) 영향 평가 체크리스트’를 사용해 인공지능에 기반한 결정의 영향을 평가하도록 했다. 이들 매트릭스와 체크리스트는 인공지능 영향평가 방안은 인공지능에 대한 해외 위험기반 접근법을 참고해 개발됐다(김기중·임완철·장여경, 2021).

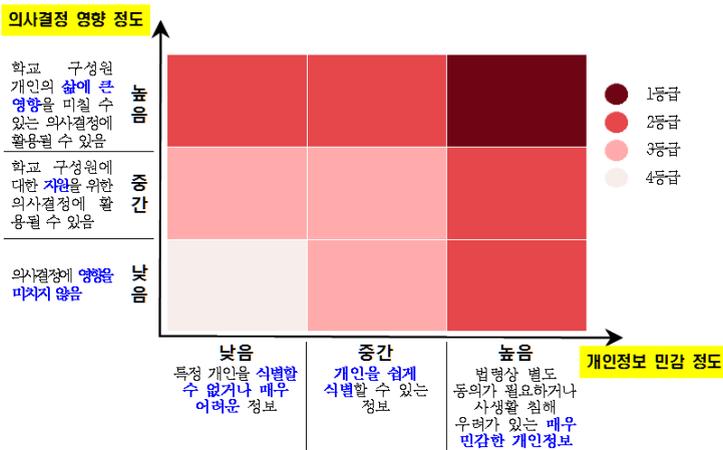
특히 이 가이드라인은 공교육에서 인공지능 적용 여부를 결정하는 기준으로 ‘개인정보 보호’를 들었다. 즉 공교육에서 인공지능을 도입하는 주체는 인공지능이 학습하거나 수집·이용하는 개인정보가 윤리와 인권 관점에서 보호되어야 하고, 그 적용 결과를 평가하고 필요한 조치를 취하기 위한 절차와 체계를 만들어야 한다. 이를 위해 인공지능 등급평가 매트릭스의 기준으로 ‘의사결정 영향 정도’와

171) 국가인권위원회 (2021). 「개인정보보호법 일부개정법률안」 의견 요청에 대한 회신.

172) 서울시교육청, 인공지능(AI) 공공성 확보를 위한 현장 가이드라인 공청회 개최(2021, 7, 30). <서울특별시교육청 보도자료>; 서울특별시교육청 (2021). <인공지능(AI) 공공성 확보를 위한 현장 가이드라인>.

함께 ‘개인정보 민감 정도’를 제시하고 인공지능 영향 등급을 평가하도록 했다. 이때 개인정보 민감정도는 특정 개인을 식별할 수 없거나 매우 어려운 정보는 민감도가 ‘낮음’으로, 개인을 쉽게 식별할 수 있는 정보는 민감도가 ‘중간’으로, 법령상 별도 동의가 필요하거나 사생활 침해 우려가 있는 매우 민감한 개인정보는 민감도가 ‘높음’으로 구분했다. 매트릭스상으로 영향 정도 수준에 따라 단위학교에 도입되는 인공지능을 바로 사용 가능하거나(4등급), 교내 AI위원회(3등급)나 외부위원을 포함하는 학교 AI위원회(2등급)에서 심의와 조치를 거쳐 사용하거나, 교육청 AI위원회(1등급) 심의를 거쳐 채택, 조치하도록 했다.

한편, 가이드라인은 인공지능 등급평가 후 인공지능의 도입 가능성 점검 목적으로 인공지능 영향 평가 체크리스트를 제공했다. 체크리스트는 교내나 학교 인공지능위원회에서 심의시 업체담당자로부터 체크리스트 항목별 내용을 확인받고, 적합하지 않은 부분이 있는 경우 업체와 조율해 도입여부 결정 목적으로 사용된다. 개인정보보호 체크리스트는 개인정보보호위원회의 <인공지능(AI) 개인정보보호 자율점검표>를 준수하도록 했다.



[그림 5-1] 서울특별시교육청 인공지능 등급 평가 매트릭스

제3절 • 소결

ICT 환경의 발달로 개인정보에 대한 권리가 발전했고, 세계 각국 이를 반영해 개인정보보호 법체계 하에서 아동·청소년의 개인정보를 보호하고 있다. UN과 유럽연합 등은 보호의 객체이자 권리의 주체로서 아동·청소년의 프라이버시를 보호하기 위해 다양한 규범을 발전시켜왔다. 아동·청소년의 권리에 대한 가장 권위 있는 국제인권규범인 유엔 아동권리협약 제16조는 “1. 어떠한 아동도 사생활, 가족, 가정 또는 통신에 대해 자의적이거나 위법적인 간섭을 받지 아니하며 또한 명예나 신망에 대한 위법적인 공격을 받지 아니한다. 2. 아동은 이러한 간섭 또는 비난으로부터 법의 보호를 받을 권리를 가진다”고 규정해 아동의 프라이버시권을 보호하고 있고, 유엔 아동권리위원회는 2021년 ‘일반논평 25호’ 디지털 환경에서 아동의 권리 보장을 발표하며 디지털 환경에서 아동의 프라이버시권과 개인정보에 대한 권리 침해에 대해 우려를 표했다.

유럽연합 GDPR도 아동을 정적 관점에서 신체적·정신적으로 성숙에 이르지 못한 사람이자 동적인 관점에서 신체적·정신적으로 발달에 이르는 과정에 있는 사람으로 보고 아동의 권리를 두 관점 모두를 인식하는 방식으로 행사해야 한다고 보고 있다. 유럽연합은 16세 미만이나 각국별 최소 13세 미만의 아동이 인터넷 서비스에 가입할 때 친권자의 동의를 받도록 했고, 국제규범에 따른 18세 미만 모든 아동에 대해 개인정보 처리에 따른 위험에 대한 인지가 부족할 수 있고 ‘취약한’ 정보주체로서 특별히 보호하며 아동의 개인정보를 수집하고 처리하는 자에게 추가적인 보호조치를 요구하고 있다. 아동으로부터 ‘설명기반 동의’를 얻었다고 인정받기 위해서는 반드시 아동이 이해할 수 있는 명확하고 쉬운 언어로 개인정보 처리를 설명해야 하며, 아동의 개인정보에 대해서는 정당한 이익에 기반해 처리하는 것이 합법성의 근거로 인정되지 않고, 마케팅 목적이나 프로파일링 처리에서는 아동의 이익에 대한 특별한 보호가 필요하다고 본다.

영국 개인정보보호 감독기관인 ICO는 아동 대상 서비스에서 높은 개인정보

보호 기준을 기본 설정으로 하는 ‘연령적합설계 실행규칙’을 마련했고, 2021년 9월부터 시행하고 있다. ‘아동 최선의 이익 원칙(Best Interests of the Child)’하에 연령별로 적합한 서비스 적용과 정보 제공, 권리 행사 보장을 요구하고 있다. 규칙에 따르면, 아동의 개인정보는 최소한만 수집하고 설득력 있는 이유가 없는 한 공유가 원칙적으로 금지되며 위치정보와 프로파일링 기능은 기본 설정에서 해제해 두어야 한다. 아동에게 해로운 방식이나 나쁜 선택을 유도하는 설계는 금지된다. 미국은 개인정보보호에 대한 일반법이 없음에도 아동의 온라인 개인정보를 보호하기 위해 2000년부터 ‘아동 온라인 프라이버시 보호법(COPPA)’을 특별법으로 시행해오고 있다. COPPA의 주요 보호 원칙은 ① 개인정보 처리 방침의 공개 ② 부모에 대한 고지 및 동의 ③ 개인정보 열람·삭제 요청 등 부모의 검토권(Review) ④ 정보보안 및 보유·파기 등을 규정하고 있다.

국내의 경우 아동·청소년의 프라이버시 보호 등과 관련해, 개인정보보호위원회가 국제규범과 「개인정보보호법」에 근거해 침해 사건에 대한 권리구제를 하고 있고, 국가인권위원회와 서울특별시 등 지방자치단체가 아동·청소년 인권관련 조례에 따라 아동·청소년 인권침해에 대한 권리구제 활동을 하고 있다. 개인정보보호법의 아동의 개인정보 처리 관련 규정은 만 14세 미만 아동의 개인정보와 관련해 법정대리인의 동의권과 관련한 사항이 유일해, 만 14세 이상 만 18세 미만 아동의 개인정보는 별다른 보호 규범 없이 성인과 동일하게 처리되는 문제점이 있다. 또한 일회성으로 끝나는 법정대리인의 동의는 이후 지속적으로 이용되는 아동의 개인정보에 대한 충분한 보호조치로 보기 어려운 한계가 있다. 만14세 미만은 물론 성년에 도달하지 않은 아동은 취약한 정보주체로서 일반 성인의 개인정보 처리 사례와 구분해 취급하고, 특히 디지털 개인정보 처리 환경이 대규모로 확산되는 만큼 아동의 개인정보 처리에 기반한 마케팅, 프로파일링 및 자동화된 의사결정에 대해 금지 방안을 마련할 필요가 있다. 아동의 개인정보가 디지털 환경에 항상 연결되어 있고 상업적인 목적으로 처리되는 경우가 증가하면서, 일회적 법정대리인의 동의권 보장이라는 소극적 수준을 넘어 아동의 개인정보 처리 주기 전반에 대해 보다 정교한 규범을 수립할

필요가 있다. 또 아동의 개인정보 유출 등 보안성 보장은 아동의 생애 전체에 걸쳐 영향을 미칠 가능성이 높으므로 엄격한 기준이 필요하다.

인공지능 기술은 장난감, 가상 비서, 비디오게임에 내장되어 있고 챗봇과 적응 학습 소프트웨어를 구동하는 등 아동은 인공지능과 다양한 방식으로 상호작용하고, 알고리즘은 아동에게 비디오, 뉴스, 음악, 친구까지 추천하며, 복지보조금, 의료와 교육서비스 접근, 가족의 주택 신청에 대한 자동화된 의사결정 시스템에 아동이 영향을 받는 상황에서 아동의 프라이버시, 안전, 보안에 대한 위험이 있다. 유니세프는 2020년 ‘아동을 위한 인공지능에 대한 정책 지침’ 초안에서 정부와 기업은 아동의 프라이버시 문제를 명시적으로 인식하고 이를 인공지능 시스템의 설계 및 구현에 적용해야 한다고 강조했다. 유럽연합은 ‘신뢰가능 인공지능 가이드라인’(2019) 등을 통해 아동 등 취약한 사람들의 권리 보장에 주의를 기울이고 있고, 유럽 집행위원회는 2021년 ‘인공지능법안’을 유럽의회에 발의해 학교 등 교육과 직업훈련에 사용되는 인공지능을 고위험으로 분류하고 엄격한 요구사항을 따르도록 했다. 국내에서 인공지능 챗봇 ‘이루다’가 만 14세 미만 아동 20여 만 명의 개인정보를 위법하게 사용해 행정제재가 부과된 후, 개인정보 보호위원회는 2021년 5월 국내 법에 도입되지 않았으나 국제적으로 통용되는 개인정보보호 중심 설계 원칙 등을 반영한 ‘인공지능(AI) 자율점검표’를 발표했다. 서울특별시교육청도 2021년 인공지능 도입 시 영향 평가 기준과 체크리스트를 담은 ‘인공지능(AI) 공공성 확보를 위한 현장 가이드라인’을 보급하며 공교육에서 인공지능 도입여부 평가 기준으로 ‘개인정보 보호’를 제시하는 등 인공지능 관련 개인정보를 보호하려는 움직임이 나타나고 있다.

제6장

아동·청소년의 개인정보와 프라이버시에 대한 인식

제 6 장

아동·청소년의 개인정보와 프라이버시에
대한 인식

1. 아동·청소년 인터뷰 개요

이 장에서는 학교, 가정, 미디어 등에서의 아동·청소년의 프라이버시 인식과 경험을 확인하려 한다. 이를 위해 미디어교육 강사, 초등학교 교사, 민간교육위원의 소개를 받아 스노우볼링기법으로 인터뷰에 참여할 아동·청소년을 모집했다. 2021년 7월 8일부터 8월 8일까지 한 달간 서울, 경기, 대전의 초등학교 4, 5학년 15명(서울 2곳)과 중학교 1, 2, 3학년 22명(서울 4곳, 경기 3곳, 대전 2곳) 등 모두 37명의 아동·청소년을 9회에 걸쳐 만났다. 참여자인 아동·청소년들이 연구에 편하게 참여할 수 있도록 평소 알고 지내는 2~7명으로 집단을 구성해 평균 1시간 30여분 동안 참여자의 학교나 집 인근에서 만나 인터뷰했다. 초등학교 13명의 경우 비대면 수업 상황이어서 인터뷰도 비대면으로 진행했다. 프라이버시에 대한 인식, 학교, 가정, 미디어 등에서 개인정보 및 프라이버시 존중 등에 대한 생각, 미디어의 이용약관과 데이터 수집에 대한 인식, 개인정보 교육에 대한 생각 등에 대해 질문했고, 답변을 바탕으로 아동·청소년에게 필요한 교육과 환경 개선점을 도출했다.

〈표 6-1〉 연구참여자의 특성

	지역 학년	성 별	SNS이용	좋아하는 앱	미디어 서비스 최초 가입 연령
1	대전 중1	남	페이스북	열불춤, 카카오톡, 페이스북	8세
2	대전 중1	남	페이스북, 인스타그램	페이스북	9세
3	대전 중1	여	인스타그램	카카오톡	7세
4	대전 중1	남	-	유튜브	10세

디지털 환경에서 아동·청소년 프라이버시 권리를 위한 교육방안과 제도개선 연구

	지역 학년	성 별	SNS이용	좋아하는 앱	미디어 서비스 최초 가입 연령
5	대전 중1	남	페이스북	Adobe Animate	카톡 10세, 틱톡 11세 인스타·페북12세
6	대전 중1	여	틱톡·인스타하다 삭제	카카오톡, 네이버	
7	대전 중1	남	트위터	원신, 유튜브	11세
8	대전 중1	여	페이스북, 틱톡	페이스북	10세
9	대전 중1	여	- (틱톡 앱 설치만 함)	네이버, 카카오톡, 유튜브	네이버 8세 카톡 11세, 틱톡 10세
10	대전 중1	남	-	게임	9세
11	경기 중2	여	트위터 (스마트폰 없음)	트위터, 네이버, 구글	15세
12	경기 중2	남	페북, 인스타그램	유튜브	10세
13	경기 중2	여	-	구글	9세
14	경기 중2	여	페이스북, 인스타그램	티빙, 웨이브, 인스타그램	11세
15	서울 중2	여	-	카카오톡, 네이버웹툰, 이비스페인트	13세 처음으로 네이버, 카톡 가입
16	서울 중2	여	인스타그램, 트위터했다 탈퇴	유튜브	12세
17	서울 중1	여	인스타그램	그림그리는 앱, 게임	
18	서울 중1	남	트위터	유튜브, 카카오톡, 네이버카페	13세
19	서울 중1	남	페이스북, 인스타그램, 틱톡	인스타그램	9세
20	서울 중3	남	페이스북, 인스타그램	유튜브, 네이버웹툰	12세
21	서울 중3	남	페이스북	유튜브, 페이스북, 네이버, 카카오톡	네이버·유튜브·카톡 11세 페북 12세
22	서울 중3	남	페이스북, 인스타그램	핸드폰 게임 런처	12세
23	서울 초4	여	-	카카오톡, 틱톡	7, 8세
24	서울 초4	여	- (스마트폰 없음)	유튜브	-
25	서울 초4	여	-	유튜브	9세
26	서울 초4	남	-	배틀그라운드	9세
27	서울 초4	여	틱톡	틱톡	네이버, 카카오톡 8세, 틱톡 9세

	지역 학년	성 별	SNS이용	좋아하는 앱	미디어 서비스 최초 가입 연령
28	서울 초4	여	-	카카오톡	9세
29	서울 초4	남	-	유튜브	
30	서울 초5	여	-	카카오톡, 파파고	10세
31	서울 초5	여	틱톡, 페이스북	카톡, 유튜브, 틱톡	9세
32	서울 초5	남	틱톡	유튜브, 포켓몬고	8세
33	서울 초5	남	페이스북, 인스타그램, 틱톡	유튜브	4세
34	서울 초5	남		로블록스	3세
35	서울 초5	여	- (스마트폰 없음)	유튜브, 네이버, 파파고, 컬러노트	네이버밴드 11세
36	서울 초5	여	(스마트폰 없음)	유튜브	10세
37	서울 초5	여	페이스북, 인스타그램, 틱톡	유튜브, 틱톡	엄마폰(7세),내폰(10세)

2. 인터뷰 진행방식 및 주요 내용

인터뷰는 연구자가 준비한 질문지와 활동지를 중심으로 진행됐다. 연구자는 참여자에게 연구참여동의서를 받은 것과 별도로 면담 전 면담에 참여하거나 중단 하는 것이 자유롭다는 것을 안내했고, 이에 동의한 학생들을 대상으로 인터뷰를 진행했다. 인터뷰가 기록(녹음)되나 연구 목적으로 사용되는 점에 대해 양해를 구하고 연구 목적을 설명하고, 연구자와 참여자가 간단히 자기소개를 한 후, 인터뷰를 시작했다¹⁷³⁾.

참여자들은 미디어 이용 시간, SNS 이용, 자주 쓰는 애플리케이션 등 미디어 이용 패턴을 적은 후, 프라이버시와 개인정보를 떠올렸을 때 생각나는 단어를 기록했고, 이를 바탕으로 프라이버시와 개인정보에 대한 인식과 교육경험 등에 관해 이야기했다. 프라이버시 침해 경험이나 우려 지점에 대해 알아보기 위해 학교, 친구, 가정, 낯선 사람, 미디어 플랫폼 이용을 중심으로 프라이버시 침해

173) 만 14세 미만의 경우 아동 본인의 동의 외에 법정대리인의 동의를 받았다.

관련 이슈를 묻고 답했다. 참여자들이 프라이버시나 개인정보 침해에 대해 어느 정도 우려하는지, 미디어 기업의 데이터 수집 등에 대해 얼마나 알고 있는지 알아보기 위해 페이스북의 데이터수집정책을 읽고 인터뷰를 했고, 아동용 약관 제공의 필요성을 확인하기 위해 영국 아동위원회가 발행한 아동용 페이스북 약관을 읽게 한 후 차이를 질문했다¹⁷⁴⁾. 데이터의 기록·저장에 대한 인식을 알아보기 위해 간단한 형태의 퀴즈를 진행했다¹⁷⁵⁾.

〈표 6-2〉 인터뷰 질문과 진행순서

주제	주요 질문
미디어 이용 패턴	<ul style="list-style-type: none"> • 디지털 기기 이용 시간, SNS 이용, 주로 사용하는 앱과 이유 등
프라이버시, 개인정보에 대한 인식	<ul style="list-style-type: none"> • 프라이버시나 개인정보를 듣고 생각나는 단어 적기 • 프라이버시, 개인정보 침해에 대한 우려
개인정보 교육	<ul style="list-style-type: none"> • 교육 경험, 교육에 대한 평가
가정영역	<ul style="list-style-type: none"> • 스마트폰 관리(감시) 앱 설치에 대한 의견 • 디지털 셰어런팅에 대한 의견
학교영역	<ul style="list-style-type: none"> • 비대면·대면 수업에서 프라이버시 침해 경험 • 사진·메시지 등이 지인에 의해 공유된 경험, 계정 공유 경험 등
모르는 사람	<ul style="list-style-type: none"> • SNS 등에서 모르는 사람에 의한 프라이버시 침해 우려
개인정보 제공에 대한 인식	<ul style="list-style-type: none"> • 서비스 가입 시 약관 읽기 경험, 읽지 않은 이유
개인 데이터 기록에 대한 인식	<ul style="list-style-type: none"> • 일상에서 기록되는 데이터에 대한 인식 • 미디어 이용 시 기록되는 데이터에 대한 인식
페이스북 데이터 수집 정책 평가 (약관 읽고 인터뷰)	<ul style="list-style-type: none"> • 약관과 약관읽기에 대한 생각 • 데이터 수집 정책에 대한 전반적 평가
영국 아동위원회 페이스북 약관 평가 (약관 읽고 인터뷰)	<ul style="list-style-type: none"> • 아동용 자료에 대한 평가와 페이스북 자료에 대한 평가
미디어의 프라이버시 침해 인식	<ul style="list-style-type: none"> • 데이터 수집 활용 행위에 대한 인식과 평가
프라이버시 및 개인정보 보호를 위한 제안	<ul style="list-style-type: none"> • SNS나 게임 등 미디어 기업 등에 요구하는 개선사항 • 필요한 개인정보와 프라이버시 교육에 대한 의견

174) 페이스북 가입 연령은 만 14세이나 만 13세인 중학교 1학년은 초등학교와 실제 다른 사회·문화적 경험과 대우를 받는 점을 등을 감안해 페이스북 약관 읽기 활동을 했다.

175) 이 활동은 3번째 인터뷰부터 시작해 전체 참여자 37명 중 27명만 참여했다.

3. 인터뷰 결과

1) 프라이버시에 대한 인식

대다수 참여자들에게 프라이버시는 익숙한 개념이 아니었다. 프라이버시에 대한 인식을 알아보기 위해 참여자들에게 프라이버시를 떠올릴 때 생각나는 단어를 적어달라고 요청한 결과, 다수 참여자들이 프라이버시와 개인정보를 구분하지 못했고, 일부 초등학생 참여자는 프라이버시를 처음 들어본다고 말했다. 개인정보에 대한 질문에 대해서는 전화번호, 이름, 계좌번호, 비밀번호 등이라고 답했다.

아이디나 계정 만들 때 입력한 거랑 개인정보 수집하는 거. (중1, 참여자 7)

개인정보나 일상생활이나 가족이랑 친구, SNS 휴대폰 인터넷 비밀번호 계정, 로그인, 사진이요. (중1, 참여자 8)

사생활이요. 사생활이라는 건 자신의 개인정보 같은 거예요. (초4, 참여자 25)

프라이버시는 일단 개인정보라고 생각하고요. 개인정보는 자신이 갖고 있는 것 중에 가장 중요한 정보. 자기만 알고 있는 거니까. (중3, 참여자 20)

프라이버시는 보호, 비밀보장, 존중, 사생활, 개인정보라고 생각해요. 프라이버시에 개인정보가 포함되어 있으니까 같다고 생각해요. 개인정보는 생년월일이나 가족관계, 아이디, 비밀번호 이런 거 포함되어 있어요. (중3, 참여자 21)



[그림 6-1] 프라이버시에 관한 답변을 모은 워드클라우드¹⁷⁶⁾

프라이버시에 대해 개인정보와는 다른 개인적으로 공유하기 싫은 것, 남이 알면 안 되는 것, 남에게 알려주기 싫은 것, 나만 알고 싶은 것 등 같이 정보의 관리 관점에서 표현하는 참여자들도 상당수 있었다.

개인적으로 공유하기 싫은 거, 넘어선 안 될 선. (중1, 참여자 3)

프라이버시는 사생활, 일기장, 시험점수, 폰 비밀번호. 개인정보는 전화번호, 통장 비밀번호, 계좌번호, 보이스피싱, 집주소 이런 걸 말하는 것 같아요. 사생활은 내가 뭐하는지 다 알게 되면 안 좋은 그런 거나 무얼 했는데 알리고 싶지 않다고 느끼는 것들. (그래서 프라이버시를 일기장이라고 썼나요?) 일기장은 선생님이 보는 건 상관없지만 선생님이 잘 썼다고 읽어주시면 다 들으니깐 그게 뭔가 가끔 안 좋거나 그럴 때가 있어서 썼어요. (초5, 참여자 35)

개인공간이나 타인에게 노출되면 불편한 거라고 생각해요. (개인공간은 무슨 뜻이죠?) 자신만 생각하고 자기 마음대로 하는 공간이요. (중3, 참여자 22)

프라이버시는 개인공간이라고 생각하고 비밀같기도 하고 내가 제일 소중한 여기고 엄청 중요한 거. (중1, 참여자 9)

176) 참여자들이 프라이버시에 관해 떠올릴 때 생각나는 단어를 다 적게 한 후, 이를 수합해 R프로그램의 워드클라우드 패키지를 이용해 분석했다.

프라이버시는 나만 알고 싶은 것들이나 나의 개인적 정보, 또 숨기고 싶은 것들, 보호하는 거, 개인정보는 개인적인 중요한 정보들이라고 썼어요. (중2, 참여자 15)

개인정보하면 떠오르는 것에 대한 질문에 대체로 이름, 생년월일, 주소 전화번호 같은 정보를 말했으나 일부 참여자들은 돈이나 도둑이라고 답했다. 이는 개인정보 교육이나 캠페인 등이 주로 금전적 피해에 초점을 맞춘 것과 관계가 있어 보인다.

내 유산, 내 돈, 전화번호. (초5, 참여자32)

돈, 전화, 도둑. 도둑이 남 몰래 물건을 훔쳐가는 사람이잖아요. 내 개인정보에서 나도 모르게 우리의 돈을 훔쳐가는 사람이니까.(초5, 참여자 34)

소수지만 개인이나 사람에 대한 정보는 보장받아야 한다는 이유를 들면서 프라이버시를 권리와 인권이라고 답하는 참여자도 있었다.

개인이 누리고 있는 권리. (중1, 참여자 1)

권리, 인권, 침해, 나, 사생활, 비밀 그런 거, 사람에 대한 정보니까 지켜져야 하니까 (중2, 참여자 14)

사생활 개인정보 인권. 개개인의 정보가 들어있으니까 기본적으로 권리를 보장받아야 된다고 생각해서 인권이라고 썼어요. (중2, 참여자 11)

2) 개인정보나 프라이버시 침해에 대한 우려

아동·청소년들이 프라이버시와 개인정보 등에 대해 관심이 없을 것이라는 통념과 달리, 참여자 중 과반 이상이 개인정보 침해 등에 대한 우려를 드러냈다. 이들은 ID 도용, 보이스피싱, 해킹 등 여러 유형의 위협에 직간접적으로 노출되고 있었다. 온라인 환경에서 프라이버시의 취약성을 언급하거나 SNS의 위협성에 대해 우려하는 참여자도 있었다.

원래는 안 그랬는데 다른 지역에서 로그인됐다고해서 네이버 비밀번호 바꾸고 정보를 넘겨받은 사건 이후 다른 지역에서 또 내 계정에 로그인했다고 할까봐 불안해서 메일을 계속 확인해요. (중1, 참여자 7)

스팀이라고 게임판매사이트에서 계정을 해킹당해서 20만 원 정도 날린 적이 있거든요. 그때 이후 비밀번호를 몇 개월마다 한 번씩 바꿔요. (중3, 참여자 22)

저희 이모가 네이버에서 다른 지역에서 누가 로그인했다는 거예요. 저도 네이버 계정 사용 중인데 그럴까봐 걱정되고. 사이트에서 아이디이랑 비밀번호 입력하면 자동 로그인할 수 있게 뜨잖아요. 전에 친구집에서 자동로그인된 줄 모르고 눌러서 제 비밀번호가 다 뜨는 거예요. (중1, 참여자 9)

구글에서 영상 보다가 실수로 허용 눌러서 개인정보 유출된 적이 있어요. 해킹당해서, 앱들이 싹 다 지워지고. (중1, 참여자 19)

오프라인은 지켜지는 것 같은데 온라인은 딱히 많이 지켜지는 것 같지는 않아요. 왜냐면 실수로 메시지 하나를 전송했는데 그걸로 정보가 틀릴 수 있잖아요. (중1, 참여자 4)

온라인은 잘 지켜지고 있다고 생각하진 않아요. 예를 들어 자기 사진을 찍어서 올렸는데 배경을 보고 어디 사는지, 남자인지, 안경 썼는지 이런 개인의 정보를 다 알아낼 수 있으니까 SNS는 그게 무서운 것 같아요. (중1, 참여자 3)

일부 참여자들은 직접적인 피해와 무관하게 언론 보도 등을 접하면서 프라이버시나 개인정보 침해에 대한 우려를 드러냈다. 대체로 개인정보 침해와 관련해, 피싱이나 해킹 같은 직접적인 피해나 보안 등 물리적 안전의 영역과 연결해 생각하는 경향이 나타났다.

만약에 내가 당하면 어떻게 될까. 유해사이트나 개인정보 빼가는 사이트에 들어가 실수로 약관에 동의했다. 그럼 집주소 이런 게 다 공유돼서 스팸메일이 올 수도 있고. 그런 생각해봤어요. (중1, 참여자 18)

카카오페이지나 핸드폰 계좌이체할 때 주민번호 입력해야 하잖아요. 믿어도 되나 싶었던 적이 있었어요. 이게 정말 내가 찾는 공식적인 앱이 맞나. (중2, 참여자 14)

3) 개인정보 교육에 대한 생각

2018년부터 초등학교와 중학교에서 정보교육이 의무화됐고, 중학교의 경우 정보 교과에서 개인정보를 교육하고 있다. 개인정보 교육경험에 대한 질문에 비밀번호 변경, 개인정보 유출 사례 등을 언급했다. 기억나지 않는다고 답하는

경우 외에 ‘저작권’이라고 말한 경우도 상당수 있었는데, 정보윤리단원에서 개인 정보와 저작권을 함께 교육하면서 생긴 일이었다.

개인정보 유출 침해 사례 그런 거. 안 좋은 거 (중1, 참여자 3)

중학교 들어와서는 침해 이런 거밖에 안 배웠어요. (중3, 참여자 21)

개인정보를 맘대로 써서 다른 사람들이 악용하는 거요. (중1, 참여자 17)

개인정보, 저작권 말고는 잘 모르겠어요. (중2, 참여자 13)

학교에서 저작권 위주로 많이 하다보니까 아무래도 이런 쪽(개인정보 등)은 거의 안해요. 페이스북의 만행이나 틱톡 사건도 말 안 해주다보니 애들이 경각심도 많이 떨어지는 부분이 있는 것 같고. (중2, 참여자 15)

무슨 영상을 틀어주셨는데 개인정보 유출되지 않게 비밀번호를 자주 바꾸고 어려운 걸로 하라는 정도로만 배웠어요. (중1, 참여자 8)

참여자들은 학교의 개인정보 수업에 대해 냉소적인 반응을 보였다. 프라이버시와 개인정보 보호와 관련해 실효성있는 강의를 필요하지만 이들이 접하는 것은 비밀번호 변경, 약관 읽기 같은 피상적인 당위론이었다. 미디어를 이용하면서 알아야 할 내용에 대한 교육이 이뤄지지 않는 점에 대해 불만을 토로했다. 한 참여자는 페이스북을 전체 공개로 설정해 낯선 사람들이 친구맺기를 신청해 두려웠던 상황을 언급하며, 학교 교육의 실효성에 의문을 표시했다. 참여자 중 일부만 플랫폼의 데이터 수집이나 쿠키 삭제 등을 알고 있었는데, 스스로 알아낸 경우였다. 다수의 참가자들은 학교 수업을 형식적, 실효성이 없다고 말하며 수업과 현실의 괴리를 토로했다.

(아까 IT나 전자기기 리뷰 영상을 많이 보고 알게 됐다고 했는데 수업으로 알기 어려운 부분이 많았다는 거예요?) 학교 수업으로는 절대 모를. 학교수업은 형식적인 것 같아요. 항상 내용이 똑같아요. 비번 자주 바꾸고, 다른 사람한테 알려주지 말고, 공용 컴퓨터에 로그인하지 말고 맨날 똑같은 것만 알려주고 자세한 건 안 알려주는 것 같아요. 학교 수업에서는 이렇게 하면 유출될 수 있고, 이런 거 조심하라고 하는데 좀 조심해야겠다는 생각이 드는데 엄청나게 들진 않아요. 근데 인터넷 영상은 사례도 보여주고 왜 유출되고 왜 유용한지 실제 일어난 일을

알려주니까 좋아요. (중1, 참여자 7)

페이스북 같은 거 할 때 선생님이 약관을 읽어보는 게 좋다고 하는데 현실적으로 페이스북 약관을 읽을 수 없어서 동의하고. 근데 정보수업에서 알려주는 건 비밀번호 바꿔라 그런 것뿐이어서 나머지는 소프트웨어, 하드웨어 그런 거고. 그런 거 배우니까 실제 사람들이 일상생활에서 사용할 때는 어떻게 해야 하는지 몰라서. 저도 언니 없었으면 계속 그런 사람들이 와서 무서웠을 것 같아요. (중1, 참여자 8)

낯선 이의 접근으로 곤혹을 치른 한 참여자의 이야기는 아동·청소년들에게 실제 필요한 교육이 무엇인지 알려준다. 참여자들이 서비스 가입과 사용에 연령 설정은 큰 의미가 없었고, 그로 인해 현실에서 부딪히는 문제를 해결하는데 더 큰 어려움을 겪는 듯 했다.

페이스북 설정에 들어가봤는데 뭔가 설정할 게 많아서 못 찾겠고, 그런 거 하는 게 처음이어서, 혼자 하다가 잘못 건드리면 더 이상해질까봐 언니한테 맡겼어요. (중1, 참여자 8)

친구가 페이스북에 진짜 집주소가 나왔었던 적 있어요. 보이게 하고 안 보이게 하는 걸 (설정)할 수 있는데, 친구는 몰랐대요. (초5, 참여자 31)

비밀번호 알려주지 말기는 학교 개인정보 교육의 핵심 내용이고, 참여자들이 비교적 많이 기억하는 내용이었다. 일반적으로 계정이나 비밀번호 공유 경험을 묻자 없다는 대답이 대다수였지만, 게임 계정 공유 여부를 묻자 다른 이야기가 나왔다. 계정이 정지되거나 높은 점수를 얻기 위해 계정을 자주 만들다보니, 계정 공유의 위험에 다소 둔감한 반응을 보였다.

연구자: 친구들에게 비밀번호를 알려주거나 게임 계정 공유하나요?

참여자19: 저는 공유 많이 해요. 애들이 게임 계정 빌려달라고 하면 항상 빌려주는데 폰 비밀번호는 안 알려주죠.

연구자: 게임 계정 알면 친구가 개인정보 알 수 있잖아요. 친구가 비밀번호를 바꿀 수 있고.

참여자19: 새로 파면되죠, 게임 계정을.

연구자: 친구가 아이디를 사칭하는 거잖아요. 게임하면서 활동이 쌓이고, 아이디가 정체성이잖아요. 친구가 ID 계속 쓴다고 할 수도 있고.

참여자19: 저는 전혀 걱정은 안 해요. 다시 파고 다시 사면되니까.

참여자22: 저는 친구한테 빌려줬다가 그에게 2주 정지 먹었어요.

연구자: 아이디 알려줘서 위험해진 건데 걱정 안 돼요?

참여자22: 저는 상관없는 게 한 게임에 계정이 너무 많아서. 20개 있어서 상관없어요.

4) 스마트폰 감시 앱에 대한 의견

참여자들은 청소년의 유해매체 접속 차단을 위해 스마트폰 개통 시 설치되는 '자녀 스마트폰 관리/감시 앱'에 대해 부정적인 의견을 표시했다. 학교와의 연락, 관계 맺기, 여가와 놀이 등 참여자 또래의 활동 대부분이 스마트폰으로 이뤄지기 때문에 스마트폰 관리 앱은 아동의 일상 많은 부분에 영향을 미쳤다. 참여자들은 스마트폰에 의해 일상이 매개되는 상황에서 꼭 필요하거나 사소한 것을 하기 위해 부모에게 허락이나 설득을 구해야 했고, 부모의 일방적 결정으로 스마트폰 사용이 제한되면서 불편을 겪어야 했다. 참여자들은 모든 행동이 “엄마 마음대로” (참여자 12), “부모의 통제”(참여자15)에 의해 중단되거나 봉쇄될 수 있다는 것에 부정적 감정을 드러냈고, 사생활 침해, 감시와 관련 신뢰관계에 대한 회의적인 의견을 드러냈다. 코로나19로 스마트폰 사용이 늘어날 수밖에 없는 상황을 포함해 아동의 입장에서 다양한 스마트폰 사용 상황에 대한 부모의 이해 부족도 참여자들을 힘들게 했다. 하지만 앱의 존재 자체를 인식하지 못하거나 위치추적, 메신저나 문자메시지 내용 확인 등 기능을 모르는 참여자도 있었다.

시간제한이 있어서 잠깐 사진을 찍으려고 해도 1시간 다 쓰면 아예 휴대폰이 안 열리거든요. 긴급전화 빼고 거의 못 해요. 카메라 같은 것도 못 쓰고. 길을 가는데 엄청 귀엽보짜한 길고양이가 있어서 사진을 찍으려고 했는데 카메라가 안 되면 너무 화가 나요. 그래서 안 좋은 것 같아요. (초5, 참여자 35)

중독을 막아줘서 좋긴한데 다른 면에서 나쁘기도 하고. (어떤 면에서?) 친구네 놀러갔는데 다른 애들은 게임하고 있는데 보고만 있어서. (중1, 참여자 1)

초등학교 저학년 때만 깔렸는데 그다지 좋은 것 같지 않아요. 학교에서 메시지 오는 것도 확인을 제때 못하게 되고 특히 카톡 못하는 게 안 좋았던 것 같아요. 감시하는 것 같기도 한데 약간 필요한 것 같아요. 너무 많이 사용해서 건강에 문제가 생길 정도로 심각하면. (중1, 참여자 3)

초등학교 때 해봤는데 안 좋은 사이트만 막는 것 보단 제가 폰을 할 수 없게 필요한 것까지도 잠가놔서 폰이 있는데 거의 폰이 없는 것처럼 살아서 되게 스트레스였어요. (중1, 참여자 8)

3학년 때 폰 처음 생길 때 깔았다가 중1때 자연스럽게 지워버렸어요. 많이 불편했어요. 엄마가 마음대로 시간을 조정할 수 있고, 시간을 다 쓰면 학교과제 같은 걸 해야 될 때 엄마한테 물어달라고 해야되는 게 귀찮기도 해서(...). (어떤 걸 엄마가 마음대로 하셨니?) 엄마가 사용할 수 있는 시간을 조정하거나 사용하지 않게 하는 앱을 따로 지정할 수 있어서 게임 같은 거 다 막았어요. (중2, 참여자 12)

저는 엄마랑 계정이 연동돼서 제가 폰 사용을 하면 엄마한테 시간이 뜨거든요. 요즘 코로나19 때문에 온라인으로 하게 되서 폰 사용 시간이 늘어나잖아요. 지금은 엄마가 공부 같은 건 폰 사용해도 상관없다고 했는데 그거 말하기 전까지는 저한테 계속 화내셔서. 먼저 물어봐주고 존중이나 배려를 해줬으면 좋겠어요. (중1, 참여자 9)

참여자들은 스마트폰 관리/감시 앱의 기능 중 하나인 위치추적, 인스턴트 메신저 사용 차단 및 내용 확인, 문자메시지 내용 확인 등에 대해 사생활 침해라는 의견을 보였다. 사실상 모든 활동이 스마트폰으로 이뤄지면서 스마트폰 활동 확인은 감시와 사생활 침해를 동반한다. 참여자들은 어리더라도 사생활이 있기 때문에 부모의 사생활 감시는 적절하지 않다고 말했고, 앱에 의해 감시와 통제받는다고 표현하는 등 프라이버시에 대한 확고한 인식을 드러냈다. 감시 앱으로 인해 자신의 행동을 ‘검열’을 하게 된다는 의견도 나왔다.

인터넷에 들어갔는데 바로 나가지는 거예요. 과제해야 되는데 몇 번을 해도 막아지니까. 메시지 같은 것도 다 뜨는데 그건 사생활인데 부모님이 그렇게까지 단속할 이유가 있나요? (중1, 참여자 1)

선 넘은 것 같아요. 그게 깔려있으면 내가 이상한 짓을 하는 것 같고, 감시받고 있는 것 같고, 강압적이어서 기분이 안 좋아요. (부모님인데요?) 개인 사생활이 있는 건데 부모님이라고 무조건 다 공유해야 되는 건 아니니까. (중1, 참여자 7)

제가 뭘 하는데 갑자기 엄마가 나올 수도 있고 그게 너무 싫어요. 뭘 통제된 느낌, 제한되는 거. (중1, 참여자 19)

부모님이 감시하는 거 별로 안 좋다고 생각해요. 단순히 숙제 같은 걸 하고 애들이랑 얘기하는 걸 감시당하면 얘가 지금 어떻게 뭘 하고 있는지 다 아니까 부모님이 통제하니까. 저학년이면 괜찮은데 초등학교 6학년인데 부모님이 침해하면 불편하고 짜증날 것 같아요. (걱정돼서 그러실 수 있잖아요?) 그렇다고 통제하는 건 아니라고 생각해요. (중1, 참여자 4)

일부 참여자들은 자녀의 사생활에 대해 존중하지 않는 사회적 분위기에 대해 비판했고, 부모가 자신을 믿지 못하는 것에 대한 서운한 감정을 토로했다. 이는 앱 설치가 단순히 유해물로부터 보호 차원을 떠나 아동(자녀)을 독립된 주체로 인정하지 않는 것과 부모와 자녀 사이의 신뢰 형성과 연결된 문제로 인식하고 있다는 것을 보여준다.

가족끼리인데 뭐 어때, 부모님인데 뭐 어때, 그런 문화가 바뀌었으면 좋겠어요. 가족이라도 사생활이 없는 건 아니니까. 제 핸드폰에 그 앱이 깔려있는데, 엄마가 가족끼리 어쩌냐고 해서 기분 나빴어요. (걱정돼서 그럴 수 있잖아요?) 걱정된다고 해서 기분 나쁜 행동을 해도 된다고 생각 안 해요. 저를 못 믿는 것 같고 감시하려는 것 같고. (중1, 참여자 7)

가족이라도 숨기고 싶은 거, 비밀이 있을 수 있으니까 부모님이 관여 안했으면 좋겠는 부분도 있고. (중3, 참여자 20)

배신감 들었어요. 동생이 엄마 몰래 폰 게임을 하다가 걸려서 혼난 적이 있거든요. 그 이후 못 믿겠다고 저희 둘 폰에 감시하는 걸 깔았어요. 플레이스토어에서 게임 까는 것만 막으면 되는데 아예 폰을 막아서. 그 이후에는 게임을 다시 안 깔았는데 엄마가 너희 못 믿겠다면서 계속 안 믿어줘서 속상했어요. (중1, 참여자 8)

일부 참여자들은 스마트폰 이용 시간 조절과 위협으로부터 보호 등을 일부 인정하면서도 사생활 침해라는 의견을 보였다.

아무래도 청소년들이 휴대폰을 보는 것이 조절이 잘 안 되는 거는 맞으니까 전체 사용시간 조절까지는 괜찮다고 생각하는데 메시지를 보거나 그러는 건 아니라고 생각해요. 애들도 자기 나름대로 숨기고 싶은 거나 친구랑 카톡에서 무슨 얘기를

할지 모르잖아요. 만에 하나 진짜 엄마 욕을 할 수도 있는 거고 근데 그걸 보게 되면 집안의 평화도 박살나고. (중2, 참여자 15)

보호하려는 건 아는데 제 자유를 억압하는 느낌이어서 좋지 않은 것 같아요. (중2, 참여자 17)

부모의 자녀 스마트폰 이용 통제는 취침시간, 사생활 전반에 대한 간섭과 통제 등과 연결되어 있다. 완벽한 통제는 불가능하기에 이러한 시도는 실효성을 크지 않은 듯 했고 오히려 동의 없는 일방적 결정은 반발과 불만을 키우는 것처럼 보였다.

시간제한 앱을 부모님이 너무 알차게 쓰고 계셔서. 앱도 한 두 시간으로 하시고 휴대폰 전체 사용시간도 정해놓으시고 잠자는 시간도 정해놓으시고 그렇게 알차게 쓰고 계십니다. 솔직히 엄마 입장에서 맨날 휴대폰 보고 있는 걸 싫은 건 맞는데 솔직히 잠드는 시간까지 제어하는 건 좀 아닌 것 같아요. (중2, 참여자 15)

일부 참여자들은 SNS의 중독을 경계하거나 사회적으로 문제있는 콘텐츠에 거리를 두면서 스마트폰 이용을 스스로 조절하는 모습을 보였다.

페이스북은 5학년 때 잠깐 깔았다가 삭제했고, 인스타랑 틱톡 했는데 하는 시간이 너무 많은 것 같기도 해서 삭제했어요. (중1, 참여자 6)

너무 중독성이 심하기도 하고, 안 좋은 말, 욕 같은 것들이 많아서. 트위터 같은 경우에는 일상적으로 욕하는 사람들이 있어서, 탈퇴했어요. (중2, 참여자 16)

5) 부모의 디지털 쉐어런팅

부모가 자녀의 동의없이 SNS나 메신저 등 디지털 공간에 자녀의 사진을 게시하는 ‘디지털 쉐어런팅’에 대해 일부 참여자는 부정적인 입장을 밝혔다. 참여자들은 성장 후에 문제가 될 수 있고, 부모가 자녀의 동의를 구하지 않은 것, 부모가 자신의 의견이 받아들여지지 않은 것을 문제라고 생각했다. 또한 디지털 공간에서의 흔적이나 자신의 평판과 연결해 우려하는 참여자도 있었고, 안전에 대해 걱정하는 참여자도 있었다.

나쁜 사람들이 개인정보를 다 빼갈 수 있으니까, 납치될 확률이 높아지니까 올리면 안 된다고 생각해요. (초4, 참여자 29)

저는 말할 수 있어요. 얼굴 자체가 개인정보라고. 그 친구의 친구의 친구가 나쁜 사람일 수도 있어. 받은 사람이 또 다른 사람한테 보냈고 계속 연결되다가 어떤 나쁜 사람한테, 착한 사람인 줄 알았던 사람이 나쁜 사람일 수도 있으니까 보내면 안 된다고. (초5, 참여자 34)

사진 찍어서 친구분들한테 보내는데 제가 그러지 말라고 맨날 발광했어요. 저는 좋지 않다고 생각해요. 개인이 원하지 않는데 올리면 프라이버시 침해잖아요. 아무리 자식이 사랑스러워 보인다고 해도 자식이 원하지 않으면 그런 행동을 삼가야죠. (중2, 참여자 11)

부모님이 자식 사진 올리는데 뭐가 문제냐고 생각할 수도 있는데 자식이 나중에 왜 올리셨냐고 원망할 수도 있을 것 같아요. 사진 주인이 안 된다고 하면 없애는 게 맞고 가족끼리 보는 용도로 사용해도 될 것 같아요. (중3, 참여자 20)

저희 가족도 사진 찍는 건 아니라서 딱히 없지만 만약 올렸다면 저는 별로 좋아할 것 같지는 않아요. 바로는 아니지만 언젠가 내려달라고 말할 것 같아요. 부모님은 자식 자랑이라고 생각하겠지만 당사자는 부끄럽거나 좀 크게 말하면 수치스러울 수도 있어서. (중3, 참여자 21)

애기 때면 상관없을 것 같긴 한데 지금은 약간 불편할 수도 있을 것 같아요. 예를 들어 인스타그램 하는 사람의 경우 옛날 사진, 지금 사진 막 붙여서 조롱거리가 될 수 있을 것 같기도 하고 다른 사람한테 옮겨가서 디페이크가 될 수도 있으니까, 초상권 침해 때문에. (중1, 참여자 18)

6) 학교와 친구의 프라이버시 침해

학교는 수업이라는 공적 커뮤니케이션과 친구 관계라는 사적 커뮤니케이션이 복잡하게 펼쳐지는 공간이다. 수업과 학교행정 등 공적 맥락에서 개인정보 수집과 프라이버시 침해 외에 친구 관계 등 사적 맥락에서 동의없이 SNS나 메신저에 사진이나 대화를 캡처해 공유하는 일은 흔하게 일어나는 일 중 하나이다. 얼굴과 대화 내용이 영상통화, 사진, 메신저, SNS 등에서 시각적으로 구현되고, 대부분 소통이 온라인에서 이뤄지면서 또래 관계에서 상대의 동의없는 대화와 사진 촬영·공유는 학교폭력으로 의제화될 정도이다. 참여자들은 당사자의 동의없는

사진 공유를 프라이버시 침해라고 생각했다. 학교폭력위원회 개최 등의 엄격한 조치 덕분인지 동의없는 사진 공유행위가 이뤄지지 않고 있다고 생각하는 참여자들도 있었고, 여전히 우려하는 참여자들도 있었다.

친구가 같이 놀면서 찍은 사진에다 모자이크 같은 거 안 하고 그냥 올리거나 이름 완전 잘 알게 ‘혜’를 ‘해’로 바꿔 올리는 거 싫었어요. 다른 사람이 알아보는 것도 싫고 제 얼굴이 친구 프사에 들어가는 게 싫고, 친구들이 놀았냐, 재미있었냐 물어보는 것도 웬지... (초5, 참여자 35)

친구랑 영상통화를 했는데 그걸 캡처해서 인스타그램에 스토리로 올린 적 있고, 전 여친한테 뿌려진 적이 있어요. 사과했는데 안 받아줬어요. 동의없이 사진을 올린 것이 되게 화났어요. (중1, 참여자 19)

친구의 친구가 페이스북에 제 친구 역사를 올린 적이 있었는데, 친구가 자기한테 왜 올리냐면서 싸웠고 학폭으로 신고했어요. 친구는 하지 말라고 했는데 친구의 친구는 계속 올리고, 자기 프사로 해놔서 친구가 되게 스트레스 받았어요. (중1, 참여자 8)

제 허락도 안 받고 올리다보면 제 흑역사가 많이 쌓이잖아요. 그럼 제가 친구들한테 비웃음거리가 되고 나중에는 더 심한 쪽으로도 발생할 수 있기 때문에 안 좋다고 봐요. (초5, 참여자 33)

대화 내용을 공유하면 다른 사람한테 개인정보가 유출될 수도 있는 거니까 안 된다고 생각해요. (초4, 참여자 29)

디지털 공간에서의 사진 캡처와 공유는 여러 차례 문제가 됐지만 특히 비대면 수업으로 인해 얼굴과 뿐만 아니라 표정과 움직임의 실시간 관찰·기록이 가능해지고, 사적인 공간인 집이 영상과 소리로 중계되면서 심각성이 더 커졌다. 대체로 남녀공학에 다니는 학생들이, 남학생보다는 여학생이 사진 캡처와 공유에 대해 더 많이 우려했다.

학교에서 워낙 강력하게 얘기하거든요. 온라인 수업 때 캡처하면 나중에 학폭도 되니까 ‘절대 그건 하지마라’고 해서 그걸 다루는 경우는 못 본 것 같아요. (중1, 참여자 18)

온라인으로 수업할 때 화면을 켜면 누가 캡처할 수도 있는 거고 사진 같은 거

찍을 수 있으니까 좀 그런 것 같아요. (중1, 참여자 6)

캡처하면 바로 신고돼서 선생님들이 못하게 하는데, 혹시 모르니까. 페이스북 스토리 보면패드 같은 걸로 수업하고 폰으로 화면 찍어서 스토리 올린 애들이 있는데 그런 일 당할까봐 얼굴을 아예 안 찍죠. (중1, 참여자 8)

카메라를 켜면 집이 공개되고 제 얼굴도 보이니까. 친구들이 캡처하는 경우도 있잖아요. 그게 너무 싫어서 가끔씩 책상만 비출 때도 있고 아예 카메라를 테이프로 막아놓고 한 적도 많아요. (중2, 참여자 14)

수업 참여 자체가 디지털 영상으로 기록되면서 학교라는 공적 영역 전반에서 프라이버시 침해 우려가 제기되고 있다. 출석, 강의, 활동, 과제제출 등 수업의 전 과정이 온라인으로 이뤄지면서 오프라인에서는 발생하지 않았을 프라이버시 침해 상황도 발견됐다. 참여자들은 학생간 프라이버시 침해뿐만 아니라 학부모 같은 제3자의 수업 시청으로 인한 프라이버시 침해, 교사의 수업 녹화, 과제 제출현황 게시 등 다양한 부분에 대해 우려했다. 이는 학생 프라이버시에 대한 교사의 기본 인식과도 연결되는 대목이다.

Zoom 녹화기능이 있는데 선생님이 녹화할 때마다 꺼려져요. 지을 것 같긴 한데, 확실히 지운다고 말해줘야 안심돼요. (중1, 참여자 3)

녹음한 다음에 파일을 다른 사람한테 공유하면 다른 친구나 선생님 얼굴 같은 게 다 공유가 되니까 녹음 같은 걸 해서 다른 사람한테 공유하면 안 된다고 생각해요. (초4, 참여자 29)

Zoom이 엄청 안전한 것도 아니니까 얼굴이 광고 같은데 나올 수도 있을 것 같아서 좀 위험할 것 같아요. (초4, 참여자 28)

친구들 중에 부모님이 어떻게 수업하는지 궁금하다며 보여달라고 해서 사진 찍어서 보여 줄까봐 걱정돼요. (초5, 참여자 34)

이제 과제 안 올리면 미인정으로 떠서 누가 냈고 안냈는지 다 나오니까 조금 짜증나요. (다른 친구들이 내가 과제 안 낸 거 아는 건가요). 네, 대놓고 앞에 벽보를 아예 붙이세요. 안 낸 사람 주르륵. (중2, 참여자 15)

사실 비대면 이전에 아동의 프라이버시와 인권을 고려하지 않는 맥락이

존재하고, 비대면 상황에서 이것이 전면화됐다고 볼 수 있다. 일부 참여자들은 비대면 수업과 별개로 일상적인 프라이버시 침해 경험을 언급했다.

선생님이 일기장 검사할 때 보는 건 상관없지만 잘 썼다고 읽어주시면 다른 친구들이 다 들으니까 안 좋을 때가 있어요. 저는 친구들과 논 걸 썼는데 논 친구들도 그닥 안 좋아할 것 같고 좀 그랬어요. (초5, 참여자 35)

7) SNS 이용과 프라이버시 침해 우려

SNS는 자기표현의 성격이 강하기 때문에 서비스 가입 시 입력하는 개인정보, 활동과정에서 생성되는 정보 이외 기본적으로 프로필 설정과 다양한 형태의 콘텐츠와 피드백 등을 통해 프라이버시나 개인정보 노출과 침해가 광범위하게 일어나는 공간이다. 연구진은 SNS의 이러한 특성과 아동 다수가 이용한다는 결과를 고려해, SNS 이용과 관련한 의견을 물었고, 참여자의 대다수가 SNS를 이용하는 것으로 나타났다. 페이스북이나 틱톡 등은 14세 이상 가입이라는 연령제한이 있지만 중학교 1학년 참여자 상당수가 페이스북 계정이 있었고, 초등학교 때 가입했다는 참여자도 상당수였고, 틱톡 계정을 갖고 있는 초등학교 참여자도 꽤 있었다. ‘아동·청소년 보호’를 위한 SNS 연령 제한은 크게 의미가 없어 보였다.

참여자들은 자신의 글, 사진, 영상을 적극적으로 게시하기보다는 정보(스포츠, 아이돌 등)를 얻거나 친구와의 소통이나 다른 사람의 콘텐츠를 보기 위해 SNS를 활용했다. 프라이버 침해 우려나 악플 등 주변의 부정적 반응으로 SNS에 콘텐츠를 게시하지 않거나 삭제했다는 의견도 있었다.

전학년 친구 멘션해놓고 대화하듯이 니네 동네 가서 놀테니까 언제 만나자고 그냥 그렇게 써요. 원래 했었는데 콘텐츠는 올리면 애들이 막 댓글에 ‘감성 판다’ 이래서 상처받아서. 캡처해서 스토리에 박제되고. (중1, 참여자 8)

예전에 틱톡에 찍어서 올렸어요. 근데 모르는 사람이 영상도 하나도 안 올리고 보기만 하는 사람인 것 같은데 ‘좋아요’ 눌러서 이상한 것 같아서 지웠어요. (초5, 참여자 33)

틱톡이나 유튜브를 보면 특히 틱톡은 댓글을 보면 조금 잘못해도 XXX라고 욕도

많이 쓰고 아예 닉네임이 욕인 사람도 있고 그냥 중간 손가락 든 것도 있고 좀 많이 불쾌해요. (초4, 참여자 27)

참여자들은 SNS에서 낯선 사람의 접근, 그들에게 정보가 공개·공유되는 것을 걱정했다. 개인정보와 프라이버시 침해와 관련해 학교, 친구, 가정, 미디어 기업 보다 모르는 사람의 납치·위협·사칭 등 범죄 위험을 우려했다.

부모님이나 친구는 친하니까 유포에 대한 걱정은 많지 않은데 모르는 사람은 그 사람이 어떤 사람인지 모르고 SNS은 얼굴도 올리고, 이름도 올리고, 생년월일도 올리니까 그런 게 다 침해되면 지역도 알 수 있으니까. 저를 찾아와서 인질로 해서 뭐가. (중1, 참여자 1)

나는 모르는데 나를 알고 있는 사람의 범위가 넓잖아요. 외국인인데 한국인인 척 할 수도 있고. 그게 더 섬뜩하고 위험할 것 같아요. 집에 찾아오거나 범죄위험도 있지만 사칭이 무서울 것 같아요. (중1, 참여자 3)

저는 그 사람을 모르는데 그 사람은 저를 아니까 위협받을 수 있다는 불안감. 저를 알고 있으면 거짓말을 유포할 수 있으니까. (중1, 참여자 4)

낯선 사람의 접근에 대해 남학생과 여학생의 태도는 달랐다. 여성 참여자 중에는 낯선 사람의 접근에 공포를 느껴서 SNS 운영을 중단한 경우도 있었다.

페이스북에서 프사가 약간 변태같은 사람들이 엄청 많이 한 30명이 저한테 계속 친추 걸고 폐쇄하자고 한 적 있어서 언니한테 말해서 언니가 공개범위를 친구된 사람한테만 공개하는 걸로 설정해줬어요. 사람들이 친추 보내도 친구 아니면 친추 거의 안 받아요. (중1, 참여자 8)

옛날에는 게시물 올렸는데 지금은 그런 얘기가 뉴스에도 많이 나오고. 성폭력까지 이어지는 경우도 있잖아요. 그래서 안 올려요. 페이스북 계정 프로필에 사진 한번 올렸거든요. 친구의 친구인데 모르는 사람이 그걸 캡처해서 친구한테 저를 안다고, 저를 잘 챙기라고 친구한테 보낸 거예요. 깜짝 놀라서 그후 아예 안 올려요. N번방 그런 것도 있고 하나까. (중2, 참여자 14)

상대적으로 적지만 남학생에게도 SNS 이용에서 위험 요인이 존재한다. 다만 그에 대한 반응은 연구에 참여한 여학생들과 확연한 차이가 있었다. 한 남학생은

성매매를 암시하는 메시지를 받은 사실을 대수롭지 않게 얘기했다.

SNS에 보통 거울샷같은 사진 올려요. 이상한 댓글도 달리죠. 악플 같은 건 아니고 하트 눌러주고 좋다는 사람들 많은데, 페이스북은 항상 섹알바 같은 게 있더라구요. (모르는 사람이 본인 사진 보는 거 걱정한 적 없나요?) 네, 한 번도 없어요. 다 모르는 사람들이 죄다 '좋아요' 눌러주고 인스타는 아는 사람만 해줘서 걱정은 딱히 없어요. (섹알바 이런 거 무섭지 않나요?) 안 무서운데, 어차피 안 할 거여서.(중1, 참여자 19)

8) 인터넷 이용에서 불편한 점

참여자들은 게임, SNS, 유튜브 등 인터넷을 이용하면서 싫거나 불편했던 점, 바뀌었으면 하는 점과 관련해, 활동을 방해하거나 콘텐츠와 구분이 가지 않는 배열, 선정적 광고 등 광고에 대해 언급했다. 광고를 포함해 지나치게 상업화된 환경에 대해 불만을 드러냈고, 광고 보기와 개인정보 제공을 전제로 한 서비스 이용 등과 관련해 무력감을 드러내기도 했다. 일부 참여자들은 청소년에게 부적합한 광고에 대해 언급했다.

유튜브에서 어떤 게임 재미있다고 추천받아서 깔았는데, 유튜브는 현실 해서 광고제거되서 그렇게 안 보였는데 현실 안 하니까 게임을 한 판 할 때마다 광고를 봐야 해서 엄청 힘들었어요. (초5, 참여자 34)

유튜브는 요즘 광고를 2개씩 넣고, 유튜브는 여러 연령층이 다 보는데 너무 폭력적이거나 선정적인 광고가 너무 많고. (중2, 참여자 15)

인스타그램에서 게시글 확인할 때 사진 막 넘겨보고 무조건 하트 누르고 가는데, 광고가 바로 아래에 비슷하게 뜨니까 나도 모르게 광고에 하트 누르고 그래서 너무 불편해요. (중2, 참여자 17)

무조건 뭘 동의해야 앱을 쓸 수 있어서 자연스럽게 개인정보가 나가는 게 싫어요. 한편으로는 앱을 쓰기 위해 그 정도 대가를 치러야한다는 생각이 들기도 하고. (중1, 참여자 18)

특히 초등학생 참여자의 경우 게임에서 사이버불링이나 악플을 경험하면서 위축된 모습을 보이기도 했다. 게임 등에서의 미숙한 행위나 작은 실수를

용납하지 않는 등 엄격하고 위계적인 환경에서 어린이들은 오프라인과 다를 바 없는 차별을 당하고 있었다.

게임하고 있는데 제가 실수로 때렸는데 어떤 사람이 패드립을 날려서 속상했던 적이 있어요. 하지 말라고 했는데 갑자기 친구들 불러서 저한테 욕하고 (캐릭터) 죽이고 그래서 엄청 울었어요. (초5, 참여자 34)

저는 틱톡할 때 댓글을 달거든요. 근데 제가 이렇게 해도 되고 저렇게 해도 되는데 이렇게만 되는 줄 오해해서 “이거 아닌가요?”하고 댓글 달았더니 갑자기 모르는 사람이 “잘 알고 말하세요”라고 해서 속상했어요. (초5, 참여자 31)

롤이라는 게임을 했는데 거기서 “상대편이 개뿔한다”고 욕을 날려서. (초5, 참여자 33)

9) 약관 읽기와 서비스 가입

참여자들은 어려서부터 포털, 소셜미디어 등 미디어 서비스나 애플리케이션에 가입해왔다. 개인정보보호법에 따라 만 14세 미만의 경우 법정대리인인 부모가 가입한 경우가 있지만 나이 인증절차 없이 서비스에 가입하는 경우도 상당수다. 서비스 가입은 정보(약관)를 바탕으로 자율적 판단에 따라 개인정보를 공개·제공하는 과정이라는 의미를 지닌다. 내 정보를 어떻게 관리할지 공식적으로 협상하는 과정이고, 약관읽기는 그 과정의 첫 번째 단계이다. 이러한 중요성에도 불구하고 절대 다수 참여자들은 약관읽기의 경험을 문자 귀찮아서 읽지 않는다고 말했다. 참여자들은 교육을 통해 ‘약관읽기’의 당위성은 알고 있지만 너무 길고, 이해하기 어려워 포기했다고 말했다. “안 읽기엔 너무 불안하고 읽기엔 너무 귀찮아요” (중2, 참여자 12)라는 말은 약관에 대한 태도를 압축적으로 드러낸다. 참여자들은 필수가 아닌 선택사항은 동의하지 않는다면 소극적 대응을 하고 있었고, 어려운 용어, 너무 많은 정보뿐만 아니라 작고 흐린 글씨 같은 물리적 요건도 약관읽기의 걸림돌이 되었다.

너무 길어서 안 읽어요. 그냥 모두 다 동의하기 체크해요. (중1, 참여자 9)

안 읽어요 선택인 건 안 누르고 필수만 해놓고(왜 안 읽나요?) 글이 너무 많아요 글씨도 너무 작아서 안 읽혀요. 색깔도 약간 회색으로 연하게 나오고. (중2, 참여자 14)

학교에서 하도 읽으라고 해서 읽어볼까하고 봤는데 글이 너무 많은 거예요. 바로 포기했어요. 몇 조 몇 항에 의거해서... 하나도 못 알아듣겠어요. (중1, 참여자 7)

약관을 읽지 않는 양상은 같았지만 그에 대한 생각은 참여자마다 차이가 있었다. 참여자들은 서비스 이용약관에 동의하면서도 불안함을 감추지 못했다.

(약관 동의하면서 모르는 내용이 있지 않나 걱정한 적 있나요?) 약관에서 개인정보라는 것만 알아듣고 나머지 하나도 모르겠어서 내가 모르는 사이에 돈이 빠져나가면 어쩌지 해서 네이버에서 동의하면 돈 나가나 검색해본 적 있어요. (중1, 참여자 8)

(왜 안 읽었나요?) 논란이 있으면 기사에 뜨지 않았을까요? (문제가 없을 거라 생각했나요?) 네 문제가 아직까지 없었으니까. (중1, 참여자 2)

약관 중에 저한테 엄청 해가 될 것도 없고 다 똑같은 내용이니까 대충 인지하고 그냥 넘기는 것 같아요. (중3, 참여자 20)

아무래도 네이버나 구글은 좀 신뢰가 쌓여있으니까. 대충 읽어보고 전체동의 누르고. (중2, 참여자 15)

확실하게 읽어본 적은 없고 동의만 누르고 내려가기만 했던 것 같아요. (왜 확실하게 안 읽었어요?) 당연히 약용할 리 없다고 생각해서. (중1, 참여자 17)

일부 참여자는 약관에 대한 동의가 다분히 형식적이라는 점을 언급했다. 약관내용에 문제가 있더라도 서비스를 이용하기 위해서 동의할 수밖에 없거나 읽어도 내용을 이해하기 어렵고, 더 나아가 이용자에게 불리한 내용을 숨기는 상황에서 진정한 ‘동의’의 의미를 찾기 어렵다는 이야기이다.

그냥 다 동의, 동의, 동의, 동의하고 넘기죠. 일단은 엄청나게 긴데 다 읽기 시간도 부족하고. 거의 95% 이상은 안 읽지 않을까 싶어요. 특히 중학생들은. 그리고 ‘개인정보 어디다가 적용할 수도 있습니다’ 그런 문장은 항상 맨 밑에 있고. 결국엔 폼수 써서 개인정보 유출을 유도하는 거죠. (어쩔 수 없이 동의한다는 건가요?) 네, 그래서 저는 최대한 필수만 동의하고, 선택은 동의 안하고. (중1, 참여자 18)

10) 미디어 플랫폼의 정보 수집

인터넷 이용은 많은 기록을 남긴다. 특히 대다수 아동·청소년이 이용하는 SNS는 가장 광범위하게 정보를 수집한다. SNS를 할 때 어떤 정보가 기록될지에 대해 문자 이름, 생년월일, 나이 등 계정을 개설할 때 입력한 개인정보를 말하는 경우도 있었고, SNS내 활동을 말한 경우도 있었다.

생년월일, 지역 (중1, 참여자 2)

인스타는 책상에 뭘 올려놓고 사진을 찍으면 이 사람은 집에 이런 재질의 책상을 갖고 있구나 이런 걸 알 수 있겠죠. (중1, 참여자 3)

계정 만들 때 개인정보랑 전화번호 같은 저의 사생활 정보 같은 거 (중2, 참여자 12)

이름이랑 전화번호랑 생년월일도 적어야 하잖아요. (중2, 참여자 14)

접속 기록, 검색 기록 그런 거 남을 것 같아요. (중3, 참여자 21)

친구가 페메로 무서운 영화를 보내서 봤는데 페이스북에서 동영상 볼 수 있는 칸에 기록이 남아서요. 무서워서 지우려고 했는데 안 지워져서 검색하니까 페이스북이 이걸 못 지우게 해서 계속 남아 있어서. 시청기록까지 다 가져가는 것 같아요. (중1, 참여자 8)

유튜브는 구독목록이랑 자기가 올린 영상, 좋아요나 싫어요를 눌렀던 영상이나 자주 보는 분야 동영상 이런 게 기록될 것 같고. 페이스북은 자기가 올린 모든 거랑 자기 페이스북에서 자기 흔적들이 기록될 것 같습니다. (중3, 참여자 20)

유튜브에서 전자기기 리뷰 영상을 즐겨본다는 한 참여자는 정보수집과 관련해 비교적 전문적인 정보를 알고 있었고, 쿠키 삭제나 데이터 수집 거부 설정 등을 하는 참여자도 있었다. 그러나 사이트 가입 시 입력한 개인정보만을 수집정보로 언급하는 참여자를 포함해 질문 자체를 어려워하는 참여자도 있었다. 데이터 수집에 관한 지식에서도 참여자간 상당한 차이를 보였다.

질문이 너무 어려워요. (중1, 참여자 9)

인터넷에서 보니까 위치정보, 클립보드에 있는 복사한 거, 전화번호부, 사진도 다 가져 가고, 인터넷 사용기록도 가져간다고 해서 못 가져가게 다 반대해 봤어요.

게임이나 앱들이 개인정보 수집하면 광고 회사한테 넘겨서 그걸로 수익을 본다는데 걸 듣고서 그 이후로는 다 동의 안 해놨어요. 아이폰에서 수집 동의 물어서 다 못하게 해놨어요. (중1, 참여자 7)

이름, 성별, 생년월일 모든 개인정보와 사진들. 그러니까 뭘 하든 간에 거의 모든 일이 기록이 다 남으니까. 인터넷을 쓰면 인터넷 방문기록도 다 남아서 쓰고 다 삭제해요. (어떻게 안 거예요?). 그냥 학교 PC에서 사이트 위에 점 세 개가 보여서 눌러봤는데 지금까지 저희가 쓴 몇 천개 방문기록이 있길래 옆에 데이터삭제 버튼을 눌러봤더니 다 없어지더라고요. 기록은 다른 곳에 남을 수 있지만 최소한 방지할 수 있는 것 같아서 삭제했어요. (뭘 방지하는 거죠?) 예를 들어 구글을 썼다면 제 컴퓨터에서 삭제하면 구글에 직접 전화하지 않고는 데이터를 못 찾을 거라고 생각해서. (중1, 참여자 18)

11) 개인 데이터 저장에 대한 인식

참여자들에게 인터넷 이용 과정에서 어떤 데이터가 수집되는지를 묻는 질문과 별도로, 참여자들이 디지털 환경에서 자신의 데이터가 수집되고 저장되는 맥락은 어느 정도 알고 있는지 보다 정확하게 알아보기 위해 참여자 27명에게 일상적인 활동이 적힌 활동지를 나눠주고 데이터 기록 여부(○×로 표시)와 데이터가 기록된 곳에 대해 물었다¹⁷⁷⁾.

〈표 6-3〉 개인 데이터 수집·저장에 대한 인식

한 일	데이터 기록 여부 (정답률)	데이터가 기록된 곳 (한 사람이 여러 개 답한 경우 있음, 괄호 속은 대답한 사람 수)
혼자 거리를 걷은 일	46%	캐시워크(2), 게임(1), CCTV(4), ZEM(2), 패밀리링크, 전리
인터넷으로 콘서트 티켓 예매한 일	62%	티켓예매사이트(6), 사이트 관리하는 회사(3), 휴대폰 앱을 깔 때, 콘서트장, 인터넷(2), 인터넷 사용기록부
친구와 문자를 주고받은 일	96%	카톡(8), 문자앱(5), 핸드폰(2), 문자내역(내폰, 친구폰), 검색목록, 문자, 통신사, 본사, 카카오톡이나 SNS 본사, 페이스북 메시지, 이메일, 게임, 채팅방, 디스코드, 인스타, 페이스북

177) 박유신 외(2020). <인공지능 시대의 포스트휴먼 수업>에 실린 퀴즈를 활용했다. 이 활동은 세 번째 FGI부터 시작했고, 27명이 참여했다.

한 일	데이터 기록 여부 (정답률)	데이터가 기록된 곳 (한 사람이 여러 개 답한 경우 있음, 괄호 속은 대답한 사람 수)
자기 전에 스마트폰으로 음악 들은 일	62%	음악앱(5), 유튜브(3), 지니뮤직(2), 유튜브구독창, 문자 내용, 스마트폰, 앱과 앱 회사, 스마트폰 최근기록, 인터넷 사용기록부, 핸드폰통제앱
교통카드 이용해서 지하철 타고 간 일	73%	교통카드(5), 교통카드회사(4), 버스카드 리더기(3), 기계, 결제내역, 교통카드 찍은 회사 전송
학교 앞 포장마차에서 떡볶이 현금으로 사먹은 일	27%	현금, 계산기, 엄마와친구들, 포장마차 주인이 국내 기관에 신고, 포장마차, CCTV(있다면)
편의점에서 현금으로 과자 사고 포인트 적립한 일	38%	편의점(2), 포인트 앱회사(2), 포스기 포인트앱(2), 교회에서 아이스크림 기프트콘, 계산기, 휴대폰, 편의점 회사, 내 계정, 편의점단말기, 사이트, 포인트적립소, 카드사데이터
유튜브에서 영상을 검색하고 '좋아요' 누른 일	81%	유튜브(9), 유튜브 계정(2), 채널(2), 유튜브, 그채널주인, 비누TV, 할머니핸드폰, 내컴퓨터, 유튜브구독창, 구글회사, 좋아요 누른 영상, 좋아요 표시한 영상목록

친구와 문자주고 받은 일처럼 눈으로 확인할 수 있는 활동에 대한 정답률은 높았다. 유튜브에서 영상 검색하고 좋아요 누른 일이나 교통카드로 지하철 타고 간 일 등도 잘 알고 있었다. 유튜브 영상의 경우 상당수의 학생이 알고리즘에 의한 콘텐츠 추천을 인식·언급하고 있는 점 등이나 클릭 행위가 바로 구현되는 점에서 데이터 기록에 대한 인식이 높은 것으로 추정된다. 같은 맥락에서 교통카드 이용도 정답률이 높은 것으로 보인다.

정답률이 높더라도 이해 수준이 높다고 단정할 수 없다. 기록 여부를 맞췄더라도 데이터가 저장된 곳에 대해 잘못 알고 있는 경우도 있기 때문이다. 예를 들어 콘서트 티켓 예매의 경우 티켓예매 사이트 같은 답변도 있었지만 콘서트장이라고 답한 경우도 있었고, 문자내역(내폰, 친구폰)이라고 물리적 기계에 주목하는 경우도 있었다. 유튜브에서 영상을 검색하고 '좋아요' 누른 일의 경우, 정답률이 높았지만 채널 주인, 구독하는 채널명이나 개별 채널, 유튜버 등의 답변이 많았고, 내 컴퓨터, 할머니 핸드폰, 좋아요 누른 영상 등이라고 답했다. 정답률이 높지 않았던 혼자 거리를 걷은 일에 대해 소수의 참여자가 CCTV(4명)를 답했고, 위치정보 등을 제공하고 포인트를 받는 앱인 '캐시워크'(3명), 잼이나 패밀리링크

같은 스마트폰 감시앱(2명), ‘젠리’같은 위치추적앱 등 세대의 미디어 이용 특성이 반영된 앱을 답했다¹⁷⁸⁾.

12) 페이스북 약관에 대한 인식

아동·청소년이 인터넷 서비스 약관에 대한 이해 수준과 약관 내용과 기업 방침에 대한 생각을 알아보기 위해 참여자들에게 10분여간 시간을 주고 페이스북의 ‘데이터 정책’¹⁷⁹⁾을 읽게 하고, 내용의 이해 여부, 읽고 난 소감을 질문했다. 앞서 약관읽기 경험과 마찬가지로 표현과 분량 때문에 페이스북 약관을 이해하기 어렵다는 의견이 압도적으로 많았다.

이거를 다 읽고 동의하겠다고 제대로 결정할 수 있을 사람은 없을 것 같아요.
너무 길고 불편해요. (중2, 참여자 13)

영어, API나 SDK 이런 거는 뭔지 모르니까요. (중1, 참여자 18)

일부 참여자들은 페이스북의 약관 설명방식에 대해 문제를 제기했다. 페이스북이 동의를 유도하기 위해 고의로 복잡하게 설명한 것 같다는 의견, 좀더 자세한 설명이 필요하다는 의견을 제시했다.

도구가 왜 나오는지 이해가 안 가고 모르는 단어가 너무 많아요. 한줄 읽자마자 정책부터 해서 추가적인 도구, 액세스 이런 것부터 해서 정보유입 못 알아듣는 말도 너무 많고 말을 한방에 줄여서 하면 좋은데 배배꼬아서 돌려서 말하는 것 같아요. (중1, 참여자 8)

일부러 포기하게 만들어서 동의하게 만들려고 한 것 같기도 하고. 읽어보려는 사람들도 못 읽을 것 같아서 알아들을 수 있게 쉽게 설명해주면 좋겠어요. (중1, 참여자 7)

아주 딱딱하다는 생각이 들었어요. 제목이나 소제목을 많이 달아서 사람들이 원하는 정보를 딱 볼 수 있게 하거나 사진 같은 걸 넣어 수월하게 읽고 할 수

178) 캐시워크의 경우 17세 이상 이용가능하다.

179) 참여자 포레들이 보편적으로 많이 이용하는 플랫폼이고 개인정보 정책에서 많은 논란이 있다는 점을 고려해 페이스북을 선정했다. 페이스북 데이터 정책 <https://www.facebook.com/about/privacy>

있을 것 같아요. 간략하게 (중1, 참여자 3)

참여자들은 약관 내용과 관련해 수집 정보가 지나치게 많은 것에 대해 놀라워하거나 비판적인 목소리를 냈다. 정보 수집범위를 필요한 것에 한정할 필요가 있다는 의견을 제시하기도 했다.

읽어보니까 서비스를 이용하는 이용자뿐만 아니라 이용자와 가까운 사람의 정보도 나 뿐만 아니라 다른 사람의 정보도 털리는 거라고 생각해서 안 좋다고 생각했어요. (중2, 참여자 11)

페이스북에서 올린 정보들을 페이스북에서만 볼 수 있는 게 아니라 다른 데서도 다 볼 수 있다는 걸 몰랐는데. (중2, 참여자 14)

카드번호까지. 진짜 상상도 못한 것까지 수집해서 깜짝 놀랐어요. 이거 다 기록한다는 거네. 뭐 이렇게 가져갈게 많아. 너에게 개인정보 따위는 없다는 것처럼 정보를 다 가져가는 것 같아요. 필요하긴 할 텐데 안 필요한 것도 가져가는 것 같아서. 진짜 수집 목적 같아서, 좀 싫어요. 다른 사이트도 다 이럴 거 같아요. (중2, 참여자 16)

SNS를 안 해서 전화번호나 메일 이런 게 어느 정도 나가겠구나 싶었는데 이렇게까지 집요하고 스토커처럼 정보를 수집할 줄은 몰랐어요. 아주 진짜 그 사람의 정말 세부적인 것까지 다 수집하는 것 같아서, 솔직히 좀 무서워요. 관심사나 생년월일 정도까지는 괜찮은데 관심있는 사람, 종교관, 정치관 연결되는 사람까지 아무래도 하기가 좀 꺼려져요. 이 조그만 거 하겠다고 이렇게 데이터를 많이 가져가는 게 살짝 좀 흑막같은. 나중에 사건이 터질 수도 있잖아요. 대국민 사기극을 칠 리는 없겠지만 이걸로 나중에 사람들의 정보를 해킹하는데 쓰는 진짜 엄청난 일이 벌어질 것 같아서, 좀 더 적은 정보를 이용해 할 수 없는지 궁금해요. (중2, 참여자 15)

딱 보니까 '내가 하는 거 내가 전부 알고 있다' 이렇게 써있는데 솔직히 몇 억 명이 가입하고 있고 마음만 먹으면 몇 억 명 다 털 수 있는 거 아니에요. 페이스북이 유명하잖아요. 회사가 마음만 먹으면 몇 억 명이 발가벗은 기분일 거 아니에요. 누가 악의를 갖고 뚫어서 개인정보를 가져갈 가능성도 있고 조금은 섬뜩한 느낌. (중1, 참여자 2)

페이스북의 데이터 수집 범위와 활용 내역 등을 고지하는 행위에 집중해

페이스북의 데이터 정책에 대해 긍정적으로 평가하는 참여자들도 일부 있었다. 이들 참여자들은 기업의 과도한 데이터 수집과 남용 보다는 외부에서의 해킹 같은 보안이나 개인 차원의 범죄에 대한 우려를 드러냈다.

참여자1: 웬지 이런 정보나 신경을 많이 쓴다는 게 느껴져요.

연구자: 그럼 좋은 건가요? 신경 많이 쓰니까?

참여자1: 좋은 건데 그런 게 뚫릴 위험이 살짝 있는 것 같긴 해요.

연구자: 누가 뚫는 건가요?

참여자1: 사람인데 페이스북 안에 있는 악한 마음을 가지고 있는 전문 해킹범.

13) 아동용 페이스북 약관읽기 경험

참여자들은 페이스북의 데이터 수집 정책을 읽고 이야기를 나눈 후, 다시 영국 아동위원회(Children's Commissioner)가 아동용으로 작성한 페이스북 약관(번역본)을 읽고 같은 방식으로 소감과 내용에 이야기했고, 페이스북 데이터 수집 정책과의 차이점에 대해서 이야기했다¹⁸⁰⁾. 대다수 참여자들은 아동위원회 자료가 페이스북의 데이터 수집 정책과 비교해 짧고 이해하기 쉽다고 답했다.

앞의 것에 비해서 짧고 간편하게 되어서 이해하기 쉬운 것 같아요. (중2, 참여자 11)

앞의 것보다 페이스북을 이용하는 사람이 읽기가 더 편하다고 생각했구요 (중3, 참여자 21)

그래서 이해가 잘 됐구나. 이렇게 하면 되는 걸. 앞의 것은 무슨 소리인지 모르겠고. 한마디로 약간 눈속임, 꼼수 같은 느낌이에요. (중1, 참여자 18).

흥미로운 점은 참가자들이 페이스북의 데이터 수집 정책의 어조를 아동위원회 자료보다 긍정적으로 평가했고, 아동위원회의 명시적 어조에 대해 차갑거나

180) 연구진은 참여자들이 답변을 마친 후, 조금 전 읽은 자료가 페이스북 데이터 수집 정책을 아동이 이해할 수 있도록 있게 만든 자료라는 것을 설명해주었다.

<https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/03/Facebook-Simplified-T-Cs.pdf>(2017. 9)

무책임하다고 반응했다.

조금 더 통보 느낌 “우린 뭘 이렇게 할 것이다” 이런 거. (중1, 참여자 18).

애(페이스북 정책)는 그냥 동의하면 어느 정도 이렇다며 조금 책임이 있는 것 같은데 애(아동위원회 자료)는 너무 무책임하다고 생각했어요. 그냥 이렇게 해 이런 느낌. 처음 건 예의바른 느낌이었는데 두 번째 거는 약간 강압적으로 무엇을 하겠다는 느낌. (중2, 참여자 14)

일부 참여자들은 페이스북의 직선적이고 간명한 설명 대신 우회적으로 설명해 분명한 내용을 가리고 판단을 어렵게 만든다고 말했고, 페이스북의 데이터 수집 정책의 의도에 대해 비판적인 태도를 보였다. 페이스북 약관의 자세하고 친절하고 책임감 있는 듯 한 단어와 설명기법이 이해를 어렵게 하거나 동의를 유도해, 많은 정보를 가져가게 허용하는 효과로 이어지는 상황에 혼란스러워하기도 했다. 일부 참가자들은 “당사는 회원님의 정보를 누구에게도 판매하지 않으며 앞으로도 판매하지 않을 것입니다. 당사는 파트너들이 당사에서 제공한 데이터를 이용하고 공개하는 방법에 엄격한 제한을 가하고 있습니다” 등의 표현처럼 모호한 표현들로 인해 내용이 충돌되는 듯한 상황에 문제를 제기했다.

더 어렵게 보이려고, 일부러 넘겨버리게 하려고 말을 꼬아서 설명하는 것 같은데. 이걸 줄여서 이렇게 짧게 나왔잖아요. 길게 풀어 쓸 필요가 있다. (중2, 참여자 16)

수집하는 정보의 유형만 이만큼이잖아요. 요만큼 줄일 수 있는데 굳이 늘려서 쓰는 건, 대충 읽고 동의하도록 유도한 것 같아요. 또 사람들이 이거 왜 이러냐고 하면 ‘너희들이 동의했잖아’ 이렇게 나올 수 있게 길게 쓴 것 같아요. (중2, 참여자 15)

첫 번째 본 거랑 애랑 똑같은 얘기잖아요. 첫 번째가 좀 더 이해할 수 없게 복잡하게 만들어서 동의하게 만든 것 같아요. (중2, 참여자 12)

일부 참여자들은 페이스북의 정보 수집과 공유 방식 등과 관련해 처음 알게 된 사실에 놀라움을 표시했고, 과도하게 많은 정보를 수집하거나 개인정보를 활용하는 방식, 그리고 이용자의 권리를 보호하지 않는다는 것에 대해 강하게 문제를 제기했다. 광고주와 나이, 위치, 성별 등을 공유하는 사실, 동의없이

상업적으로 이용과 대가를 지불해도 되지 않는다는 사실과 광범위한 위치정보 수집(데이터 수집에 “위치 관련 정보(회원님의 현재 위치, 거주지역, 가고싶은 장소, 주변에 있는 업체 및 사람)를 이용합니다” 등으로 표현)에 대해 문제를 제기했다.

읽다 보니까 내용이 좀 충격적이네요. 개인의 아이디어나 생각 사상 이런 걸 동의없이 상업적으로 이용할 수 있고 심지어 그것의 원작자를 언급하지 않아도 된다고. (중1, 참여자 3)

당신의 이메일 주소를 공유하지 않지만 나이, 위치, 성별, 관심사를 전세계 광고주와 공유한다고 하는데, 이메일 주소를 몰라도 여차피 내가 어디 사는지, 나이, 성별, 관심사를 알면 이름도 이메일 주소도 알아낼 수 있으니까. 내 개인정보를 광고주와 공유한다는 게 위험한 것 같아요. (중1, 참여자 4)

다른데 들어갈 때도 위치나 그런 거 수집한다고 그랬잖아요. 내 위치를 페이스북이 다 알고 있다니까 위험할 것 같아요. (중1, 참여자 9)

내용만 보면 페이스북이 당신의 정보를 마음대로 이용하고 그에 대해 돈을 지불하지 않는다, 책임이 없다 이런 식으로 말하는데 그래도 최소한 어딘가에 공유되었을 때 그걸 삭제할 수 있는 권리는 주어야하지는 않을까요. 심지어 ‘다른 사람의 사진을 계속 올리시면 회원님의 계정을 삭제할 수 있습니다’라고 하는데 또 앞에서는 ‘계정을 삭제하면 게시한 내용은 삭제되지만 다른 사람이 공유한 내용은 삭제되지 않습니다.’ 이렇게 되면 이거랑 아까 말한 거랑 살짝 부딪히는 것 같은 느낌이잖아요. 근데 이걸 이렇게 해놓은 게 이상한 것 같아요. 아무래도 자기네들한테 유리한 조건을 내건 거 같은데, 여기서 보면 복사·저장해도 자기 책임 아니라고 하고 정보도 다 공유할 거고, 게시한 내용도 내 알바 아니고 이런 식으로 나오는데 여기서는 또 우리는 돈 벌 수 있고 너한테는 돈 안 줄 거야. 이 계정은 나한테 달려있다. 이 사진을 삭제해봤자 우리한테 저장되어있었다 이런 식으로 되어있는 건 살짝 반협박성인 것 같기도 한데. 자기들 자유라고 하고, 발을 들인 이상 너희는 여길 어떻게 나가 이런 느낌. 주의를 줘야하는 입장에서 이거를 가지고 이용하는 것 같은 느낌이 들어요. (중2, 참여자 15)

약관 안 읽고 넘기는 사람들도 많잖아요. 근데 이렇게 이용될지는 몰랐는데 읽고 정말 충격을 받았어요. 정말 사용에 관련된 모든 정보를 가져가는 것 같은 느낌이 들어서요. 되게 신기하기도 했고 무섭기도 해요. 이권(이용자의 권리) 너무 적은데 이권(페이스북의 권리) 너무 많아요. 동등해져야 하지 않나. 자기네들도 그만큼 돈을 주던가, IP주소를 주던가. 뒤에는 약간 계정이란 개인정보랑 모든지 약간

자기들한테 달려있고, 올리는 거 조심해야 하는 거 맞는데 그거를 저장하게 할 수 있는 건 좀. (중2, 참여자 16)

광고주, 광고하는 사람한테 넘어가서 관심 분야를 광고할 수 있다 이런 거. (중1, 참여자 18)

‘페이스북이 팔리게 되면 자신의 정보도 같이 팔린다’는 건 새로 알게 된 거 같아요. (중3, 참여자 21)

‘이용자 권리’ 5번 ‘공식적으로 회원님이 동영상을 소유하고 있지만 페이스북이 원하는 대로 사용할 수 있고, 돈을 지불할 필요가 없다’는 건 처음 알게 됐고, 사실상 페이스북이 동영상 소유자로 올린 것을 맘대로 사용할 수 있다는 게 의아했어요. (중3, 참여자 20)

참여자들은 페이스북 등의 플랫폼의 정보 수집·저장을 프라이버시 침해라고 생각했다. 특히 다른 앱의 활동이 수집·기록되는 것에 강한 반감을 드러냈다.

사생활 침해라고. 그 앱에서 이용하는 걸 아는 거는 어느 정도는 그럴 수 있다고 생각하는데 밖의 다른 앱에서 이용자가 사용하는 것을 아는 거는 사생활 침해이지 않나. (중3, 참여자 21)

사생활 침해를 받고 있다고 생각해요. 프라이버시를 개인공간이라고 생각하고, 자신의 프로필은 개인공간이라고 했는데 다른 공간의 내용이 수집되거나 공유돼서, 개인공간을 침해받고 비밀보장이 되지 않는다고 생각해요. (중3, 참여자 22)

참여자 중 일부는 페이스북 같은 미디어 기업이 아닌 해커나 범죄에 대해 우려했고, 페이스북이 안전에 대해 노력한다고 말했다. 이러한 인식의 기저에는 페이스북이 거대 기업이라는 것이 한몫했다. 일부 참여자는 페이스북의 데이터 수집 정책 등을 이용자의 책임으로 생각하는 경우도 있었다.

누군가가 페이스북을 사면 개인정보를 같이 사니까 악한 마음을 갖고 사서 수억 명의 정보를 유출하고 공유하면, 범죄의 경우도 있고, 내가 어디 사는지 개인정보가 침해될 수 있는. (정보를 파는 건 문제지만 페이스북이 갖고 있는 건 괜찮나요?) 페이스북이 관리를 잘 하니까 수 억 명이 가입을 하는 거고, 이걸 사는 사람이 어떤 사람인지도 모르는데. 큰 회사 같은 사람이 사면 대기업이니까 개인정보를 보호해줄 테니까. 소기업이나 1인 기업이 사면 안심이 안 될 수밖에

없을 것 같아요. (중1, 참가자 1)

페이스북에서 안전을 향상시키려고 노력을 많이 하는 것 같긴 한데 페이스북이 팔리면 우리 정보도 팔린다는 거도 그렇고, 페이스북이 수집하는 여러 정보들이 퍼질 수 있는 게 그런 것 같아요. (중1, 참가자 6)

페이스북이나 SNS들이 운영자(기업)가 아니라 자신에 대한 책임이 더 크다고 생각해요. 공유하거나 거기서 다른 걸 접속하는 것도 운영자는 알지만 그에 대해서 딱히 간섭이나 그런 걸 하지 않는다고 생각해서 '운영자보다는 내 책임이 더 크다'라고 생각했어요. (중3, 참여자 21)

14) 개인 데이터 수집·저장과 알고리즘에 대한 인식

개인 데이터의 수집·저장은 페이스북에서만 이뤄지는 것은 아니다. 각종 추천 서비스 또한 콘텐츠 이용, 검색, 좋아요 기록 등 데이터 수집을 전제로 이뤄진다. 다수의 참여자들이 콘텐츠 추천의 편리함에 동의했으나 일부 참여자들은 콘텐츠 추천 이면의 개인정보 수집이나 잘못된 정보 추천 등에 대해 언급했다.

추천 콘텐츠에 제가 관심있는 새로운 영상도 있잖아요. 그 영상 보고 재밌으면 그것도 관심사가 될 수 있고 그게 정말 좋은 것 같아요. (초4, 참여자 27)

원래 알고리즘에 그림만 떴었는데 애니메이션에 관심을 갖게 돼서 두 번 정도밖에 안 봤는데 갑자기 그게 알고리즘에 떠버리니까 좀 있다 보려고 기억해냈던 알고리즘이 사라지고 기억이 안 나고 당황스러웠어요. (중1, 참여자 5)

확실히 제가 보고 싶은 거를 다시 검색해서 볼 필요는 없어서 좋고 편하기도 한데 어떻게 보면 제가 게시글을 확인했던 거나 '좋아요' 눌렀던 걸 다 알고 그거를 보여주는 거라서 소름 돋는 것 같아요. (중1, 참여자 17)

콘텐츠 추천에 대해 긍정적으로 생각하면서도 상품추천이나 광고 발송 등에 대해 비판적인 참여자도 있었다. 직접적인 광고 노출 이외에 콘텐츠와 광고의 모호한 구분, 과도한 상업적 이용, 부적절한 콘텐츠 노출에 대해 우려했다.

유사정보가 뜰 수 있어서 좋지는 않을 것 같아요. 관심사를 역이용해서 사이트 가입과 같은 게 뜨는데, 제 취미인 운동 이런 건 줄 알고 들어갔는데 운동에서 조금 바뀐 '스포츠토토' 이런 것일 수도 있고. 안 좋은 정보, 유해사이트들이 되게

많이 노출되니까 안 좋은 것 같아요. (중1, 참여자 18)

개인정보 이용해서 광고 내보내는 거 법으로 금지했으면 좋겠어요. 내 개인정보 어떻게 사용되는지 똑바로 얘기했으면 좋겠어요. (중1, 참여자 7)

특히 참여자들은 다른 플랫폼의 활동 정보가 수집·활용되는 경험에 대해 부정적으로 평가했다. 미디어 기업이 이용자 IP, 사이트 방문, 검색 기록 등을 수집해 스마트폰, SNS 등에서 관련 광고를 내보내는 것을 부정적으로 생각했다¹⁸¹⁾. 콘텐츠 추천에 대해서는 긍정적 입장이었으나 광고 추천에 대해서는 부정적 입장을 보였다.

유튜브 알고리즘 같은 건 좋긴 한데 쿠팡에서 물건을 구입하면 페이스북에서 광고 뜨는 건 없어졌으면 좋겠어요. (중1, 참여자 8)

인터넷에서 어떤 물건 찾아보기만 해도 ‘이 상품은 ~에서 최저가로 쓰세요’ 그런 것 계속 뜨니까 너무 짜증나고 관련 없는 게 나오고. 그냥 그 제품을 보고 싶었던 것뿐인데 사고 싶은 게 아니어도 자꾸 뜨니까 불편해요. (중1, 참여자 17)

유튜브도 그런 것 같은데, 편리하게 해주는 것들이 있고 마음을 불편하게 만드는 것들이 있는데 어쩔 수 없이 이걸 이용하려면 해야 하는 거니까 또 안할 수도 없고. 그래서 그냥 놔두고 있어요. (중2, 참여자 16)

악용만 하지 않는다면 괜찮다고 생각하는데, 페이스북은 좀 선을 넘지 않았다. 유튜브 같은 경우 계정이 있든 없든 사이트를 타고 들어갈 수 있는데 사이트를 타고 들어가도 알고리즘이 계속 추천을 해주거든요. 유튜브는 어떻게 할 수가 없는 것 같아요. (중2, 참여자 15)

그걸 수집해서 알고리즘에만 이용하면 편할 것 같은데 다른 곳에 잔뜩 이용되면 너무 찝찝할 것 같아요. 맞춤형 광고는 동의 안 동의한다 해놔서, 완전히 동의를 받아야 할 것 같아요. (중1, 참여자 7)

181) 당사는 회원님이 사용하여 Facebook 제품과 연결되는 컴퓨터, 전화, 스마트 TV 및 기타 웹 연결 기기로부터 그에 관한 정보를 수집하고, 회원님이 사용하는 여러 기기에 이 정보를 결합합니다. 예를 들어 당사는 회원님의 휴대폰에서 Facebook 제품 이용에 관해 수집한 정보를 이용하여, 회원님이 노트북이나 태블릿과 같은 다른 기기에서 Facebook 제품을 이용할 때 보게 되는 콘텐츠(광고 포함) 또는 기능을 회원님에게 맞춤화하거나, 다른 기기에서 회원님의 휴대폰에 표시된 광고에 대한 회원님의 반응 여부를 측정합니다(페이스북 데이터 정책 중 일부).

기본 좋지는 않죠. 그 사람들이 제 정보를 다 가져가서 넘기고 돈을 버니까. (중1, 참여자 18)

개인과 관련한 정보의 저장에 대해 비판적인 참가자도 있었지만 알고리즘을 사람과 별개의 독립적 영역으로 보거나 알고리즘과 인공지능에 대한 안전성 등에 대해 막연한 기대와 신뢰를 보이는 참가자들도 있었다. 인공지능에 대한 사회적 담론의 일부를 반영하는 것으로 보인다.

연구자: 유튜브에서 추천해주는 것 좋다고 얘기했잖아요. 이걸 여러분이 뭘 좋아하는지 유튜브가 알고 있는 거잖아요. 알아요 괜찮아요?

참여자32: 알고 있어도 좋은 것 같기도 하고 안 좋은 것 같아요.

참여자34: 인공지능도 웬지 알고 있으면 안 된다고 생각해요. 왜냐하면 자신이 좋아하는 거나 그런 것도 개인정보라는 생각이 들어서요.

참여자31: 괜찮다고 생각해요. 사람은 안 지켜도 AI는 개인정보를 지켜주지 않을까 생각해요.

참여자33: 유튜브 업체에도 직원이 있는데, 만약에 AI가 직원들, 사람들에게 정보를 막 보내면 좀 기분 나쁠 것 같아요. AI가 누가 뭘 좋아하고 이런 거를 보낼 수 있잖아요.

15) 프라이버시 침해 영역과 개선 방안

디지털 환경에서 프라이버시가 존중받는지에 관한 질문에 학교, 부모, 친구보다 미디어 기업의 프라이버시 침해 가능성을 언급했다. 부모와 친구와 달리 통제권한을 벗어나거나 영리 목적으로 이용될 수 있다는 점에 주목했고, 정보 수집의 범위와 광범위성, 기록 목적 등에 대해 문제를 제기했다.

미디어 같은 게 제일 침해하는 것 같아요. 가족이나 친구는 ‘하지마’하면 그만두는데 이걸 한번 동의하면 막을 수가 없잖아요. 그렇게 거기서 정보를 가져가고. (중2, 참여자 12)

미디어 플랫폼이 가장 많이 침해한다고 생각해요. 왜냐하면 가족 같은 경우 제가 방문한 사이트 같은 걸 볼 수 없잖아요. 근데 이런 플랫폼들은 거기 안에서 그런 것을 다 추적할 수 있는 거잖아요. 그래서 침해된다고 생각해요. (중2, 참여자 11)

어디가 심한지 잘 모르겠는데 똑같은 정보를 수집한다면 기업이 제일 위험할 것 같아요. 부모님이랑 친구는 악용하지 않을 거고, 돈을 벌려고 광고하는 사람들이 더 위험하니까. (중2, 참여자 13)

존중해주는 것 같지 않아요. 정보를 다 공유하고 계정을 나가더라도 정보가 바로 삭제되지 않고. (중2, 참여자 14)

너무 과도하게 수집하는 것 같아요. 페이스북 자체에서 광고하는 것도 아니고 광고에서 하는 걸 정보를 주고 돈을 버는 거잖아요. 내 개인정보를 사고파는데 기분이 안 좋죠. (중1, 참여자 7)

참여자들은 미디어기업으로부터 프라이버시 침해를 받더라도 사용할 수밖에 없는 딜레마를 드러내기도 했다.

저희가 동의한 거니까 가져간다는데 어떻게 할 수는 없잖아요. 동의를 안했는데, 앱을 지웠는데도 가져간다면 프라이버시 침해지만 일단 동의했기 때문에 뭐라고 할 수 없는 것 같아요. 프라이버시 존중 같은 게 필요한 것 같긴 한데 존중은 안 해주는 것 같고 그냥 쓰는 거죠. (중2, 참여자 16)

참여자들은 개인의 프라이버시나 권리 확보를 위한 정부, 기업, 사회 등의 변화와 관련해, 아동이 쉽게 이해할 수 있는 약관 제공, 무차별적인 개인정보 수집 금지와 정보 판매 최소화, 정보처리 단계별 동의 절차 구비를 강조했다.

페이스북 같은 거 만 14세 미만 사용 못한다고 하지만 애들이 나이 속이면 쉽게 빠져나갈 수 있잖아요. 정부에서 그런 걸 못하게 법을 만들면 좋을 것 같아요. (중2, 참여자 13)

안 좋은 계정이나 이상한 게시물을 필터링할 수 있는 시스템이 구축됐으면 좋겠어요. (중2, 참여자 11)

맞춤형광고 같은 거 동의를 법적으로 의무화했으면 좋겠어요. 개인정보 가져가는 게 절대 당연한 일은 아니잖아요. (중1, 참여자 7)

종교관이나 정치관 가져서 뭐해요. 회사가 돌아가기 위해서 필요한 정보들만 수집해야 한다고 생각해요. 진짜 불필요한 정보는 수집하지 않는 걸로. (중2, 참여자 15)

개인정보를 다른 사람, 기업에 공유할 때 이용자에게 동의하는지 물어봐주었으면

좋겠어요. (중3, 참여자 21)

약관에서 대부분 사람들이 너무 길고 귀찮아서 동의만 누르고 넘어가니까 '우리는 이게 필요하다. 너네는 ~를 할 수 있다' 이 정도로 써서 우리가 확인하게 편하게만 해줘도 일단 만족할 것 같아요. (중2, 참여자 17)

4. 소결

참여자 다수는 프라이버시를 이름, 주소, 전화번호 등과 같은 '개인정보'와 같은 개념으로 생각했고, 개인정보와 프라이버시 모두 유출, 추적, 도난, 돈, 도둑 등 부정적 단어와 연결하는 등 '침해'와 '보호' 맥락에서 인식하는 경향이 나타났는데, 이는 개인정보 교육에서 금전적 피해가 강조된 부분과 관련된 것으로 보인다. 일부 참여자는 프라이버시를 인권 개념으로 파악했지만, 전반적으로 정보 주체로서 프라이버시 권리에 대한 인식이 아직은 부족한 것으로 나타났다. 아동·청소년들은 다양한 형태의 개인정보 유출 위협에 노출됐고, 우려했으나 이들이 받는 교육은 미디어 이용 상황을 반영하지 못하는 당위론적 교육(비밀번호 변경하기, 개인정보 유출 피해 사례, 약관 읽기)이었다.

참여자들은 가정, 학교, 미디어 등의 환경에서 프라이버시에 대한 위협을 받는 것으로 나타났다. 먼저 가정에서 부모의 동의없는 사진 공유 외에 스마트폰 감시앱에 의한 프라이버시 침해에 대해 많은 문제제기를 했다. 학교와 연락, 관계 맺기, 여가와 놀이 등 참여자 또래의 일상 대부분이 스마트폰으로 이뤄지기 때문에 감시앱은 1차적으로 생활에 큰 불편을 초래했고, 사생활 침해, 감시, 통제로 인식했다. 이런 면에서 감시앱은 어려서부터 감시를 내재화하게 만들 뿐만 아니라 프라이버시와 미디어 리터러시에 대한 감수성의 발달을 방해할 가능성이 높다. 또한 부모 자녀간 신뢰 형성에도 부정적 영향을 미칠 수 있다.

학교의 영역에서는 코로나19로 인한 온라인 수업 확대로 오프라인에서는 발생하지 않았을 프라이버시 침해가 일어났다. 교사뿐만 아니라 동료 학생, 심지어 학부모 등의 제3자에 의한 프라이버시 침해 가능성도 언급했다. 얼굴과

대화 내용이 영상통화, 사진, 메신저, SNS 등에서 시각적으로 기록되고, 대부분의 소통이 온라인에서 이뤄지면서 상대의 동의없는 사진 촬영·공유는 빈번하게 나타났다. 또한 참여자들은 낯선 사람의 접근을 경험한 적이 있었고, 특히 여성 청소년의 경우 많은 우려를 드러냈다.

미디어와 관련해, 참여자들은 어려서부터 인터넷 서비스에 가입했고, 많은 앱에 가입된 상태이며, 서비스 약관 동의와 가입 과정에서 정보 비대칭성 등으로 인해 미디어 이용의 대가로 개인정보를 불평등하게 교환해야 했고, 일종의 무력감을 느꼈다. 참가자 일부는 정보 부족으로 거대 미디어 기업에 근거없는 신뢰를 드러내기도 했다.

아동들이 가장 많이 이용하는 SNS인 페이스북과 관련해, 대다수 참여자가 약관의 내용이 너무 어려워 사실상 읽지 못했고, 이 때문에 페이스북의 데이터 수집과 공유에 대해 모르고 있었다. 약관 읽기를 통해 페이스북이 과도하게 많은 정보를 수집하거나 부당하게 개인정보를 활용하고, 이용자의 권리를 보호하지 않는다는 것을 알게 된 경우도 있었지만 일부는 거대 미디어 기업에 대한 막연한 신뢰를 드러내며, 부당한 계약에 대해 우려하지 않는다는 입장을 보였다. 하지만 8700만명의 이용자 정보가 유출돼 최악의 개인정보 유출 사건으로 알려진 페이스북의 케임브리지 애널리티카 사건 당시 이용자가 설정을 조정해 전화번호 등 개인정보 유출을 미리 차단할 수 있지만, 대다수 사용자는 해당 기능을 모르거나 거의 사용하지 않았다는 것과 이 사건 이후 사회적 비판이 일자 페이스북이 2018년 약관을 이해하기 쉽게 개정한 일은 이들의 낙관이 아무런 근거가 없음을 보여 준다¹⁸²⁾. 또한 미디어 기업의 개인 활동 데이터 저장과 콘텐츠 추천과 광고 추천의 연관성을 생각하지 못하는 것으로 나타났다. 개인정보 수집·저장·이용에 대해 비판적 입장을 보이는 참가자도 있었지만 일부는 알고리즘을 사람과 독립된 개체(기계)로 취급하거나 막연한 기대와 신뢰를 보인

182) 이코노미조선(2018.4.9). 8700만 고객정보 악용소지 인식...저커버그가 문제 핵심.

http://economychosun.com/client/news/view.php?boardName=C24&t_num=13256(검색일: 2021. 11. 1)

참가자도 있었다. 이는 인공지능에 우호적인 사회적 분위기를 반영하는 것으로 보인다.

참여자들은 자신의 통제권한을 벗어나고 자신의 정보 영리목적으로 이용되는 점에서 미디어 기업의 프라이버시 침해를 우려했고, 프라이버시를 지킬 수 있는 방안으로 아동이 쉽게 이해할 수 있게 서비스 약관 제공, 정보의 제한적 수집과 판매 최소화, 정보 처리 단계별 동의 등을 강조했다.

요약하면, 학교나 가정의 영역에서 아동을 독립된 인격체로 보지 않고, 프라이버시 권리 등을 인정하지 않는 반면, 미디어 영역에서는 아동의 발달과정을 인정하지 않고, 아무 보호 장치 없이 성인과 똑같이 취급하며 이들의 프라이버시를 침해하는 것으로 나타났다.

제 7 장

아동·청소년 개인정보 교육과 제도에 관한 전문가 평가 및 의견

제 7 장

아동·청소년 개인정보 교육과 제도에 관한 전문가
평가 및 의견

1. 전문가 인터뷰 개요 및 방법

아동·청소년 프라이버시와 개인정보 관련 현행 제도와 미디어 교육의 평가와 개선점을 알아보기 위해 제도와 교육 분야(개인정보 법제, 정보인권, 미디어 리터러시 분야)에서 전문가 평가 및 의견을 들었다. 다양한 의견을 수렴하기 위해 교육계, 학계, 공공기관, 시민사회단체 등에서 전문가를 선정했다. 전문가 명단은 <표7-1>과 같다.

〈표 7-1〉 인터뷰 대상 전문가 프로필

구분	영역	직업 및 분야
A	제도	변호사 (정보인권, 아동인권)
B	제도	정보인권단체
C	제도	개인정보보호 기관
D	제도	공공기관 연구원(법학)
E	제도	대학교 교수 (사회교육, 법학)
F*	교육	초등학교 교사 (미디어리터러시)
G	교육	초등학교 교사 (미디어리터러시)
H	교육	초등학교 교사 (미디어리터러시)
I	교육	중학교 교사 (미디어리터러시)
J	교육	고등학교 교사 (미디어리터러시)
K	교육	고등학교 교사 (미디어리터러시)
L	교육	고등학교 교사 (학생 정보인권)
M	교육	대학교 교수 (윤리교육)
N	교육	미디어리터러시 연구자
O	교육	공공기관 연구원 (디지털시민성교육)
P	교육	공공기관 연구원 (디지털시민성교육)

개인정보와 프라이버시를 중심으로 아동·청소년이 마주한 디지털 환경에 대한 진단(미디어, 가정, 학교 등), 아동·청소년의 프라이버시 권리 보장을 위한 법제도 개선 방안, 아동·청소년 개인정보 교육평가(학교교과, 정부기관 교육안) 등에 관해 질문했고¹⁸³⁾, 구체적인 인터뷰 내용은 <표 7-2>와 같은 항목으로 구성했다. 인터뷰는 2021년 9월13일부터 27일까지 서면으로 진행했고, 전화통화 등을 통해 일부 내용을 보완했다. 질문은 제도(5인)와 교육(10인) 분야의 전문성을 살려 다르게 구성했고, 학교에서의 프라이버시 침해 가능성이나 개인정보 교육에 대한 평가 등은 공통으로 질문했다.

<표 7-2> 전문가 인터뷰 질문

주제	질문	분야
아동·청소년 프라이버시 환경 진단	<ul style="list-style-type: none"> • 미디어 이용에서 아동·청소년 프라이버시·개인정보 위협 요인 • 학교 환경에서 프라이버시·개인정보 위협 요인* • 가정 등 사적 영역에서 프라이버시·개인정보 위협 요인 • 스마트폰 관리(감시)앱에 대한 의견 • 디지털 환경에서 그밖의 아동·청소년 권리 위협·침해 요인 	제도
법제도 개선 방안	<ul style="list-style-type: none"> • 아동·청소년 프라이버시 관점에서 국내 법제도 평가 • 아동·청소년 프라이버시 권리 보장을 위한 법제도 개선방안 • 법제도 이외 영역에서 개선 사항* 	제도
교육 평가	<ul style="list-style-type: none"> • 중학교 정보교과 개인정보 교육 평가* • 개인정보보호위원회 개인정보 교육 평가* • 개인정보 교육에 대한 아동·청소년의 평가 분석 • 기존 교육의 보완점과 프라이버시와 개인정보 교육 방향 	교육

* 표시 부분은 제도, 교육 분야 공통 질문

183) 교육분야 전문가 10인에게 연구결과를 토대로 구성한 프라이버시 교육방안에 대한 자문을 구했고, 그 내용은 8장 교육안에 반영했다. 전문가 F의 경우 학교 개인정보 관리현황을 파악하기 위해 전문가 인터뷰 이전에(2021.6) 인터뷰를 했다. 전문가F의 인터뷰 내용도 전문가 인터뷰에 함께 소개한다.

2. 인터뷰 결과(법제도 분야)

1) 미디어 이용에서 프라이버시와 개인정보 침해 위험

전문가들은 미디어 이용에서 아동·청소년의 프라이버시나 개인정보 위험 요인에 대해 미디어 기업의 과도한 정보 수집과 개인정보와 프라이버시 침해행위 파악의 어려움 등을 언급했다. 또한 어려서부터 개인에 관한 정보가 누적·기록되는 점과 프라이버시에 대한 인식부재 외에 주민번호의 취약성 등이 복합적으로 작용해 아동·청소년의 프라이버시와 개인정보를 위협한다고 보았다.

구글, 페이스북 등 빅테크의 정보독점이 문제다. 빅테크들이 경쟁우위를 갖게 된 근본적 이유는 방대한 개인정보를 보유해 광고 수익뿐만 아니라 경쟁업체에 비해 경영정보 취득과 전략적 활용에서 유리한 위치를 점하고 있기 때문이다. 이는 아동만의 문제는 아니지만, 유튜브·인스타그램 등은 젊은층이 주로 이용하고 이들의 개인정보가 어려서부터 누적·기록된다는 점에서 영향이 크다. 이들 기업은 개인정보를 활용한 비즈니스에 그치지 않고, 이를 기반으로 이용자의 경제적 선택뿐만 아니라 문화적·정치적 선택을 유도한다는 점에서 이에 대한 수용성이 높을 수 있는 아동에게 더욱 위협하다. (전문가 B)

서비스 제공자(주로 글로벌 빅테크)와 개별 이용자의 관계는 심각하게 불균형하다. 빅테크 미디어가 명시적으로 선언하고 약속하는 내용이 제대로 지켜지는지를 확인하고 신뢰할만한 근거가 희박해서 아동·청소년의 신중함이 필요하다. 개인정보의 목적 외 활용과 공유(2차사용)가 위협이 될 수 있다. 특히 소셜미디어는 가능한 더 많은 개인정보를 확보해 상업화하는 것이 목적이어서 온갖 개인정보가 무차별 수집될 위험성이 농후하다. 또 소셜미디어에 제공된 개인정보가 어떤 용도와 목적으로 공개·공유되었는지 파악할 수 있는 구체적 장치가 없다. 법적으로 자신의 개인정보를 청구할 수 있지만 상대가 글로벌 규모인데다 해외에 있는 경우가 많아 개인의 프라이버시 권리를 주장하기가 어렵다. 게다가 개별 이용자의 기술과 프라이버시 이해가 부족하다. 급속히 진화·확장하는 미디어 기술과 그에 따른 프라이버시 영향을 제대로 파악하고 이해하는 문제는 계속 난제일 것이다. (전문가 C)

전문가들은 근본적으로 국내 법제에서 아동·청소년 보호 차원에서 개인정보

활용과 관련해 원칙상 금지되어야 할 부분이 사실상 방치된 점과 ‘설명기반 동의’가 아닌 형식화된 사전동의절차 등과 같은 취약한 정보주체에 대한 보호미비 등 법제도의 허술함과 구조적 환경의 미비에 대해 언급했다.

사인(예. 기업)에 의한 프라이버시나 개인정보에 대한 간섭이 법적으로 제대로 규율되지 않고 있다. 아동의 개인정보 활용은 원칙적으로 금지되어야 할 부분이 있는데, 현행 개인정보보호법 등 관련 법제에는 아동의 개인정보에 대한 특별보호가 공백으로 남아있다. 가령 아동 개인정보의 무분별한 가명화 및 활용, 딥러닝을 위한 개인정보 활용, 자동화된 의사결정 금지 등 국제인권법상 필요한 규제가 공백 상태다. 아동의 개인정보자기결정권을 포함하는 프라이버시권의 완벽한 향유를 위한 제반제도 역시 제대로 마련되어 있지 않다. 가령 개인정보의 제공·동의·고지 등에 필요한 아동친화적 설명이 제도적으로 구축되고 있지 않으며, 14세 미만 아동의 개인정보자기결정권을 전면적으로 박탈하는 등의 문제가 있다. (전문가 A)

아동·청소년 프라이버시 관련 쟁점은 아동·청소년의 행태데이터의 축적이다. SNS와 스마트폰 등 미디어 이용과정에서 발생할 수 있는 행태정보의 수집·축적과 결부되어 있는 문제이다. 특히 우리나라는 결국 주민등록번호(생년월일)와 친화적인 행태정보들이 축적될 가능성이 높기 때문에, 다른 국가들의 아동·청소년 프라이버시 문제보다 심각한 상황이라 할 수 있다. 유럽의 경우 아동·청소년의 프라이버시 문제에 대해 제도적으로 고민하고 있으나 우리나라는 그렇지 못하다. (전문가 E)

국내 동의제도는 형식화된 사전동의를 요구해 동의내용에 대한 이해를 돕기보다 절차적으로 적법한 동의의 형식을 갖추려는 경향이 있다. 방대한 내용을 담은 긴 글 형식의 일반적인 동의서 양식은 아동·청소년에게 개인정보 처리와 관련된 사항을 명확하게 인지시키기 어렵다. 특히 개인정보보호법 제22조의 “필요한 최소한의 정보”는 법정대리인의 동의없이도 수집할 수 있는데, 사유에 대한 구체적 지침이 없어 아동·청소년 특화 서비스가 아닌 일반 서비스의 경우 아동·청소년을 위한 별도 동의방법을 갖추지 못하고 있다. (전문가 D)

2) 학교에서 프라이버시와 개인정보 침해 위협

학교공간은 코로나19로 인한 온라인수업 등 원격교육이 강화되면서 급격한 변화를 겪었다. 디지털화된 학교환경(교실 등 물리적 학습공간, 교육과 학습 맥락, 교육행정 등)에서 아동·청소년의 프라이버시나 개인정보는 다양한 차원에서

위협받고 있었다. 전문가들은 디지털화와 무관하게 학생 인권과 프라이버시에 대해 둔감한 교육행정과 학교환경이 프라이버시 침해가 쉽게 발행할 수 있는 온라인 수업환경과 결합하면서 아동·청소년의 프라이버시가 전방위적으로 위협받고 있다고 진단했다. 프라이버시 침해 주체는 교사, 미디어와 에듀테크 기업, 동료 학생과 학부모까지 다양했다. 학생 인권과 프라이버시에 대한 교사와 학교, 교육당국의 인식부재, 온라인 환경에서의 프라이버시 인식부재와 온라인 수업 운영에 대한 교사·학생의 이해·교육의 부재, 에듀테크기업의 데이터 수집과 활용 문제까지 다양한 문제가 지적됐다.

(1) 원격수업과 사기업의 학생 정보수집 논란

비대면 수업 시행으로 온라인 학습 시스템을 통한 수업이 일상화됐다¹⁸⁴⁾. 학생들은 학교나 교사가 선정한 플랫폼에 가입한 후 수업을 들을 수 있다. 전문가들은 플랫폼 가입 과정에서 학생들의 개인정보가 수집되고, 비대면 수업 과정에서 학생 학습데이터가 축적되는 등 대규모의 학생 개인정보와 데이터가 사기업으로 유입되는 상황에 대해 우려했다. 선택권 없이 의무적으로 특정플랫폼에 가입해야 하는 상황, 학생 정보와 학습기록 같은 공적 활동의 기록·수집·활용 그리고 활용결과에 대해 학생들이 알 수 없는 점이 문제로 제기됐다.

원격교육이 학교 밖의 플랫폼에서 이루어지면서 학생들의 학습정보가 학교가 아닌 기업의 자산이 될 수 있다. 즉, 외부업체가 학교교육을 지원하는 단순한 위탁관계가 아니라 기업이 플랫폼을 구축하고 학교, 선생님, 학생이 플랫폼의 이용자가 되는 관계가 형성되고 있다. 이때 생성된 학생들의 학업정보(수강과목, 성적, 학업 태도 등)가 플랫폼에 기록되는데, 학교와 선생님에게 일정한 접근권을 주더라도 기업 역시 이러한 정보에 대한 통제권을 가지고 있을 가능성이 크다.

184) 원격수업에 사용되는 학습관리시스템(LMS)은 공공 차원의 'EBS온라인클래스'(EBS), 'e학습터'(한국교육학술정보원), 온라인학습 커뮤니티 '위두랑'(한국교육학술정보원) 등과 민간의 '하이클래스'(아이스크림미디어), '클래스팅', '구글 클래스룸' 등이 있고, 시스템 부재 등으로 공공 사이트보다는 민간 사이트가 더 광범위하게 사용되는 경향이 있다. 학교나 교사의 선택으로 일괄 이용되는 경우도 있고, 교사가 적극적으로 가입·활동해, 학생들이 가입하는 경우도 있다(예. 하이클래스).

그리고 이는 이후 학생들에 대한 또 다른 비즈니스로 연결될 수도 있다. 이처럼 외부 플랫폼을 활용한 원격교육 과정에서 선생님과 학생의 개인정보에 대한 권리를 어떻게 처리할 것인지 정리될 필요가 있다. (전문가 B)

미디어를 활용한 교육활동에서 개인정보에 대한 우려, 비대면 상황에서 온라인 교육 도구 등의 활용에서 아동·청소년의 개인정보 활용수준 등에 대한 사전점검 등 검토가 필요하다. 에듀테크들은 필연적으로 온라인 활동에 대한 추적이나 흔적이 남게 된다. 따라서 학교 현장에서 이들 도구를 선택할 때, 많은 고민이 필요하다. 스마트교육을 활용할 경우, 아동·청소년의 활동관련 개인정보들이 수집될 가능성이 높고, 보안정도에 따라 개인정보 유출 가능성도 있다. 이에 대한 철저한 보안이 필요하다. (전문가 N)

전문가들은 학생 인권이나 프라이버시에 미칠 영향이나 교육 전반에 미칠 영향에 대한 검토없이 온라인 교육 플랫폼 도입 등 기술 시스템을 도입·활용하는 상황에 대해 우려했다. 전문가들은 이런 현상의 배경으로 최신 기술에 대한 추종과 무비판적 수용을 언급했다. ‘에듀테크’를 통해 학생 정보가 기업에게 흘러들어가는 과정에서 학교가 주도적으로 교육 플랫폼에서 아동 프라이버시를 보호하기 위해 노력하거나 아동 대상 기업 노력이 필요하다고 지적했다.

교육현장에 인공지능, 빅데이터 등이 들어올 때 기술담론과 국가예산이 밀고 들어오는 상황에서 기술부터 도입되고, 어떤 결과를 가져올지에 대한 성찰이 거의 작동하지 않는다. 과거 3D 프린터가 들어올 때 유해성 진단도 없이 기술부터 들어왔고, 나중에 유해성이 밝혀져 사라지게 됐다. 사기업들 통해 학생 데이터가 수집되는 현재 상황도 우려스럽지만 디지털 교과서가 전면화되는 상황은 심각하게 걱정된다. 인공지능을 이용해 학습기록을 수집·반영하고, 클라우드에 공유되는 형태일 수 있는데, 특정 학생의 활동기록, 예를 들어 박물관에서 활동한 내용을 올리면 클라우드를 통해 활동이 같은 교과서를 사용하는 다른 학생에게도 공유될 수 있다. 학생의 학습과 교육 활동 즉 거의 모든 개인정보와 활동을 사기업이 관리하는 것이 우려스럽다. (전문가 F)

원격교육이 제공되는 디지털 환경에 대한 이해가 부족하다. 교육서비스를 제공하는 학교와 교육기관은 서비스의 편의와 기술의 첨단성에만 이끌리는 것을 경계하고, 서비스 제공 과정의 잠재적 위험이나 위협을 미리 검토·파악해 대책을 세워야 한다. 학생 개인정보가 어떤 목적에서 왜 필요한지 명확히 규정해서 서비스에 필요한 최소한의 개인정보만을 수집·사용·공유토록 해야 한다. 개인

정보가 애초 약속된 목적에만 사용되도록 감사와 감시장치가 마련될 필요가 있다. 서비스를 증가하는 플랫폼이나 기술기업은 기술의 최초 설계단계에서 사용자의 프라이버시를 어떻게 보호할지, 어떤 보안대책이 필요한지 미리 계획하고 적용하는 ‘프라이버시 중심 디자인’, ‘보안 중심 디자인’ 개념을 적용할 필요가 있다. (전문가 C)

(2) 원격수업의 프라이버시 침해와 학생정보 활용 우려

전문가들은 원격수업 관련, 온라인에서 얼굴을 보여야하는 상황이 프라이버시 침해가 될 수 있다며 얼굴 공개를 강제하는 수업방식에 대해 언급했다. 얼굴 등의 공개 과정에서 개인공간이 드러나 아동과 아동 가족들에 관한 정보 등 사생활 전반이 노출되거나 제3자에게 유출될 우려도 있다. 전문가들은 프라이버시 노출이 타인에 의한 사진 공유행위나 온라인 괴롭힘 등과 연결되거나 학부모 등이 수업을 ‘시청’하면서 학생과 교사에 대한 프라이버시 침해가 발생할 가능성도 있다고 진단했다.

비대면 수업 과정에서 발생하는 얼굴 등 신상정보의 활용은 큰 문제로 대두되고 있다. 초중등의 경우 실시간 화상 수업에서 카메라를 켜 줄 것을 요청하는데, 이 과정에서 영상정보가 아동의 프라이버시를 침해할 위험성이 크다. (전문가 E)

원격수업 과정에서 개인공간이 노출되면서 학생들의 가정환경과 생활수준 등이 드러날 우려가 있다. 또한, 컴퓨터 사용 능력이 미숙한 학생의 경우 파일 공유·전송 과정에서 적절하지 못한 파일이나 사진이 전송된다거나 컴퓨터로 어떠한 작업을 했는지 등에 관한 사생활이 공개·노출될 수 있다. 수업에서 개인공간에 대한 블러(마스킹)처리 의무화나 녹음·녹화시 활용가능 범주 등 아동·청소년의 사적 정보를 보호하기 위한 별도의 영상정보 처리방침을 마련할 필요가 있다. (전문가 D)

학생들은 원격수업 중에 화상에서 얼굴이 부각되는 것을 프라이버시 침해로 보고, 자신의 공간을 교사나 다른 사람이 보는 것을 불편해한다. 출결체크를 위해 얼굴을 보여주기기를 원하는 교사와 신체 일부를 조금만 보여주기만 원하는 학생간의 갈등이 있다. 초등학생과 중학생의 경우 원격수업중 학부모의 간섭행위가 발생하기도 하는데 프라이버시 침해라는 인식이 매우 낮다. (전문가 I)

교사의 프라이버시에 대한 인식부재와 온라인 수업지침의 부재로 학생들의

모습이 담긴 온라인 수업이 수업 이외의 목적으로 활용되는 상황도 벌어지고 있다. 특히 녹화수업을 활용하는 경우나 일명 ‘ 쌤튜브 ’로 수업을 활용해 수익을 내는 활동까지 교사에 의한 프라이버시 침해 양태가 다양하게 존재한다.

일부 교사의 경우 수업을 촬영해 유튜브에 올려 수익을 창출한다. 학부모와 학생의 동의를 의무적으로 받아서 진행하도록 강화해야 한다. (전문가 J)

원격수업을 녹화·녹음하는 경우 플랫폼을 통해 동의를 구하더라도 영상 활용이 교육 목적에 한해야 하는데, 이를 수집한 주체(학교나 교사)가 평가나 사적인 다른 목적으로 활용하는 경우 개인정보의 목적 외 이용 및 제공에 해당하는 것으로서 개인정보보호법 제18조 위반 우려가 있다. (전문가 D)

인공지능을 활용해 학생들의 표정이나 행동 등을 분석해 수업집중도를 알아보는 연구가 국내에서 진행 중이고, 홍콩에서 교실에 설치된 CCTV로 학생의 실시간 얼굴 표정을 수집·분석해 수업집중도 등 수업태도를 파악했다는 연구가 나온 상황에서 교육효과성 측정 목적으로 한 학생 데이터 활용에 대한 우려도 제기되고 있다¹⁸⁵⁾. 전문가들은 프라이버시에 대한 고려없음과 기술에 대한 무비판적 수용으로 자료가 수집·활용되는 상황이 지속될 경우, 학생 평가 목적의 데이터 활용 가능성도 배제할 수 없다고 말했다.

본격화되진 않았지만 최근 교육 효과성을 측정하기 위한 데이터 활용·분석이 제기되고 있고, 이러한 데이터 활용이 증가할 것으로 보인다. 예를 들어, 수업의 집중도 등을 측정하기 위해 수업과 관련한 다양한 행태정보를 활용하고, 결과를 축적하는 경우, 이는 향후 심각한 프라이버시 침해요인이 될 가능성이 높다. 물론 제도적으로 가명처리 등 가명정보를 활용해 프라이버시 침해를 최소화할 수 있겠지만, 어디까지나 최소화이지 프라이버시 침해를 온전히 방지할 수는 없을 것이다. 교육 효과성 측정·분석을 위한 데이터 활용에 관한 특화된 대응이 필요해 보인다. (전문가 E)

185) Altimes (2021.3.31.). AI기술로 혁신하는 교육, 커리큘럼부터 시험까지 개인 맞춤형
<http://www.aitimes.com/news/articleView.html?idxno=137679>(검색일: 2021.10.1.)

(3) 온라인 수업환경에 대한 이해 및 교육 미비

온라인 수업은 단순히 수업전달 방식이 대면에서 비대면으로 바뀐 것이 아니다. 교사-학생의 관계, 학생간의 관계, 정보공유 범위와 방식 등이 전면적으로 확대·세분화되고 서로 동시에 영향을 미치면서 학생들은 확장된 공간에 놓여지게 됐고 이는 프라이버시에 영향을 미치게 됐다. 전문가들은 교육현장에서 온라인 수업을 수업전달 방식의 변화 정도로 좁게 이해하는 등 온라인 환경에서의 지도에 대한 준비가 부족하다며 관련해 교사 교육이 필요하다고 말했다.

아동, 보호자, 교원 등에게 디지털 환경에서 이루어지는 온라인 교육지도를 위한 교육 등이 충분히 이루어지고 있는지 의문이다. 가령 출석체크를 위해 화면을 켜게 하는 지도 등은 아동의 사생활을 현저히 침해할 수 있다. 교육행정 등에서 학생들에 대한 차별을 양산할 수 있는 인공지능 활용 등을 규제하기 위한 법제도 구축되어있지 않으며, 데이터베이스화되는 학생정보의 오·남용을 방지하기 위한 대책이 필요하다. (전문가 A)

원격수업 확대로 학교에서 다양한 온라인 플랫폼을 사용하면서 수집되는 학생 개인정보도 늘고 있다. 학생 개인정보를 관리하는 교사들에 대한 철저한 교육이 필요하다. 이전에 비해 학생들의 개인정보가 유출될 가능성이 많아 보인다. 수업에서 공개해야하는 것 이상의 개인정보나 사생활을 공개하는 경우가 많아 학생들도 온라인에 콘텐츠를 올릴 때는(수업시간이더라도) 철저한 점검이 필요해보인다. (전문가 K)

교사들의 학생들의 프라이버시 침해, 개인정보의 사적활용에 대한 인식이 제고될 필요가 있다. 학교홍보나 교사의 외부활동 등에 학생 사진이나 정보가 활용되거나 다양한 수업용 도구 등의 활용에서 학생들의 개인정보 관리 등을 검토할 수 있는 이해와 실천이 필요하다. (전문가 N)

비대면 교육에서 다양한 방식으로 개인정보가 사용될 수 있으며, 교육 후 수업자료 게시 과정 등에서 무의식적으로 개인정보 등이 사용되는 경우가 생길 수 있으므로 개인정보 보호에 더욱 민감하게 대응할 필요가 있다. (전문가 P)

전문가들은 학생에 대한 교육 필요성도 언급했다. 플랫폼을 통해 개인정보가 수집된다는 사실과 프라이버시 침해 가능성, 다른 사람의 프라이버시를 침해할 수 있는 가능성, 얼굴과 사적 공간뿐만 아니라 수업과 관련된 학생의 모든 활동이

기록되면서 모든 것이 전파·확산될 수 있는 온라인 환경에 대해 주지시킬 필요가 있다고 말한다.

원격수업에서 동영상 과제 제출이나 토론, 댓글 활용 등이 일상화되면서, 학생들의 초상권 보호, 자기정보결정권 등이 소홀히 다뤄지는 경우가 많아졌다. 학생이 제출한 동영상을 교사가 모두에게 보여주면서 논평하는 경우도 사전동의나 고지가 필요하다는 것을 교사가 인지할 필요가 있다. (전문가 M)

수업 관련사이트에 가입할 때, 개인정보에 대한 안내가 부족하다. 교육청에서 개인정보에 대한 자료는 보급하고 있으나 수업 전 의무교육은 아니다. 기본적으로 모든 수업 전에 프라이버시나 개인정보에 대한 안내가 필요하다. (전문가 J)

원격학습이 강화되면서 학급 SNS가 개설되고 미디어에서의 의사소통이 잦아졌다. 이 과정에서 학생들의 프로필사진 등이 공개되면서 몇몇 아이들은 학급아이들 사이에 놀림거리가 되기도 하고 친하지 않은 친구에게도 SNS 게시물이나 프로필 사진이 원치 않게 공유되는 사례가 있다. 이런 일은 자칫 사이버폭력, 학교 폭력으로 이어질 위험이 있다. (전문가 G)

수업에서 친구나 교사 얼굴을 캡처해 공개게시판에 합성해 공유하는 경우도 있다. 온라인으로 교육이 진행되면서 본인 정보(출석체크를 위한 학번, 이름 댓글달기 등)를 온라인에 게시하는 것이 점점 거리낌이 없어지고 있다. 우리만의 공간이라고 생각하지만 누군가 캡처해 외부로 유출할 가능성이 크다. 교사나 학부모가 더욱 경각심을 갖고 살피고 주의를 주는 것이 필요하다. 여행사진을 단체 밴드나 학급커뮤니티에 게시하거나 학생의 결과물(사진, 주소 등)을 함께 볼 수 있는 자료실에 게시하는 것도 학급원들에게만 공개되었다고 생각하지만 그렇지 않은 환경이라는 것을 교사들도 인지하고 조심할 필요가 있다. (전문가 O)

원격교육 등으로 학생들이 다양한 플랫폼에 가입해야 해당 플랫폼을 활용할 수 있는데 이 과정에서 개인정보가 사용되고 있으나 학생들이 이런 사실을 인지하지 못할 수 있다. 교육용 플랫폼에서 수집되는 개인정보의 경우 제한적이긴 하나 원격교육 전 필수적으로 개인정보 보호교육을 하는 것이 필요하다. (전문가 P)

전문가들은 프라이버시 침해 우려 등이 디지털 교육 환경에서만 발생하는 문제가 아니라 오프라인에서 존중받지 못하는 학생들의 사생활이나 인권 관련 사안들이 디지털 환경에서 재현되거나 확장된 형태로 나타난 것이라고 진단했다.

근본적으로 디지털화된 학교만이 아니라 현재 학교에서 발생하는 과도한 개인

정보 수집, 사생활 침범 등에 대해 규율하기 위한 법제가 불충분하다. 학생인권 조례가 제정되지 않은 지역이 있으며, 제정되더라도 유명무실화되는 경우가 있다. 초·중등교육법은 학생인권 보장을 형식적으로 선언할 뿐 구체적 규율이 이루어지고 있지 않다. 교육행정 등에서 학생들에 대한 차별을 양산할 수 있는 인공지능의 활용 등을 규제하기 위한 법제도 구축되어 있지 않으며, 데이터베이스화되는 학생 정보의 오·남용을 방지하기 위한 대책이 필요하다. (전문가 A)

학교가 아동·청소년의 프라이버시에 대해 진지하게 고민해야 할 지점이 많다. 행정의 편리함을 위해 개인 프라이버시가 침해되는 경우도 있는데, 온라인 서비스 활성화로 학생정보를 종이로 보관·폐기처분하는 과거보다 파일로 저장·유포하는 것이 훨씬 개인정보 유출의 구조적 위험성을 안고 있다. 줌의 경우 화상수업에서 노출되는 개인의 정보 외에 플랫폼이 안고 있는 개인정보보호 관련 위험 요소가 있다. 미디어 환경이 변화하면서 새로운 프라이버시 문제가 대두될 가능성이 있지만 학교가 따라가지 못하는 지체현상이 나타나고, 문제 인식 후에도 시간이 지나야 대책이 수립된다. 학교 현장이 프라이버시 문제에 대한 정책적 민감성을 지니도록 노력해야 한다. (전문가 I)

3) 가정에서 프라이버시와 개인정보 침해 위협

전문가들은 가정 영역에서 아동·청소년의 프라이버시를 위협하는 요인으로 스마트폰 감시앱 설치와 자녀 동의없이 자녀 사진을 무단공유하는 ‘디지털 셰어 런팅’을 언급했다. 또한 코로나19로 인해 아동이 생활할 수 있는 오프라인 공간이 줄어들면서 프라이버시 향유가 어려워지는 점, 학업·관계·놀이 등 모든 일상이 온라인에서 이뤄지는 상황에서 가정에서 디지털 기기를 공동 사용할 경우 온라인 프라이버시 권리가 위축될 수 있다는 점 등을 언급했다.

부모가 아동·청소년의 얼굴과 목소리가 포함된 데이터를 무분별하게 SNS 등을 통해 공유하는 경우 이는 사실상 정보주체의 동의없는 개인정보의 이용 및 제공에 해당하는 수준의 불법성을 가지는 것으로 평가할 수 있다. 부모와 보호권자에 의한 프라이버시 침해 문제가 생각보다 심각하다. 보호권자의 보호 목적의 프라이버시 제한이더라도, 과거에 비해 보다 폭넓은 프라이버시 침해가 발생할 수 있다는 점에서 주로 인격적 문제들을 유발할 것으로 보인다. (전문가 E)

디지털 네이티브 세대 관점에서 셰어런팅을 통해 웹에 공개된 개인정보 등이 전 생애에 중대한 영향을 미칠 수 있다는 점에서 각별한 주의가 필요하다. (전문가 A)

가정 내에서 가족 구성원마다 컴퓨터 등 디지털 기기를 소유하지 않고 함께 활용할 경우, 프라이버시권을 제한할 수 있다. 공용 컴퓨터를 사용한다면 다른 가족 구성원의 눈을 의식해 활용이 위축될 수 있고, 이용기록이 원치 않게 다른 가족 구성원에게 노출될 경우, 갈등의 빌미가 될 수 있다. (전문가 B)

전문가들은 전기통신사업법에 따라 청소년의 스마트폰에 설치해야 하는 스마트폰 감시앱이 아동·청소년의 프라이버시와 개인정보자기결정권과 사생활의 비밀과 자유, 인간이 누려야 할 헌법적 권리 등을 침해하는 점을 근거로 강한 비판과 우려를 드러냈다.

아동의 개인정보자기결정권, 사생활의 비밀과 자유를 침해한다. 스마트폰 감시앱을 설치하는 목적이 불분명하고, 선화하더라도 추상적인 위협성인데 이를 기본권을 제한하는 정당한 목적이라고 볼 수 없다. 더불어 아동의 동의를 받는 방법 등이 고려되지 않고, 동선과 민감한 사생활에 대한 광범위한 제약이 초래되는 점에서 헌법과 국제인권법이 요청하는 필요성, 비례성의 원칙을 충족하지 않는다. (전문가 A)

실제 활용되는 감시앱은 법이 요구하는 것보다 훨씬 다양하고 침해적인 기능이 있다. 스마트폰 사용시간, 사용한 앱, 문자나 SNS 사용내역, 검색기록, 현재위치 등 개인에 대한 전면적인 감시를 가능하게 한다. 이는 유해정보에 대한 접근 통제라는 목적을 훨씬 넘어선 것이며, 자녀를 통제하려는 부모의 욕망을 반영하는 것이다. 청소년의 개인정보자기결정권과 프라이버시권의 침해이다. 이것이 과연 교육적 측면에서 바람직한지, 자녀와의 건강한 관계 형성에 도움이 될지 의문이다. 나아가 가정 내 폭력이 있는 경우 청소년이 이를 신고하기 어렵게 만들기도 한다. 전기통신사업법의 개정을 넘어서 인권침해적인 감시앱에 대한 규제가 필요하다. (전문가 B)

‘청소년’이라는 이유로 감시앱 설치를 의무화한 것은 정부권력의 남용이다. 그런 강제 규정은 프라이버시와 정보자기결정권은 물론 인권침해 소지가 다분하다. 국가가 개별 사용자의 스마트폰 사용에 개입하고 감시하게 하는 행위는 이른바 자유민주주의를 표방하는 나라에서는 도저히 상상하기조차 어려운 인권 침해이다. (전문가 C)

아동·청소년은 보호 대상이자 인격적 욕구의 충족 내지는 참여의 주체라는 특성을 함께 보유하고 있고 그에 따른 규범적 지위를 획득하고 있다. 청소년도 개인정보자기결정권에 관한 기본권의 주체임은 명확하나, 감시 앱 강제 설치가 청소년

보호의무라는 합목적성 실현에 적절한 수단인지를 판단해봐야 할 것이다. 스마트폰 사용 실시간 모니터링, 스마트폰 사용시간 제한, 유해 콘텐츠 차단 등은 기본권 침해 여지가 없지만 문자메시지 내용 확인, 특정번호 수신·발신차단, QR코드를 이용한 본인확인 제한 등의 기능은 인권침해 요소가 있다. (전문가 D)

4) 교육권과 정보격차에 따른 권리 침해

전문가들은 아동·청소년의 프라이버시 권리에 대한 침해 우려 이외에 원격교육의 확대 속에서 아동·청소년의 교육권이 침해받거나 정보격차로 인해 교육격차 등이 발생해 차별받을 수 있는 상황에 대해 우려했다.

헌법 제31조에 따르면 모든 국민은 능력에 따라 균등하게 교육 받을 권리를 가지며, 특히 초등교육과 법률이 정하는 교육은 무상으로 받을 권리를 가진다. 그런데, 원격교육 환경에서는 가정에서 보유하고 있는 ICT 인프라(망 속도, 웹캠 및 컴퓨터 장비 등) 수준이나 부모가 학습 환경 조성에 기여할 수 있는지 여부가 곧바로 교육수용도로 나타날 가능성이 크다. 따라서 원격교육 환경에서 학생간 편차가 줄어들 수 있도록 제반여건을 마련해 학생간 평등한 교육권을 확보해 줄 필요가 있다. (전문가 D)

정보격차, 교육격차, 사회보장권에 대한 부당한 제약도 발생할 수 있다. 디지털 환경을 향유하기 위한 전제조건(가령 원격교육에 필요한 기기)에 대한 제도적 지원이 충분히 구축되지 않는 경우 정보격차, 교육격차 등이 초래될 수 있다. 디지털 환경을 향유할 수 없는 가정이 사회보장체계 내에서 차별받거나 배제되는 상황이 발생할 수 있다. (전문가 A)

디지털 공간에서 나타날 수 있는 사이버불링, 허위정보, 섹스팅 등의 문제에 아동·청소년이 더 취약한 부분과 청소년을 규제하는 각종 제도로 인해 표현의 자유가 위축·침해될 수 있는 점, 플랫폼 기업의 영향력 확산에 따른 감시와 자율성 침해에 대한 우려도 나왔다.

아동·청소년이 디지털 환경에서 알 권리나 표현의 자유, 문화의 권리 등이 광범위하게 제약될 수 있는 상황이다. 가령 청소년보호법이 규정하는 각종 제한들이 남용될 수 있고, 그 결과 아동이 원하는 정보에 대한 접근이 제약될 수 있고, 이는 알 권리나 표현의 자유 및 문화의 권리 침해에 이를 수 있다. (전문가 A)

빅테크의 권력 확대, 인공지능 기술의 발전 등으로 인해 개인정보와 프라이버시권 침해를 넘어 여러 가지 문제가 제기될 수 있다. 감시앱의 경우에도 프라이버시권 뿐만 아니라 아동·청소년의 정보접근권과 표현의 자유를 침해한다. 적절히 규제되지 않은 인공지능 서비스가 나타날 경우, 취약계층이나 소수자인 아동·청소년들이 차별에 노출될 수도 있다. 나아가 빅테크나 인공지능 기술이 아동이 인지하지 못하는 사이에 특정한 행동이나 선택을 유도한다면, 이들의 문화적·정치적 자율성을 침해할 수 있다. 검색결과나 타임라인에 숨겨진 알고리즘에 따라 어떠한 정보가 노출되는지에 따라 우리의 인식, 관점, 선호 등이 영향을 받을 수 있다. (전문가 B)

프라이버시와 사생활 보호는 전부는 아니지만 다른 권리들이 더 잘 보장되도록 도와주는 바탕이 되고, 다른 권리들이 보장됨으로써 프라이버시와 사생활이 더 잘 보호되는 결과로 이어진다. 디지털 환경의 빈부격차는 사회적·정치적 이슈로 떠오를 것이다. 디지털 환경에서 표현의 자유, 그와 직결된 허위정보, 온라인 괴롭힘과 따돌림 문제도 중요한 이슈이고, 디지털 환경을 악용한 인신매매, 마약밀매, 디지털 성착취물 등도 아동·청소년의 권리를 위협하고 침해하는 문제가 될 것이다. (전문가 C)

5) 아동·청소년 개인정보 관련 법제도의 문제점과 개선 방향

(1) 법제도의 문제점

전문가들은 국내 개인정보 관련법과 제도가 아동·청소년을 독립된 인격체이자 권리주체가 아닌 보호대상으로 보고 있고, 동시에 법과 제도, 기관 모두가 아동·청소년의 프라이버시나 개인정보에 대해 큰 관심을 보이지 않았다는 점을 지적했다. 전문가들은 디지털 환경에서 아동·청소년의 권리를 확보하기 위해서는 개인정보법 개정뿐만 아니라 학생인권조례 의무화 등 학생 권리 관점으로 확장해 아동·청소년의 프라이버시 권리를 보장할 필요가 있다는 의견을 제시했다.

아동 최상의 이익, 특별한 보호의 권리, 피청취권, 참여권을 반영하는 차원에서의 법률이나 제도가 수립되어 있지 않다. 법률이나 제도가 정보주체로서 아동의 권리를 규정하는 특별법이나 필요한 특별 조항을 두고 있지 않다. 법뿐만 아니라 행정제도가 아동친화적이지 않은 것도 문제이다. 가령 고지절차 등에서 아동친화적 절차가 마련되어 있지 않고 초·중등교육법 등 학생의 사생활을 보장하기 위한 법제도 충분히 구축되지 않은 상태이다. 학생인권조례가 의무화되지 않고, 학칙

제·개정 절차에 아동이 배제되어 있으며, 학생에 대한 사생활 인권침해에 대한 규율이 이루어지고 있지 않다. 나아가 만 14세 미만의 아동의 의사와 무관하게 법정대리인이 아동의 개인정보 처리를 허용·행사할 수 있는 등 아동을 권리주체가 아닌 보호대상으로만 보는 문제도 있다. (전문가 A)

우리나라의 개인정보 보호법제는 아동·청소년의 프라이버시 보호에 관해 특별한 관심을 가지고 있지 않다. 주로 아동의 개인정보 수집 및 활용에서 보호자의 동의 등을 추가적 요건으로 기술하는 내용들이 통상적이다. 개인정보 보호법 제39조의3 제6항에서 “보호위원회는 개인정보 처리에 따른 위험성 및 결과, 이용자의 권리 등을 명확하게 인지하지 못할 수 있는 만 14세 미만의 아동의 개인정보 보호 시책을 마련하여야 한다”고 규정하고 있으나 아직까지 구체적인 시책이 마련되지 않았다. 최근 개인정보보호위원회가 영국의 개인정보규약 등을 참조해 국내에서도 가이드라인을 제시하겠다고 밝혔다. 가이드라인을 만들면서 외국 사례를 단순 참조해 제시하는 것보다 학교교육이 강조되는 우리 실정을 심본 감안할 수 있는 가이드라인을 제시할 필요가 있다. (전문가 E)

개인정보보호법에서는 아동의 개인정보를 수집할 때, 아동의 정보주체로서의 권리 보장을 위해 법정대리인의 동의를 받도록 하고 있고, 고지할 때 이해하기 쉬운 양식과 알기 쉬운 용어를 사용하도록 하고 있다. 다만, 구체적인 구현방법에 관한 지침이나 관행은 미흡하다. 대체로 국내 법제는 아동보호를 명목으로 오히려 아동·청소년을 통제 대상으로 바라보는 경우가 많다. 감시앱 설치를 의무화한 전기통신사업법이 대표적이고, 게임셧다운제 등도 그렇다. (전문가 B)

또한 전문가들은 개인정보보호법 이외 다른 제도들이 충분하지 않은 점이나 아동의 맥락에서 제정된 미국의 ‘아동 온라인 프라이버시 보호법’(COPPA)이나 아동의 프라이버시 침해에 대해 징계를 강화하는 미국 ‘캘리포니아주 소비자 프라이버시 법안’(CCPA) 등을 참고사례로 언급했다.

한국의 개인정보보호법은 아동·청소년의 프라이버시 권리를 별도로 다루지 않고, 만 14세 기준으로 보호자의 동의를 요구하는 정도의 규정에 그치고 있다. 또한 한국의 개인정보보호법은 개인의 프라이버시 권리를 구체화하고 강화했다고 평가되는 유럽연합의 GDPR에 상응하는 수준의 프라이버시 보호 조항을 담은 것으로 보이지만 그에 맞는 정부기관과 기업의 지침, 정책, 제도는 여러모로 미흡하다. 특히 온라인 환경에서 아동과 청소년의 프라이버시 권리 보호에 주목한 미국의 COPPA는 여러모로 참조할 만하다. (전문가 C)

국내법에서는 개인정보 일반에 관한 쟁점이 우선 논의되다 보니, 아동·청소년에 관한 특칙적 보호 규정 마련에 미흡한 측면이 있다. 특히 아동의 권리를 적극적

으로 보호하고 있는 미국의 CCPA의 경우 18세 미만에 대해 아동으로서 별도의 특칙을 적용하고 있다. “부모는 자녀들의 어떤 정보가 수집·판매·저장되는지를 통제할 수 있어야 하며, 수집된 자녀들의 정보를 삭제할 것을 기업에 요구할 권리를 가져야 한다”고 규정하고 있다. 아울러 “기업은 소비자의 프라이버시권을 침해한 경우 그에 대한 책임을 져야하며, 침해가 아동에게 영향을 미칠 경우에는 징계의 수위를 높여야 한다”고 규정했다. 이에 비해, 우리 법은 부모 등 보호자(법정대리인)에게 아동의 정보주체로서 권리를 행사하도록 하는 것을 주요 보호 수단으로 택하고 있지만, 보호연령이 다소 낮은 편이다. 아동 개인정보에 대한 보호는 법정 대리인의 후견적 역할을 통제함으로써 완전히 해결될 문제는 아니므로, 아동이 정보주체로서 역량을 강화시키는 교육적 지원도 필요하다. (전문가 D)

(2) 법제도 개선 방안

전문가들은 아동·청소년의 프라이버시 등 디지털 환경에서의 권리를 확보하기 위해 프로파일링 등 자동화의사결정 금지, 동의없는 가명처리와 아동의 개인정보의 영리목적 활용금지 등과 같은 아동·청소년에 특화된 특별조항 개설과 유도 등을 통해 아동의 개인정보를 부당하게 수집하는 행위 금지, 정보 삭제권, 아동을 정보주체로 보고 이들이 참여할 수 있도록 개인정보 처리과정 전반에서 아동친화적 절차 도입을 제안했다. 또한 온라인 서비스의 ‘privacy by design’ 등의 적용을 제안했다.

아동의 권리에 대한 특별한 보장이 필요하다는 인식 아래 특별조항이나 개별법이 제정될 필요가 있다. 가령 아동의 개인정보에 대한 프로파일링 등 자동화의사결정 금지, 동의없는 가명처리와 아동의 개인정보의 영리목적 활용금지 등의 규제가 특별조항이나 법률의 제정을 통해 도입될 수 있다. 아동의 의사와 참여를 실제 반영할 수 있는 조항도 마련할 필요가 있는데, 개인정보 처리과정 전반에서 아동친화적 절차 도입, 법정대리인이 아동의 개인정보를 전적으로 처리할 수 있도록 하는 현행 법률조항 개정, 인증제도 도입 등 과제가 있을 것이다(가령 아동의 의사확인, 법정대리인에 의한 부당한 개인정보처리를 제한하는 조항 마련 등). 아동의 개인정보를 유도 등을 통해 부당하게 수집하는 행위를 금지할 필요도 있다(가령 인터넷 서비스상의 정보기입을 유도하는 다크패턴 규제). 이와 함께 학교에서 프라이버시권을 비롯한 인권이 존중될 수 있도록 학생인권조례 의무화와 그 효력을 학칙 상위로 하는 법률 도입, 학교가 수집하는 개인정보에 대한 폐기·

관리의무 강화 등 규제 강화 등을 담도록 초중등교육법을 개편할 필요가 있다.
(전문가 A)

연령에 따른 개인정보 수집 고지 방식 등과 같은 아동의 개인정보를 요구하거나 정보주체의 권리를 보장하기 위한 구체적인 지침이 개발되고, 관행으로 정착될 필요가 있다. 전기통신사업법이나 게임법 등 가부장적 시각으로 만들어진 기존 법의 개정도 필요하다. 이 과정에서 청소년/단체들의 의견을 반드시 수렴할 필요가 있다. (전문가 B)

아동·청소년의 보호를 위해 온라인 서비스의 디자인과 디폴트 옵션, 특정목적으로 처리 금지 등 다각도의 접근이 필요하다. 이를 위해 부모 등 보호자의 후견적 역할에 전적으로 의존할 것이 아니라 국가가 아동의 최선의 이익을 발견하고 보호자와 개인정보처리자 등의 바람직한 역할을 분담해 제도적으로 실현해야 한다. 보호대상으로서 아동의 범주를 UN 아동권리협약의 아동이나 민법상 미성년자로 확대하거나 국가가 규제나 권장을 통해 개인정보처리자가 아동 보호를 위해 ‘privacy by design’, ‘privacy by default’ 원칙 적용 등을 준수하도록 하는 방안을 고려해볼 수 있다. (전문가 D)

유년기부터 축적된 정보들이 지속적으로 데이터화된다는 점은 심각하다. 특정 요건을 갖추는 경우 이러한 정보의 삭제를 요청할 수 있는 법적 대안이 필요하다. 데이터와 개인정보의 산업적 활용 과정에서 아동 데이터의 일률적 삭제 요청은 무리가 있으므로, 동의에 관한 적법 요건이 갖춰지지 않은 경우, 데이터의 삭제를 가능하게 하는 방안 등 섬세한 디자인이 필요하다. 물론 현행법 해석으로도 이러한 방식의 규제가 불가능하지 않지만, 아동의 개인정보와 프라이버시 보호를 위해 상징적으로 입법하는 것도 충분히 가능하다. (전문가 E)

아동·청소년의 개인정보를 보호하고, 온오프라인에서 안전하고 건강한 삶을 이어갈 수 있도록 보장하는 원칙은 기술 변화와 무관하고 무관해야 한다. 그런 원칙을 새로운 기술 환경에 맞춰 기민하게 대응·활용하고 잠재적 부작용을 막아줄 제도적 장치 마련이 필요하다. 글로벌 빅테크 기업에 대한 글로벌 차원의 협력과 소셜미디어에 대한 정부의 대응 변화가 필요하다. 특히 소셜미디어의 감시자본주의 속성을 고려하면 자율규제는 실효성이 적으므로 적극적·중도적·교육과 캠페인을 결합된 온건한 규제 등을 유연하게 적용할 필요가 있다. (전문가 C)

3. 인터뷰 결과(교육 분야)

1) 중학교 정보 교과에 대한 의견

전문가들은 중학교 '정보' 교과 구성이나 교육시간 문제뿐만 아니라 정보교과가 기술에 대한 이해에 초점을 맞추고 있어, 개인정보 교육도 미디어 이용 맥락과 사회문화적 접근이 생략된 채 개인차원의 ICT 중심 접근으로 이뤄지고 있다고 지적했다.

ICT 교육을 메인에 두고 개인정보 보호 관련 성취기준을 구색맞추기로 넣은 것이 아닌가 싶다. 짧은 지면으로 인해 다룰 수 있는 내용에 한계가 있을 수밖에 없다. 기능을 중점적으로 공부하다가 끼어넣기식으로 교육하는 것은 중요성이 떨어질 것이다. (전문가 K)

개인정보교육이 기술적 맥락에서만 구성된 점은 아쉽다. 개인정보는 미디어 이용과 연결되어 있으며 정보유출이나 관리도 온라인평판과 정체성, 디지털 발자국, 의사소통, 미디어 문화 향유 등 미디어의 맥락과 함께 이루진다. 현재 교육내용은 기술적(비밀번호를 자주 바꿔라, 어렵게 만들어라 등)차원에 그치고, 이런 관점은 실제 미디어에서 개인정보 보호가 다른 영역과 분리된 것처럼 보일 수 있고, 또 미디어라는 사회적 맥락에서 개인정보를 인식하는 것이 아니라 온전히 개인이 관리해야 하는 영역이라는 고정관념을 줄 수도 있다. 실제 아이들이 겪는 개인정보 유출은 매우 다양한 맥락에서 벌어지고 있다. 가령 뉴스에 보도된 '페이스북 고객 휴대전화번호 유출'처럼 기관이나 기업의 정보유출 사건은 학생들에게 크게 와닿지 않는다. 휴대전화번호 유출로 인한 직접 피해가 없을 수도 있고, 정보유출이 자신의 개인정보보호 역량과 관계없이 벌어진 것이기 때문이다. 이에 비해 지인 능욕, 보이스 피싱, 스미싱 등 SNS나 게임에서 친하게 접근하면서 개인정보를 캐내는 사례 등은 학생들이 실제 겪어봄직하고 개인정보유출의 다양한 맥락을 이해할 수 있어 개인정보 보호역량 강화에도 도움이 될 것 같다. (전문가 G)

개인정보 이슈를 개인정보 유출에 따른 피해의 관점에서만 접근해 개인정보의 중요성을 제대로 인식하지 못하게 하거나 개인정보 이슈에서 개인을 수동적으로 위치시키고, 자신과 관련 있는 문제로 받아들이지 못하게 만들어 오히려 교육 효과를 떨어뜨릴 수 있다는 지적도 제기됐다.

개인정보 유출에 따른 ‘피해’에만 초점을 맞춘 나머지, 개인정보를 왜 특별히 소중히 여기고 조심해야 하는가라는 ‘이유’에 대한 접근이 부족할 가능성이 커 보인다. (전문가 M)

초등의 경우 개인정보와 저작권이 하나로 카테고리화되어 성취기준이 제시되어 있다. 개인정보와 저작권 개념은 별도로 제시되어야 하고 나와 타인의 권리를 지키는 관점에서 접근할 필요가 있는데 피해사례로 인한 사후처벌과 관련된 내용이 주를 이룬다. 정보, 실과의 다른 기술적 이슈에 비해 분량도 매우 미미하다. 수업 방식이나 성취기준도 개인정보 유출로 인한 피해사례를(보이스피싱이나 금전적 피해를 중심으로) 확인하고 제시해 학생의 공감과 교육효과가 떨어질 것으로 생각된다. 자신의 정보를 선별적으로 게시, 공유하는 것에 거리낌없는 학생들에게는 사례 맞춤형 교육이 적합한데, 그에 대한 논의가 없고 전문성과 시의성이 부족하다. (전문가 O)

전문가들은 피해 담론과 함께 개인정보 교육의 한축을 형성하는 윤리담론의 문제점을 지적했다. 윤리논의는 개인정보를 둘러싼 다양한 논의를 막은 채 무조건 지켜야 할 것이라고 상황을 단순하게 인식하게 만들고, 이어지는 피해 담론은 윤리를 지키지 못한 결과로 개인정보 피해를 인식하게 만들기 때문이다. 이러한 접근은 개인정보 이슈를 윤리와 역량으로 환원시켜 개인의 책임으로 돌릴 가능성이 크다. 전문가들은 디지털윤리가 아닌 디지털시민성 차원에서 권리의 개념으로 개인정보에 접근하는 것이 필요하다고 강조했다. 개인을 정보주체로 설정해 개인정보 이슈를 프라이버시 권리 관점에서 접근할 필요가 있다고 봤다.

지켜야 할 개인정보나 저작권에 머물지 말고 지키고 누려야 할 개인정보와 저작권이라는 개념, 즉 책임과 권리의 균형 측면에서 접근이 필요하다. 디지털윤리 보다는 디지털시민성 개념으로 접근하는 것이 미디어리터러시 교육 관점에서 더 바람직해 보인다. 미디어로 자기를 표현하고 사회적 관계를 맺고 소통하는 과정에서 발생하는 이슈를 파악하는 과정에서 개인정보나 프라이버시를 다루고 학생들이 이를 해결하기 위한 대응법을 모색하고 실천하는 태도를 기르도록 구성하는 게 필요하다. (전문가 K)

정부는 ‘정보 윤리’라는 용어를 많이 사용해왔다. 그런데 정보사회에서 무엇이 올바른지는 유동적이고 논쟁적이다. 주민등록번호, 저작권, 개인정보 등 현재 제도도 논란이 됐고 변화해왔다. 주민등록번호의 보편적 사용은 윤리적인가?

정보사회에서 정보공유가 아닌 저작권, 즉 지식과 문화에 대한 배타적 권리 부여가 올바른 것인가? 감시업의 사용은 윤리적인가? 특정한 윤리를 일방적으로 설명하기보다는 기술과 사회의 변화 과정에서 다양한 쟁점과 논리를 접하면서 자신의 의견을 형성하도록 할 필요가 있다. (전문가 B)

중학교 정보교과 개인정보 교육에서 개인정보를 인권으로 이해하는 접근이 부족하고 새로운 기술의 습득을 중심으로 이루어지고 있다. 물론 새로운 기술의 습득과 이해는 디지털시대에 필요하나 인권중심적 사고가 필요하다. 가령 인공지능 등 기술에 의한 차별효과 등이 설명될 할 필요가 있다. (전문가 A)

현재 정보교과 등의 교육은 대체로 지식중심의 개념과 단편적으로 개인정보 보호를 위한 근거 등을 파악하는 형태로만 구성되어있다. 개인정보유출 피해사례 조사와 실천방안 수립 정도가 아니라, 근본적으로 '개인의 정보주체권'에 대한 논의가 포함되어야하고, 빅데이터 환경 등에 대한 논의로 확대될 필요가 있다. 미디어교육의 경우 대상자의 일상과 경험에 기반해야 하는데, 교육내용에 반영되었는지 검토가 필요하다. (전문가 N)

전문가들은 기술중심적 접근이 아니라 사회문화적 맥락이 고려된 미디어리터러시 관점의 교육이 이뤄져야 하고, 좁은 의미의 '개인정보'보다 '프라이버시'로 확장해 교육하는 것이 중요하다는 의견을 제시했다. 개인정보나 데이터를 이용하려는 기업, 국가 등 다양한 주체의 양상을 배제한 채, 개인의 영역에만 한정하는 것은 권리로서 프라이버시에 대한 이해를 반영하지 못한다는 의견도 나왔다.

교육내용 적정성과 관련해 실과는 기술의 가치와 영향력에 대한 부분이 없고, 중학교 정보는 수동적인 내용으로 진술했다. 개인중심으로 정보윤리가 서술되었다. 실제로 공공기관, 포털 등 개인정보와 관련된 사회적 책무성이 함께 소개되어야 한다. (전문가 J)

소프트웨어 소양 교육을 바탕으로 한 정보교육 일환의 현재 방식보다 개인정보가 얼마나 중요한 가치인지, 침해로 인한 피해사례와 침해를 방지하기 위한 조치 등에 대해 학습해 개인정보의 중요성을 인식하게 하는 것이 리터러시 소양을 갖추는데 더 효과적일 수 있다. 그리고 중고등학교 과정도 개인정보 관련 스스로 결정할 수 있는 권리에 대한 이해와 이행을 위해 필수적으로 알아야 할 법률지식, 정보주체로서 바람직한 태도 등 사회문화적인 접근이 보다 강조되어야 한다. (전문가 D)

특정 개인식별가능성을 가지는 정보를 ‘개인정보’로 설정하고 이에 대해 법적 보호를 부여하는 방식이 현행 개인정보 보호법제가 취하는 접근방식이다. 이러한 방식은 데이터 및 정보의 활용이라는 측면을 원활하게 해주지만, 보다 본질적인 사생활 보호, 즉 프라이버시 침해의 문제를 등한시하게 만드는 경향이 있다. 개인 식별성이 명확하게 포함되지 않은 정보는 자유롭게 활용해도 된다는 논리이나 데이터 분석 기술은 날로 발전하고 있기 때문에, 식별가능성이 없다고 판단되는 정보도 결합을 통해 충분히 식별가능성을 가지는 정보로 탈바꿈할 수 있다. 따라서 교육적 관점에서 ‘개인정보’보다는 ‘프라이버시’의 중요성을 교육하는 것이 중요하다. 이 부분에서 유의할 점은 아직 국내 실무계에서는 개인정보와 프라이버시를 구분하지 못하고 있다는 점이다. 그러나 교육에서 중요한 것은 인격적인 가치라는 점을 분명히 해야 한다. (전문가 E)

정보 교과와 기술중심적 입장과 관점의 부재는 저작권이나 사이버중독 같은 연관성이 떨어지는 주제를 개인정보와 묶어서 교육하는 결과로 이어진다.

초등학교 실과교육도 사이버중독, 개인정보보호, 지식재산 등 인터넷 활용에서 발생할 수 있는 다른 영역의 이슈를 다루고 있어 충분한 교육이 이뤄진다고 보기 어렵다. (전문가 P)

2) 개인정보보호위원회 교육에 대한 의견

전문가들은 개인정보보호위원회의 교육이 중학교 정보교과 등과 비교해 개인정보에 대한 개념을 구체적으로 다루고 있음에도 미디어 리터러시에 기반한 접근이 아닌 보호주의 관점이 지배적이라고 평가했다. 개인정보를 다루는 다양한 주체들에 대한 논의는 배제한 채, 지나치게 개인에게 초점이 맞춰진 부분도 지적했다.

디지털 환경이 보편화되면서 개인정보 개념이 매우 빠르고 폭넓게 바뀌고 있는데, 아직까지 인터넷 중심 시대의 개인정보 차원에서 멈춰있다. 단순하게 정보를 제공하거나 보호주의 입장에서 접근하는 강의 방식을 넘어 학생들이 변화하는 환경에서 문제를 새롭게 정의하고, 스스로 개인정보에 관심을 갖고 참여할 수 있는 시민교육적인 접근이 필요하다. (전문가 H)

보호주의 관점에서 서술하고 있다. 개인 영역에서 서술되고 있는데, 원격수업에서 사기업에 개인정보가 제공되는 것이나 학교나 구청 등 공공기관에서 다루는 개인

정보, 대학입시 과정에서 나가는 정보 등 공공영역에서 다루어지는 개인정보에 대한 인식도 필요하다. 개인정보를 스스로 공개하는 경우 유튜브 채널, 블로그 등 공개의 판단기준을 교육할 필요가 있고, 자신의 정보를 상품화하는 문제도 교육할 수 있다. 개인정보 공개 동의, 상황에 따른 공개범위 선택은 스스로 결정하기 때문에 자기결정능력에 대한 교육이 필요하다. (전문가 J)

이용자로서 개인정보에 지나치게 편향되어 있다. 최소한 중고등 과정에서는 국가의 개인정보 수집이나 근로자의 개인정보 수집에 대해 일부 다뤄줄 필요가 있지 않을까 한다. (전문가 B)

상식적 사례나 유의점 설명에 그쳐 우려된다. 정보주체로서 자신의 개인정보에 대해 가지는 권리에 대한 인식, 타인의 권리에 대한 존중 등이 보다 상세하게 설명되어야 한다. (전문가 A)

교육 내용이 피해예방이나 행동지침에 가깝다는 평가도 나왔다. 전문가들은 데이터와 프라이버시의 포괄적 맥락을 다루지 못하고 피해와 예방 패러다임에 갇혀있고, 개인 관련 정보 통제 주체로 보는 시각이 아닌 외부 위협이나 범죄에 수동적·소극적 대처하는 내용이 부각되고 있다는 점을 언급했다.

주로 개인정보 피해사례와 예방교육으로 보여진다. '개인정보 개념→범죄사례·위험한 사례(피해발생)→예방과 보호방법'의 프레임으로 설정된다. 미취학아동부터 초중고등학교가 모두 유사한 패턴이다. 개인정보가 정보사회에서 어떠한 기능과 역할을 하고, 나를 나타내주는지, 올바른 활용을 위해 어떻게 해야하는지 등 긍정적·부정적 측면을 모두 다루는 것도 필요하다. 어려서부터 개인정보 관련해 범죄, 위험, 피해 등 매우 부정적 인식만 심어줄 위험성도 있다. 또한 예방이나 대처방법 등도 다소 소극적으로 제시되고 있다. 중고등학교의 경우 개인정보 보호나 관리법에만 머물 게 아니라 개인정보 관련 법조항도 살펴보고, 문제해결을 위한 개인적 실천이나 제도도의 개선이 필요한 사항들도 탐색할 기회를 제공해 교육내용을 질적으로 심화할 필요가 있다. (전문가 L)

개인정보 개념, 보호 이유, 보호 지침으로 구성되어있어, 교육내용이 행동지침에 가깝다. 미디어교육이 요구하는 '성찰'적 측면이 부족하고, '지식'중심 교육이 이루어지고 있다. 미래지향적 논의가 필요하다. 예를 들어 개념, 필요성, 지침 가이드 정도가 아니라 정보주체, 빅데이터 환경에서 정보주권에 기반한 사례와 이에 대한 토론 등을 통한 이용자의 성찰적 자세, 그리고 사업자를 위한 가이드나 교육 등이 언급되어야한다. 현재 제시된 내용은 일방적 강의, 일회성 교육으로

구성될 것으로 파악된다. 개인정보 교육을 위한 다양한 가이드와 지침, 사례 등을 제공하는 것이 맞을 것 같다. (전문가 N)

일부 전문가들은 학생들의 경험을 고려한 사례를 제시하거나 학부모 교육 등을 강조한 점은 긍정적으로 평가했다.

최소 3차시 이상을 초중고교생에게 사례중심으로 교육하는 것은 적절해 보인다. 특히 어린이 교육과정 중 부모에 대한 개인정보 교육은 반드시 필요하다. 아이들은 크면서 부모의 미디어 이용을 보고 배운다. 사진 공유, 다른 가족에게 여행 및 위치 등 동선 공유 등의 모습을 보면서 본인 정보의 공유에 대한 거리낌이 없어진다. 개인정보보호 교육은 부모와 교사를 중심으로 실생활, 수업과 연계해 교육하는 것이 중요하다. (전문가 O)

사안을 지나치게 단순화했다는 비판을 살 수 있지만 아동·청소년 관점을 적극 고려했다는 인상이다. 특히 아동·청소년에 대한 정보 교육은 ‘놀이’의 요소와 커리큘럼을 5-15분 단위로 잘게 쪼개주는 이른바 ‘마이크로 교육’의 방법론을 적극 도입할 필요가 있다. (전문가 C)

3) 학생들의 개인정보 교육 비판에 대한 의견

전문가들은 ‘학교의 개인정보 교육이 형식적이거나 실효성이 크지 않다’는 중학생 인터뷰 결과(6장 참조)에 대해 대체로 동의하며, 그 원인을 사이버윤리 교수학습법과 같은 초기 개인정보 교육의 패러다임과 윤리적 측면에서 ‘금지’와 ‘배려’ ‘존중’ 등의 덕목을 강조하는 개인정보 보호 교육, 원론과 원칙만을 나열하는 강의식 교육의 한계로 분석했다. 원론만 가르치기 때문에 학년이 바뀌어도 같은 내용을 교육하게 되고, 이로 인해 학생들이 형식적이라고 생각한다는 것이다.

초창기 사이버윤리 교수학습방법이 학교교육에서 답습됐기 때문으로 보인다. 꼭 알아야 할 수칙들을 열거, 설명하는 교수법보다는 학생이 주체가 돼 활동중심의 다양한 교수법을 추가해야 한다. (전문가 K)

학교수업의 가장 큰 문제는 일회성, 단회기로 진행되며, 강의방식이 주를 이루기 때문에 학생들에게 의미있게 다가가기 어렵다. 또한 교사들도 개인정보에 대한 최신 정보가 없어 윤리적 측면에서 “하지마라” 방식으로 접근해 학생들이 다 아는

내용일 경우가 많다. 개인정보나 리터러시 교육은 지속적으로 이뤄져야하나 교육과정에서 다뤄야 할 부분이 너무 많고 교사의 전문지식이 떨어져 수업시간에 관련 교육을 하는 경우가 많지 않고 외부 수업에 의존하는 경우가 많아 외부강사의 질이 담보되지 않으면 교육 효과는 낮다. (전문가 H)

학생들의 미디어 경험에 대한 충분한 인식과 이해가 있어야 하는데 가르치는 사람의 미디어 리터러시 역량이 부족하다. 지금처럼 개인정보 보호를 위해 비밀번호를 바꿔야 하고 개인정보 침해로 어떤 피해가 있는지 등의 ‘금지’와 ‘배려’ ‘존중’의 덕목을 강조하는 교육으로 문제를 타개할 수 없다. (전문가 I)

개인정보 교육이 미디어와 연계되어 있지 않기 때문이다. 미디어는 학생들의 삶에 매우 중요한 영역이고, 개인정보는 미디어와 학생들의 삶이 이어지는 중요한 연결고리이다. 하지만 현재 교육과정은 이러한 맥락이 제대로 반영되어있지 않다. 정보교과는 자료와 정보, 문제 해결과 프로그래밍, 컴퓨팅 시스템 등 주로 디지털 기술과 관련된 교육내용이 주를 이루기 때문에 개인정보를 미디어와 연결해 가르치는 것이 어렵다. 미디어의 맥락이 반영되어있지 않고, 이로 인해 교육의 내용과 방법도 ‘요약정리’식으로 지도할 수밖에 없는 한계가 있다. 학생들의 실제 삶과 괴리된 내용으로 가르치게 되고 아이들 입장에는 ‘실효성이 없다’고 느껴진다. 게다가 중학교 교과와 초등 실과교과서 내용이 크게 다르지 않아 더 ‘형식적’이라고 느껴질 것이다. (전문가 G)

학생들의 일상의 경험이나 구체적인 방법을 알려주기보다는 초기 개인정보 보호 교육에서 확장되지 않은 것이 문제이다. 학생들이 사용하는 미디어가 워낙 다양해 미디어의 각기 다른 개인정보 활용·관리방법을 학교에서 모두 다루는 것은 불가능하고, 교과서 기반으로 교육할 경우 실제 교육대상의 경험에 기반한 구체성을 가진 교육이 이루어지기 어렵다. 특히 교과서는 대부분 일반적 개인정보 관리와 관련된 내용만 다룬다. 실제로 소셜미디어 서비스들이 업데이트 등을 통해 서비스를 확장해서, 교과서에서 자세히 다루기 어려운 점이 있다. (전문가 N)

전문가들은 ‘가르치려는’ 어른들의 관점과 강의식 교육이 아닌 학생들이 공감할 수 있는 일상에서 출발하는 교육이 필요하다고 강조했다.

학생의 관점보다는 ‘가르치려는’ 어른의 관점으로 접근하는 외부강사들의 방식이 개선되어야한다. 교육 효과를 높이기 위해 학생들을 이해하고 접근하는 방식이 필요하다. 틱톡이나 제페토 같은 현실 사례를 들어가며, 아이들이 모르는 부분을 언급해주는 것이 필요한데, 기존 교육방식은 단시간에 개인정보를 소개하고, 보호 방법을 나열해서 전달하는 방식이다 보니 효과가 떨어진다. 비번 변경하고, PC방

에서 로그아웃하고, 부모님 개인정보로 이벤트 참여하지 말라는 것은 과거부터 들어왔던 이야기라 학생들 입장에서는 뻔한 내용으로 들릴 수 있다. (전문가 O)

4) 프라이버시와 개인정보 교육 방향

프라이버시 등 디지털 환경에서 아동·청소년의 권리 보장을 위해 필요한 교육 내용과 관련해 전문가들은 법적 권리로 좁게 접근하기보다 인권으로서 프라이버시에 대한 근본적 인식을 바탕으로 프라이버시와 개인정보에 대해 교육할 필요가 있다고 제안했다. 동시에 미디어 기술이 개인, 인간에게 영향을 미치는 과정에 대해 교육할 필요하다고 봤다.

국제인권법 등 인권으로서 프라이버시권의 이해와 중요성, 타인의 인권으로서 프라이버시권, 아동이 자신의 개인정보에 대해 행사할 수 있는 권리, 권리 구제 방법, 디지털 전환이 가져 올 수 있는 인권 제약과 차별의 문제, 데이터 수집이 초래할 수 있는 문제, 기술과 인권의 문제, 특히 인공지능 기술 등에 대해 교육해야 한다. (전문가 A)

프라이버시 뿐만 아니라 전반적인 인권교육과 연계될 필요가 있다. 특히 인공지능 등 신기술은 프라이버시권에만 영향을 미치는 것은 아니기 때문이다. 때로 프라이버시 등의 권리도 다른 인권과 충돌하는 것처럼 보이거나 상호 영향을 미치는 경우도 있다. (전문가 B)

디지털 시민으로서 사회에 적극적으로 참여할 수 있도록 개인정보와 저작권을 다루어야 할 것이다. 미디어 이용 과정의 하나로 책임과 권리의 균형 관점에서 비판적으로 인식하고 대응할 수 있는 방법을 교육하는 것이 중요하다. (전문가 K)

전문가들은 개인정보 이슈를 유출과 피해의 프레임 혹은 무조건적 보호가 아니라 프라이버시 권리로 확장할 필요가 있고, 아동·청소년의 실제 미디어 이용 상황과 연계해 권리를 어떻게 발현시킬지 교육하는 게 필요하다고 말했다. 정보 공개에 따른 평판 형성과 평판에 의한 의사결정, 서비스 이용 편의를 위한 데이터 공개와 기업의 데이터 축적·활용을 둘러싼 양상 등 정보 공개·제공이 불러일으킬 수 다양한 이슈를 제시하고, 그에 대해 판단할 수 있는 교육이 필요하다는 의견도 제시했다.

프라이버시 교육에서 중요한 점은 현재 자신이 남긴 여러 ‘디지털 발자국’이 향후 자신에 대한 의사결정(신용도 및 평가)에 영향을 미친다는 점을 교육하는 것이다. 이런 교육을 통해 아동·청소년의 자기정보결정권이 의미있게 발현될 수 있을 것이다. 그렇지 않으면, 단순히 자신의 정보를 제공하고 반대급부로 얻게 되는 이용상의 편의성만을 중시할 가능성이 높다. 즉 저작권 보호와 마찬가지로 법적 권리만 침해하거나 침해받지 않으면 그만이라는 논리는 결국 돌이킬 수 없는 프라이버시 침해로 연결될 수밖에 없다. (전문가 E)

미디어리터러시 교육관점에서 교육 대상의 미디어 사용에 대한 기본적 이해가 필요하다. 자신의 정보를 SNS에 게시해 평판을 쌓는 학생들에게 개인정보는 어떤 의미인지, 어디까지 누구에게 공유할지, 개인정보가 원치 않는 곳으로 도달할 가능성과 그 경우 나와 지인들에게 끼칠 피해가 어느 정도인지 토론해보고, 예방법을 논의하는 교육이 필요하다. 자신의 정보 뿐 아니라 친구나 가족의 정보를 무의식중에 공개하는 것에 대한 경각심도 교육과정에 포함되었으면 한다. 틱톡이나 제페토와 같은 현실 사례를 들어가며, 아이들이 모르고 있던 부분을 언급해주는 것이 필요하다. 개인정보 보호교육을 포함한 디지털시민교육에서 효과성을 높이려면 ‘시의성 있는 사례와 실 적용 가능한 보호방법, 해결책’을 제시해야 한다. 단순히 자신의 개인정보를 전화번호, 주민번호 등으로 한정해 사기, 스미싱 등에 범법행위에 사용되는 것을 강조하기 보다는 사진, 동선 공개 등이 어떠한 영향력을 갖고 있고, 부정적 방향으로 나에게 어떻게 돌아올지에 대한 내용이 추가될 필요가 있다. 메타버스 등과 같이 본인을 새롭게 나타내는 과정에서 본인을 어느 정도 노출할지, 타인의 개인정보를 어떻게 보호해야 하는지 심도있는 접근이 중고생에게는 필요해 보인다. 단순히 ‘개인정보보호’의 분절된 접근보다는 미디어와 함께 살아가야 하는 청소년들에게 개인정보, 평판, 디지털의 영속성 등을 종합적으로 접근하는 것이 효율적인 교육이 될 것이다. (전문가 O)

전문가들은 교육 대상에 대한 이해가 필요하다고 보았다. 학생들이 사용하는 플랫폼의 구조, 이용 양상 등 아동·청소년의 미디어 경험에 대한 이해를 플랫폼에 대한 지식 등을 바탕으로 자신의 문제로 받아들이게 하는 교육이 필요하고, 실제적으로 경험할 수 있는 사례를 제시하는 것이 필요하다고 언급했다.

학생들의 미디어 경험에 대한 충분한 인식과 이해가 있어야 한다. 학생들이 사용하는 플랫폼 접근역량도 필요하고 플랫폼의 구조, 특성, 성격, 사용 실태 등에 대한 구체적인 이해가 있어야 한다. 플랫폼의 특성을 아우르는 개인정보 문제에 대한 본질적인 이해를 추구할 수 있는 심층적 접근이 요구된다. (전문가 I)

학생 맞춤형 강의안의 개발이 필요하다. 개인정보 침해 사례로 소개되는 온라인 쇼핑몰이나 금융기관의 개인정보 유출은 학생들에게 와닿지 않는다. 학생들이 주로 접하는 환경 등을 파악하고, 학생들이 공감할 수 있는 실재나 가상 맞춤형 사례 개발이 중요하다. 또한 동일 매체라도 시기별로 개인정보 이슈는 달라지고 있다. 과거 무분별한 친구맺기, 페이스북 등의 개인정보 유출(단순정보)로 인한 사이버불링 등이 주요 이슈였다면 최근에는 사진을 합성해 소위 ‘능욕짤’ 만들고 개인정보를 동시에 유출하는 사례’ 등 보다 악질적 형태로 발전하고 있다. n번방 사건도 결국 개인정보를 자의, 타의로 유출한 학생들이 피해자가 되는 경우들이 많았다. 해당 시기에 학생들이 공감할 만한 사례를 수집하고 이를 교육 내용으로 적절히 바꿔 전달하는 방법이 필요하다. (전문가 P)

수업 방법과 관련해 학생들의 미디어 이용 경험을 바탕으로 두고, 일방적 강의보다는 실습이나 체험 교육을 제안했다. 개인정보 사례의 공감을 위해, 자신의 일로 인식할 수 있도록 학생들이 경험하는 다양한 사례에 대한 수집이 필요하고, 해결할 수 없는 문제로 인식하지 않도록 구체적인 실천 방법이나 효능감을 불러일으키는 교육을 주문했다.

현재 내가 하고 있거나 과거 했던 행동을 살펴보고 성찰할 기회를 제공할 필요가 있다. 문제 상황을 제시하고 해결할 수 있는 교육, 새로운 미디어 환경에서 일어날 수 있는 내용을 포함해야 한다. (전문가 J)

학생들이 실제 알고 할 수 있도록 경험을 제공하는 것이 필요하다. 컴퓨터실에서 해당 사이트에 들어가서 직접 해보고, 안 되는 부분은 친구들에게 묻고, 교사나 전문가의 조언을 얻어 성공적으로 경험해보는 것이 중요하다. 개념 설명이나 사례 제시 같이 강의식이 아니라 실습, 실천 과정에서 배우는 것이 효과적이다. 아이들 몇 명이 실제 프로젝트를 해보고, 나눠보는 것이 좋을 거라 판단된다. (전문가 L)

꼭 알아야 할 수칙들을 설명하는 교수법보다는 학생들이 주체가 되어 자료들을 활용해 자신의 것으로 만들 수 있는 활동중심의 교수법이 추가해야 할 것이다. 현재 학생들이 많이 사용하는 SNS를 기반으로 워드 클라우드 만들기, 생선가시 만들기, 개인정보 트레일러 만들기 등등 학생들이 주체적으로 재구성할 수 있는 교수법이 필요하다. (전문가 K)

개인정보보호를 ‘위험 사례-처방 안내’의 방식보다 ‘관리’의 관점에서 실제 비밀번호를 바꿔보거나 SNS 게시물의 공개범위를 수정하거나 개인정보 유출이 의심되는 SNS친구와 친구 끊기, 의심되는 앱 삭제나 사이트 탈퇴하기 등 실습이나

체험을 하고 이에 대한 결과나 생각을 공유하는 식으로 학습하면 좋겠다. (전문가 G)

개인정보에 대한 인식은 분명 높아졌지만 개인정보 제공에 따르는 편리함이나 보상에 쉽게 넘어가고, 귀찮은 절차나 부당한 개인정보 요구의 관행을 개선하기 위해 개인이 할 수 있는 구체적 노력에 대해 알지 못하는 문제가 있다. 읽기 어려운 형식으로 제공하는 약관에 대해 저항하거나 항의하는 방법을 알려 주고, 그러한 노력들을 결집해 의미있는 사회운동으로 만들어나가는 역량을 강조하면 좋겠다. (전문가 M)

다양한 디지털 서비스 이용에 필요한 '동의의 방식과 절차'에 대해 구체적인 교육을 진행할 필요가 있다. 필수와 선택 동의구분, 동의철회 방법, 열람·정정·삭제·처리정지권 등 기존의 정보주체 권리를 행사하는 방법과 현재 입법 논의중인 프로파일링거부권이나 전송요구권 등에 대한 지식 전달과 지능화 시대의 정보주체로서의 올바른 참여 인식 제고 등과 관련해 교육이 필요하다. (전문가 D)

자신의 개인정보가 노출되었거나 원치않은 타인에 의해 제공되었을 때 어떻게 해야하는지 118 신고를 넘어서 체감할 수 있는 방안 제시도 필요하다. (전문가 O)

5) 법제도 이외 개선방향

전문가들은 아동·청소년이 프라이버시 권리를 누리기 위해서 법제도 개선 이외 교육, 학부모 교사 인식개선 및 교육 등 다양한 방안을 제안했다. 교육당국, 교사, 학부모가 아동·청소년의 프라이버시 등 아동·청소년의 권리를 존중하는 자세가 필요하다고 제언했다.

기본적으로 현행 개인정보 보호법제의 원칙은 개인 식별이 가능한 정보(개인정보)에 대해 법적 보호를 부여하는 방식이어서 교육현장과 학부모들은 형식적으로 개인정보 침해 여부만을 따지는 경향이 있다. 이렇게 될 경우 개인정보에 대한 법적 보호는 가능할지 몰라도 보다 인격적이고 본질적인 프라이버시(사생활 보호)의 보호는 등한시될 수 있다. 단순히 개인정보 보호가 아니라 프라이버시 보호의 중요성을 각인할 필요가 있다. (전문가 E)

정보인권 교육이 적극적으로 이뤄질 필요가 있다. 유엔 아동권리위원회 일반논평 등 국제인권법 분야에서 발간되는 문헌을 토대로 교육 프로그램이 개발될 필요가 있다. 특히 디지털네이티브가 아닌 세대들을 위해 디지털시대에서 개인정보의 중요성에 관한 인식개선 프로그램이 필요하다. 디지털 환경에서 권리를 향유하기 위한 사회보장제도, 기기 지원제도 등을 마련하고, 아동이 직접 참여할 수 있는

제도 수립이 필요하다. 아동의 개인정보가 특별히 보호되어야 하는 점, 아동의 개인정보자기결정권에 대한 존중, 아동의 사생활에 관한 내용 등에 대한 학부모, 교사 교육이 필요하다. 특히 아동의 프라이버시권과 관련해 보호적 시각 아닌 권리중심 시각에서의 접근이 필요하고, 적극적 교육과 인식개선이 필요하다. (전문가 A)

인권 영역에서 접근할 필요가 있다. 자신의 프라이버시가 중요한 만큼 타인의 프라이버시도 존중되고 보호되어야 한다는 권리의식을 갖게 하는 것이 중요하다. (전문가 L)

우리 사회는 청소년을 ‘권리와 삶의 주체’가 아니라 ‘보호 대상’으로 보는 시각이 강하다. 감시업이 인기를 끄는 이유 중 하나는 이를 요구하는 부모가 많기 때문이다. 아동·청소년에 대한 보호는 필요하지만, 그것이 부모와 사회의 아동에 대한 통제 욕망이 되지 않도록 주의할 필요가 있다. 이를 위해 가정, 학교, 국가·사회 모든 차원에서 아동·청소년의 목소리가 반영될 수 있는 구조가 마련될 필요가 있다. (전문가 B)

교사 등 관련 전문가들은 현재 교육 방식에 대해 적극적인 문제를 제기했다. 미디어에 대한 인식의 변화와 학습을 방해하는 미디어 과의존, 개인정보 유출과 같은 부정적 측면의 강조가 아닌 실제 삶과의 연관성 속에서 교육이 필요하다고 보았다.

이제 우리의 삶은 온라인과 오프라인을 구분해 존재할 수 없다. 디지털 환경의 권리도 실제 권리와 똑같이 중요하게 인식돼야 한다. 하지만 학생과 학부모는 물론 대다수 교사나 교육행정가는 미디어나 디지털 기술을 단순히 수단으로만 여기고, 그러다보니 관련 교육은 ‘활용’, ‘제작’에 초점을 두는 경우가 많다. 디지털 환경의 프라이버시도 실제 프라이버시와 연결해 논의돼야 하고, 이를 위해 미디어의 사회적 맥락과 학생의 실제 삶을 충분히 반영하는 것이 필요한데 현재는 정보나 실과 등 특정 교과나 특정 단원에서 제한적으로 지도되고 있다. 디지털 환경의 권리는 모든 교과와 단원에서 적극적으로 다뤄져야 한다. (전문가 G)

프라이버시나 개인정보, 미디어 리터러시 교육은 단순히 학습을 방해하는 미디어 중독, 게임 중독, 개인정보 유출과 같은 부정적 측면을 해결하기 위한 방식이 아니라 디지털 사회에서 어떻게 시민으로 살아가야 할지에 대한 학생, 학부모, 학교, 사회의 공감대와 고민 속에서 이뤄져야 한다. 사후약방문격의 접근이 아니라 학생의 삶과 연계된 교육이 이뤄져야 한다. (전문가 H)

학생들이 무엇을 공개하고 무엇을 비공개로 해야 할지에 대한 판단 능력을 기를 수 있는 교육이 필요하다. 개인정보나 프라이버시 중요성을 인식시키고 구체적으로 어떻게 관리해야 할지를 체득할 수 있는 활동중심의 프로그램이 절실하다. 개인정보를 다루는 주체들(교사, 행정실, 학급임원)에 대한 철저한 교육이 필요하다. (전문가 K)

전문가들은 교사와 부모 세대의 인식 변화를 위한 교육의 필요성을 언급했다. 한국사회가 프라이버시에 대한 인식이 미비하고, 교사와 부모세대는 집단주의적 문화에서 성장해 개인과 프라이버시에 대한 인식 자체가 약하고, 아동의 디지털 문화에 대한 이해도 부족하다. 여기에 아동을 보호와 통제 대상으로 대할 경우 프라이버시 권리를 무시할 가능성이 높다. 전문가들은 프라이버시에 대한 학교 현장의 변화도 주문했다. 교사와 학교당국이 행정편의주의에서 벗어나 학생들의 프라이버시를 존중하는 환경을 조성하는 것이 필요하다고 봤다.

비대면 교육에서 학생의 개인정보가 침해되지 않는지를 검토할 필요가 있다. 교원에게 비대면 교육방식에 대한 안내와 개인정보보호 교육을 할 필요가 있다. 현재 교육부 등에서 비대면 교육환경에 대응한 여러 정책 등을 수립·실시하고 있지만, 이에 더해 개인정보보호위원회 등과 함께 필요한 관련 교육정책을 마련할 필요가 있다. (전문가 P)

학부모 인식개선이 매우 중요하다. 학생의 학습권과 교육권이라는 이름으로 원격 수업에 동의 없이 들어오고, 학생 ID로 들어오는 것 등은 다른 학생들의 학습권과 프라이버시 침해인데 인식하지 못하고 있다. 아이들은 자신의 얼굴을 다른 사람이 지켜보고 평가할 거라고 생각하지 못하다가 어느 날 맘카페에서 ‘어느 반 누가 수업 중에 안색이 안 좋더라’는 이야기를 듣고 충격을 받을 수 있다. 개인정보와 프라이버시는 인권영역이라 스펙트럼이 넓고 학생이 어떻게 느끼는지가 중요하다. 교사들은 행정편의를 찾을 게 아니라 수업이나 행정영역에서 학생의 프라이버시가 존중될 수 있도록 다양한 선택지를 줄 필요가 있다. (전문가 L)

법제도상 청소년의 권리가 미약하므로, 청소년 권리에 대한 교육이 반드시 필요하다. 이와 관련해 부모가 아동·청소년의 자기결정권을 인정해줄 수 있도록 인식 교육이 선행되어야 한다. 교사나 교육행정에서도 아동·청소년들의 프라이버시를 보호하기 위한 교육과 가이드가 강력하게 제시될 필요가 있다. (전문가 N)

지금 아동·청소년의 부모세대는 SNS 뿐만 아니라 미디어 사용에 익숙하다. 이러한

미디어 이용 습관은 아이들에게도 전달되고, 정보공유(개인정보 노출)에 익숙해 지기도 한다. 학부모들은 자신이 공개한 다양한 정보들이 아이들의 평판이 될 수 있고 범죄에 노출될 수 있다는 것을 정식으로 배운 경험이 없을 것이다. 초등학교 학부모를 대상으로 꾸준히 건강한 인터넷 이용습관을 가질 수 있도록 교육해야하며, 부모가 실천하는 모습을 보여야할 것이다. 더불어 학교에서 교사가 학생들을 대할 때 개인정보보호를 실생활에서 느끼고 전달될 수 있도록 체험형 교육과정이 필요하다. (전문가 O)

4. 소결

전문가들은 미디어 이용, 학교, 가정 등 영역에서 아동·청소년의 프라이버시나 개인정보를 위협하고 있다고 우려했다. 미디어 이용과 관련해 미디어 기업의 과도한 정보 수집과 개인정보 및 프라이버시 침해 행위 파악의 어려움 등을 언급했다. 아동·청소년 보호 차원에서 개인정보 활용과 관련 금지해야 할 부분이 공백인 점과 개인정보에 대한 형식화된 절차인 점 등 국내 법제도의 허술함과 환경의 미비를 언급했다. 전문가들은 국내 개인정보 관련법과 제도가 아동·청소년을 권리주체가 아닌 일방적 보호대상으로 보는 동시에 아동·청소년의 프라이버시나 개인정보에 대해 관심을 기울이지 않는다고 말했다.

학교 공간과 관련, 디지털화와 무관하게 학생인권과 프라이버시에 둔감한 교육 행정과 학교환경이 코로나19 이후 개인정보와 프라이버시 침해가 쉽게 발행할 수 있는 온라인 수업 환경과 결합하면서 아동·청소년의 프라이버시가 광범위한 형태로 위협받고 있다고 진단했다.

프라이버시 침해 주체는 교사, 미디어와 에듀테크 기업, 동료 학생과 학부모 까지 다양했다. 온라인 학습시스템 기반 수업으로 학습데이터 등 다양한 학생 데이터가 사기업으로 대규모 유입되고 관리·감독되지 않은 상황과 근본적으로 학생인권이나 프라이버시, 교육 전반에 미칠 영향에 대한 검토없이 기술을 도입·활용하는 상황을 지적했다. 또한 온라인수업에서 얼굴을 노출해야하는 상황 자체가 프라이버시 침해이고, 학생 평가목적으로 학생 수업집중도 등 데이터를 활용하는 가능성도 문제를 제기했다. 전문가들은 가정에서 청소년 스마트폰에

설치하는 감시앱이 아동·청소년의 프라이버시와 사생활 비밀과 자유 등을 침해하고 있다고 지적했다.

전문가들은 중등 정보교과와 개인정보보호위원회 등 기존 개인정보 교육이 디지털(미디어) 환경에 대한 비판적 이해 등의 미디어 리터러시 교육과 무관하다고 진단했다. 기업, 국가 등에 대한 논의를 배제한 채, 피해와 예방 중심의 보호주의 관점에서 개인정보 문제를 개인의 책임과 윤리의 문제로 다루고 있다고 지적했다. 전문가들은 ‘금지’, ‘존중’ 등 윤리 덕목을 강조하는 과거의 사이버윤리 교육 프레임과 원칙만 나열하는 강의식 교육으로 인해 개인정보의 중요성을 제대로 인식하지 못하게 한다고 진단했다. 전문가들은 기술중심주의에서 벗어나 사회문화적 맥락을 전제로 한 교육과 함께 법적 의미의 ‘개인정보’가 아닌 디지털 시민성 차원에서 ‘프라이버시 권리’로 확장해 교육하는 것이 중요하다는 의견을 제시했다.

전문가들은 법제도 개선과 관련해, 디지털 환경에서 아동·청소년의 권리를 확보하기 위해 개인정보 관련법 개정뿐만 아니라 학생인권조례 의무화 등 학생권리 관점으로 확장해 아동·청소년의 프라이버시 권리를 구체적으로 보장할 필요가 있다고 말했다. 개인정보에 대한 프로파일링 등 자동화의사결정 금지, 동의 없는 가명처리와 아동의 개인정보의 영리목적 활용금지 등과 같은 아동·청소년에 특화된 특별조항 개설과 다크패턴 규제, 정보삭제권, 개인정보 처리과정 전반의 아동친화적 절차 도입 등을 제안했다. 전문가들은 아동·청소년 교육과 법제도 개선 외에, 개인과 프라이버시에 대한 인식과 아동의 디지털 문화에 대한 이해 부족을 언급하며 교사와 부모 세대의 인식 변화와 교육의 필요성을 언급했다.

전문가들은 개인정보와 프라이버시 교육 방안에 대해 법적 권리로 좁게 접근하기보다 인권으로서 프라이버시에 대한 인식을 바탕으로 프라이버시를 교육할 필요가 있다고 제안했다. 전문가들은 권리와 책임의 균형감을 익히고, 정보공개에 따른 평판형성, 서비스 이용 편의를 위한 데이터 제공과 기업의 데이터 축적·활용 등 개인 정보공개·공유에 따른 다양한 상황에 대한 판단을 돕는 교육이 필요하다는 의견을 제시했고, 아동·청소년의 미디어 경험을 바탕으로

프라이버시 등을 자신의 문제로 받아들여지게 하고, 정보를 통제할 수 있는 구체적 실천방안을 제공하는 교육을 주문했다.

제8장

결론

제 8 장

결 론

제1절 • 아동·청소년 프라이버시 교육방안

1. 교육의 필요성

앞서 논의한 것처럼 데이터 시대 프라이버시는 중요한 개념이다. 일상의 대화부터, 학습, 보건, 이동, 소비, 금융 등 생활 모든 영역에서 데이터와 정보가 생성되고, 거의 모든 정보의 저장·수집·분석이 가능해졌다. 무엇보다 개인의 데이터가 본인 인식하지 못하는 새, 저장·수집·추적·이용되고, 동시에 스마트 토이, 베이비캠 등 다양한 형태의 디지털 기기들이 일상에 자연스럽게 스며들면서, 디지털 기술과 프라이버시 관련해 전에 비해 더 낮은 기준을 적용하는 경향이 나타나고 있다(Richardson & Milovidov, 2019). 이러한 상황에서 디지털 정보 환경을 정확히 인식하는 미디어 리터러시와 자신의 정보를 통제할 권리로서 프라이버시를 이해하고 실천하는 것은 더욱 중요해지고 있다.

프라이버시는 민주주의 사회의 기본적 권리이자 자유로운 의사표현과 참여, 비판적 의식의 근간이 되는 미디어 리터러시가 발현되기 위한 전제이다. 그럼에도 미디어 리터러시 교육에서 프라이버시는 주변적 이슈로 다뤄졌고, 이 때문에 유네스코는 프라이버시는 디지털 시대 개인에게 직접적이고 부정적인 영향을 미칠 수 있으므로 프라이버시 교육은 미디어 리터러시 교육에서 가장 중요하다고 강조했다. 미디어 리터러시 역량을 교육할 때 정보, 미디어와 기술의 이용과 정보 접속, 표현의 자유, 정보에 대한 권리, 인권, 경제와 상업적 맥락같은 민주적이고 사회경제적 이슈의 연관성을 고려해, 프라이버시 권리를 교육하는 것은 프라이버시와 미디어 리터러시 교육에서 매우 중요하다(Culver & Grizzle, 2017). 특히

빅데이터 시대에 이름, 주소 같은 형태가 정해진 식별가능한 정보가 아닌 쿠키(cookie)처럼 과거에는 의미없던 데이터들이 상업적으로 활용될 뿐만 아니라 상품구매, 투표, 이슈에 대한 입장 등 특정한 경제·정치·사회적 판단을 유도할 수 있고, 더 나아가 데이터를 기반으로 개인에 대한 판단이 이뤄진다는 점에서 교육의 중요성은 더욱 크다. 디지털 환경에서 나고 자란 아동·청소년의 경우 출생 전부터 정보가 남고, 성장과정에서 개인의 정보가 지속적으로 변하는 점을 감안할 때, 아동·청소년을 정보의 주체이자 특수한 보호 대상으로 바라보고 개인정보 관련 제도를 개선하는 것뿐만 아니라 프라이버시를 교육하는 것은 매우 필요하다.

이런 맥락에서 유럽평의회(Council of Europe)는 프라이버시 교육을 디지털 시민성(digital citizenship) 교육의 한 영역으로 다루고 있다. 유럽평의회는 프라이버시를 포함한 디지털 시민성을 인간의 존엄성과 인권에 귀 기울이고, 관찰하고, 존중하는 것과 같은 핵심 역량을 바탕으로 문화적 다양성을 중시하고 언어와 의사소통에 대한 비판적 이해를 발전시키는 방법을 배우는 과정으로 이해했다. 유럽평의회는 디지털 기술이 본질적으로 파괴적인데다가 끊임없이 진화하므로, 프라이버시 등 디지털 시민성 역량(competence)을 아주 어린 시절부터 가정과 학교, 공식·비공식 교육 환경 모두에서 시작해 평생을 배워야 하는 과정으로 강조하고 있다(Richardson & Milovidov, 2019).

2. 교육 목표

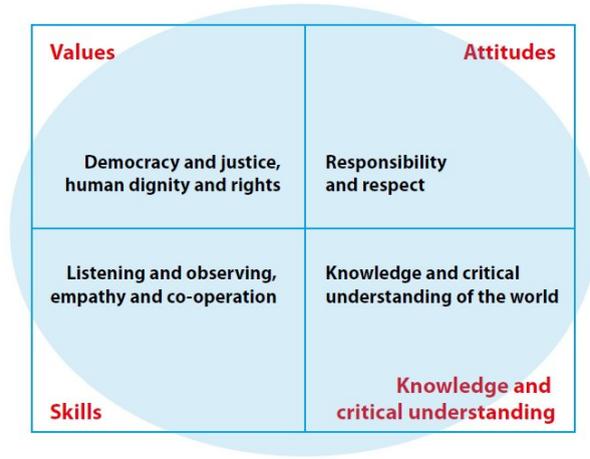
유네스코는 자기 권능을 부여하고(empowerment), 자기결정권의 효과를 강조하는 입장에서 프라이버시 권리를 접근한다. 온라인 환경에서 단순한 보호를 넘어서 아동·청소년의 창의성, 표현욕구, 활동성을 축소시키지 않으면서 아동·청소년이 역량을 기르고 권능을 갖는 것을 목표로 한다. 프라이버시 역량은 일반적인 미디어 사용능력 뿐만 아니라 디지털 시민권과 매우 밀접하게 연관이 있다(Culver & Grizzle, 2017). 유럽평의회는 디지털 환경에서 살아가는 젊은 세대를 위해 10개 영역의 디지털 시민성 개념을 통해 프라이버시 교육의 목표를

제시했다. 유럽평의회는 ‘민주적 문화를 위한 역량’으로서 가치, 태도, 기술, 지식, 비판적 이해 4개 영역의 20개 역량을 분류하고, △온라인에서 존재하기 △온라인에서 잘 지내기(well-being) △온라인 권리로 구성된 10개 영역의 디지털 시민성을 제안했다. 10개 영역은 민주주의, 인권, 법치의 원칙을 뒷받침한다(Richardson & Milovidov, 2019). 유럽평의회는 디지털 시민의 이상향을 폭넓은 역량 개발을 통해 지역, 국가, 글로벌 차원의 온오프라인 커뮤니티에 적극적, 긍정적, 책임 있게 참여할 수 있는 사람으로 봤고, 창조, 소비, 공유, 놀이, 사회화부터 연구, 의사소통, 학습과 일 등의 다양한 활동이 디지털 시민성과 참여에 포함되고, 디지털 시민은 인권과 문화 간 차이를 존중하면서 학습, 일, 고용가능성, 여가, 통합과 사회 참여와 관련된 새롭고 일상적인 과제에 대응할 수 있다고 봤다.

〈표 8-1〉 유럽평의회 of 디지털 시민성 영역

온라인에서 존재하기	온라인에서 잘 지내기	온라인 권리
접속과 포용 학습과 창의성 미디어와 정보 리터러시	윤리와 공감 건강과 웰빙 온라인에서 자신을 드러내기와 커뮤니케이션	적극적 참여 권리와 책임 프라이버시와 보안 소비자 의식

이러한 측면을 고려할 때, 프라이버시 교육의 목표는 민주주의 사회에서 인권으로서 프라이버시의 의미와 가치를 이해하고, 정보를 통제할 수 있는 주체로서 개인을 인식하고, 미디어 정보 환경에 대한 비판적 이해와 판단을 바탕으로 자신의 정보를 통제할 수 있고, 타인의 프라이버시를 존중하고, 개인적·사회적 차원에서 프라이버시 권리를 실천할 수 있는 방안을 포함한다.



[그림 8-1] 유럽평의회 프라이버시와 보안의 핵심역량 (Richardson & Milovidov, 2019, 그림.17 참고)

3. 교육 방향

유네스코는 미디어 리터러시 교육 환경에서 온라인 프라이버시 이슈는 개인 프라이버시 필요성과 가치 이해, 디지털 기술을 사용할 때 프라이버시 함의 이해, 프라이버시와 투명성의 균형 설명하기, 표현의 자유, 정보에 대한 접근을 포함한다고 봤다. 개인의 프라이버시를 가장 잘 보호하거나 개인정보 접근을 허용하는 방법을 결정하는데 도움이 되는 미디어 리터러시는 개인정보나 다른 데이터의 공유와 함께 개인정보 문제가 발생했을 때 정보를 바탕으로 결정하는 것을 의미한다. 특정 정보가 개인으로 식별될 수 있는 상황을 이해하는 능력은 비자발적으로 수집된 메타데이터를 어떻게 처리할지 등을 포함해 매우 복잡한 판단을 필요로 한다(Culver & Grizzle, 2017).

앞서 논의한 것처럼 프라이버시 교육은 미디어리터러시 교육으로서 권리에 대해 인식하고, 이를 실천할 수 있는 역량을 지원할 수 있는 교육이어야 한다. 현행 개인정보 교육체계는 '개인정보 개념 → 범죄·피해 사례 → 예방과 보호'의 프레임이 주를 이루는데, 근본적으로 개인정보에 대한 포괄적인 접근이 필요

하다. 아동·청소년 인터뷰에서 대체로 법적 의미에 근거해 식별가능한 정보로 ‘개인정보’(주로 당사자가 입력한 정보)로 한정해 개인정보와 프라이버시를 인식하는 경향을 보였다. 교육, 여가, 놀이, 소비 등 일상생활에서 발생하는 개인의 정보와 프라이버시 침해에 대해 인식하지 못하는 경우가 많았다. 전문가들의 제안처럼 개인정보와 프라이버시 이슈를 개인정보보호법상의 침해와 법적 권리로 접근하는 방식은 사생활 보호와 정보를 통제할 수 있는 권리로서 프라이버시 침해라는 본질적 문제를 등한시하게 만든다는 점에서 한계가 있다. 데이터 분석 기술이 발전하는 상황에서 식별가능성이 없다고 판단되는 정보도 결합을 통해 충분히 식별가능성을 가지는 정보가 되기 때문이다¹⁸⁶⁾.

따라서 교육적 관점에서 디지털 정보 환경에 대한 이해를 바탕으로 프라이버시의 중요성을 교육하는 것이 필요하다. 디지털 환경에서 자신에 관한 정보를 통제할 수 있는 주체로서 개인을 인식하게 하고, 인간의 기본권으로서 프라이버시와 개인정보에 대해 교육할 필요가 있다. 유네스코도 미디어 리터러시에서 프라이버시 권리는 온라인과 오프라인의 인권과 연결해야한다고 봤다. 인터넷에 대한 접근과 차별받지 않음, 표현의 자유와 정보의 자유, 집회의 자유, 결사와 참여의 자유, 아동·청소년을 위한 특별보호 등이 포함되어야 한다는 것이다. 프라이버시를 개인정보 침해만이 아닌 인권, 표현의 자유, 인터넷 자유, 경제와 사회 개발 등과의 관련성을 이해할 경우, 프라이버시에 더 적극적이고 비판적으로 관여할 수 있다(Culver & Grizzle, 2017). 이는 개인정보의 유출과 피해를 바탕으로 ‘보호’프레임을 벗어나는 것과 연관된다. 인터뷰에서 아동·청소년들은 프라이버시와 개인정보 침해에 대한 우려와 관련해, 해킹·도난을 통한 물질적 피해나 낯선 사람의 접근에 민감하게 반응했고, 오히려 학교에서의 프라이버시 침해 상황에 둔감하거나 미디어 기업의 데이터 수집·활용 등 일상적 프라이버시

186) 유럽평의회는 아동의 프라이버시 권리와 관련해 ‘개인 데이터(Personal data)’ 개념을 사용하고 있다. 개인 데이터는 식별되거나 식별할 수 있는 개인(any information relating to an identified or identifiable individual, “데이터 주체”)과 관련된 모든 정보로, 위치데이터, IP주소, cookie ID 등을 포함한다(Livingstone, Lievens, & Carr, 2020).

침해와 위협 등은 잘 인식하지 못했다. 모르는 사람의 침해로부터 ‘보호’라는 인식은 눈에 보이는 피해가 발생하지 않거나 법적으로 문제가 없으면 프라이버시와 개인정보 침해는 문제가 없다는 생각을 낳고, 공적·사적 영역에서 일상적으로 일어나는 프라이버시 침해를 인식하지 못하게 하거나 개인이 조심하면 되는 것 수준으로 단편적으로 인식하게 할 우려가 있고, 개인정보와 프라이버시를 개인이 책임져야 하는 영역으로 생각하게 할 가능성이 높다. 동시에 자신에 관한 정보 공개·공유행위나 다른 사람이나 기관이 자신의 정보를 보유·이용하는 것의 의미에 대해 종합적으로 사고할 수 있는 관점을 기르지 못한 채 위협, 범죄, 피해 등과 같은 부정적 인식만 키울 수 있다. 이와 관련해 컬버와 그리즐(Culver & Grizzle, 2017)은 프라이버시 가치를 전파하기 위해 공포에 소구하는 방식을 사용하지만 ‘안전’ 담론 프레임에 주의해야한다고 말한다. 안전 담론보다는 개인의 프라이버시 권리와 보안에 대한 균형을 맞추기 위해 필요성(민주주의에서 개인 권리에 대한 간섭이 실제적이거나 위협 인식을 바탕으로 한 ‘긴급한 사회적 요구’에 해당하는지)와 비례성(필요한 행동이 추구하는 목적의 정당성에 비례하는지)의 문제와 함께 실제 위험을 평가할 수 있게 교육하는 것이 중요하다고 봤다.

공적, 사적 영역에서 개인의 데이터가 수집·활용·처리되는 방식에 대한 종합적 이해를 돕는 교육이 필요하다. 인터뷰에서 아동·청소년들은 데이터 수집을 단편적으로 이해하는 경향을 보였다. 광고 추천과 관련 개인 정보 수집에는 부정적이면서 콘텐츠 추천은 편리하다고 생각했다. 미디어 기업이 데이터 수집을 기반으로 콘텐츠를 추천하고 행동을 유도하는 것(광고노출과 구매 혹은 플랫폼 체류시간 증가)이 광고 추천과 같은 맥락이라는 것을 인식하지 못했다. 이러한 인식의 단절은 디지털 환경에서 미디어 기술(기업)이 개인, 인간에게 미치는 영향에 관한 인식, 더 나아가 기술(기업)에 대한 인간의 태도에 대한 인식 부재와 관련이 있다. 일부 아동·청소년은 글로벌 미디어 기업에 막연한 신뢰를 보이거나 미디어 기업의 정책을 무비판적으로 수용하는 모습을 보이고, 알고리즘, 인공지능 등을 중립적이고 완전무결한 존재로 생각하는 경향을 보였다. 이는 프라이버시 교육이

미디어 리터러시 교육으로서 기술과 미디어 기술(기업)에 대한 비판적 이해와 연결될 수밖에 없다는 것을 보여준다. 온라인에서 개인 프로필과 정보의 상품화와 수익화에 대한 인식 또한 프라이버시 역량으로 교육할 필요가 있다. 인터넷과 미디어의 ‘무료’서비스 이용에 자신의 정보를 제공하는 ‘비용’이 든다는 것, 그리고 이 ‘비용’이 절대 남용되어서 안 되며 투명한 사용자 동의가 필요하다는 점이다. 개인들이 자율적으로 정보에 근거해 소셜미디어, 전통적인 미디어나 모바일앱의 ‘무료’서비스에 대한 대가로 개인 데이터 등 개인정보를 제공하는 것 등을 결정할 수 있어야 하고, 더 나아가 개인정보가 개인의 동의하에 이윤 창출에 사용되는 경우, 공정한 소득 분배나 이익 공유를 요구하거나 협상할 수 있어야 한다(Culver & Grizzle, 2017). 이는 미디어리터러시 차원에서 인터넷 앱과 서비스의 비즈니스 모델을 인식하면서 인터넷/기술 제공자와 미디어가 프라이버시 정책에 책임을 있다는 것을 인식하는 것과도 연결된다. 인터뷰에서 아동·청소년들은 약관읽기의 의미와 구체적인 계약 내용에 대해 이해하지 못하는 경우가 많았는데, 아동·청소년이 약관을 이해하고, 기업의 제안을 어느 선에서 수용하고, 요구할지 등 일종의 협상력을 기르는 것은 프라이버시 역량의 중요한 부분이다. 콘텐츠 공유와 자기표현 등과 같은 아동·청소년의 미디어 이용 상황과 연계해 프라이버시를 어떻게 적용시킬지와 동시에 개인의 정보 공개에 따른 평판 형성과 평판에 의한 의사결정, 서비스 이용 편의를 위한 데이터 공개와 기업의 데이터 추적·활용을 둘러싼 양상 등 정보 공개·공유가 불러일으킬 수 있는 다양한 상황을 판단하게 할 수 있게 돕는 교육이 필요하다.

해외 주요국들은 단순히 아동·청소년과 관련된 개인정보 유출사례 소개와 예방법이 아닌 연령별 주요 이용 온라인 플랫폼에서 발생할 수 있는 프라이버시 위협, 개인정보 수집 방식의 악용 사례 등을 연구하고, 이에 대해 아동·청소년이 연령별로 관련 사항에 개인정보자기결정권을 행사할 수 있는 역량을 키울 수 있도록 교육하고 있다. 영국 교육부의 ‘관계 교육, 관계와 성 교육, 보건교육에 대한 법정 지도안’ 초안(2018)에는 관계, 온라인 미디어, 인터넷 안전과 해악에 대한 지식으로 온라인 데이터와 프라이버시에 대해 언급하고, 정부가 대인관계와

상업적 맥락 모두에서 개인의 정보가 온라인에서 공유, 사용되는 방법을 아이들에게 가르쳐야 한다고 제안한다. 예를 들어 데이터가 온라인에서 생성·수집·공유·사용되는 상황으로 개인 데이터가 소셜미디어에서 캡처되는 방식이나 기업의 데이터 활용에 대한 교육이 가능하다(Livingstone et al., 2019). 영국의 아동·청소년들은 ‘내가 누구인지, 혹은 내가 무엇을 하는지에 관한 모든 정보’가 개인정보에 속한다는 사실과 일상적 온라인 활동에서 정보가 수집되는 방식과 어떤 목적으로 활용/악용되는지를 배우고(ICO, 2021), 호주도 정부차원에서 2021년 아동·청소년을 대상으로 개인정보 관리와 보안 교육에 대한 수업 개정안에서 이름이나 생년월일 같은 개인정보를 공유하지 말기 같은 기초적인 것부터 온라인 서비스에 저장될지 모르는 개인정보의 종류, 이를 기반으로 하는 위치/신원 추적의 원리 등 개인정보에 대한 위협과 작동 방식 등을 필수적으로 가르친다.

프라이버시 교육은 학습자의 경험을 고려해야한다. 아동·청소년 인터뷰와 전문가 인터뷰에서 미디어 이용 상황을 전혀 반영하지 못한다는 것이 공통적으로 제기됐다. 미디어는 학생들의 삶에 매우 중요한 영역이고, 개인정보는 미디어와 학생들의 삶이 이어지는 중요한 연결고리이다. 하지만 현 교육과정에서는 개인정보보호 교육이 게임, SNS 등 청소년의 미디어 이용 경험을 전혀 반영하지 못해, 아동·청소년들은 법적 개념과 금전적 피해 등만 기억할 뿐 교육을 현실과 연결시키지 못했다. 정보주체들이 구체적 미디어 이용 상황에서 개인정보 노출의 위험성을 인식하고, 능동적·주체적으로 대응할 수 있는 방법을 교육함으로써 위험 행동을 최소화하고, 일상적으로 겪는 어려움을 해소하는 내용이 교육과정에 반영되어야 한다. 또한, 가정과 학교 등 일상의 변화와 함께 가는 교육이 필요하다. 이를 통해 아동·청소년은 자신을 정보의 주체로 인식할 수 있다.

4. 교육 방안

앞서 논의한 것처럼 프라이버시 교육은 아동·청소년이 실행할 수 있는 교육

이어야 한다. 개인정보라는 한정적 개념에서 벗어나 확장된 민주주의 사회 권리로서 프라이버시 개념과 디지털 환경에 대한 이해를 바탕으로 기술적·사회적으로 실천할 수 있는 교육이 필요하다. 이와 관련해 유네스코는 미디어 리터러시 교육 환경에서 온라인 프라이버시 문제는 개인 프라이버시 필요성과 가치 이해, 디지털 기술을 사용할 때 프라이버시 합의 이해, 프라이버시와 투명성의 균형 설명하기, 표현의 자유, 정보에 대한 접근을 포함한다. 유네스코가 제안한 미디어리터러시로서 제안한 프라이버시 역량은 다음과 같다(Culver & Grizzle, 2017, p. 17-18).

- 사이버공간에서 개인의 프라이버시 권리가 왜 필요하고 중요인지 이해하기
 - 개인정보와 프로필이 특히 온라인에서 급속히 상품화, 상업화되는 경향을 인지하기
 - 언제, 어떻게 프라이버시와 익명성을 요구할지, 언제 타인의 프라이버시와 익명성을 존중할지 이해하기
 - 온라인이나 오프라인에서 언제 개인정보를 공유할지 판단하기
 - 온라인 플랫폼을 비롯한 여러 기관들의 프라이버시 정책과 정보관리 행태를 평가하기
 - 디지털 환경의 프라이버시 위험과 혜택을 이해하고, 그에 따라 프라이버시 설정과 수준을 적절히 조정하기
 - 타인의 개인정보를 윤리적으로 사용하고 타인의 프라이버시를 존중하기
- 커먼센스의 경우 데이터 프라이버시와 디지털 흔적과 평판으로서 프라이버시를 다루며, 온라인 프라이버시 개념을 소개하고, 개인정보를 친구, 일반 대중, 온라인 플랫폼, 앱 개발기업 등 다양한 층위의 사람들과 공유할 때의 결과를 알려준다. 개인정보 공유는 사교와 개인의 성장을 도와주는 자연스러운 활동이지만 범위와 속도, 특성이 다른 온라인 환경에서는 정신적·물리적 위험을 초래할 수도 있고, 신상 도용이나 사기 등의 피해로 이어질 수도 있다는 점을 일깨우며 정보공유의 혜택과 위험을 균형잡힌 시각으로 보여주려 한다. 청소년의 민감한 개인정보를 외부 위험으로부터 어떻게 안전하게 보호할지에 초점을 맞춘다. 개인정보가 과다 노출되거나 본인 의사와 상관없이 유출될 수 있는 상황과 위험들, 이를테면 계정

등록과 설정, 소셜미디어 포스팅, 온라인 구매, 알고리즘, 얼굴·음성 인식기술, 사물인터넷 등을 설명한다. ‘인간적 기술 센터’는 기술이 주는 혜택의 관점에서 프라이버시를 설명한다. 기술이 거래라는 면을 강조하면서, 기술이 앱의 편리성이나 다른 사람과의 연결을 가능하게 하지만 그것을 통해 내 개인정보를 내주거나 한정된 자원인 주의력을 빼앗기는 것, 다른 활동의 기회를 잃는 것 등을 생각하게 한다. ‘티치프라이버시’는 프라이버시를 ‘무엇인가를 비밀로 유지하고 싶어하는 사람들의 의도를 존중하는 것’이며 ‘프라이버시는 얼마나 많은 정보를 남과 공유할지 경계선을 정하고, 다른 사람들의 경계선을 존중하는 것’으로 보고, 인지·보호·수집·공유 차원으로 프라이버시를 접근한다. 개인정보가 수집·사용되는 방식, 다양한 기술 사용에 따른 혜택과 위험 평가(인지), 신상도용, 피싱과 온라인 위협에 대한 대응, 해커·피싱·바이러스를 판별하고 막는 법(보호), 타인의 프라이버시에 대한 윤리적 존중과 정부의 감시이슈(수집), 온라인 가십과 자기노출의 부정적 결과, 사이버 불링과 온라인 학대, 섹스팅(공유) 등의 내용을 다루고 있다.

앞서 언급한 교육방안과 교육 내용 등을 참조해, 초등학교 고학년과 중등용으로 교육안을 제시하면 다음과 같다. 교육안은 연구진이 구성한 교육안을 연구자, 교사 등 미디어 리터러시 전문가 10인의 자문을 반영해 수정한 것이다. △1차시는 프라이버시의 개념과 중요성을 익히는 것을 주안점으로 한다. 나와 관련된 다양한 정보가 있다는 것을 알고, 상황과 대상(공개범위)에 따라 공개 가능한 정보의 범위의 의미를 익히는 것이 핵심이다. 개인정보와 프라이버시가 나에게 어떤 의미인지, 왜 중요한지를 알고, 개인에 관한 정보는 무조건 알려주지 말아야 할 것이 아니라 정보의 성격과 대상이나 상황(친구, 학교나 병원)에 따라 공개할 수 있다는 것을 알고 이를 판단할 수 있는 기준을 익히게 한다. △2차시는 개인정보와 프라이버시에 대한 기본적인 이해를 바탕으로 온라인과 SNS에서 프라이버시 특성과 정보 공개·공유 상황을 이해하는 방법을 다룬다. 기존 연구에 따르면 아이들은 오프라인 세계의 프라이버시에 대해서는 자연스럽게 이해하고 있지만 온라인에서는 프라이버시에 대해서는 무감각한 경우가 많다. 이를 테면

오프라인에서 문을 닫고 이야기하는 등의 감각이 있지만 온라인에서는 오프라인의 공개된 장소에서 말하지 않을 내용도 거리낌없이 이야기하는 등 오프라인의 습관이 온라인 의사결정으로 항상 이어지지 않는다는 것이다(Allen, 2018). 오프라인의 프라이버시 원칙을 온라인과 연결시키고, 온라인과 SNS 특성(특정할 수 없는 수용자, 확장성, 영속성 등)을 바탕으로 온라인에서 프라이버시가 더 중요하게 다뤄져야 하는 이유, 이를 SNS 등 미디어 환경에서 어떻게 적용할지 배운다. △3차시에서는 개인과 대인 관계를 넘어서 일상의 다양한 부분에서 기록되는 데이터의 형태와 정부, 기업의 적극적인 개인들의 정보 수집·추적 양상을 배운다. 인터넷의 무료 서비스가 개인의 모든 활동기록의 수집·제공을 전제로 한다는 것의 의미도 교육한다. 4차시에서는 구체적 미디어 이용 상황에서 자신의 정보를 스스로 관리, 통제하는 경험을 하는 것을 목적으로 한다. 스마트폰, SNS 등 주요 미디어 서비스의 설정 변경하기 등의 활동을 통해 이전 차시의 내용을 실천해본다.

〈표 8-2〉 아동·청소년 프라이버시 교육안¹⁸⁷⁾

		학습목표	수업 내용
1	프라이버시 의미 이해하기	<ul style="list-style-type: none"> 개인정보와 프라이버시가 무엇 인지 안다 프라이버시의 중요성을 안다 공개할 개인정보와 대상을 안다 	<ul style="list-style-type: none"> 프라이버시와 개인정보의 개념과 중요성 이해하기 나와 관련된 다양한 정보 이해하기 (활동) 공개가능한 정보 분류하기 (활동) 내 정보 공개범위 결정하기
2	온라인, SNS 프라이버시	<ul style="list-style-type: none"> 온라인 공간의 특성을 안다 SNS의 특성을 알고 그에 맞게 정보를 공개·공유한다 SNS에서 정보를 공유할 때 주의 할 점을 안다 	<ul style="list-style-type: none"> 온라인 공간 특성 이해하기 SNS의 특성 이해하기 디지털 평판 이해하기 (활동) SNS 프로필 구성하기 (활동) SNS 업로드시 체크리스트 작성하기
3	온라인에서 내 데이터와 흔적 이해하기	<ul style="list-style-type: none"> 미디어 이용 등 온라인에서 내 정보가 수집·저장·이용된다는 것을 안다 미디어 이용 등 온라인에서 내 정보가 수집·저장·이용되는 방식을 안다 	<ul style="list-style-type: none"> 미디어 이용(예. 검색)과 서비스(예. 페이스북)별 수집·저장되는 정보 유형 이해하기 기업과 정부의 개인 데이터 수집·활용 이유와 방식 이해하기 (활동) 미디어 이용 과정에서 기록되는 정보 썸보기 (활동) 추천콘텐츠와 광고의 공통점과 차이점 논의하기
4	미디어 이용에서 프라이버시 실천하기	<ul style="list-style-type: none"> SNS 등 미디어에서 내 정보를 관리하는 방법을 안다 기업의 정보 수집과 추적에 대해 조치할 수 있다 	<ul style="list-style-type: none"> 미디어 이용 과정에서 내 정보 통제 방법 이해하기(예. 쿠키 삭제, 추적 금지 설정) 주요 미디어의 프라이버시 설정 이해하기 (활동) 미디어 약관 읽고 분석하기 (활동) 페이스북 프라이버시 설정해보기

187) 구체적인 수업지도안은 시청자미디어재단 홈페이지(kcmf.or.kr)를 참고하면 된다(시청자미디어 재단 홈페이지)미디어리터러시>미디어교육 자료)

제2절 ● 디지털 환경에서 아동·청소년의 프라이버시 권리 보장 방안

1. 법제도 개선

디지털 환경에서 아동·청소년이 프라이버시 등 권리를 누리기 위해서는 교사와 부모 등 성인세대의 프라이버시에 대한 인식 제고와 교육이 필요하다. 성인세대들은 집단주의적 문화에서 성장해 개인정보, 프라이버시 개념과 경험이 부족하고, 아동·청소년을 성인과 동등한 개별 인격으로 존중하는 태도가 부재하므로, 개인적·사회적 차원에서 인식 전환이 필요하다. 예를 들어 안전과 보호를 이유로 자녀들에게 설치한 스마트폰 감시앱이나 집안 내 CCTV(홈캠, 베이비캠)와 같은 감시와 통제적 양육방식을 지양할 필요가 있다. 미디어 이용과 관련해 과의존 예방에 초점을 맞춘 미디어 이용 시간 통제 담론에서 벗어날 필요가 있다. 감시앱은 미디어 이용 시간이 단축시키는 효과는 있을 수 있지만 부모의 신뢰를 받지 못한다는 느낌으로 인해 아이가 부모에게 부정적 감정을 느낄 수 있고, 어릴 때부터 가장 가까운 사람에게서 감시받는 상황은 아이의 성장과 프라이버시 감각을 키우는데 매우 부정적인 영향을 미칠 수 있다.

2. 부모 세대의 교육과 인식 전환

발달과 성장 단계에 있는 권리주체인 아동·청소년의 특별보호 맥락을 고려한 법제도의 개선이 필요하다. 아동·청소년 관련 만 14세 미만 아동의 보호자 동의가 전부인 현재 개인정보보호법 체계는 개인정보 처리 등에서 아동의 의사는 반영되지 않는데 아동·청소년 동의와 협의를 구하는 절차를 명시할 필요가 있다. 만 14세 이상에서 만 18세 이하 청소년은 아직 성장 단계임에도 성인과 동일하게 취급해, 아동으로서 보호받지 못하는 상황에 대한 해결도 필요하다. 형식적 동의가 아닌 설명기반 동의를 비롯해 아동·청소년 수준에 맞는 약관제공과 GDPR이나 영국 등의 아동·청소년 관련 개인정보와 프라이버시 정책 수준으로 법제도를 개선할 필요가 있다.

3. 교사와 학교당국의 태도 개선

프라이버시 교육과 함께 아동·청소년이 프라이버시에 대한 감각을 기를 수 있도록 자신의 개인정보와 프라이버시가 존중받고 있다는 것을 일상에서 경험할 수 있게 해주는 것이 필요하다. 이를 통해 타인의 프라이버시도 존중받아야 한다는 것을 자연스럽게 경험할 수 있다. 예를 들어 학교 행정 차원이나 개인정보 동의서를 기록하는 상황, 학급에서 사진을 공유하는 상황 등에서 학생들에게 동의를 구하는 과정 등이 필요하다. 아동·청소년 개인에 관한 정보를 수집할 때, 해당 정보가 왜 필요한지와 어떻게 쓰이는지에 대해 안내하는 과정과 법정대리인인 부모의 동의를 받는 과정의 의미 등을 적극적으로 알리는 과정이 필요하다. 교육행정을 위해 적법한 절차를 거쳐 수집된 정보에 대한 철저한 관리뿐만 아니라 수업(특히 온라인) 등 일상적 환경에서도 학생 개인정보와 프라이버시를 존중할 수 있도록, 교사 연수 등에서 관련 내용을 교육할 필요가 있다.

4. 아동·청소년 프라이버시 권리를 존중하는 환경 조성

아동·청소년의 프라이버시 권리를 보장하기 위해서는 아동·청소년 권리를 존중하는 사회적 환경 조성이 필요하다. 프라이버시 위협과 침해가 일상적으로 일어나는 가정, 학교, 미디어 환경에서 아동·청소년이 프라이버시에 대한 감각이나 인식을 갖기 어렵다. 아이들이 자신의 미디어 이용을 스스로 관리하고, 정보를 스스로 통제할 수 있는 힘을 기르며, 외부의 정보 수집이나 감시에 대한 문제의식을 기르기 위해서는 일상적 환경 개선이 필요하다. 어린이용 약관 제공이나 아동·청소년 대상 개인정보 교육(예. 네이버) 등과 함께 기업은 최소한의 필요한 정보 수집, 정보 수집과 관련해 투명한 공개와 동의, 상업적 이용을 제한적 영역에서 해야 하고, 정부는 아동·청소년 개인정보와 프라이버시 보호를 위한 제도와 인식 개선에 적극적으로 나서야 한다. 또한 미디어 리터러시 영역에서도 프라이버시 교육뿐만 아니라 스마트폰 감시 앱 등 아동·청소년의 권리를 침해하는 시도에 대해 적극적인 비판과 성찰의 목소리를 내야 한다.

 ■ 참고문헌 ■

- 개인정보보호위원회(2021). 생체정보 보호 가이드라인.
- 개인정보보호위원회(2020). 2020 개인정보보호 연차보고서.
- 개인정보보호위원회(2021). 2021 개인정보보호 연차보고서.
- 국가인권위원회(2005). 학교식당 지문인식기 설치 및 학생지문날인 요구는 인권침해, 보도자료 2005.10.20.
- 국가인권위원회(2011). 세종시 스마트스쿨, 학생출석확인 위한 지문인식시스템 도입은 인권침해 보도자료 2011.10.31.
- 국가인권위원회(2018). 유엔아동권리협약의 이해. Retrieved from https://www.humanrights.go.kr/site/inc/file/fileDownload?fileid=1068179&filename=in_11812121421595880141.pdf.
- 국가인권위원회(2019). 인권위, 초등학교 지문인식출입시스템 다른 방안 강구해야, 보도자료 2019.7.26.
- 국가인권위원회(2021). 청소년유해매체물 차단 등을 위한 앱의 아동·청소년 기본권 침해 최소화 방안 마련해야, 보도자료 2021.3.2.
- 김기중·임완철·장여경(2019). 인공지능 활용 교육을 위한 학습자 개인정보 보호 정책 및 규약 분석. <한국교육학술정보원 이슈리포트>, RM 2019-18.
- 김기중·임완철·장여경(2021). <공교육에 적용되는 인공지능 알고리즘의 공공성 확보 방안 연구>. 서울특별시교육청 2020 위탁연구보고서.
- 김선기(2020). 스마트스피커의 IoT기기 결합과 개인정보자기결정권, 『법학연구』, 31(3), 93-96.
- 김유정(2013). 소셜네트워크서비스 이용에 대한 비교 연구 : 싸이월드, 페이스북, 트위터 간의 이용동기와 만족 비교. 『한국지역언론학회』, 13(1), 5-32.
- 나종연·김지혜·한슬기(2020). 아동 소비자의 온라인 개인정보보호 인식과 행동에 대한 연구. 『소비자학연구』, 31(4), 113-138.
- 나종연·조은선·이승은(2021). 아동 이용자에게 특화된 온라인 개인정보보호 이슈 : 사례연구를 중심으로, 『디지털융복합연구』, 18(10), 23-31.

- 샤오진화·이상기(2020). 중국 청소년의 틱톡(Tiktok) 이용동기가 이용만족도와 지속 사용의도에 미치는 영향, 『The Journal of the Convergence on Culture Technology (JCCT)』, 6(2), 107-115.
- 세이브더칠드런(2020). 아동·청소년 디지털 플랫폼별 경험조사 요약보고서.
- 심홍진·황유선(2010). 마이크블로깅 이용동기에 관한 연구: 트위터를 중심으로. 『한국방송학보』, 24(2), 192-232.
- 심홍진(2018). 인공지능(AI)과 프라이버시의 역설: AI음성비서를 중심으로. KISDI Premium Report, 한국정보통신정책연구원.
- 염정운·정세훈(2019). 청소년 개인정보 보호 교육 효과 연구: 부모-자녀교육의 효과를 중심으로. 『사이버커뮤니케이션학보』, 36(2), 44-45.
- 윤주희(2014). 아동의 개인정보보호를 위한 법정대리인의 동의제도와 연령기준에 대한 연구, 『서울법학』, 22(1), 187-232.
- 유지연(2013). 아동의 온라인 개인정보 보호 재고찰. 『방송통신정책』, 25(16), 35-54.
- 이근영(2016). 금융권의 웨어러블 기기 활용 및 보안 동향. 『전자금융과 금융보안』, 6, 49-70.
- 이상운·김병수·오병일·이은우·장여경·최규진(2016). 바이오 정보 수집, 이용 실태조사. 국가인권위원회 2016년도 인권상황실태조사 연구용역보고서.
- 이은경(2018). 정보교육의 전망과 과제 : 미래 정보과 교육과정 개발 방향. 『컴퓨터 교육학회 논문지』, 21(2), 1-10.
- 이정연·김명랑·권경림·최보미(2020). <2020 경기도 학생인권 실태 조사>. 경기도 교육연구원.
- 이희정(2019). 아동의 온라인 프라이버시 보호. 『2019 NAVER Privacy White Paper』.
- 이희정(2021). 아동의 온라인 개인정보 보호에 관한 소고. 『국가법연구』, 17(2), 157-190.
- 전윤선·나종연(2020). 아동 소비자의 온라인 개인정보보호 관련 미국, EU, 영국, 한국의 법제도 비교 고찰. 『소비자문제연구』, 51(2), 1-35

- 전창욱·유진호(2020). 근거이론을 통한 아동 개인정보 유출에 대한 질적연구. 『정보 보호학회논문지』, 30(2), 263-277.
- 정보통신정책연구원(2018). 어린이와 청소년의 휴대폰 보유 및 이용행태 분석. <KISDI STAT Report>, 18(20). 1-17.
- 정영식·유정수·김철(2021). 학습 격차 해소를 위한 초등 정보 교과 신설 방안, 『정보 교육학회논문지』, 25(1), 33-40.
- 조도은·김시정(2018). 스마트 홈에서 프라이버시 보호를 위한 이용자 동적 접근제어. 『JOURNAL OF PLATFORM TECHNOLOGY』, 6(3), 17-22.
- 정찬모(2014). 미국의 아동 온라인 프라이버시보호법 최근동향과 시사점, 『법학연구』, 17(1), 77-108.
- 최미경·최정민(2019). CCTV 통합관제센터 운영실태 및 개선방안. 국회입법조사처 입법정책보고서 29호.
- 최흥규·고범석(2021). 유튜브 아동보호 가이드라인의 구성요소에 관한 연구: 가이드 라인 및 소셜 빅데이터 이슈를 중심으로. 『교육정보미디어연구』, 27(2), 470-472.
- 통계청·여성가족부(2021). 2021 청소년 통계.
- 트위터 대한민국(2021). Z세대의 트위터 활용법을 확인하세요. <트위터 대한민국 블로그>. Retrieved from https://blog.twitter.com/ko_kr/topics/insights/2021/genz-research
- 한국갤럽마켓(2021). 마켓70 2021 미디어·콘텐츠·소셜 네트워크 서비스 이용률. Retrieved from <https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1205>
- 한국인터넷진흥원(2020). TikTok의 개인정보 침해 이슈 및 국가별 조사 진행 현황 검토, 1-6.
- 행정안전부·개인정보보호위원회(2018). 『2017 개인정보보호 실태조사』 황혜정(2019). 트위터, 기업과 고객의 소통채널 될까. 『Weekly 포커스』, 40-46.
- Allen, S. J. (2018, August 28). Warning Kids About Digital Privacy Doesn't Work. Here's What Does. Retrieved from <https://www.consumerreports.org/>

- privacy/kids-and-digital-privacy-what-works/
Apptopia & Braze(2020). 2020 The Year of Streaming. Retrieved from https://info.braze.com/rs/367-GUY-242/images/2020_The_Year_of_Streaming.pdf
- Barron, C. M.(2014). I had no credit to ring you back: Children's strategies of negotiation & resistance to parental surveillance via mobile phones. *Surveillance & Society*, 12(3), 401-413.
- Bowler, L., Acker, A., & Jeng, W.(2017). 'It lives all around us': Aspects of data literacy in teen's lives. 80th Annual Meeting of the Association for Information Science & Technology. Washington, DC, USA, 27-35.
- Chaudron, S., Di Gioia, R. & Gemo, M.(2018). Young children (0-8) & digital technology: A qualitative study across Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.
- Children's Commissioner(2017). Life in 'likes': Children's Commissioner Report into social media use among 8-12 year olds. London, UK: Children's Commissioner for England, 1-42
- Children's Commissioner(2018). Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data. London, UK: Children's Commissioner for England, 1-25.
- Chen, G. M.(2011). Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others. *Computers in Human Behavior*, 27(2), 755-762.
- COMMITTEE OF MINISTERS(2021, April 29). *European states must step up efforts to protect children's privacy in digital environment, especially in the COVID-19 pandemic context, says Committee of Ministers of the Council of Europe*, Newsroom, Retrieved from <https://www.coe.int/en/web/portal/-/committee-of-ministers-european>

- states-must-step-up-efforts-to-protect-children-s-privacy-in-digital-environment
- Culver, S. H. & Grizzle, A.(2017). Survey on privacy in media & information literacy with youth perspectives. UNESCO Series on Internet Freedom. Paris, France: UNESCO.
- ICO(2021, July 5). *New class resources will help empower young people to take control of their online privacy*. Retrieved from <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/new-class-resources-will-help-empower-young-people-to-take-control-of-their-online-privacy/>
- ICO(2021, July 28). *Blog: Spotlight on the Children's Code standards - best interests of the child, detrimental use of children's data and data minimisation*. Retrieved from <https://ico.org.uk/about-the-ico/news-and-events/blog-spotlight-on-the-children-s-code-standards-best-interests-of-the-child/>
- Livingstone, S. (2014) Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications. The European Journal of Communication Research* 39, 283-303.
- Livingstone, S. (2018) Children: a special case for privacy? *Intermedia* 46(2), 18-23.
- Livingstone, S. Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science
- Livingstone, S., Lievens, E., & Carr, J. (2020). *Handbook for policy makers on the rights of the child in the digital environment*. Council of Europe.
- Nissenbaum, H. (2010). *Privacy in context. Technology, integrity of social life*. Stanford: Stanford University Press.

- Ofcom(2017a). Report on Internet Safety Measures. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-internet-safety-report.pdf
- Ofcom(2017b). Children and parents: Media use and attitudes report. London: Ofcom. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-useattitudes-2017.pdf
- Pangrazio, L., & Selwyn, N. (2021). Towards a school-based 'critical data education'. *Pedagogy, Culture & Society*, 29(3), 431-448.
- Raynes-Goldie, K. & Allen, M.(2014). Gaming privacy: a Canadian case study of a children's cocreated privacy literacy game. *Surveillance & Society*, 12(3), 414-426.
- Redden, S. M. & Way, A. K.(2017). 'Adults don't understand': exploring how teens use dialectical frameworks to navigate webs of tensions in online life. *Journal of Applied Communication Research*, 45(1), 21-41.
- Richardson, J. & Milovidov, E. (2019). *Digital Citizenship Education Handbook*. Council of Europe.
- Ropek, L. (2021 April 30). *Australia Wants to Teach Basic Cybersecurity to 5-Year-Olds*. Retrieved from <https://gizmodo.com/australia-wants-to-teach-basic-cybersecurity-to-5-year-1846799379>
- Selwyn, N. & Pangrazio, L. (2018). Doing data differently? Developing personal data tactics & strategies amongst young mobile media users. *Big Data & Society*, 5(1), 1-12.
- Sharwood, S. (2021 April 30). *Australia proposes teaching cyber-security to five-year-old kids*. Retrieved from https://www.theregister.com/2021/04/30/eaching_cybersecurity_to_five_year_olds/
- Shin, W., Huh, J., & Faber, R. J. (2012). *Tweens' online privacy risks and*

- the role of parental mediation. Journal of Broadcasting & Electronic Media*, 56(4), 632-649.
- UN Committee on the Rights of the Child (2021). general comment No. 25 on children's rights in relation to the digital environment.
- UNICEF(2018). Children's Online Privacy and Freedom of Expression.
- UNICEF(2019). Faces, Fingerprints & Feet - Guidance on assessing the value of including biometric technologies in UNICEF-supported programs.
- UNICEF(2020). Data governance for young people in the commercialized digital environment. Issue brief, 3, 1-7.
- van der Hof, S.(2016). I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, 34(2), 409-45.
- Wisniewski, P.(2018). The privacy paradox of adolescent online safety: a matter of risk prevention or risk resilience? *IEEE Security & Privacy*, 16(2), 86-90.
- Wisniewski, P., Jia, H., Xu, H., Rosson, M. B., & Carroll, J. M.(2015, February). "Preventative" vs. "Reactive" How Parental Mediation Influences Teens' Social Media Privacy Behaviors. *In Proceedings of the 18th ACM conference on computer supported cooperative work & social computing (pp. 302-316)*.

■ 저자소개

이선민

- 연세대 커뮤니케이션대학원 석사
- 연세대 커뮤니케이션대학원 박사
- (현) 시청자미디어재단 선임연구원

김법연

- 광운대 법학과 석사
- 고려대 정보보호대학원 공학박사
- (현) 고려대 정보보호대학원 연구교수

김상현

- 캐나다 토론토대 삼림보전학 석사
- 캐나다 요크대 법학 석사
(프라이버시와 사이버보안 전공)
- (현) 캐나다 BC주 수도권청 정보공개 및
개인정보보호 담당관

장여경

- 고려대대학원 과학기술협동과정학과 석사
- (전) 개인정보보호위원회 비상임위원
- (현) 국가인권위원회 정보인권포럼 위원
- (현) 사단법인 정보인권연구소 상임이사

오병일

- KDI 국제정책대학원 공공정책 석사
- (현) 진보네트워크센터 대표
- (현) 정보인권연구소 연구위원
- (현) 정보공유연대 IPLeft 대표

정책연구 2021

**디지털 환경에서 아동·청소년 프라이버시
권리를 위한 교육방안과 제도개선 연구**

2021년 12월 31일 발행

발행인 조한규

발행처 시청자미디어재단
서울시 영등포구 국회대로 74길 4
www.kcmf.or.kr